FA CCTV SYSTEM

Volume III

Operations & Maintenance Manual

This Page Left Intentionally Blank

AVIGILON CONTROL CENTER SOFTWARE

Operations & Maintenance Manual
December 2015

Avigilon Control Center 5.0 software with HDSM™

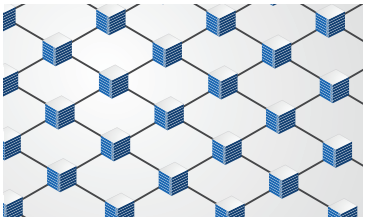
Avigilon™ Control Center (ACC) is the industry's easiest-to-use video management software, and has revolutionized how security professionals manage and interact with high definition video. As a distributed network platform with enterprise-class reliability, Avigilon Control Center is able to efficiently capture, manage and store high definition surveillance video while intelligently managing bandwidth and storage. Avigilon Control Center can be pre-installed and configured on an Avigilon Network Video Recorder (NVR) or work as stand-alone software, to meet the needs of any type of installation.

Avigilon Control Center records and manages both video and audio from Avigilon's line of megapixel cameras (from 1 MP to 29 MP). ACC can seamlessly integrate conventional analog cameras, along with a broad range of third-party IP cameras and encoders, giving you the ability to build a hybrid system – providing you with a budget-conscious migration from analog to digital. ACC's easy-to-use interface allows personnel to evaluate and respond to events with minimal training.

HDSM Technology

Avigilon Control Center uses our unique HDSM™ software technology to efficiently compress and preserve image quality while intelligently managing HD image transmission throughout the Avigilon system — sending only the requested portions of captured images to operator workstations. This technology delivers the best possible image quality while providing immediate savings in transmission bandwidth allowing operators to use less powerful workstations and thereby reducing costs. Our HDSM technology leverages leading imaging, hardware, data compression and information technologies to maximize performance of the Avigilon system.

COLLABORATIVE INVESTIGATIONS



ENTERPRISE SERVER MANAGEMENT

INTELLIGENT VIRTUAL MATRIX

Avigilon Control Center 5.0 Features

User Interface

Powerful software doesn't have to be complicated. That's why we've made the easiest-to-use interface on the market even easier. Avigilon Control Center's system explorer functionality gives you more control over what you see at your workstation or video wall by allowing you to resize the interface — so you can focus on image windows rather than a complicated screen layout. For greater efficiency, we've made the controls you use most often the easiest to access, and the ones you use the least, tucked away nearby for easy accessibility.

Collaborative Investigations

ACC 5.0 allows multiple operators to view and interact with the same layout and interface in real time. Now a user can push their feed to another workstation, and they both have complete control to manipulate and maneuver it on their own, saving the users time by letting them demonstrate incidents and review HD video together — all without ever being in the same room.

Available in: Enterprise

Crash-Proof Enterprise Server Management

Up to 100 servers can be synchronized as a single cluster, operating as one unit, with no dedicated management server required. So if one goes down, the others are still fully operational and already have the information and settings that would normally be lost. And adding new servers is as easy as plugging them in — they'll automatically grab all the user's information and settings, with no setup required.

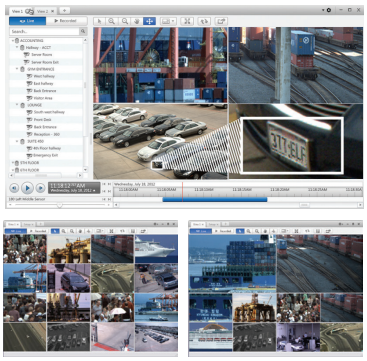
Available in: Enterprise

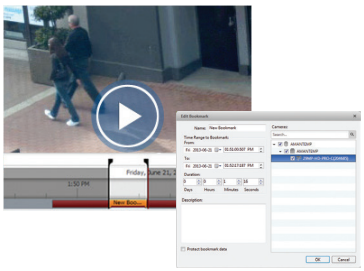
Intelligent Virtual Matrix

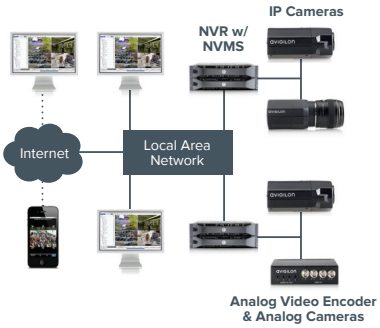
With ACC 5.0, you can flawlessly transform your static video wall into an intelligent video wall, finally utilizing its full capabilities — easily maneuver through camera feeds, manipulate your wall's layout, interact with video, zoom, rewind, isolate, and much more.

Available in: Enterprise

Avigilon Control Center 5.0 software with HDSM™







Multi-Megapixel High-Dynamic-Range Image Display

- Analyze detailed regions from single or multiple cameras.
- Use viewing tabs to allow single operators to switch between multiple cameras located throughout large enterprise systems.
- Digitally zoom and pan within an image with a mouse or surveillance joystick. Automatic dynamic contrast enhancement reveals low-light details for unmatched digital PTZ performance.
- View live or recorded high definition surveillance footage.

Data Protection and Storage Management

- Redundant recording to multiple NVRs allows a full live mirror of all high definition video. Automatic fail-over NVRs ensure uninterrupted recording if an NVR becomes unavailable.
- Integrated backup and restore functionality allows recorded HD video from multiple cameras to be securely transferred from an NVR on a defined schedule.
- Allocate more storage capacity to recent events and taper archived surveillance footage for maximum record times with data aging.

Integrated Graphic Mapping for System Layout

- Graphic-mapping interface lets operators layout cameras and servers on an imported map for easy navigation of large surveillance systems.
- Maps can be layered and nested, allowing easy navigation through satellite maps, multi-story buildings and very large areas.

HD Recording and Playback Timeline

- Timeline interface with integrated drag-to-zoom capability allows full control over high definition surveillance video playback, in forward and reverse, at variable speeds—up to 8 times faster than real time.
- Rapidly updating playback system allows intuitive jog or shuttle playback to identify key events and subtle changes.

Bandwidth Management and Remote Viewing

- Fine-tune camera bandwidth usage to optimize image quality and network bandwidth availability with HDSM.
- Remotely connect to multiple recorders to view live and recorded surveillance footage over the local area network (LAN) or a wide area network (WAN) connection.

Bookmark and Export HD Surveillance Footage

- Bookmark and export movies or still images in industry-standard formats or in Avigilon loss-less format for third-party forensic work.
- Exported video can be managed via the Avigilon Control Center Player — which provides all the tools required for analyzing and reviewing captured HD surveillance footage.
- Bookmarked events are indexed to allow rapid searching using user defined metadata.

Video Search

- Unique sub-region thumbnail searching allows you to rapidly find small changes within HD surveillance, covering large areas.
- Quickly and accurately navigate through large amounts of recorded high definition video with camera-specific event logs.
- Search through alarms, point-of-sale transactions, license plates and bookmarks.

Advanced Control Center Features

Alarm Monitoring

- Allows the creation of complete end-to-end workflows for the monitoring, assignment, and acknowledgement of alarms.
- Can be triggered by any internal system event, as well as external third-party access control and building management system triggers.

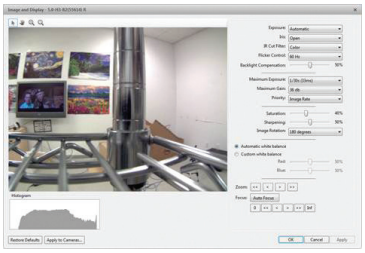
POS Transaction Engine

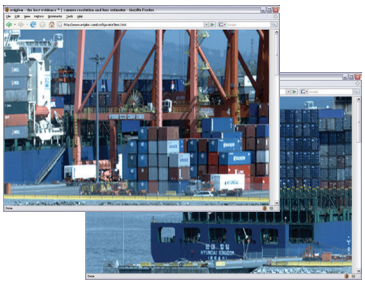
- Link HD surveillance footage (viewed instantly) with transaction data to address compliance requirements and reduce shrinkage and theft.
- Exception filtering and reporting allows the triggering of events when transactions match specified criteria.

Acquisition Manager

- Ensures that all Avigilon cameras, regardless of resolution, are always configured to collect the best possible image over a wide range of lighting conditions.
- Configure multiple independent camera-specific motion-detection zones for pre- or post-motion-triggered recording.

Avigilon Control Center 5.0 software with HDSM™





Simple Camera and Server Installation

- Unique plug-and-play capabilities for NVRs and cameras automatically identify themselves on the network, without manual configuration or searching—eliminating complex network configuration.

Detailed Management, Monitoring, and Reporting of System Status and Security

- Detailed logs of storage, network, and overall system status to ensure the highest possible system uptime for critical applications.
- Powerful rules engine lets administrators and operators map any camera or system event to an action, such as triggering output alarm relays, for faster identification and improved response times.
- Programmable email alerts provide rapid remote notification in the event of camera tampering, a system alert, an alarm or a motion event.

Scalable Integration with Legacy Systems

- Distributed architecture features a .NET-based API that can easily be integrated with other systems, such as access control and building management.
- Benefit from a new level of HD video surveillance while maintaining a single interface and minimizing training costs.

CORE, STANDARD & ENTERPRISE

To create the best-matched system for your surveillance needs, the Avigilon Control Center software is offered in three editions: Core, Standard and Enterprise. The Enterprise edition includes more advanced features for a sophisticated solution, whereas the Standard edition is used for more focused needs or for those looking to transition to HD surveillance in the most cost-effective way. ACC Core is an entry-level version of our award-winning software that delivers advanced high definition surveillance capabilities, ease of use, and superior image quality to smaller implementations. No matter what the size of your installation, you can customize a solution that is right for you.

System	Core	Standard	Enterprise
Number of cameras per server	24	48	128
Number of servers per site	1	1	100
Number of concurrent server connections	1	24	Unlimited
Number of client licenses per server	2	5	Unlimited
High Definition Stream Management (HDSM)™	Yes	Yes	Yes
Industry's most powerful VMS engine	Yes	Yes	Yes

Device Support	Core	Standard	Enterprise
Automatic device discovery	Yes	Yes	Yes
Third-party IP cameras & encoders	Yes	Yes	Yes
ONVIF cameras & encoders	Yes	Yes	Yes
HD, HD H.264, HD panoramic cameras	Yes	Yes	Yes
Avigilon encoders	Yes	Yes	Yes
H.264 support	Yes	Yes	Yes
MPEG4 support	Yes	Yes	Yes
MJPEG support	Yes	Yes	Yes
JPEG2000 support	Yes	Yes	Yes
HD professional cameras	No	No	Yes

Client	Core	Standard	Enterprise
Powerful, easy-to-use client interface	Yes	Yes	Yes
Web browser client interface	Yes	Yes	Yes
Joystick support	Yes	Yes	Yes
ACC mobile / gateway	Yes	Yes	Yes
Saved views	No	Yes	Yes
Maps	No	Yes	Yes
Web pages	No	Yes	Yes
Windows user authentication	No	No	Yes
Editable Site View	No	No	Yes
Intelligent Virtual Matrix	No	No	Yes
Collaborative investigations	No	No	Yes

Recording, Searching and Playback	Core	Standard	Enterprise
Hourly configurable recording schedule	Yes	Yes	Yes
Loss-less recording	Yes	Yes	Yes
Pixel search	Yes	Yes	Yes
Thumbnail search	Yes	Yes	Yes
Event search	Yes	Yes	Yes
Multi-camera export	Yes	Yes	Yes
Live export	Yes	Yes	Yes
POS transaction search	No	Yes	Yes
Alarm search	No	No	Yes

For the most current list of integrations and add-ons supported by Avigilon Control Center, please visit avigilon.com

Add-On Modules and Integrations	Core	Standard	Enterprise
Point of Sale Transaction Engine	No	Yes	Yes
Avigilon developed and supported integrations	No	Yes*	Yes
3rd party system integrations	No	Yes	Yes

*RS2 AccessIt, DDS Aamadeus 5 and DSX only

Additional Features	Core	Standard	Enterprise
E-Mail event notification (motion & system event)	Yes	Yes	Yes
Digital input email trigger	No	Yes	Yes
Manual digital output trigger	No	Yes	Yes
Audio recording	No	Yes	Yes
Audio output	No	Yes	Yes
Rules engine	No	3	Unlimited
Redundant recording	No	No	Yes
Failover connections	No	No	Yes
Alarm management	No	No	Yes
Scheduled and one-time backup	No	No	Yes

Avigilon Control Center 5.0 software with HDSM™

Detailed Product Features

Integration Options

- Records and manages video from the full range of Avigilon high definition cameras.
  - Avigilon HD Cameras (1 – 5 Megapixel)
  - Avigilon HD Dome Cameras (1 – 5 Mega pixels)
  - Avigilon Panoramic HD Dome Cameras (8 Megapixel)
  - Avigilon Day/Night H.264 HD Cameras (1– 5 Megapixel)
  - Avigilon Day/Night H.264 HD Dome Cameras (1– 5 Megapixel)
  - Avigilon HD Bullet Cameras (1– 5 Megapixel)
  - Avigilon HD Micro Dome Cameras (1– 2 Megapixel)
  - Avigilon HD Pro Cameras (8 – 29 Megapixel)
  - Avigilon Day/Night HD PTZ Dome Camera (1–2 Megapixel)
  - Composite video from analog cameras, PTZ domes and thermal imagers via Avigilon ENC-4PORT and ENC-4P-H264 analog encoders
- Supports the recording and management of a wide range of third-party video and audio sources including:
  - ACTi Cameras/Encoders
  - Arecont Cameras
  - Axis Cameras/Encoders
  - Bosch Cameras/Encoders
  - IQInvision Cameras
  - Mobotix Cameras
  - ONVIF 1.00, 1.01, and 1.02 Cameras
  - ONVIF Profile S Cameras
  - Panasonic Cameras
  - Pelco Cameras
  - Samsung Cameras/Encoders
  - Samsung Techwin cameras
  - Sanyo Cameras
  - Scallop Cameras
  - Sightlogix Cameras
  - Sony Cameras
  - VideoIQ Cameras/Encoders
- Supports the control of digital input triggers and triggering digital outputs through an I/O board.
- The Avigilon Application Programming Interface (API) enables the seamless integration of Avigilon video surveillance with third-party applications to receive:
  - Bi-directional alarm event processing for monitoring and acknowledgement
  - Card access activity events
  - Digital input events
  - Intrusion zone events
- The Alarms tab provides the ability to monitor live alarm events received by access systems integrated with the Avigilon software. Users are given the ability to assign, acknowledge and investigate alarm video.
- The Armed Image Panels display live alarms as they are triggered within the video monitoring workspace, and provides the ability to acknowledge and investigate the live video.
- Integration alarms only need to be acknowledged in one system to be marked as acknowledged and processed in both.
- Avigilon develops and maintains integrations to a variety of 3rd party applications. The current list of available integrations is provided here: http://avigilon.com/support-and-downloads/for-software/acc-integration-and-plug-in-downloads/
- Avigilon offers an SDK for 3rd parties to create system integrations with the Avigilon Control Center software. Some of the available integrations are listed here: http://avigilon.com/support-and-downloads/for-software/system-integration-features/
- Receives and translates transaction information from point-of sale sources in multiple encoding formats.
- Provides the ability to link point-of-sales sources with video for the ability to monitor and review sales transactions.
- Rules can be used to generate events based on point-of-sale transaction exceptions.

Recording

- Streams live and recorded video up to 60 frames per second.
- Streams live and recorded video from cameras up to a resolution of 29 MP (6576 x 4384).
- Decompresses H.264 video through the client graphics card to optimize the client's total processing power.
- No proprietary recording hardware, hardware multiplexer or time-division technology is required for running the Avigilon system.
- Scalable to support up to 100 servers and/or 2000 cameras per site.
- All recorded video and audio is digitally signed using 256- bit encryption so video can be authenticated for evidentiary purposes.
- All command and control data is securely transmitted via TCP/IP using cryptographic keys based on SSL to prevent eavesdropping or tampering.
- External system alarms can be can be pre-selected and configured to be monitored and trigger event driven video operations.
- Video and audio recording can be defined by a recording schedule assigned to each video source.
- Recording schedules are based on event types that trigger video recording over a time period each day per week. Event types include:
  - Continuous
  - Motion
  - Digital Inputs
  - Alarms
  - POS Transactions

Avigilon Control Center 5.0 software with HDSM™

- Video recording can also occur manually by user triggered recording.
- Each recorded event includes a pre-event and post-event recording option to provide context for a given situation.
- Reference frame recording is an option when no events are detected.
- Motion detection is provided for each individual video source with adjustable sensitivity, threshold and detection zones.
- Primary and secondary video stream from each H.264 video source is recorded and maintained for a set amount of time before the primary stream is discarded as a means of increasing record time.
- The maximum recorded video retention time can be set for each video source.

Security

- Each system user can be granted specific live monitoring, investigative, system administration, and device access.
- Live monitoring operator access includes:
  - View live images
    - Use PTZ controls
    - Lock PTZ controls
    - Trigger manual recording
    - Trigger digital outputs
    - Listen to microphones
  - Broadcast to speakers
- Investigative operator access includes:
  - View recorded images
    - Export images
    - Backup images
  - Initiate collaboration sessions
  - Access to individual video and audio sources
- System administrator access includes:
  - Manage saved views
  - Manage maps
  - Manage web pages
  - Manage virtual matrix monitors
  - Manage user sessions
  - View server status
- Setup cameras
- Setup sites
- Setup servers
- Device access can be specific to cameras, encoders, maps, web pages and saved views.
- Windows Active Directory groups can be imported and automatically synchronised with the Avigilon system.
- Imported Windows users can use their Windows crednetials to access the Avigilon system.

System Administration

- Recorded video can be automatically backed up on a schedule.
- Automatic backups can be configured to span a specific time period, cameras, or age of video.
- The system can be set to delete the oldest backups when the disk is full to make room for new video recordings.
- Backup video can be saved to:
  - Local folder
  - Mapped network drive
  - Storage area network
  - USB or direct attached storage
- Email notifications are available to tell users and system administrators when an event or system health error occurs. Emails can be set to occur on a schedule, and can include camera snapshots related to an event.
- The system maintains an information log which can be used to trigger rules or email notifications:
  - Server Events
  - Device Events
  - User Events
  - Alarm Events
  - POS Transaction Events
- When a rule is triggered, the system can be set to execute any of the following actions in response:
  - User Notification Actions
  - Monitoring Actions
  - Device Actions
  - PTZ Actions
  - Alarm actions
- Users can be set to receive customized on-screen messages related to a rule event.
- On-screen messages are displayed in one location and the importance of each message is color coded.
- A maintenance log and audit trail of all system errors and events is accessible through the client software and the Admin Tool.
- The health of all servers within a cluster can be monitored, with the option to export the information in PDF format.

Avigilon Control Center 5.0 software with HDSM™

Video and Audio Controls

- Pan, tilt, zoom (PTZ) controls through the RS-485 interface of a video source can also be used and configured by the Avigilon system.
- The following PTZ camera protocols are supported by Avigilon systems:
- American Dynamics Sensormatic
  - AXSYS
  - AXSYS DCU
  - Ernitec ERNA
  - Honeywell Diamond
  - Kalatel ASCII
  - Pelco D
  - Pelco P
  - TEB Ligne
  - Vicon extended
  - Vicon normal
  - Videotec Legacy
  - Videotec MACRO
- The network settings for a video and audio source can be changed through the Avigilon software.
- Each camera's image quality and image rate can be changedn without affecting the settings of other cameras.
- The system automatically displays an H.264 camera's secondary stream for live viewing when there is insufficient bandwidth to display the primary stream.
- A camera's exposure, iris, IR filter, backlight compensation, gain, priority, sharpening, saturation, focus, and white balance can be set through the Avigilon system.
- The image dimensions of a JPEG2000 camera video can be changed.
- Camera image can be rotate 90°, 180° or 270°.
- Privacy zones can be added to a camera's field of view to block private areas in live and recorded video.
- Manually triggered video recording can be set to stop after a maximum recording duration.
- Audio input, output, gain and volume can be changed.
- Optional full-duplex two- way audio communication.
- Any audio source can be linked to any video source.

System Display and Control

- Supported joysticks, include:
  - Traditional style matrix controller with Pan, Tilt, Zoom, display control and function.
  - USB "gaming style" joystick controller.
  - Microsoft's Kinect© controller.
- Keyboard commands can control:
  - User Notification Actions
  - Monitoring Actions
  - Device Actions
  - PTZ Actions
  - Alarm Actions
- 1 to 36 video streams can be displayed simultaneously on a single monitor with the following standard layouts:
  - Full Screen
  - 2 x 2
  - 3 x 3
  - 4 x 4
  - 5 x 5
  - 6 x 6
  - 1 x 5
  - 1 x 7
  - 1 x 12
  - 2 x 8
- Live and recorded video can also be displayed in non-standard, customizable layouts.
- The system can be set to bias video display to a lower frame rate or to a lower image resolution if the client network bandwidth or client processing power is insufficient to display the full frame rate and image resolution.
- The following information can be displayed over live or recorded streaming video:
  - Camera Name
  - Camera Location
  - Timestamp
  - Record Indicator
  - Motion Activity
- The ability to stream video and audio is limited only by the system hardware capabilities.
- The application window display can be shared with other users for collaborative investigations while viewing both live and recorded video.
- Live and recorded video and audio can be streamed simultaneously on the same monitor.
- Avigilon Virtual Matrix software can be used to provide remote control of multiple monitor displays, including video walls, that can be controlled by remote users with the appropriate rights and permissions.
- The same live or recorded video stream can be viewed at different zoom levels and areas of interest.
- Switch from live to recorded video on demand for an instant replay of recently recorded video.
- Create and save customized video stream layouts for easy access
- Display video in full-screen view.
- Save views for reuse.
- Cycle through a series of opened views (guard tour) based on a specified interval.
- All video sources connected to the system are displayed.
- Drag and drop a video source from a tree of video sources into a window for live or recorded video and audio monitoring.

Avigilon Control Center 5.0 software with HDSM™

- Drag and drop a saved view from a tree of views into a window for live or recorded video and audio monitoring.
- Configure how the tree of video sources, maps, web pages and views is displayed.
- Armed image panel is one or more regions in a window for displaying video directly linked to triggered alarms and rules.
- Alarms can be acknowledged directly from an armed image panel.
- Digital outputs can be manually triggered from the video monitoring area.

Maps

- Create a map to represent the physical location of cameras and other devices throughout the surveillance system.
- Maps are created from images stored in JPEG, BMP, PNG, or GIF image formats.
- Maps can contain links to other maps and reference a subsection of a camera's field of view.
- Drag and drop a video source from a map into a window for live or recorded video and audio monitoring.
- Cameras on a map are highlighted if the camera is linked to an alarm that has been triggered.
- A map within a map is highlighted if it contains a camera that is linked to an alarm that has been triggered.

Avigilon Control Center 5.0 software with HDSM™

System Requirements

System requirements for a machine that will only be used as a remote monitoring client with a single monitor with a resolution of 1280 x 1024. Additional monitors and higher resolutions may require additional processing resources.

Avigilon Control Center Client

	Recommended
Operating System	Windows XP with Service Pack (SP) 2 or later, Window Vista, or Windows 7 (32-bit or 64-bit)
Processor	Intel Dual Core 2.0 GHz
System RAM	2 GB
Video Card	PCI Express, DirectX 10.0 compliant with 256 MB RAM
Network Interface	1 Gbps
Hard Disk Space	500 MB

System requirements for a HD NVR Server with a recording capacity of 32 MB/s (256 Mbps) from up to 128 cameras. The specifications below are intended for an HD NVR Server with only remote viewing.

Avigilon Control Center Server - Server Configuration

	Recommended
Operating System	Windows XP SP2, Windows XP SP2 x64, Windows Vista 64-bit, Windows Server 2003 SP2, Windows Server 2008, or Windows 7.
Processor	Intel Quad Core Xeon 2.0 GHz
System RAM	4 GB DDR2
Network Interface	1 Gbps Intel Pro/1000 or Broadcom NetXtreme II server adapters
Hard Drives	SATA-II 7200 RPM Enterprise Class Hard Drives

System requirements for a HD NVR Workstation with a recording capacity of 10 MB/s (80 Mbps) from up to 64 cameras and the ability to view live and recorded image data locally. This system should be able to support up to two monitors with a resolution of 1280 x 1024 each.

Avigilon Control Center Server - Workstation Configuration

	Recommended
Operating System	Windows XP SP2, Windows XP SP2 x64, Windows Vista 32-bit or 64-bit, Windows Server 2003 SP2, Windows Server 2008, or Windows 7
Processor	Intel Quad Core Xeon 2.0 GHz
System RAM	2 GB DDR2
Network Interface	1 Gbps
Video Card	nVidia Quadro FX 570 dual DVI
Hard Drives	SATA-II 7200 RPM Hard Drives

Avigilon Control Center Gateway can be installed on the same computer as Avigilon Control Center Server, but for optimal performance results it is recommended that the Gateway be installed separately. The Gateway can handle up to 36 concurrent video streams if installed on a computer with the listed requirements:

Avigilon Control Center Gateway

	Recommended
Operating System	Windows XP SP2, Windows XP SP2 x64, Windows Vista 64-bit, Windows Server 2003 SP2, Windows Server 2008, or Windows 7
Processor	Quad Core 2.0 GHz
System RAM	4 GB DDR2
Hard Drive Capacity	500 MB

This Page Left Intentionally Blank

Keyboard Commands

AVIGILON
THE BEST EVIDENCE™

Switch to live View — Ctrl + L

Switch to recorded View — Ctrl + P

Select camera/ add camera to View — / + logical ID + Enter

Toggle PTZ — Ctrl + D

Zoom in — +

Zoom out — -

Pan — ↑ ← → ↓

Play/pause — Spacebar

Forward 5 seconds — Ctrl + Shift + →

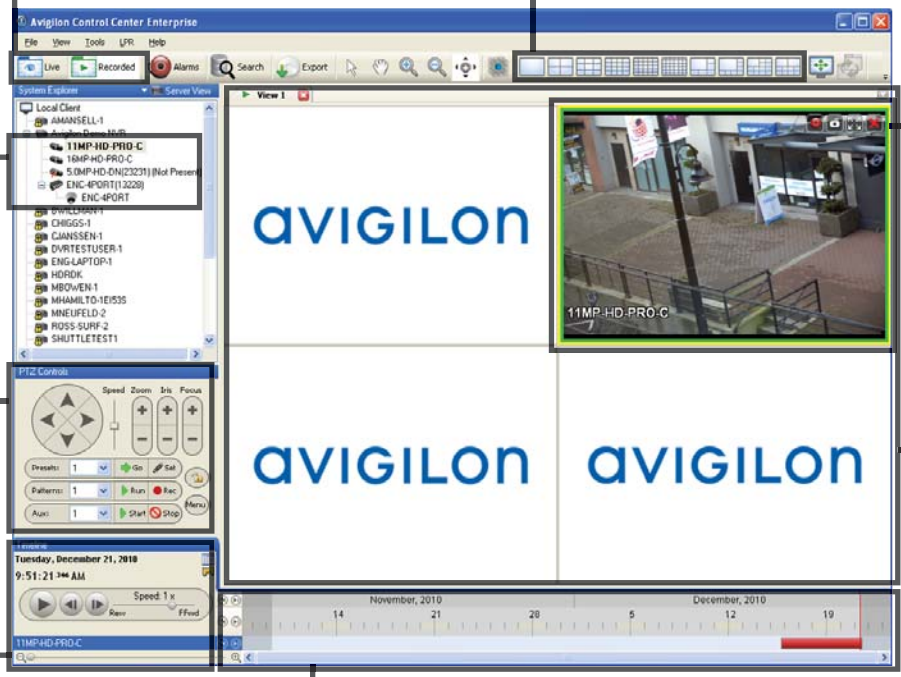
Forward 1 second — Ctrl + →

Forward 1 frame — Shift + →

Increase playback speed — Page Up

Decrease playback speed — Page Down

Select View layout — Alt + 1 2 3 4 5 6 7 8 9 0



Choose image panel — * + image panel# + Enter

Next image panel — Tab

Previous image panel — Shift + Tab

Clear image panel — Backspace

New View — Ctrl + T

Next View — Ctrl + Tab

Previous View — Ctrl + Shift + Tab

Close current View — Ctrl + W

Full screen — F11

Remove all cameras/ Clear screen — Ctrl + Backspace

Zoom in Timeline — Ctrl + Alt + +

Zoom out Timeline — Ctrl + Alt + -

Go to start of Timeline — Ctrl + Alt + Home

Center on Timeline marker — Ctrl + C

Scroll forward on Timeline — Ctrl + Alt + →

Go to end of Timeline — Ctrl + Alt + End

This Page Left Intentionally Blank

Avigilon™ Control Center Server User Guide

Version 5.4.2

Avigilon Corporation
http://www.avigilon.com

Revised: 2014-12-09

PDF-SERVER5-E-Rev1

Table of Contents

What is the Avigilon™ Control Center Server?

The Avigilon Control Center Server software is the application that captures and records surveillance data from network cameras and encoders. The captured data is then sent to the Avigilon™ Control Center Client software for you to review.

The Avigilon Control Center Server software contains two key parts — the Avigilon Control Center Server Windows service and the Admin Tool. The Avigilon Control Center Server Windows service directs video to where it needs to be stored or streamed in the network, while the Admin Tool is the interface that allows you to configure the Avigilon Control Center Server's administrative settings.

There are three editions of the Server software available: Core, Standard and Enterprise. The edition of the Server software determines how many cameras can be connected to the system and the number of simultaneous client connections. The edition of the Server software also determines what features are available in the Avigilon Control Center Client software. Visit the Avigilon website for an overview of the features available with each edition license: **http://avigilon.com/products/avigilon-control-center/editions/**

System Requirements

Recording capacity:	**32MB/s Up to 128 cameras** *Remote viewing only.	**10MB/s Up to 64 cameras** *Can view live and recorded images locally
OS	Windows Vista (64-bit), Windows Server 2008, Windows Server 2012, Windows 7, Windows 8, or Windows 8.1 A 64-bit operating system is recommended	Windows Vista (32-bit or 64-bit), Windows Server 2008, Windows Server 2012, Windows 7, Windows 8, or Windows 8.1 A 64-bit operating system is recommended
CPU	Intel Quad Core Xeon 2.0 GHz processor	Intel Quad Core Xeon 2.0 GHz processor
System RAM	4 GB DDR2	4 GB DDR2
Video Card	n/a	nVidia Quadro FX 570 dual DVI
Network Card	1 Gbps Intel Pro/1000 or Broadcom NetXtreme II Server Adapters	1 Gbps
Hard Drives	SATA-II 7200 RPM Enterprise Class Hard Drives	SATA-II 7200 RPM Hard Drives

For More Information

Visit Avigilon at **http://www.avigilon.com/** for additional product documentation.

The Avigilon Training Center

The Avigilon Training Center provides free online training videos that demonstrate how to set up and use the Avigilon Surveillance System. Register online at the Avigilon Partner Portal site to begin: **http://avigilon.force.com/login**

Support

For additional support information, visit **http://avigilon.com/support-and-downloads/**. The Avigilon Partner Portal also provides self-directed support resources - register and login at **http://avigilon.force.com/login**.

Regular Avigilon Technical Support is available Monday to Friday from 12:00 a.m. to 6:00 p.m. Pacific Standard Time (PST):

- North America: +1.888.281.5182 option 1
- International: +800.4567.8988 or +1.604.629.5182 option 1

Emergency Technical Support is available 24/7:

- North America: +1.888.281.5182 option 1 then dial 9
- International: +800.4567.8988 or +1.604.629.5182 option 1 then dial 9

E-mails can be sent to: **support@avigilon.com**.

Upgrades

Software and firmware upgrades will be made available for download as they become available. Check **http://avigilon.com/support-and-downloads/** for available upgrades.

Feedback

We value your feedback. Please send any comments on our products and services to **feedback@avigilon.com**

Navigating the Application

The Avigilon Control Center Server software contains two parts: the Avigilon Control Center Server Windows service and the Admin Tool.

The Avigilon Control Center Server Windows service runs automatically when your computer starts.

The Admin Tool is used to configure the Avigilon Control Center Server Windows service. From the Admin Tool you can add licenses, define the network, and configure the backup and storage settings for the Avigilon Control Center.

Control Center Server

The Control Center Server is a Windows service, so it runs automatically in the background.

If required, you can configure the Control Center Server properties in the **Services** window.

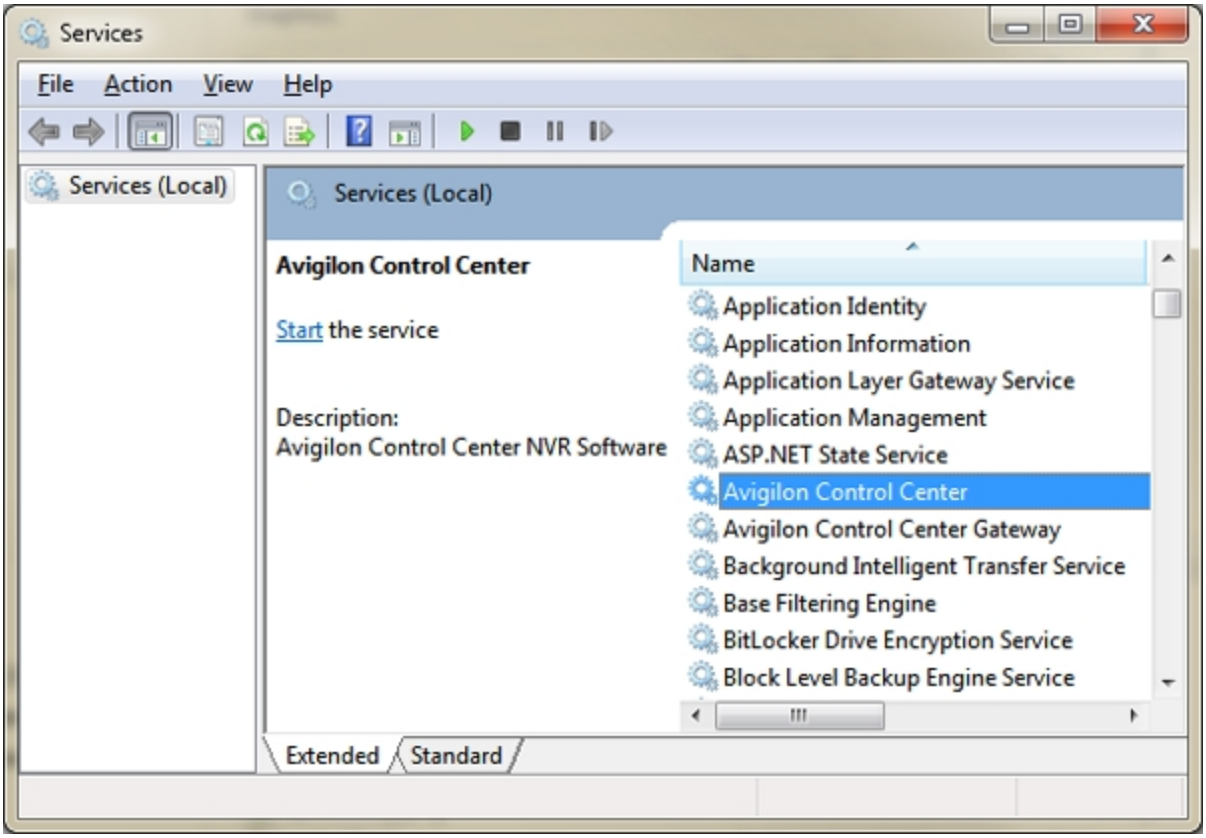


Figure 1: Services window

Admin Tool

The Admin Tool is used to configure your Control Center Server settings. From the Admin Tool, you can configure the size of the surveillance data storage space, the file backup location, the licenses for the Avigilon Control Center, and network ports.

Accessing the Admin Tool

The Admin Tool can be accessed in the following ways:

- From the Start menu, select **All Programs** or **All Apps** > **Avigilon** > **Avigilon Control Center Server** > **Admin Tool**
- Double-click the  shortcut icon on the desktop.

Admin Tool Window

From the Admin Tool, you can start up or shut down the Control Center Server at any time. For more information, see **Starting Up and Shutting Down the Control Center Server**.

The Admin Tool window contains two tabs: the **General** tab and the **Settings** tab.

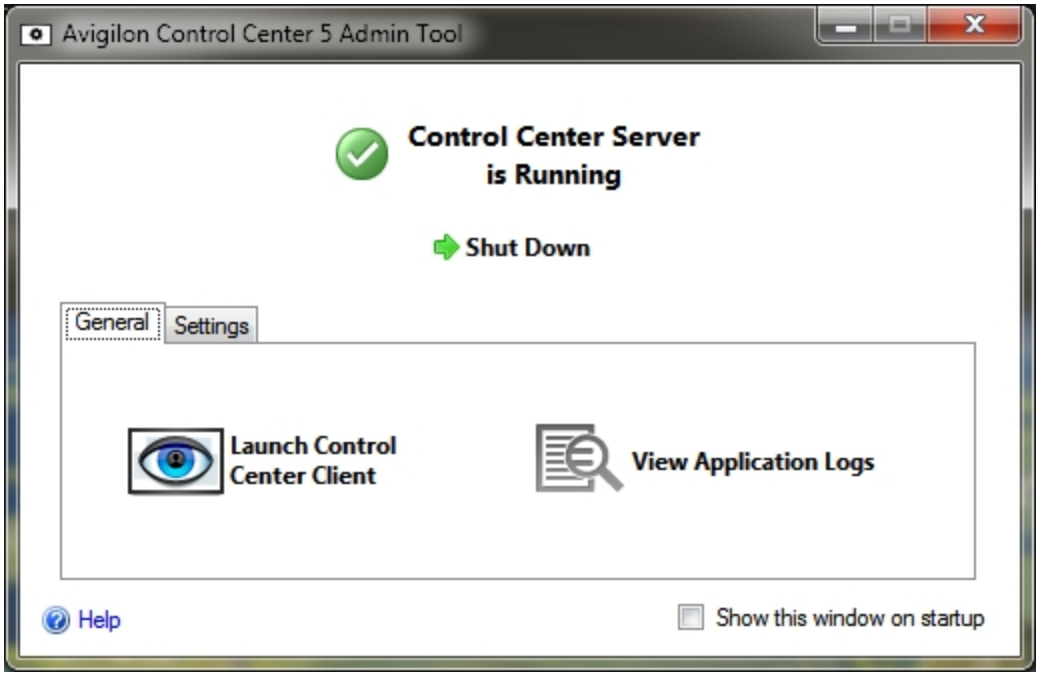


Figure 2: Admin Tool window, General tab

Feature	Description
	Click this button to start the Avigilon Control Center Client software.
	Click this button to view the Control Center Server error logs.

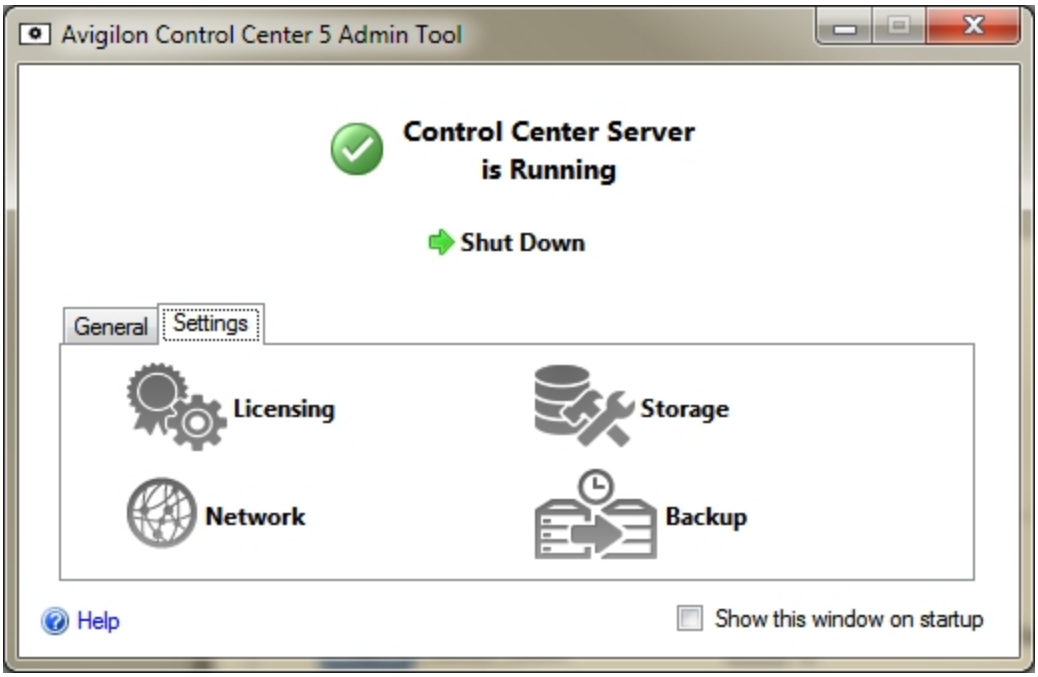


Figure 3: Admin Tool, Settings tab

Feature	Description
	Click this button to view and add licenses to your Avigilon Control Center system. For more information, see **Licensing the Server**.
	Click this button to define the amount of server space allocated to surveillance data storage. For more information, see **Configuring the Server Storage Settings**.
	Click this button to define the network ports. For more information, see **Configuring the Server Network Settings**.
	Click this button to define where backup files are stored. For more information, see **Configuring the Server Backup Settings**.

Setup

Complete the following procedures to configure the Control Center Server to fit your requirements.

Licensing the Server

After the Control Center Server software has been installed, you must apply your software license to the application or the Control Center Server will not run.

Your server can be licensed for the Core, Standard or Enterprise edition. If you are running the Enterprise edition, this procedure is also used to add integration licenses.

Accessing the Server Licensing Settings

1. In the Admin Tool, select **Settings** >  .

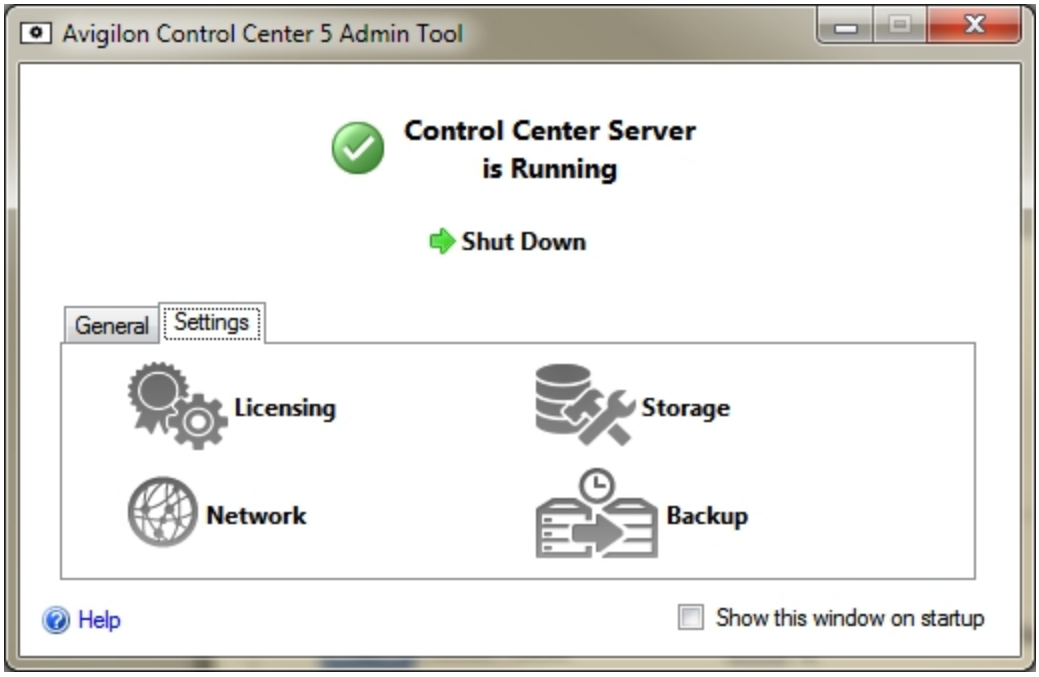


Figure 4: Admin Tool window, Settings tab

2. In the License Activation dialog box, you can see the server's license edition and optional license features.

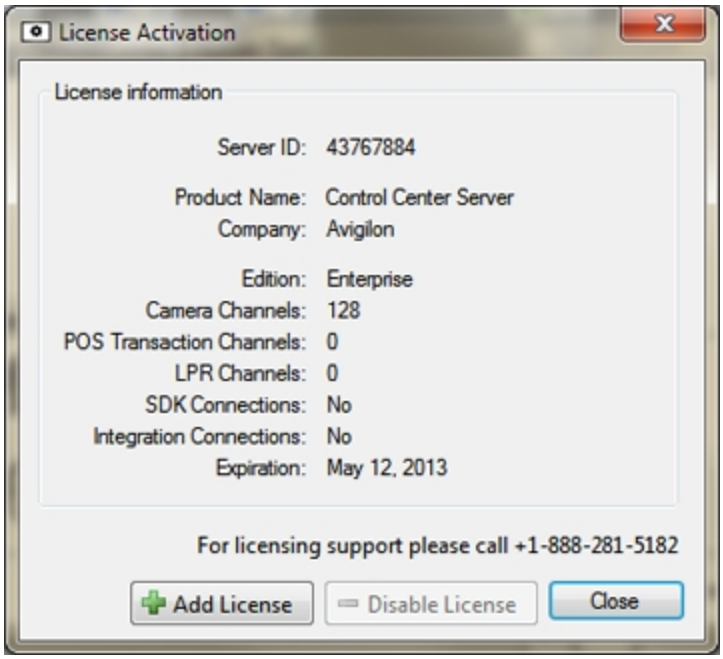


Figure 5: The License Activation dialog box

The Server ID: is unique to each server running the Avigilon Control Center software. If you need help licensing the software, call Avigilon Technical Support and give them the Server ID:.

If you need to upgrade your server hardware, you can disable the license on the current server and reuse the license on the new server. For more information, see **Deactivating Licenses**.

Activating a License Over the Internet

If you have internet access, the Admin Tool will connect to the internet automatically and help you activate your license.

1. In the Admin Tool, select **Settings** >  .
2. In the License Activation dialog box, click  .
3. If an internet connection was detected, click **Internet Activation (Recommended)**. If an internet connection was not detected, see **Activating a License Manually**.

Figure 6: The Activate Control Center Server page

4. Enter the product key; a check mark will appear if it is valid. If you have multiple product keys, click **Add additional key** and enter the next product key. When all the licenses for this server have been added, click **Next**.

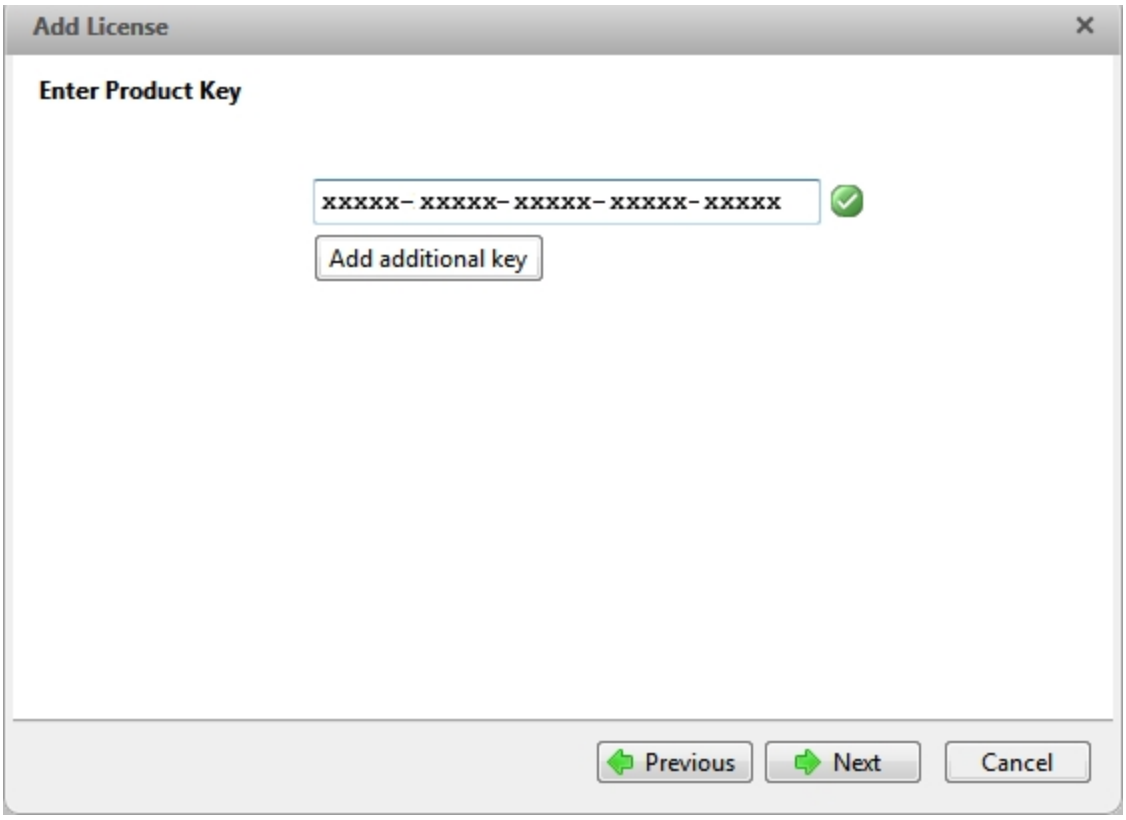


Figure 7: The Enter Product Key page

5. Complete the Product Registration page to receive product updates from Avigilon, then click **Next**.

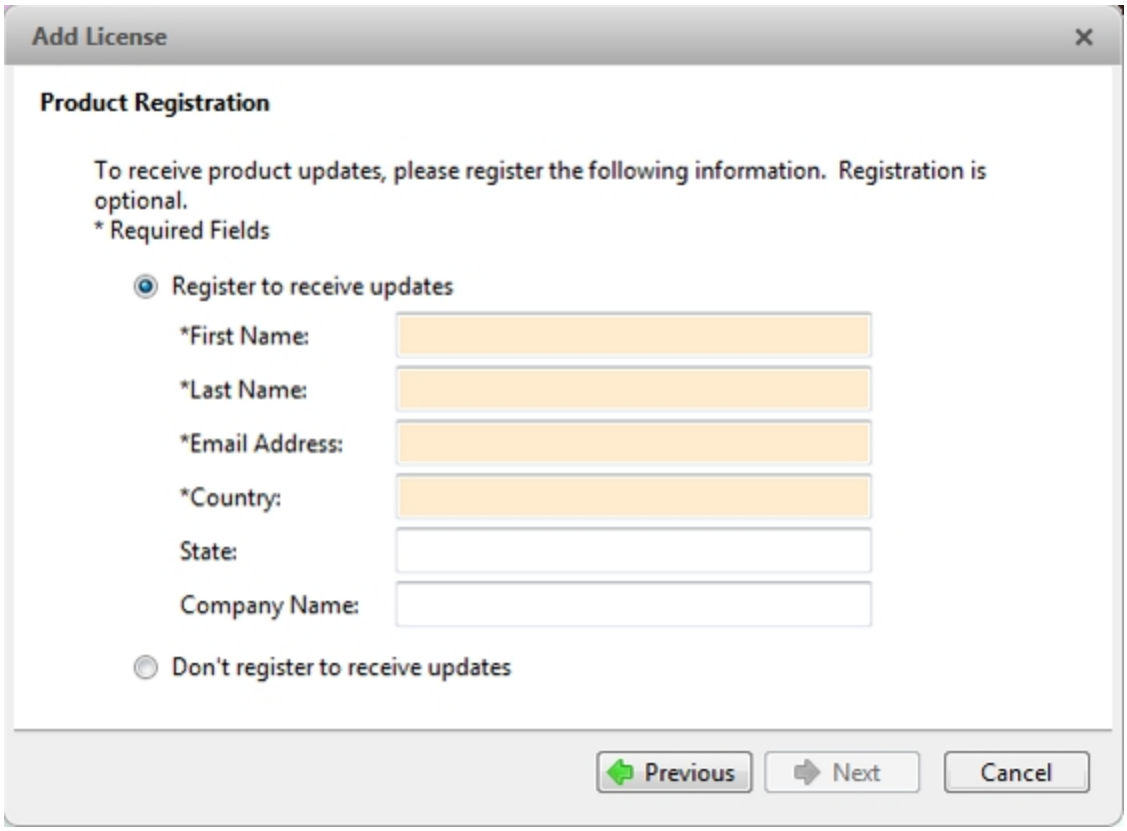


Figure 8: The Product Registration page

6. The Admin Tool will connect to the Avigilon licensing server and activate the license. When the *Activation Succeeded* message appears, click **Finish**.

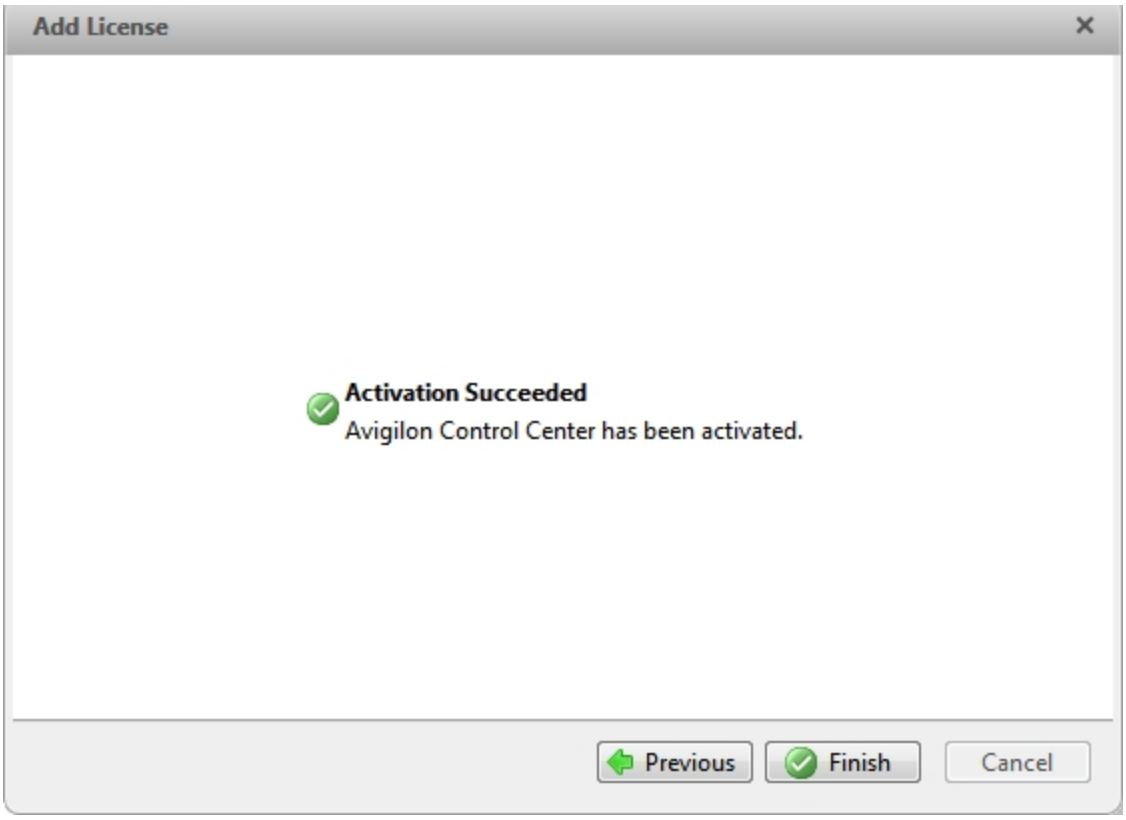


Figure 9: The Activation Succeeded page

Activating a License Manually

If your server does not have internet access, you can activate your license manually by downloading the license file and activating the license on a computer with internet access.

1. In the Admin Tool, select **Settings** >  .
2. In the License Activation dialog box, click  .
3. If an internet connection was not detected, click **Manual Activation (Recommended)**.

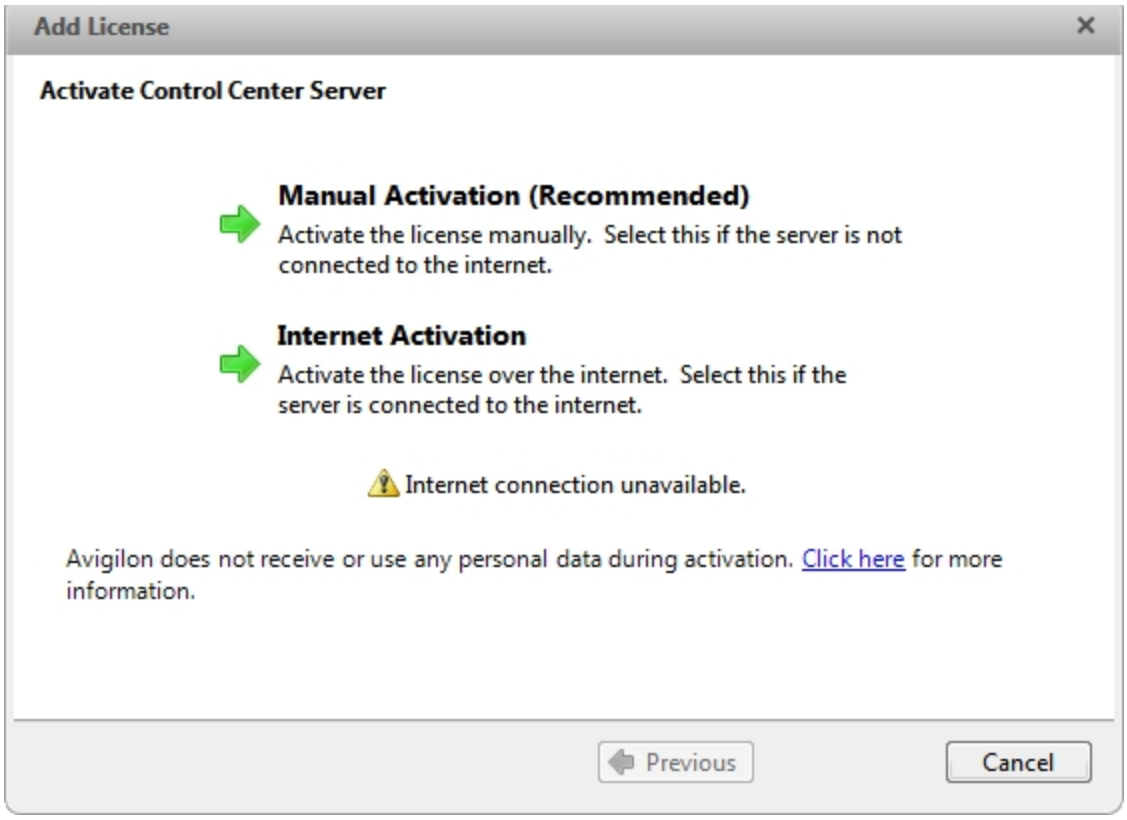


Figure 10: The License Activation page

4. Click **Step 1: Generate Activation File**.

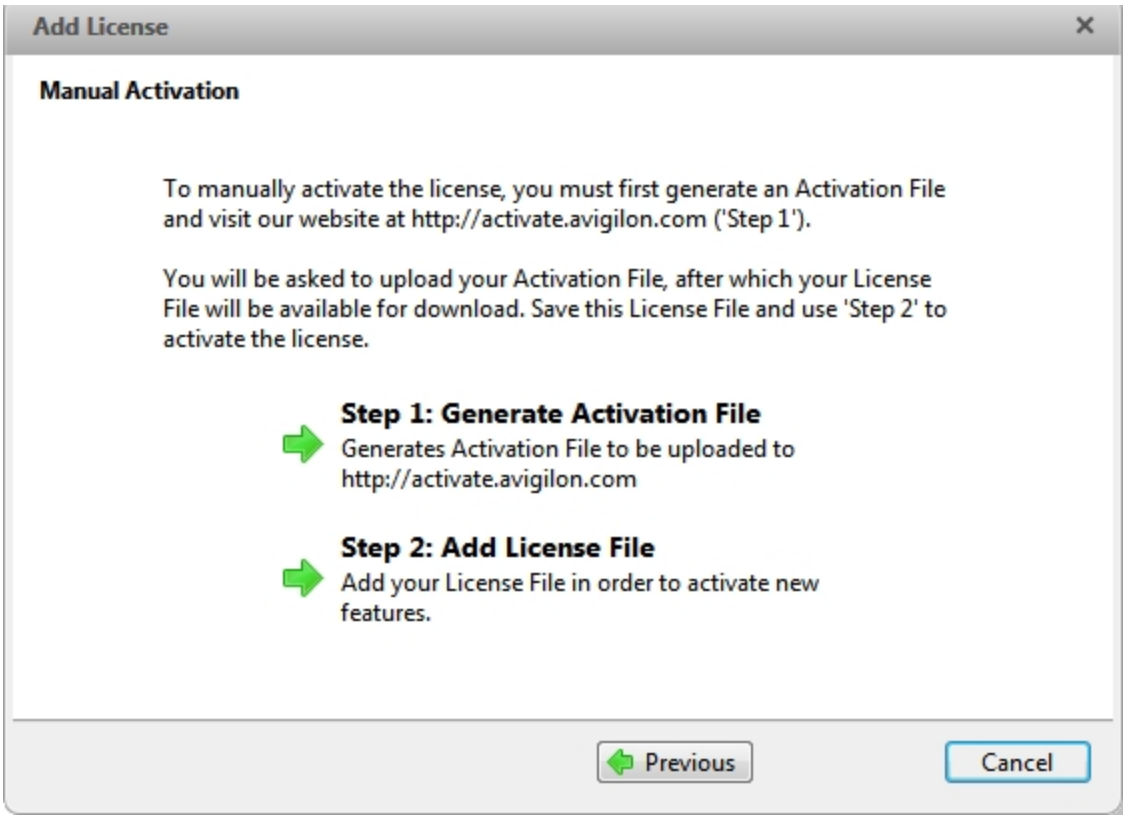


Figure 11: The Manual Activation page

5. Enter the product key; a check mark will appear if it is valid. If you have multiple product keys, click **Add additional key** and enter the next product key. When all the licenses for this server have been added, click **Next**.

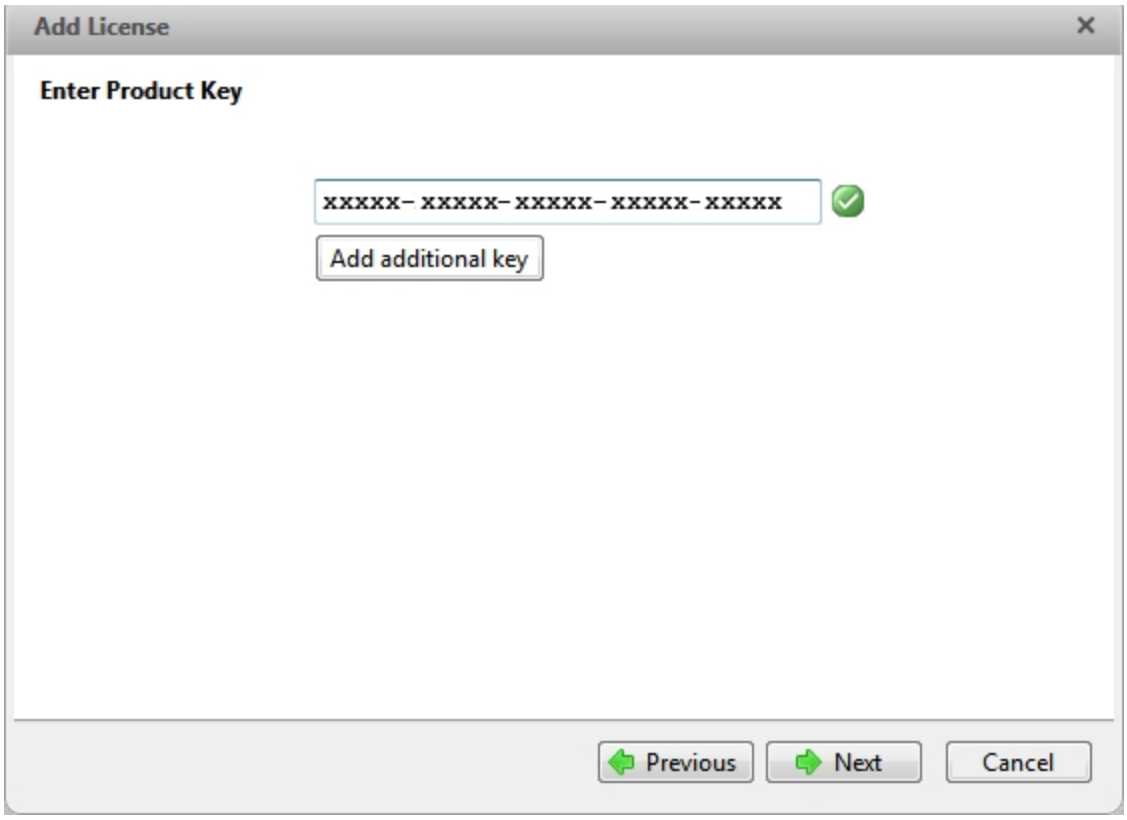


Figure 12: The Enter Product Key page

6. Select a location and file name for the activation file, then click **Next**.

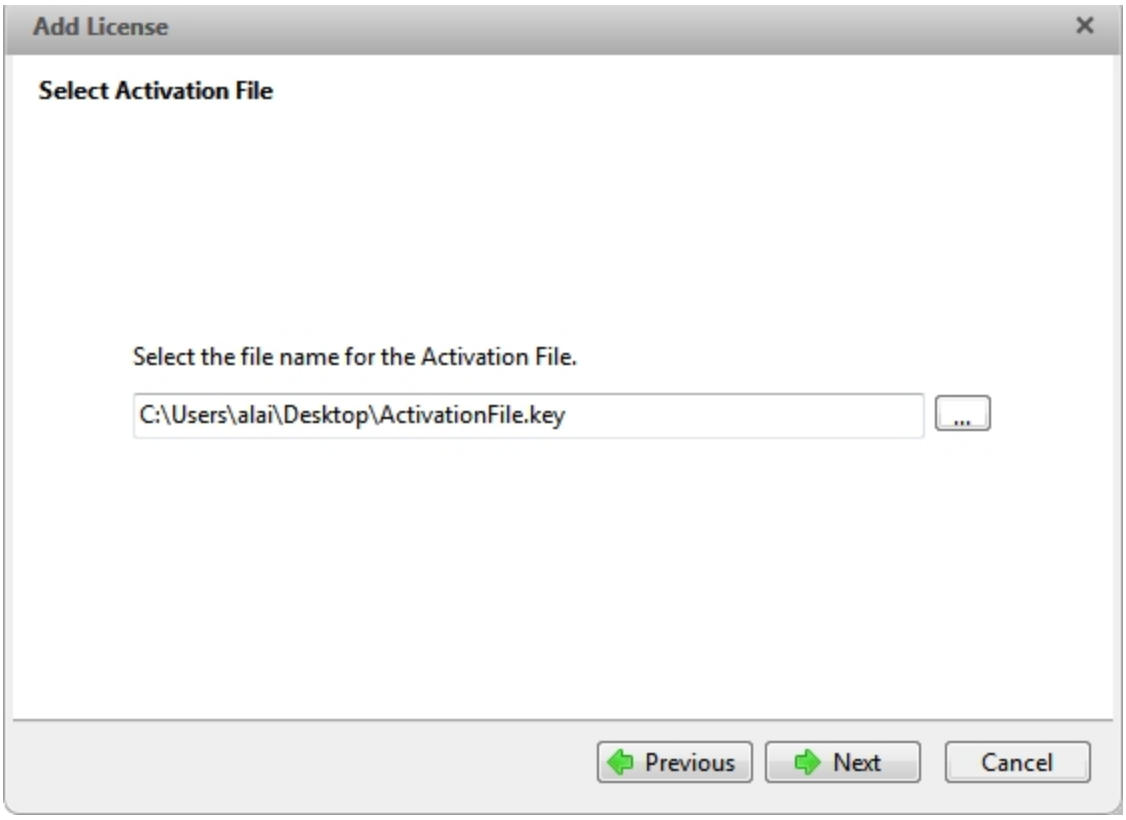


Figure 13: The Select Activation File page

7. The activation file is saved at the location you specified. Click **Next**.

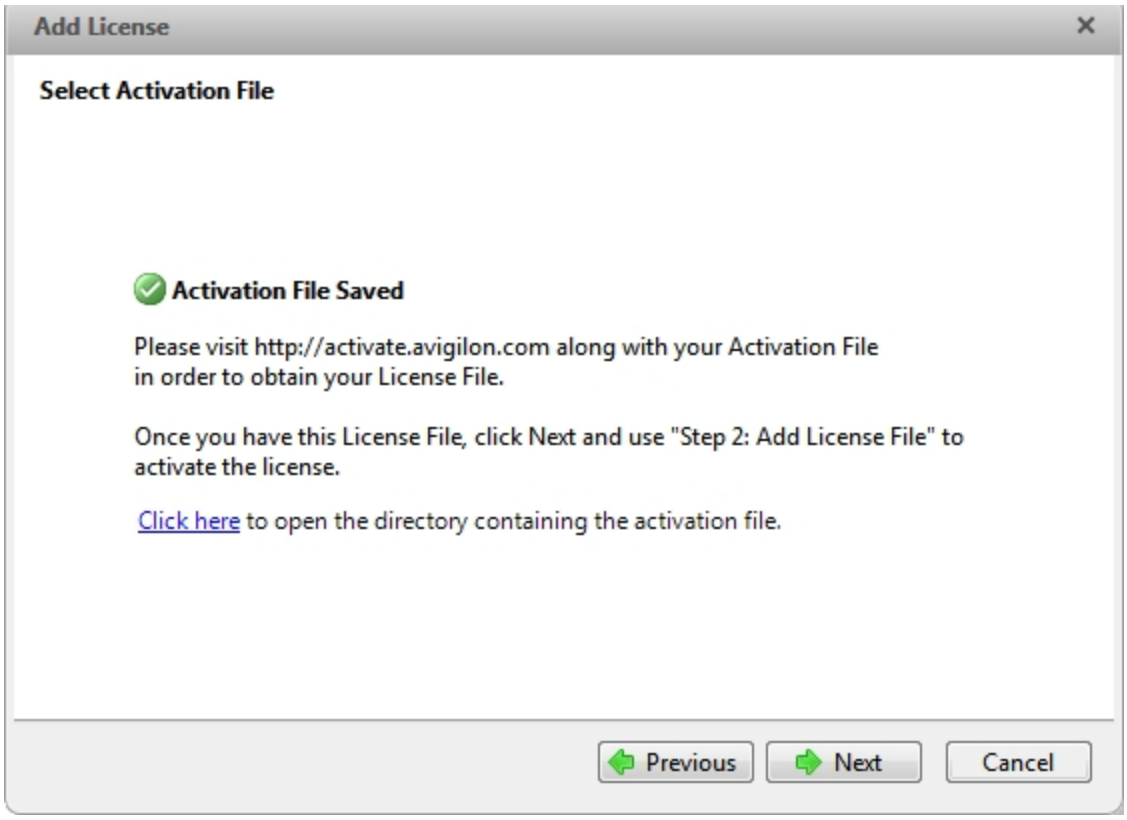


Figure 14: The Activation File Saved page

8. Copy the saved activation file to a computer with internet access.
9. Open a web browser and go to **http://activate.avigilon.com**.
10. Browse to the location of your activation file then click **Upload**.

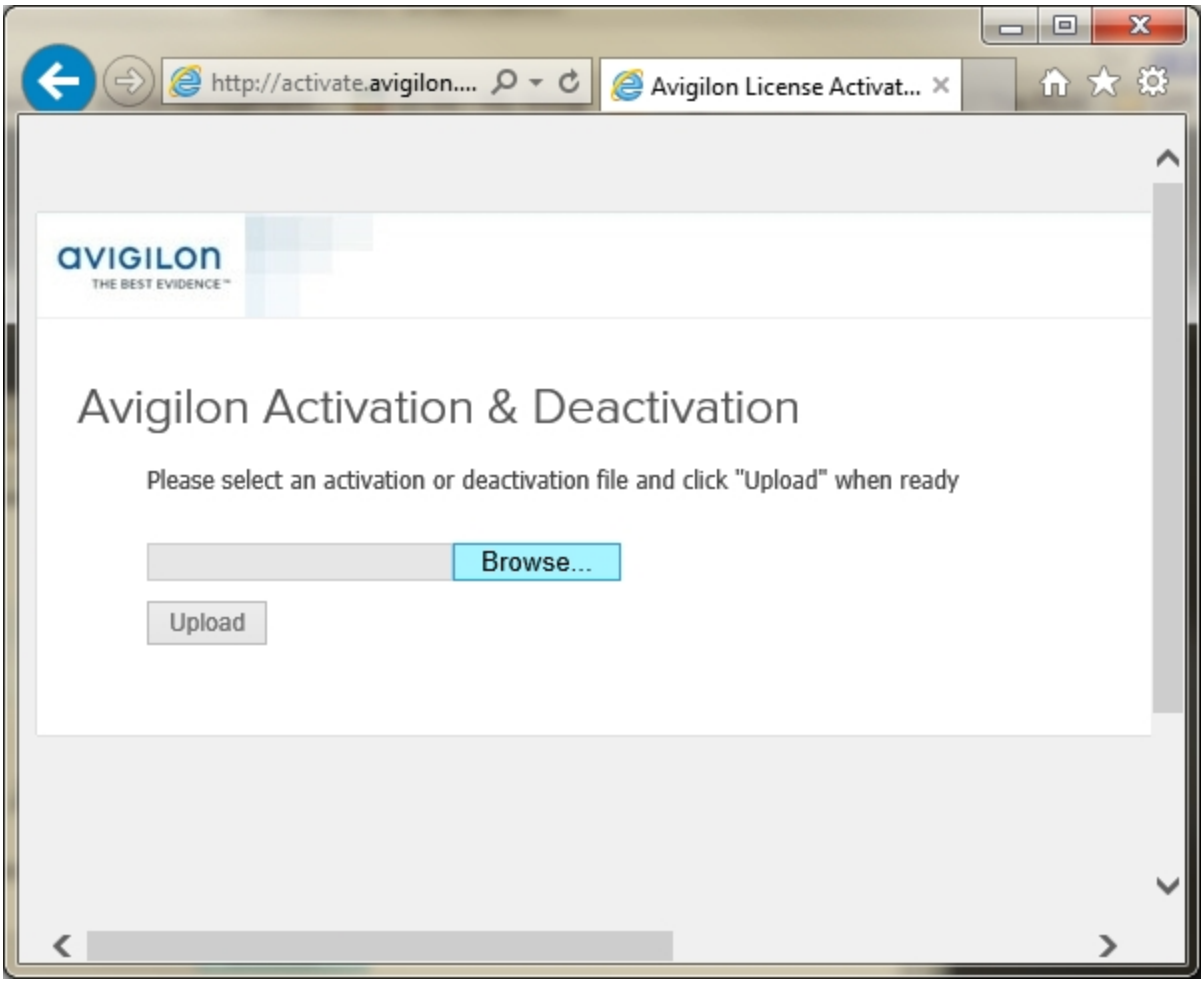


Figure 15: Activation Website

The activated license file should download automatically. If it does not, allow the download to occur when you are prompted.

11. Complete the product registration page to receive product updates from Avigilon, then click **Register**.

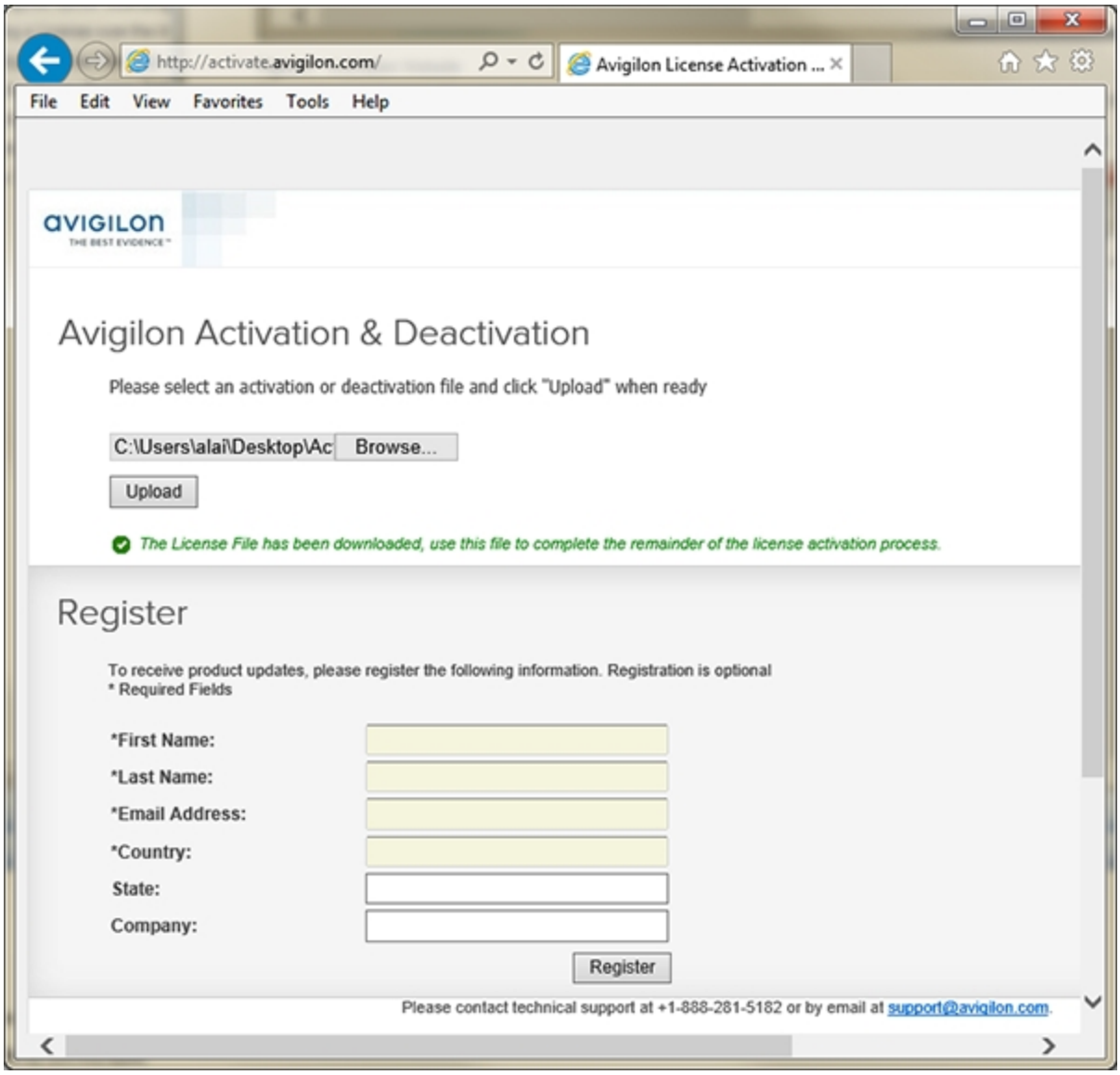


Figure 16: Registration Website

12. Copy the downloaded license file onto the server you are activating.
13. Click **Step 2: Add License File**.

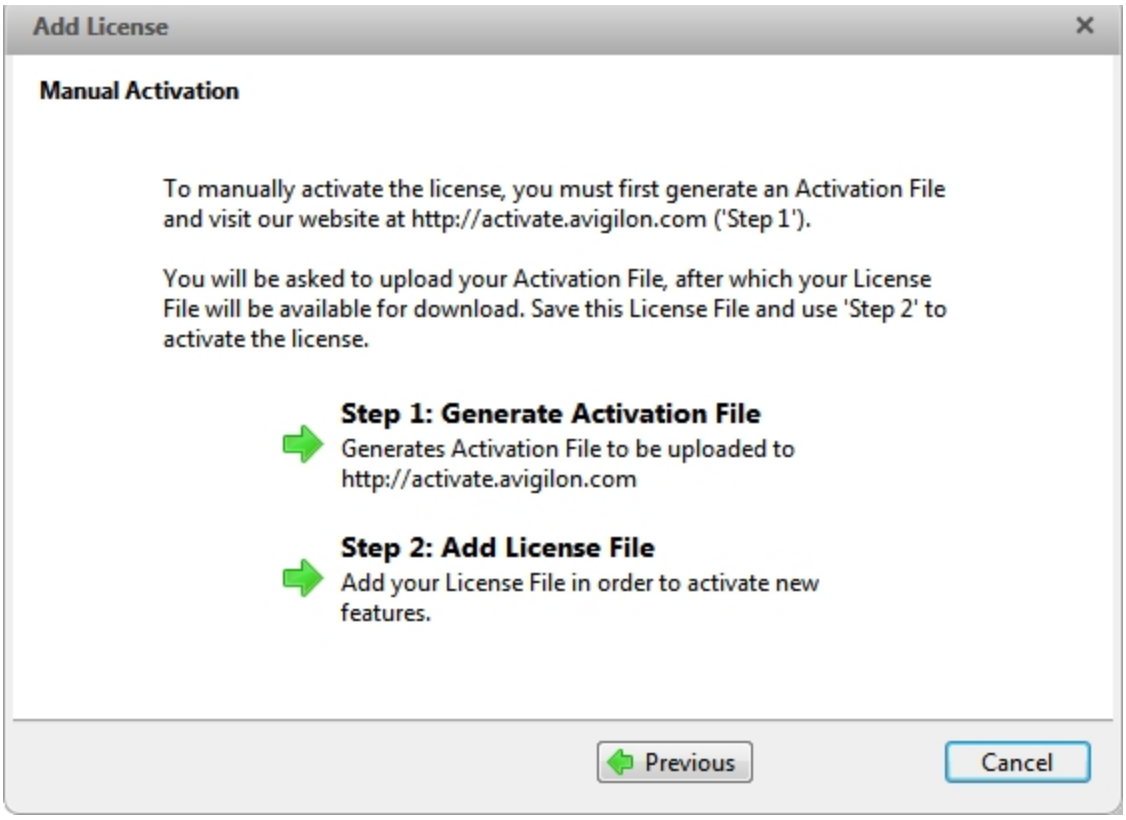


Figure 17: The Manual Activation page

14. Enter the location of the license file then click **Next**.

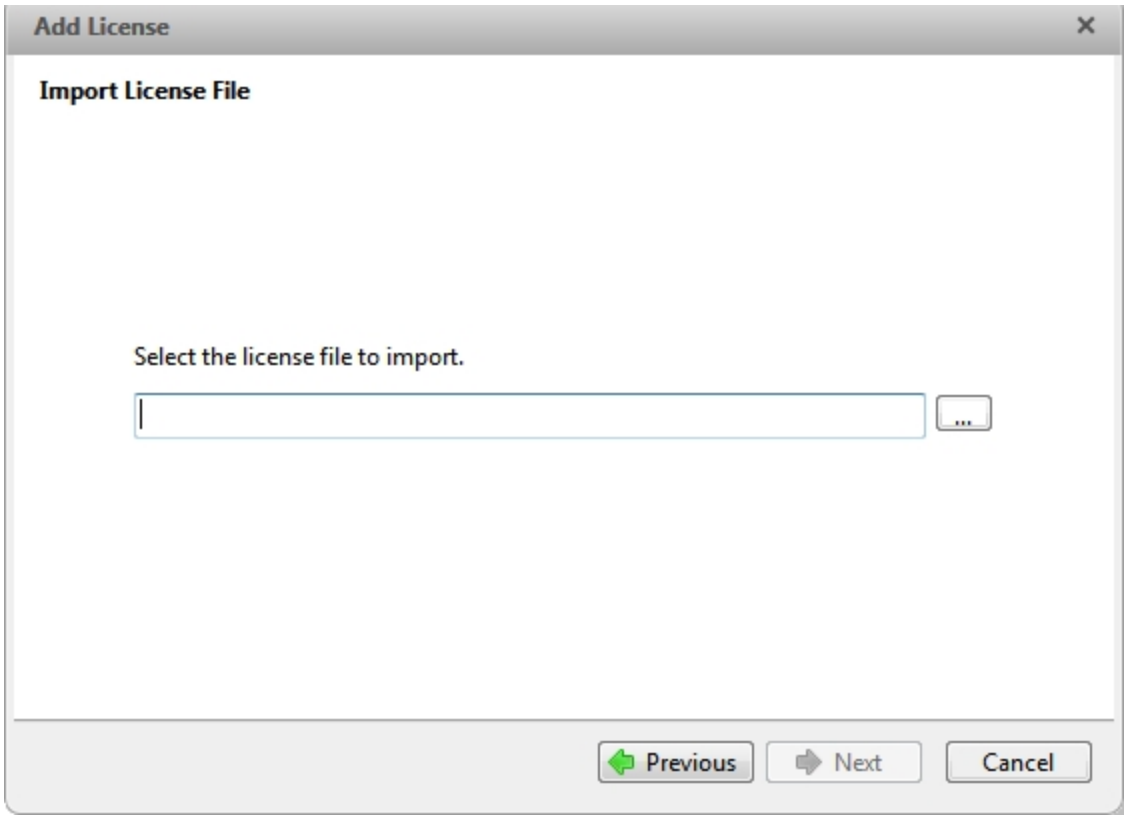


Figure 18: The Import License File page

15. When the *Activation Succeeded* message appears, click **Finish**.

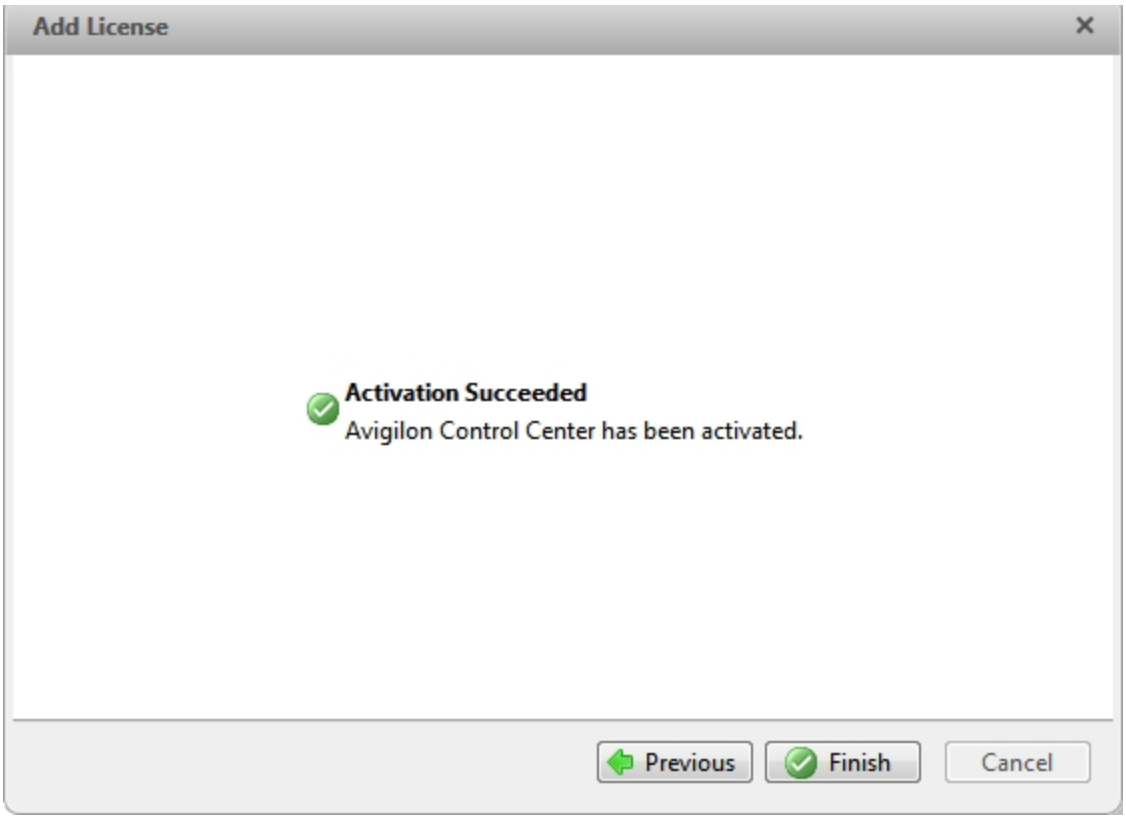


Figure 19: The Activation Succeeded page

Configuring the Server Storage Settings

You must configure the server storage settings so the Avigilon Control Center Server software knows how much space is allocated for storing surveillance data, and where it is located.

If the Admin Tool detects that there is no existing storage configuration, it will launch the Set Up Storage Configuration dialog box.

Accessing the Server Storage Configuration

1. In the Admin Tool, click **Shut Down**. The Control Center Server must be shut down before the storage configuration can be viewed or edited.
2. In the Settings tab, click  .

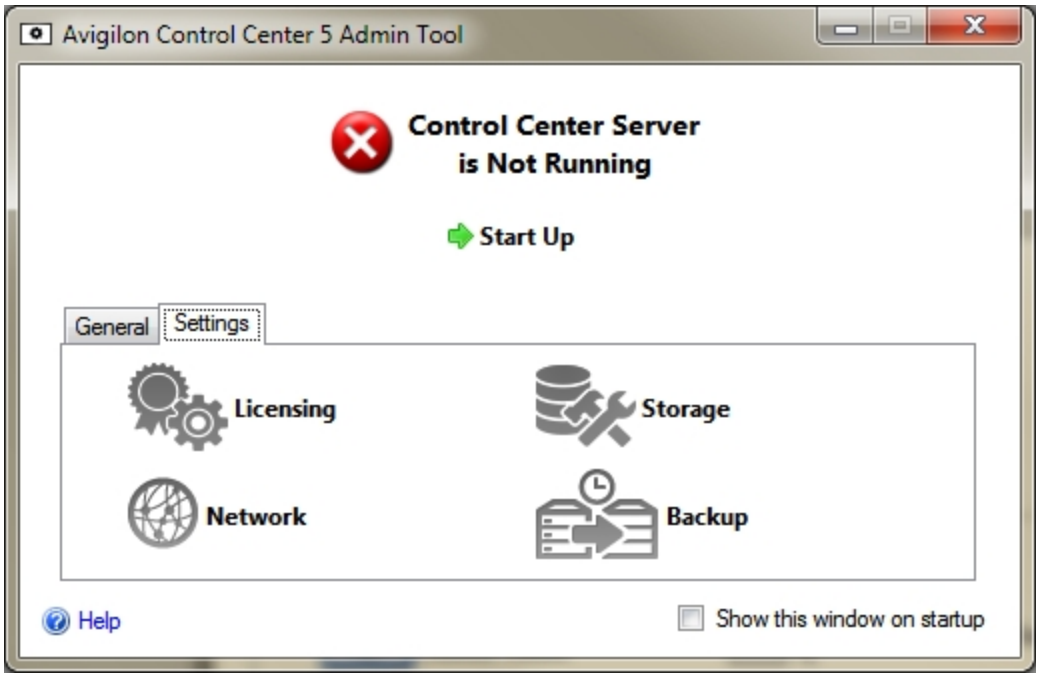


Figure 20: Admin Tool Window, Settings tab

3. In the Storage dialog box, you can see the current storage configuration.

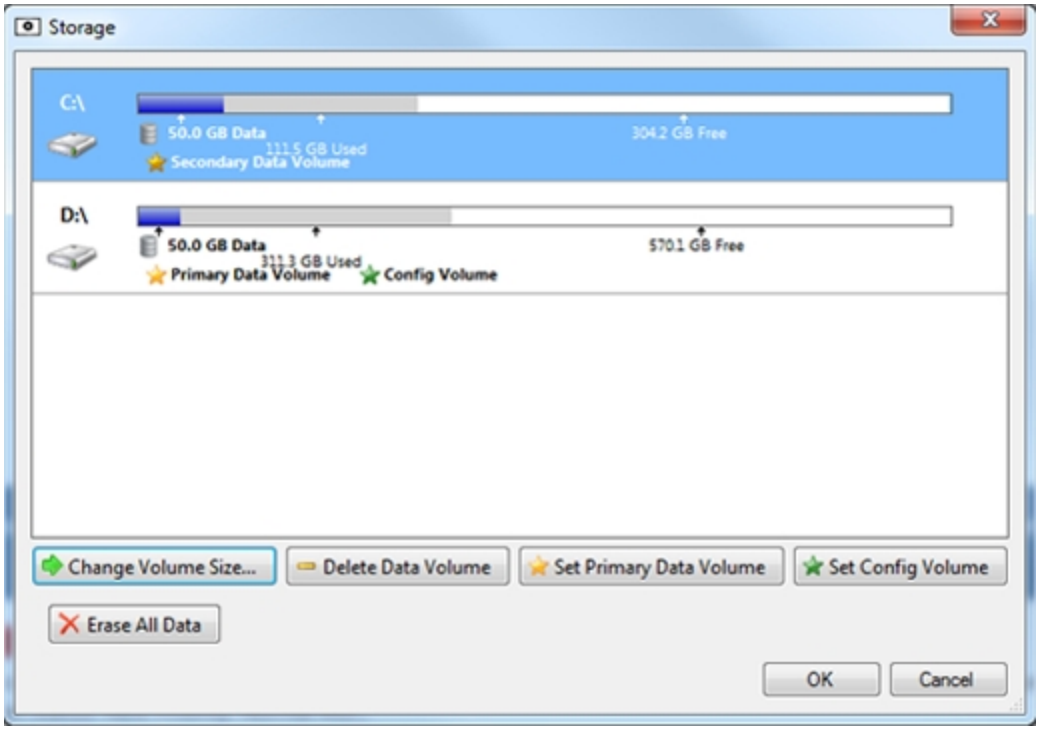


Figure 21: The Storage dialog box

Setting Up the Initial Server Storage Configuration

When the Admin Tool detects that there is no existing storage configuration, it will launch the Set Up Storage Configuration dialog box with the recommended storage configuration.

By default the software will assign most of the available storage to the Primary Data Volume for storing recorded video.

- If the recommended configuration is acceptable, click **Finish**
- If you want to change the configuration click **Change Storage Configuration**. For more information, see **Changing the Storage Configuration**.

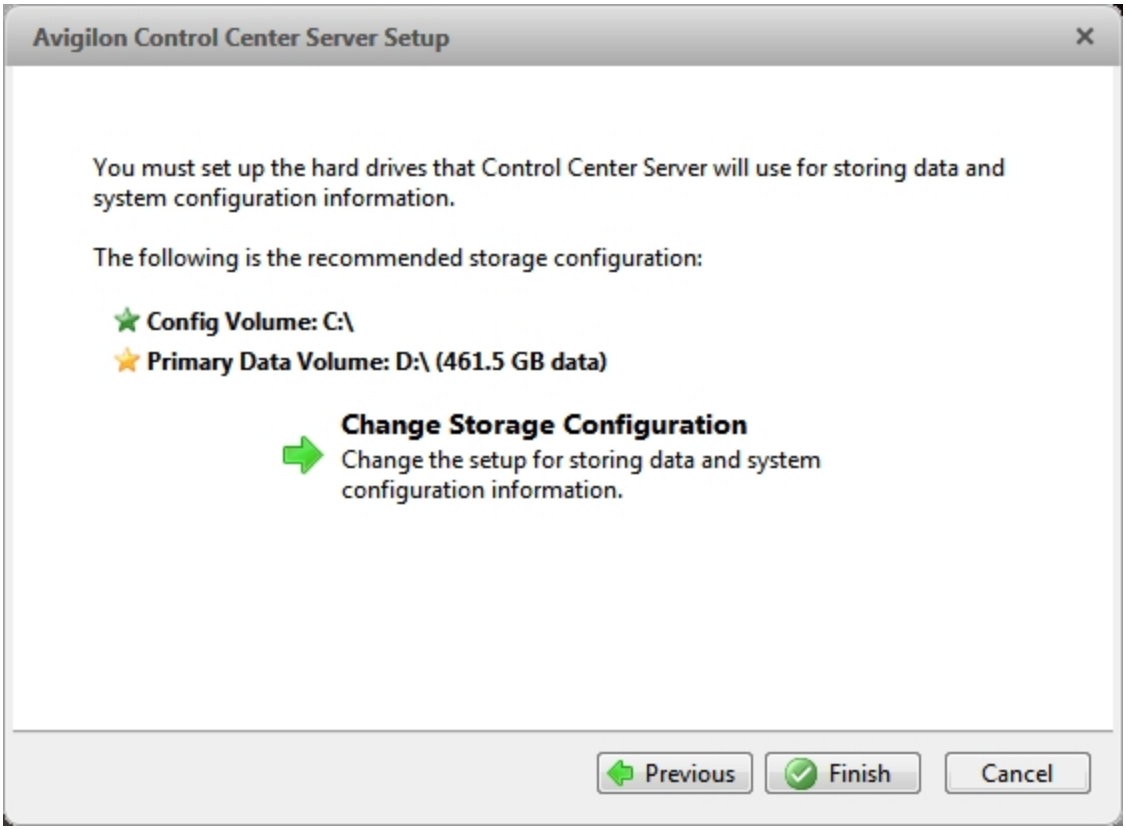


Figure 22: The Set Up Storage Configuration dialog box

Changing the Storage Configuration

You may need to change the storage configuration in the following situations:

- If you are unsatisfied with the storage configuration suggested by the application, click **Change Storage Configuration** to define the storage settings to fit your needs.
- If you recently chose to Erase All Data, you must reset the Storage configuration before you can continue.

Complete the following procedure in the Storage dialog box:

If the Storage dialog box is not already open, see **Accessing the Server Storage Configuration**for more information on how to open it.

1. In the Storage dialog box, select the drive for storing the Config Volume and click **Set Config Volume**.

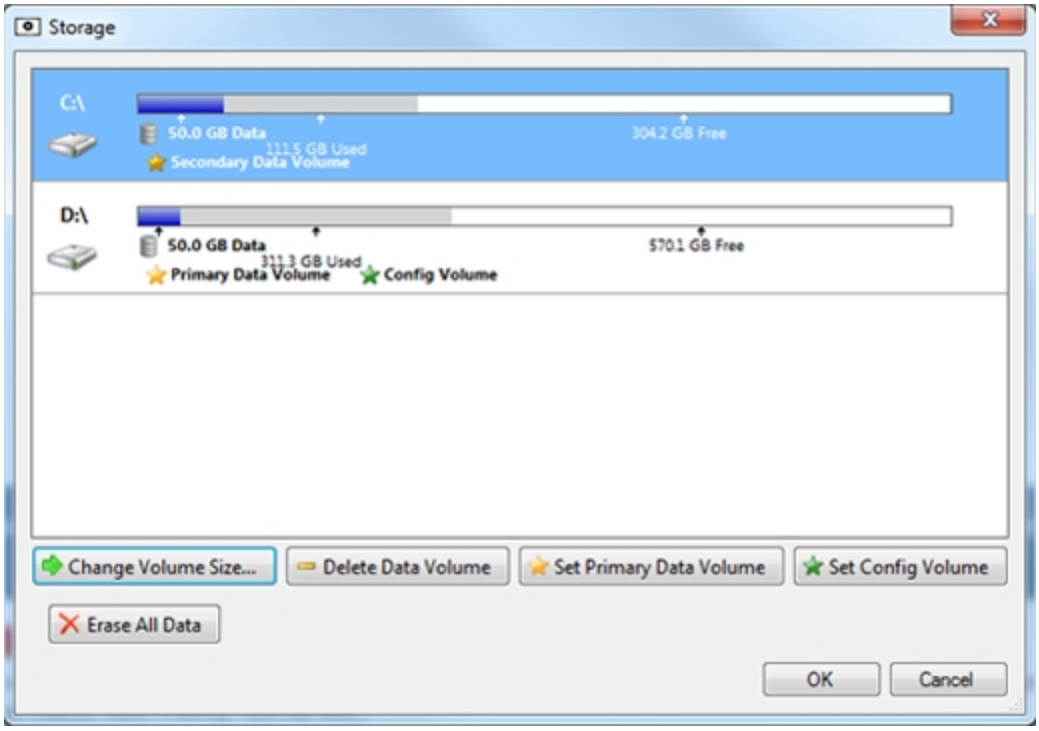


Figure 23: The Storage dialog box

NOTE: Some of the buttons in the figure may not be available if the drive cannot accommodate the setting.

2. To add a data volume, select the drive and click **Add Data Volume...**. The button is not available if the drive already has a data volume.

    - In the Add Data Volume dialog box, enter the preferred data volume size, then click **OK**.

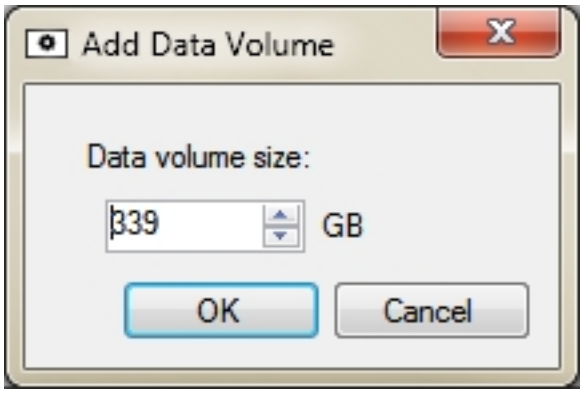


Figure 24: The Add Data Volume dialog box

3. To delete a Secondary Data Volume, select the drive and click **Delete Data Volume**. Deleting a data volume will erase all recorded data from that drive.

NOTE: You cannot delete a Primary Data Volume, you can only erase all data.For more information, see **Erasing the Storage Configuration**.

4. If you are not satisfied with the location of the Primary Data Volume, select the drive you prefer and click **Set Primary Data Volume**.

   The Primary Data Volume contains the database that indexes the surveillance data.

   NOTE: The drive must have a data volume before it can be set as the Primary Data Volume.

5. When you are satisfied with the storage configuration, click **OK**.

Erasing the Storage Configuration

NOTE: If you choose to erase all stored data, be aware that all recorded surveillance data and server settings will be lost.

1. Open the **Storage** dialog box. For more information, see **Accessing the Server Storage Configuration**.
2. Click **Erase All Data**.
3. When the confirmation dialog box appears, click **Yes**.
4. You will need to create a new storage configuration before you can start up the Control Center Server again. For more information, see **Changing the Storage Configuration**.

Configuring the Server Backup Settings

To allow the system to automatically back up recorded video, you must enable **Backup** in the Admin Tool and assign a backup location for the backup files.

1. In the Admin Tool, select **Settings** >  .

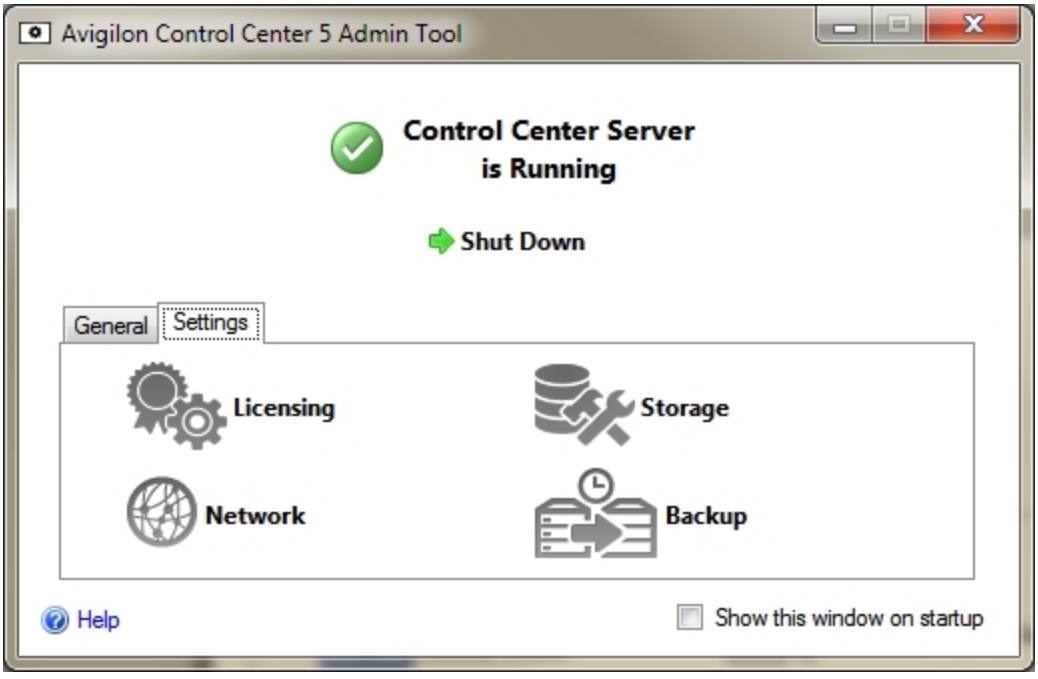


Figure 25: Admin Tool window, Settings tab

2. In the Backup dialog box, select the **Enable Backup** check box to allow the server to back up video files.

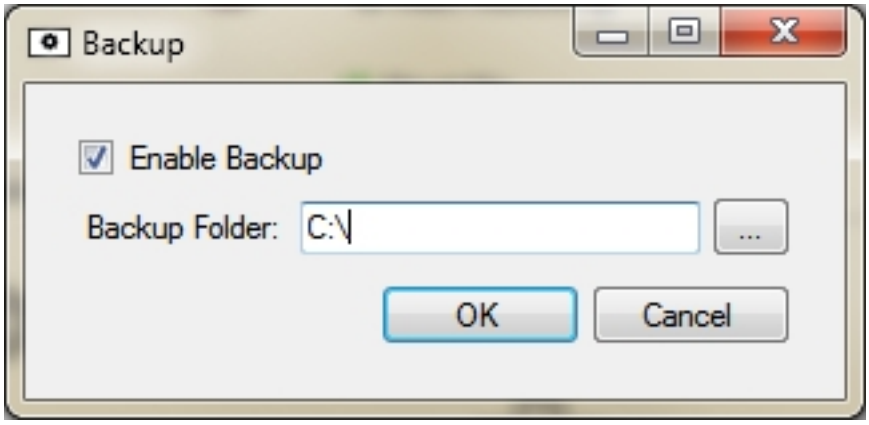


Figure 26: The Backup dialog box

3. Enter a location for the **Backup Folder:**. Click **[...]** to browse to the backup folder location.
4. Click **OK**.

To initiate a backup or set up automatic backups, see *The Avigilon Control Center Client User Guide*.

Configuring the Server Network Settings

The server communicates with the Avigilon Control Center Client software through a range of UDP and TCP ports. The port ranges only need to be changed if the Client software is trying to access two or more servers that are behind the same NAT device (e.g. router), or if there is a port conflict with other software running on the same computer as the Avigilon Control Center Server software.

1. In the Admin Tool, select **Settings** >  .

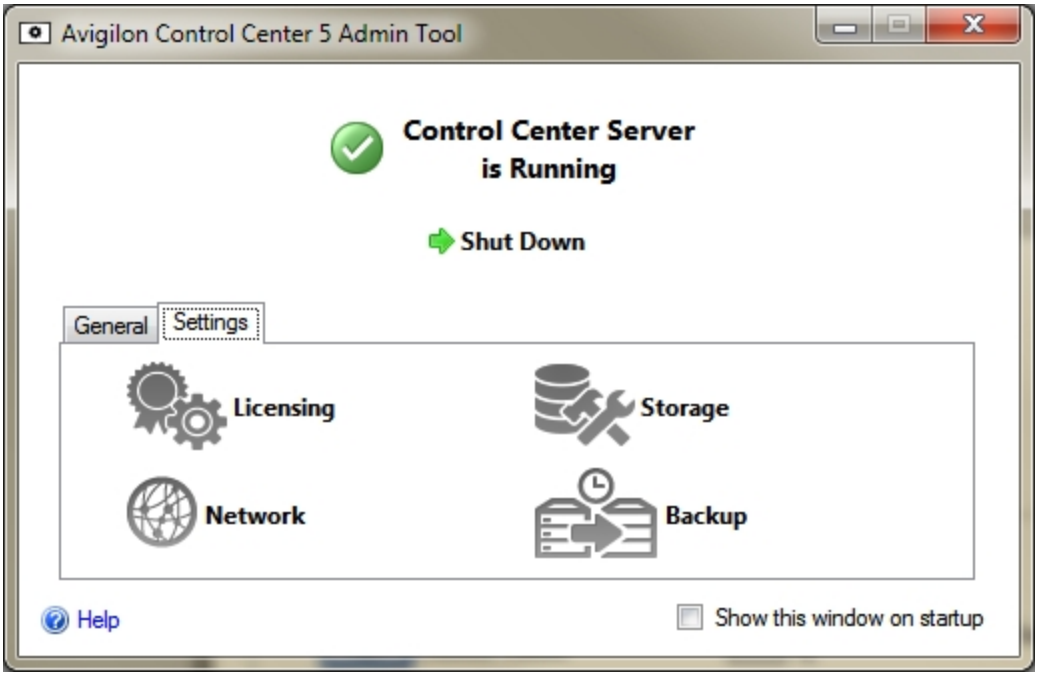


Figure 27: Admin Tool window, Settings tab

2. In the Network dialog box, enter the desired base port then click **OK**.

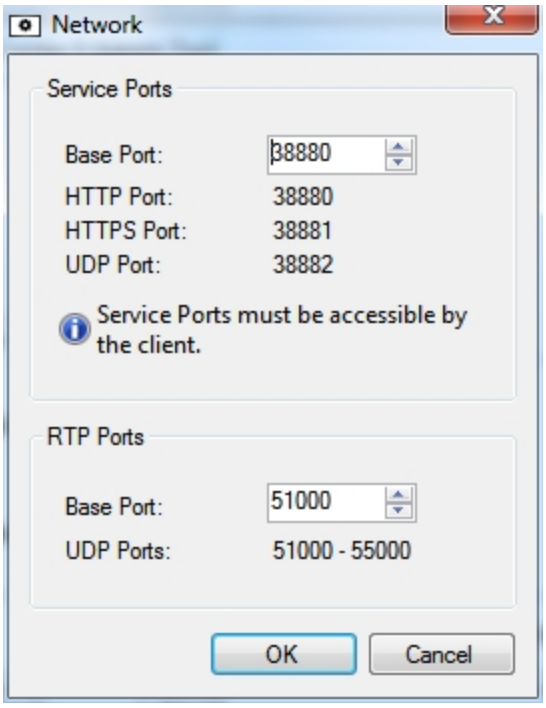


Figure 28: The Network dialog box

- The service ports used by the Server software are updated as the base port changes.
- The RTP port range must be accessible by the Client computer and can be forwarded on any router or network address translation point between the Client and Server.

Using the Admin Tool

In addition to configuring the server, the Admin Tool can also be used to start up and shut down the Control Center Server software, launch the Client software, and display the Application Logs.

Starting Up and Shutting Down the Control Center Server

The Control Center Server software automatically starts when Windows starts, but it can be manually shut down and started through the Admin Tool.

Starting Up the Control Center Server

1. In the Admin Tool, click **Start Up**.

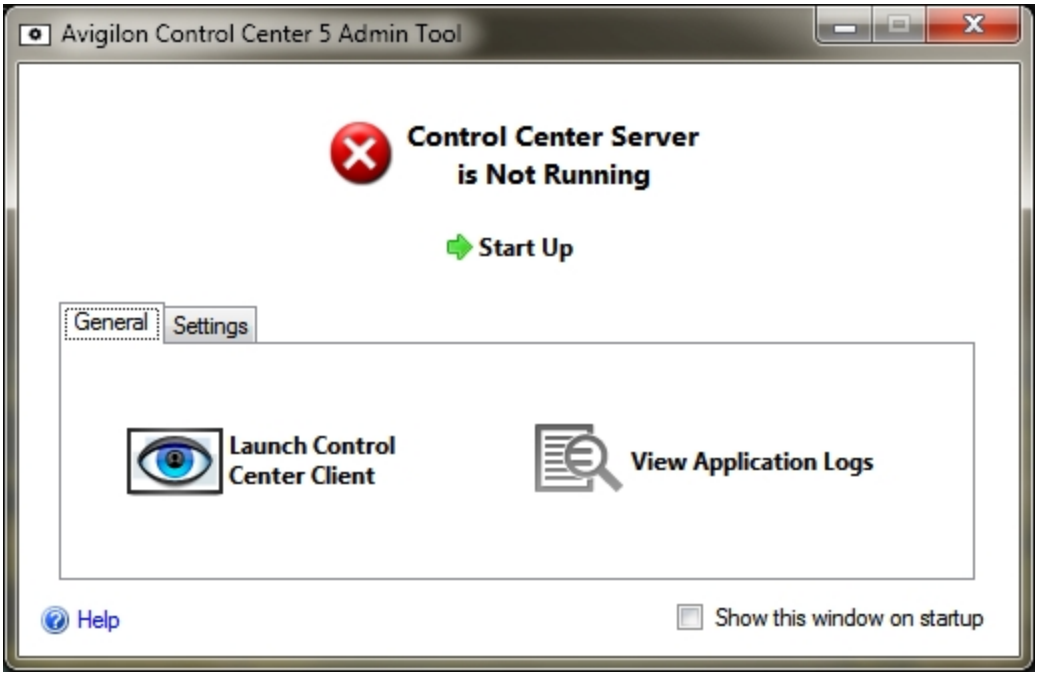


Figure 29: Admin Tool window, Control Center Server is Not Running

When the Control Center Server has started properly, the Admin Tool will display *Control Center Server is Running*.

Shutting Down the Control Center Server

When the Control Center Server is shut down, all video recording is stopped until the Control Center Server is started again.

1. In the Admin Tool, click **Shut Down**.

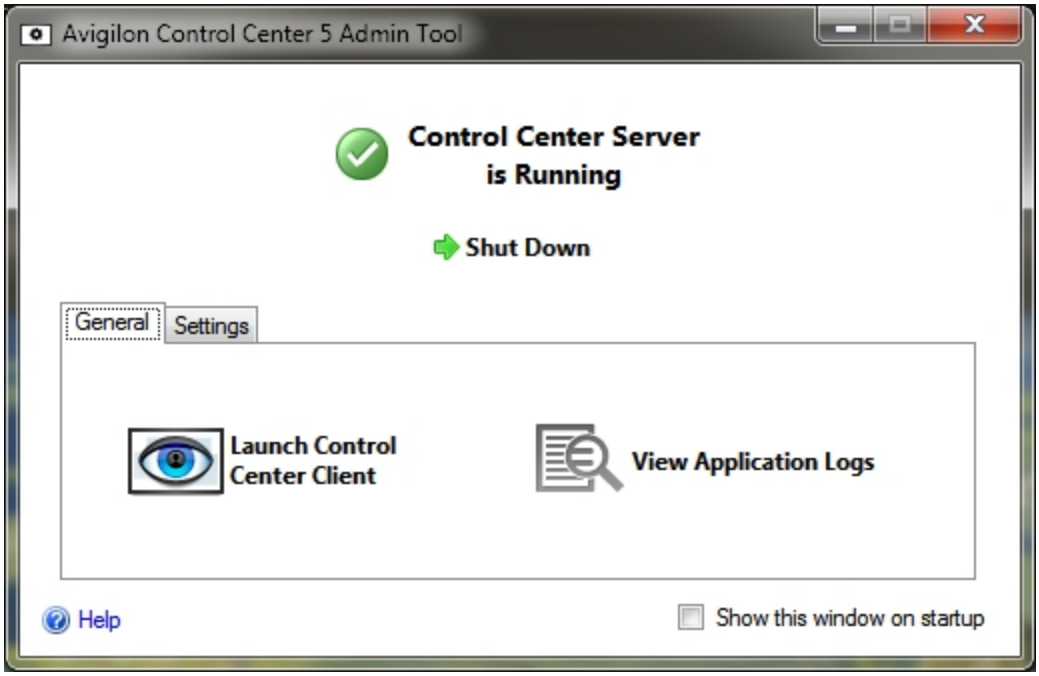


Figure 30: Admin Tool window, Control Center Server is Running

When the Control Center Server has shut down properly, the Admin Tool will display *Control Center Server is Not Running*.

Starting the Control Center Client

The Avigilon Control Center Client software can be started up through the Admin Tool.

1. In the Admin Tool, select **General** >  .

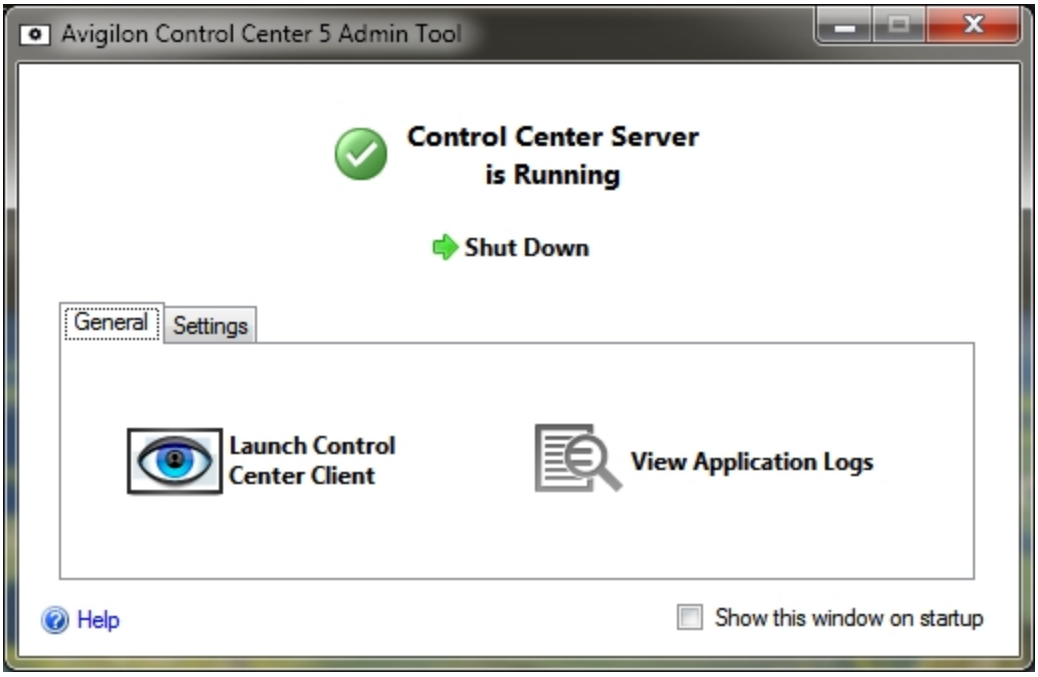


Figure 31: Admin Tool window, General tab

If the Client software is not installed, the Admin Tool will prompt you to install it.

Viewing Application Logs

You can view the Avigilon Control Center application error logs through the Admin Tool. This can assist in diagnosing problems with your system.

1. In the Admin Tool, select **General** >  .

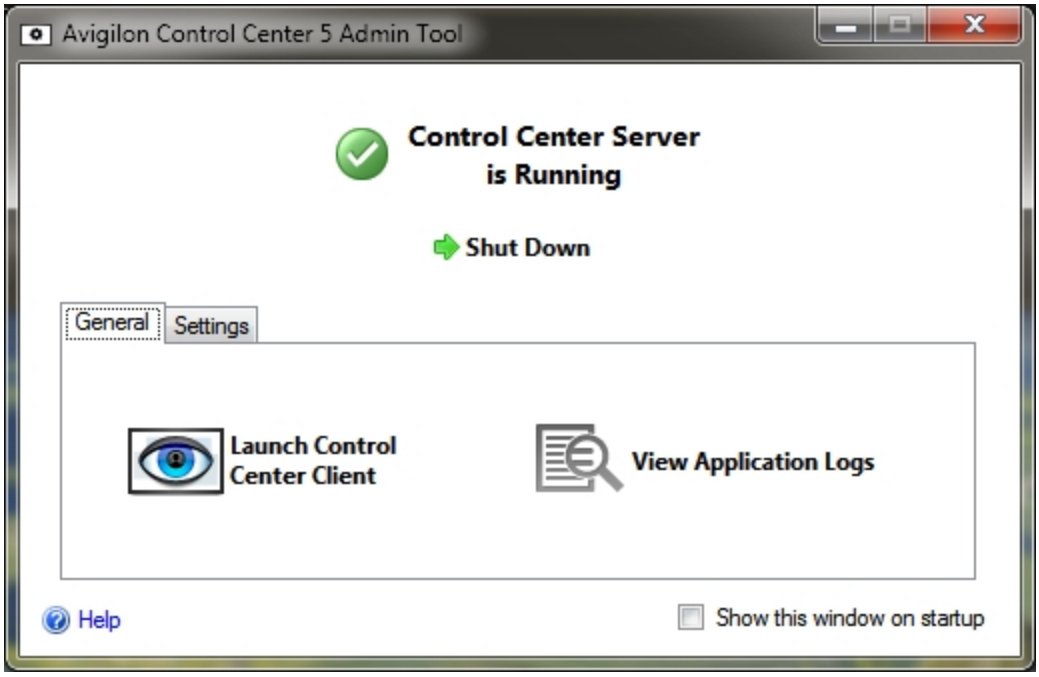


Figure 32: Admin Tool window, General Tab

2. The Application Logs dialog box will appear. Double-click an error to view the details.

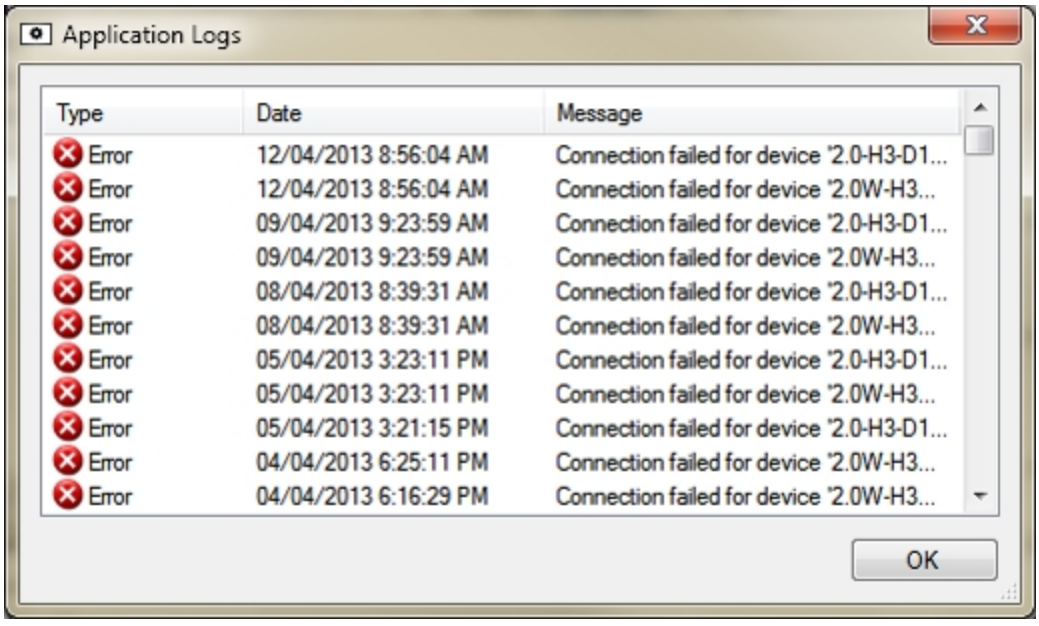


Figure 33: The Application Logs dialog box

3. Click **OK** to close the dialog box.

Appendix

Resetting the Administrator Password

To reset the administrator password, you must delete all existing user and group account information from the server Config Volume.

Tip: You can avoid this procedure if you have a user account that has all the same permissions as an administrator. You can use this user account to reset the administrator password in the Avigilon Control Center Client software.

1. In the Admin Tool, click **Shut Down**. If you have multiple servers in your Site, you need to shut down all the servers in your Site.
2. Select **Settings** >  .
3. In the Storage dialog box, make note of which drive holds the Config Volume.
4. Access the Config Volume drive and navigate to the `AvigilonConfig\Db\DirectoryShared\Users` folder.

   For example, `D:\AvigilonConfig\Db\DirectoryShared\Users`.
5. Delete all the files in this folder. If you have multiple servers in your Site, you need to delete this folder from every server in your Site before you do the last step.

   The server automatically resets all the user and group settings back to the factory default.
6. In the Admin Tool, click **Start Up**. Repeat for each server in your Site.

Once all the servers have come back online, you can log into the Site using the default administrator credentials:

- **User Name:** administrator
- **Password:** <leave blank>

To add users and groups to the server, see *The Avigilon Control Center Client User Guide*.

Deactivating Licenses

If you are replacing your current server with a new one, you must manually deactivate the license on the old server before the license can be reused on the new server.

If you are unable to access your old server to deactivate the license, contact Avigilon Technical Support.

NOTE: You cannot deactivate individual licenses. When you deactivate licenses in the Admin Tool, you are deactivating all the licenses on the server.

1. In the Admin Tool, select **Settings** >  .
2. In the License Activation dialog box, click .
3. Select a deactivation method.

   Like the license activation procedure, you have the option of deactivating the license over the internet or manually.

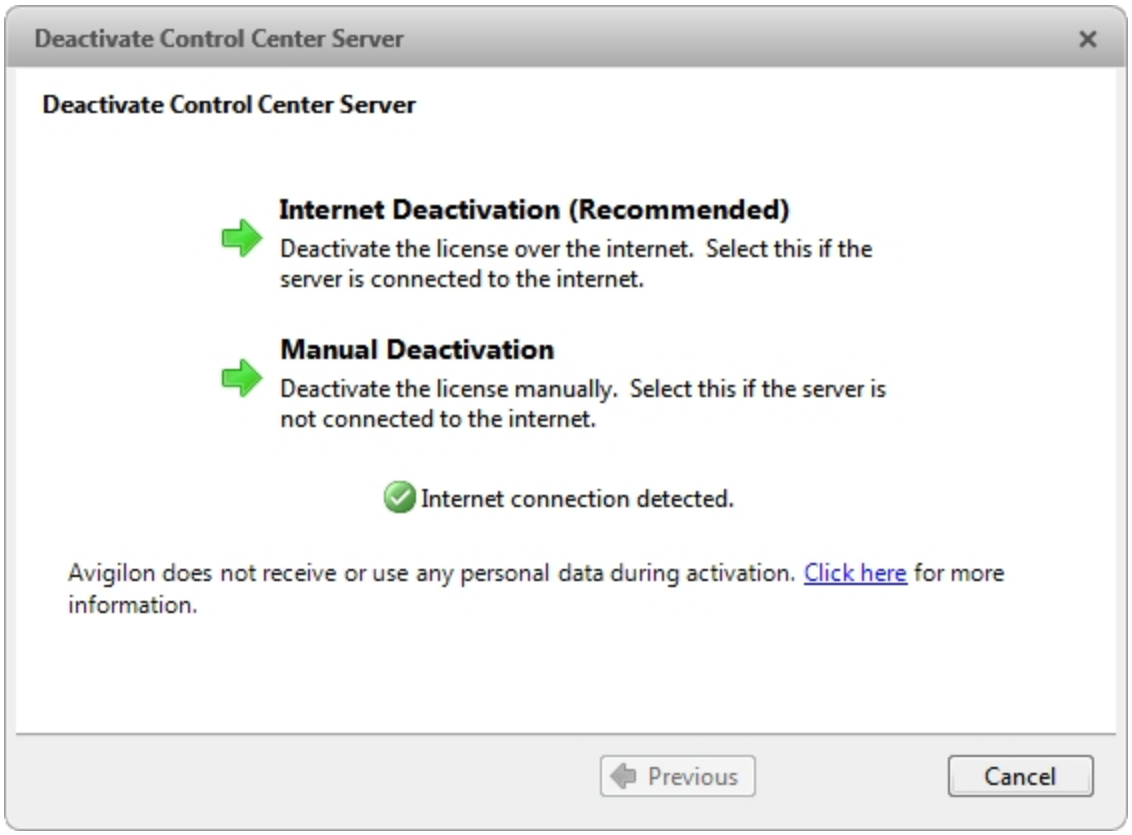


Figure 34: The Deactivate Control Center Server dialog box

4. Click **Copy To Clipboard**, then paste the product key into a text file for reference.

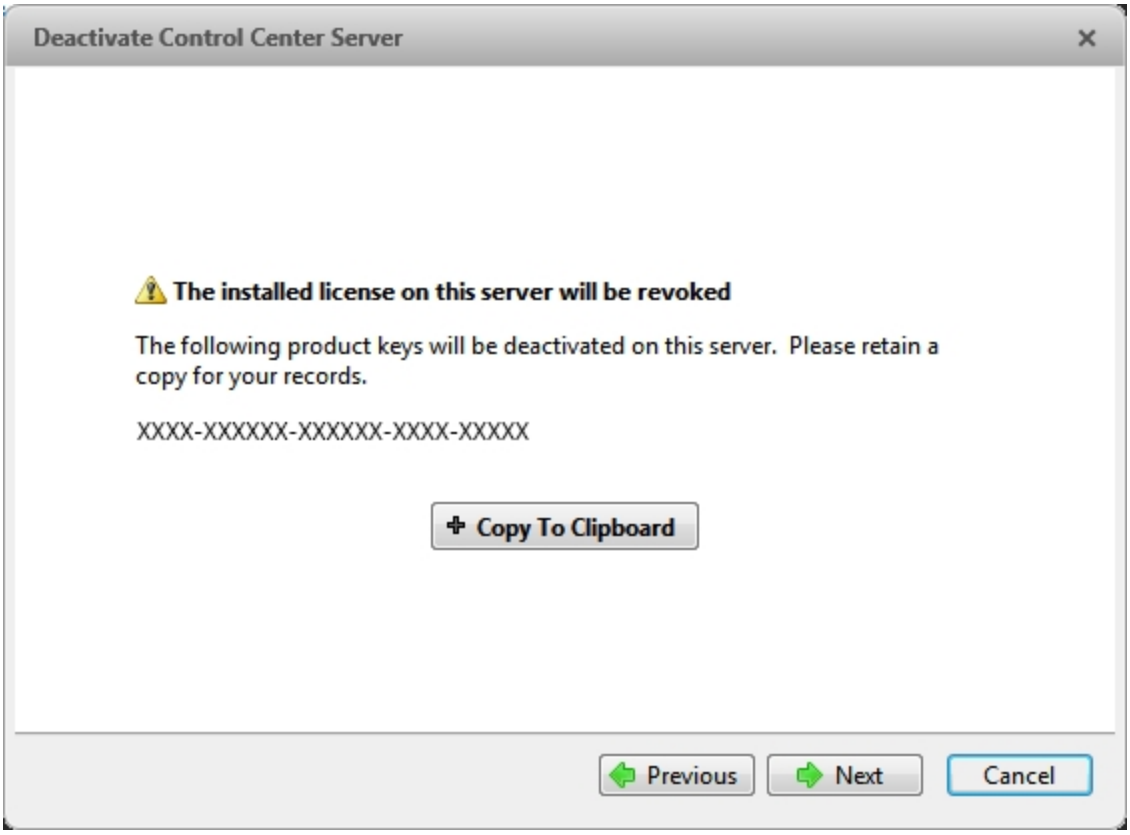


Figure 35: The Deactivate Control Center Server dialog box

It is recommended that the product key be saved to a flash drive so that you can easily access the product key on the new server.

5. Click **Next**.
   - If you selected Internet Deactivation, the system will automatically deactivate the server license.
   - If you selected Manual Deactivation, complete the following steps:
     a. On the following page, download the **`DeactivationFile.key`**.
     b. Copy the saved deactivation file to a computer with internet access.
     c. Open a web browser and go to **http://activate.avigilon.com**.
     d. Browse to the location of your deactivation file then click **Upload**.

   When you see the confirmation message, the license has been deactivated.

Once a license has been deactivated, you can reuse the product key on the new server. For more information, see **Activating a License Over the Internet**.

This Page Left Intentionally Blank

Avigilon Control Center Client User Guide

Version: 4.6 Standard

OLH-CLIENT-B-Rev2

Avigilon
Tel +1.604.629.5182
Fax +1.604.629.5183
http://www.avigilon.com

Revised 2010-11-22

Table of Contents

Monitor resolution	1280 x 1024	1280 x 1024
OS	Windows XP with Service Pack (SP) 2 or later, Windows Vista, or Windows 7	Windows XP with Service Pack (SP) 2 or later, Windows Vista, or Windows 7
CPU	Intel Single Core 2.4 GHz processor	Intel Dual Core 2.0 GHz processor
System RAM	1 GB	2 GB
Video card	PCI Express, DirectX 9.0c compliant with 128 MB RAM (Intel GMA 900 or better, NVIDIA 6600 or better, ATI X1300 or better)	PCI Express, DirectX 10.0 compliant with 256 MB RAM (NVIDIA GeForce 8000 series or better)
Network card	100 Mbps	1 Gbps
Hard disk space	500 MB	500 MB

For More Information

Visit Avigilon at http://www.avigilon.com/ for additional product documentation.

Avigilon University

The Avigilon University provides free online training videos that demonstrate how to set up and use the Avigilon Surveillance System. Register online at the Avigilon Partner site to begin: http://avigilon.com/partners/

Support

For additional support information, visit http://www.avigilon.com/support/.

Regular Avigilon Customer Support Center hours of operation are from 6:00 a.m. to 6:00 p.m. Pacific Standard Time (PST) and can be reached by calling the toll-free number: +1.888.281.5182.

E-mails can be sent to: support@avigilon.com.

For emergency technical support 24 hours a day, 7 days a week, please call the Avigilon Emergency Technical Support Hotline at +1.604.506.3117.

Upgrades

Software and firmware upgrades will be made available for download as they become available. Check http://www.avigilon.com/support/software for available upgrades.

Feedback

We value your feedback. Visit our feedback page to comment on our products and services: http://avigilon.com/feedback/

Getting Started

Once the Avigilon Control Center Client software has been installed, you can start using the Avigilon High Definition Surveillance System immediately. Refer to any of the following procedures to help you get started.

To watch a video overview of the application, see *Module 1 - Introduction to Avigilon Control Center Client and Viewing Live Video* in the Avigilon University - End User Stream.

Starting and Shutting Down the Avigilon Control Center Client

The Avigilon Control Center Client software can be started or shut down at anytime. The Avigilon Control Center Server software is a Windows service and will continue to run in the background even when the Client software is shut down.

Starting the Control Center Client

Perform one of the following:

- From the Windows Start menu, select **All Programs > Avigilon > Avigilon Control Center Client > Avigilon Control Center Client**.
- Double-click the  **Avigilon Control Center Client** shortcut icon on the desktop.
- From the Avigilon Control Center Admin Tool, click **Launch Control Center Client**. See the *Avigilon Control Center Server User Guide* for more information.

Log in to the appropriate server when the Log In dialog box appears. See Logging_In for more information.

Shutting down the Control Center Client

1. In the Avigilon Control Center Client software, select **File > Exit**.
2. In the confirmation dialog box, click **Yes**.

Locating Servers

The Avigilon Control Center Client software must communicate with the Avigilon Control Center Server software to access and configure your surveillance system. If the server is on the same network segment (subnet) as the computer running the Client software, the server will be automatically discovered by the Client software and will appear in the System Explorer on the left side of the application window.

If the server is on a different subnet, the server must be manually discovered. There is no limit to the number of servers that could be discovered by the Client software.

Discovering and Managing Server Connections

1. Open the Find Server dialog box.
    - In the Log In dialog box, click **Find Server...**.
    - In the application window, select **File > Manage Server Connections**. In the Manage Servers dialog box, click **Find Server...**

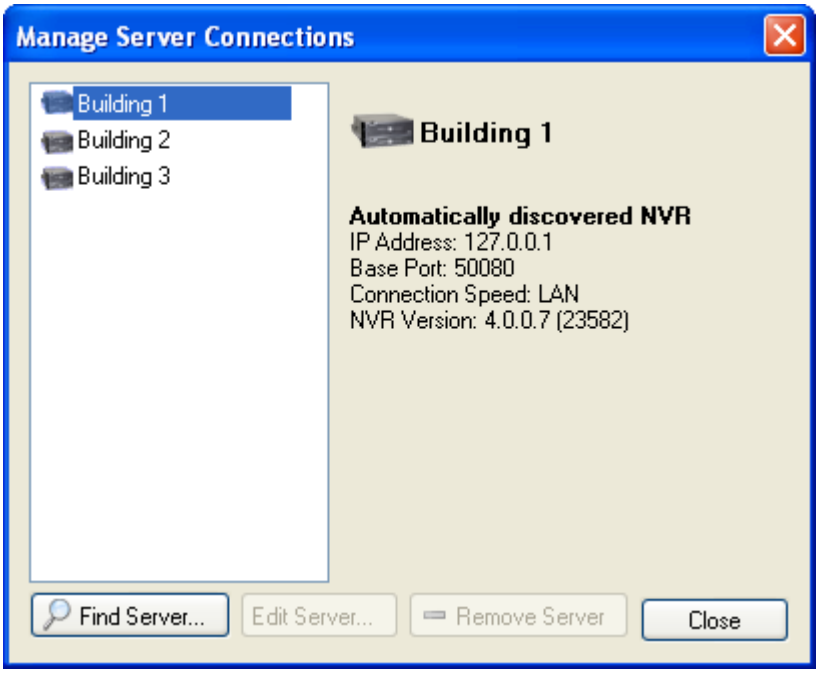


Figure A. Manage Server Connections dialog box

2. In the Find Server dialog box, enter the **Hostname/IP Address**, the **Base Port**, and the **Connection Speed** of the server you want to discover.

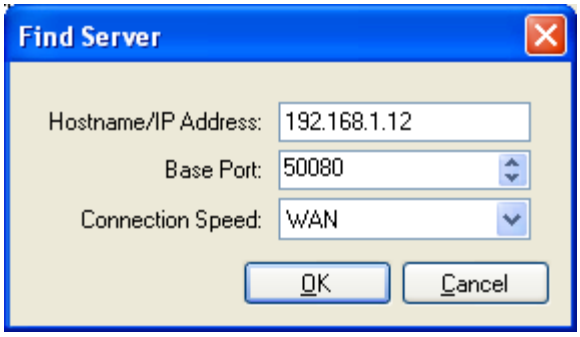


Figure B. Find Server dialog box

The base port is 50080 by default. You can change the base port number in the Avigilon Control Center Admin Tool. See the *Avigilon Control Center Server User Guide* for more information.

> **Tip:** Set the **Connection Speed** to WAN if you are on a low bandwidth network (i.e. internet or wireless network), and select LAN if you are on a high bandwidth connection (i.e. office or home network). This enables the Avigilon Control Center to better manage your bandwidth and image rate.

3. Click **OK.**

If the server is found, the server will appear in the Manage Server Connections dialog box.

If the server is not found, ensure the network settings are configured correctly, the firewall is not blocking the application, and the Avigilon Control Center Server software is running on the server, then try again.

Logging Into and Out of Servers

To access your Avigilon High Definition Surveillance System through the Client software, you must log in to the servers running the Avigilon Control Center Server software. Whenever the Client software detects a server with the Server software installed, you are prompted to log in.

The default administrator access uses *administrator* as the username and no password. To maintain the security of the administrator account, it is recommended that your system administrator immediately create a password for this account after the first login. Your system administrator can then create user accounts for other users.

If the Client software does not detect any servers, click **Find Server...** and enter the server IP address in the dialog box. See Locating Servers for more information.

Logging In

Be aware that the number of servers you can log into at one time is determined by the type of server you can access. Standard edition servers only allow you to be logged into three servers simultaneously, while Enterprise edition servers allow you to be logged into an unlimited number of servers.

Note: You cannot access Standard edition servers and Enterprise edition servers at the same time.

1. Open the Log In dialog box. The Log In dialog box automatically appears when a server is detected by the Client software.

   To manually access the Log In dialog box, perform one of the following:

   - From the **File** menu, select **Log In** to log in to all available servers
   - In the System Explorer, right-click a server and select **Log In**.

2. In the Log In dialog box, select a specific server or select **All Servers** from the **Log in to** drop down list.

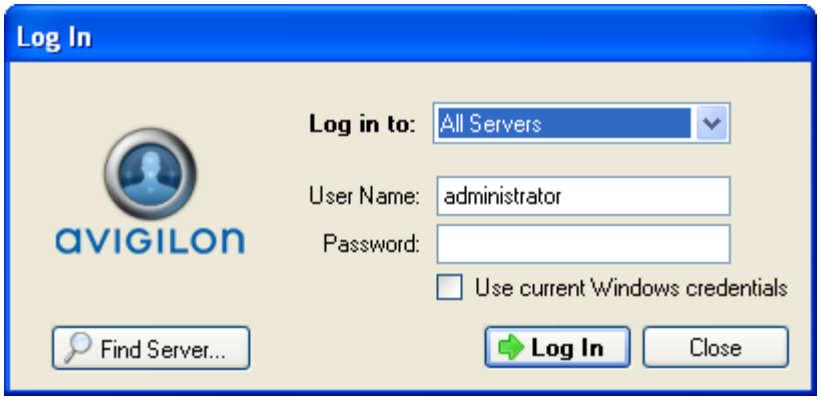


Figure A. Log In dialog box

   Tip: If you accessed the Log In dialog box from a specific server, you will not have the option of logging into All Servers.

   If the server you want to log into is not shown, click **Find Server...** to attempt to locate the server.

3. Enter your **User Name** and **Password**, or select the **Use current Windows credentials** check box if your system administrator has imported your Windows account information into the server.

4. Click **Log In**.

After logging in the first time, you can configure automatic login from the client Setup dialog box. See General for more information.

Logging Out

You can log out of one or all servers at any time in the Client software.

To	Do this
Log out of an individual server	1. Right-click the server in the System Explorer and select **Log Out**.
Log out of all servers	1. Select **File > Log out**. 2. When the Log Out dialog box appears, click **Yes**.

Navigating the Application

Once you log in, the Avigilon Control Center Client application window is where you setup your surveillance system, monitor video, and view, search, and export recorded video.

Note: Some features are not displayed if the server does not have the required license, or if you do not have the user permissions to access the feature.

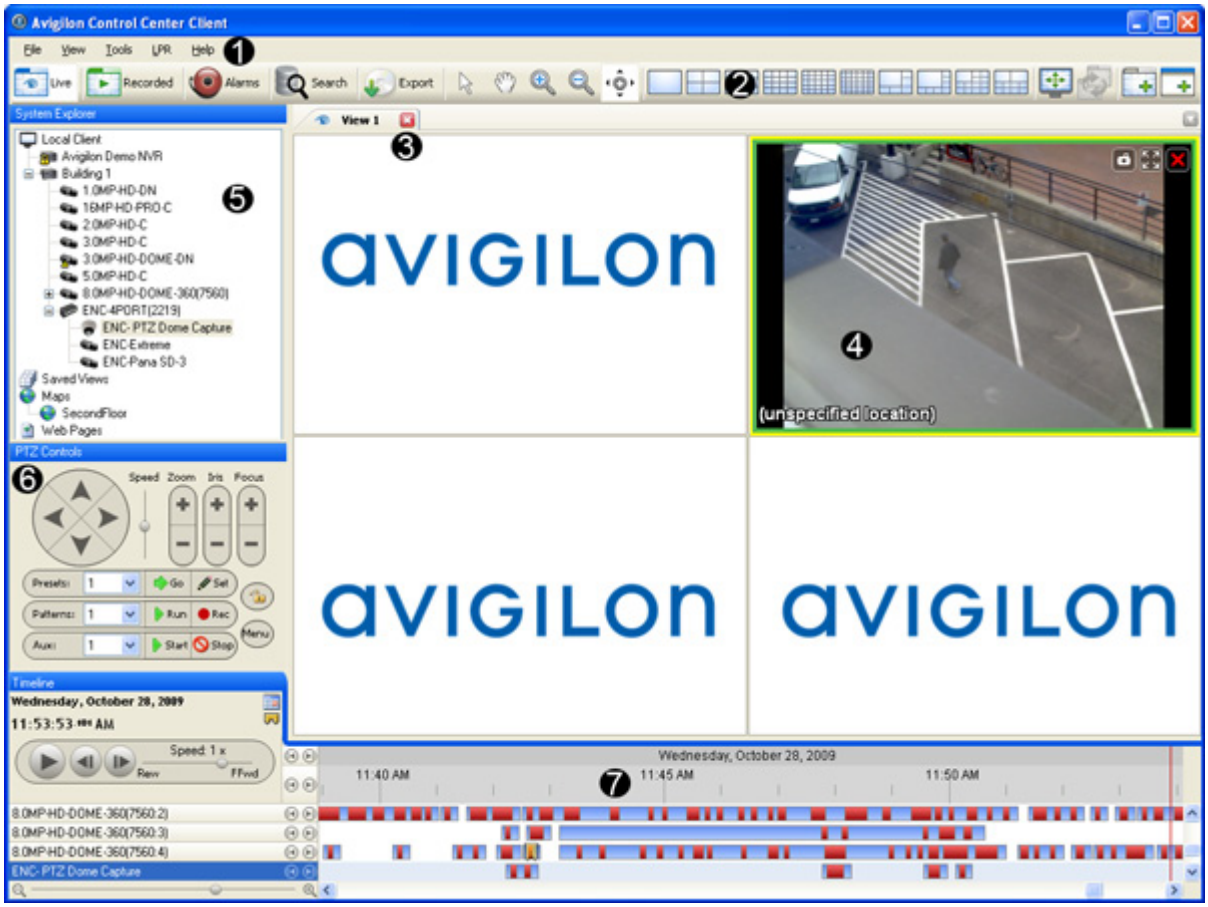


Figure A. Avigilon Control Center Client application window.

	Area	Description
	Workspace	The right pane where the feature tabs appear.
1	Menu bar	A standard Windows application menu that provides access to application features not available on the Toolbar.
2	Toolbar	Provides quick access to commonly used tools. If any buttons are missing from your toolbar, click the small down arrow on the right-edge of the toolbar to display the hidden buttons.
3	View	Provides a way to organize image panels. You can have multiple Views open at once. This is the most common tab in the Workspace.
4	Image panel	Displays live or recorded video from a single camera.
5	System Explorer	Displays surveillance system components such as servers,

		cameras, views, and maps.
6	PTZ Controls	Provides a way to control pan and tilt and zoom (PTZ) cameras.
7	Timeline	Displays the timeline for a recorded video, and contains color-coded events. This tool allows you to select a date and time for playback, and controls the playback rate. **Note:** The Timeline only appears when displaying recorded video.

Viewing Live and Recorded Video

Live and recorded video are displayed in Views. A View is a tab composed of image panels. Views allow you to organize how video is monitored, while image panels allow you to control the video image display quality and other features that are directly related to the video. To customize the way video is displayed, refer to the *Video* section of this guide.

Note: Some features are not displayed if the server does not have the required license, or if you do not have the user permissions to access the feature.

Tip: You can choose to simultaneously watch live video in some panels and recorded video in other panels, or only view one type of video per View.

1. Drag a camera from the System Explorer pane to an empty image panel in the View.

   The video from the camera is displayed. By default, live video is displayed when you first add a camera to an image panel.

2. To switch the View between live and recorded video, perform one of the following:

   - Select **View > Live** or **Recorded**.
   - On the toolbar, select either 

or 

.

3. To switch individual panels between live and recorded, right-click the image panel and select either **Live** or **Recorded**.

Image panels displaying live video appear with a blue border, while image panels displaying recorded video appear with a green border.

Setup

The default settings configured in the Avigilon Control Center Client software allows you to start working with the application immediately after installation.

If you have special requirements, refer to the following sections to configure your settings:

Note: Some features are not displayed if the server does not have the required license, or if you do not have the user permissions to access the feature.

Connect/Disconnect Cameras

You can connect and disconnect cameras to servers using the Connect/Disconnect Cameras dialog box.

A camera's connection status is indicated by the status icon beside the camera name in the System Explorer.

Icon	Definition
 **Camera Connected**	The camera is connected to the server.
 **Camera Connection Error**	The camera cannot connect to a server. This may be because the camera is no longer on the network or there is a network conflict
 **Camera Disconnected**	The camera is disconnected from the server but there is recorded video for the camera remaining on the server.
No icon	The camera is disconnected from the server and there is no recorded video remaining on the server.

Discovering a Camera

When cameras are connected to the Avigilon HD Surveillance System, they should be automatically discovered by the Avigilon Control Center Client software.

If a camera is not automatically discovered, you can attempt to manually discover the camera on the network.

1. From the **Tools** menu, select **Connect/Disconnect Cameras**.

   In the Connect/Disconnect Cameras window, all Avigilon cameras located on the same subnet as the computer running the Avigilon Control Center Server software are automatically detected and appear in the Discovered Cameras area.

If the camera you want to connect to is on a different subnet, or is manufactured by a third party, perform the following:

1. At the top of the Connect/Disconnect Cameras dialog box, click **Find Camera...**.
2. In the Find Camera dialog box, complete the following fields:

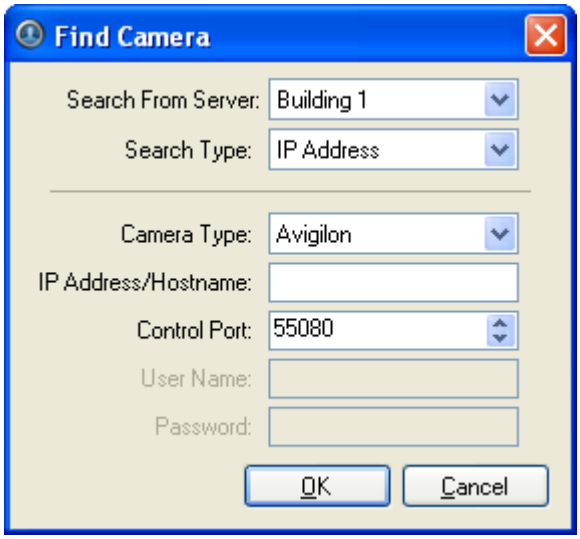


Figure A. Find Camera dialog box: IP Address

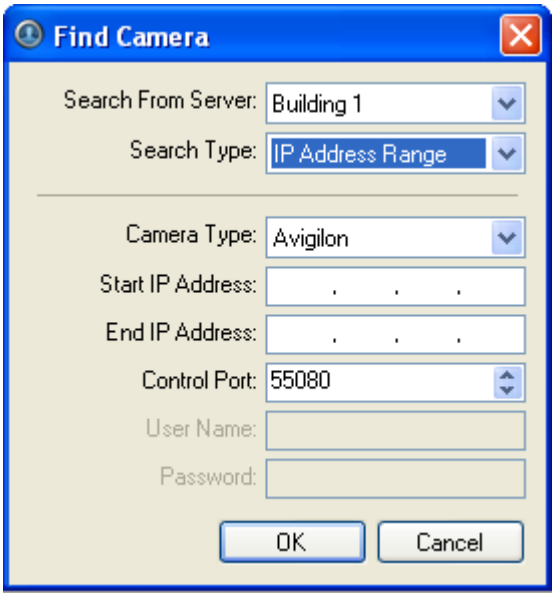


Figure B. Find Camera dialog box: IP Address Range

- **Search From Server:** select the server that you want the camera to connect to.
- **Search Type:** select a search type.
- **Camera Type:** select the camera's brand name.

  Tip: Select ONVIF to discover cameras that are ONVIF complaint.

- **IP Address/Hostname:** (For IP Address search only) enter the camera's IP address or hostname. The camera and server's gateway IP address must be set correctly for the camera to be found.
- **Start IP Address** and **End IP Address:** (For IP Address Range search only) enter the start and end IP addresses. Only addresses in that range will be searched for the selected camera type.
- **Control Port:** enter the camera control port number.
- Provide the **User Name** and **Password** for the camera if required by the camera manufacturer .

3. Click **OK**.

If the camera is discovered, it will appear in the Discovered Cameras area.

Connecting a Camera to a Server

Once the camera has been discovered on the network, it can be connected to the server.

1. From the **Tools** menu, select **Connect/Disconnect Cameras**. The Connect/Discover Cameras dialog box appears.

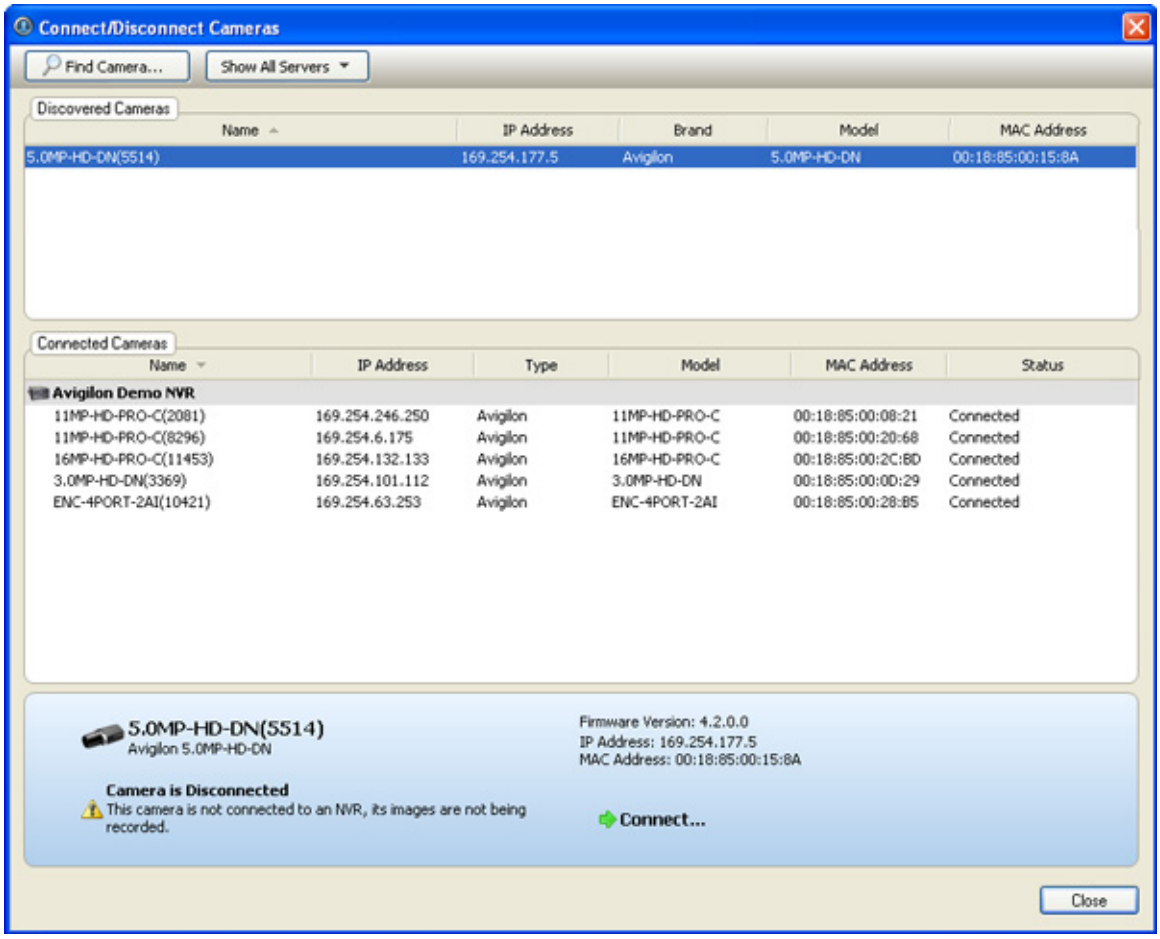


Figure A. Connect/Disconnect Cameras dialog box

2. In the Discovered Cameras area, select a camera then click **Connect...**.

   Tip: You can also drag the camera to a server on the Connected Cameras list, then you can skip the following step.

3. In the Connect Camera dialog box, select the server you want the camera to connect to.

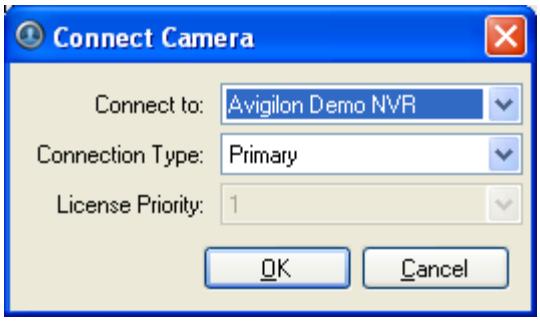


Figure B. Connect Camera dialog box

4. Click **OK**.

5. If the camera is password protected, the Camera Authentication dialog box appears. Enter the camera's username and password, then click **OK**.
6. Close the Connect/Disconnect Camera dialog box.

Editing the Camera Connection to the Server

1. From the **Tools** menu, select **Connect/Disconnect Cameras**.
2. In the Connect/Disconnect Cameras dialog box, select the camera connection you want to edit from the Connected Cameras list.
3. Click **Edit** and make the required changes to the Connection Settings dialog box.
4. Click **OK**.

Disconnecting a Camera from a Server

1. From the **Tools** menu, select **Connect/Disconnect Cameras**.
2. In the Connect/Disconnect Cameras dialog box, select the camera you want to disconnect from the Connected Cameras list.
3. To disconnect the camera from the server perform, one of the following:
    - Click **Disconnect**.
      The camera is disconnected from the server and moved to the Discovered Cameras list.
    - Drag the camera into the Discovered Cameras list.

Server Setup

The Avigilon Control Center Server is setup by default to only record image data when events occur. In the Client software, you can use the server Setup dialog box to configure the server to record continuously, or schedule cameras to only record at specific times.

The server Setup dialog box also allows you to set user access permissions, configure email notifications, and add POS transaction engines.

Note: Some features are not displayed if the server does not have the required license, or if you do not have the user permissions to access the feature.

Accessing the Server Setup

Perform one of the following steps to open the server Setup dialog box:

- Select **Tools > Setup...** then select the server you want to setup from the left pane.
- In the System Explorer pane, right-click the server and select **Setup**.

Note: Some features are not displayed if the server does not have the required license, or if you do not have the user permissions to access the feature.

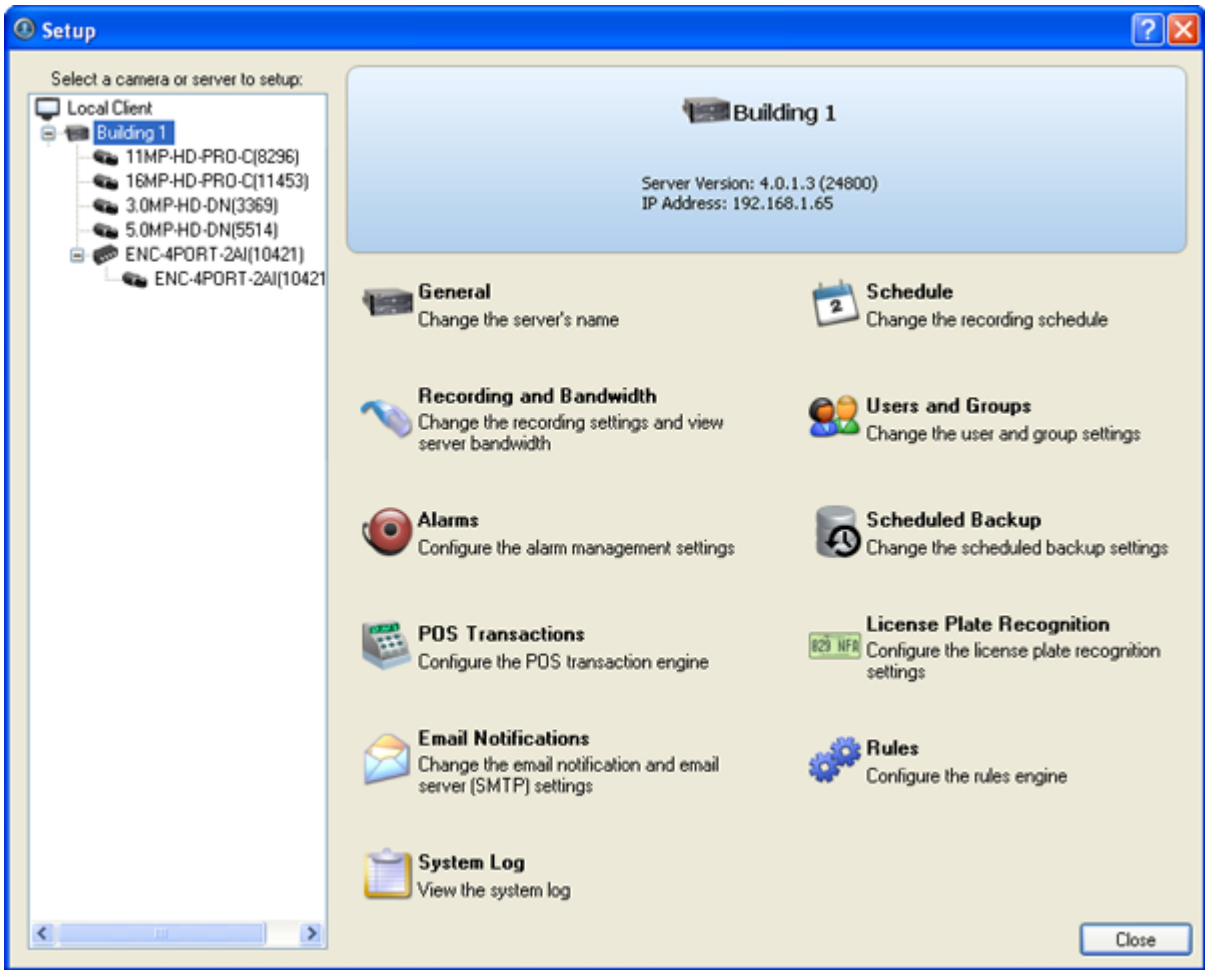


Figure A. Server Setup dialog box

General

Use the General dialog box to customize the identity of each server.

Changing the Server's Name

The default name for the server may not be useful for your purposes. Use the General dialog box to change the server's name to something more appropriate to your needs.

1. Right-click a server in the System Explorer and select **Setup** to open the server Setup dialog box. See Accessing the Server Setup for more information.
2. Click **General**.
3. In the General dialog box, enter a new server name.

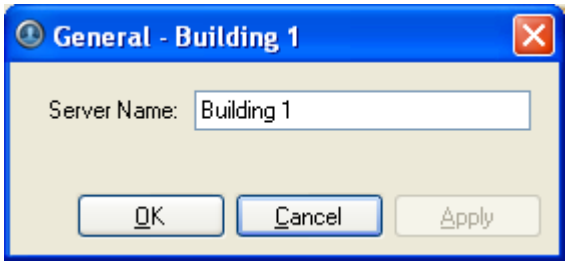


Figure A. General dialog box

4. Click **OK**.

Schedule

Use the Schedule dialog box to customize the recording schedule for the cameras connected to the server. All Avigilon High Definition Surveillance Systems are set to record whenever motion or events occur by default .

Once the recording schedule is set, camera recordings are made automatically.

Using Templates to Modify the Recording Schedule

You can modify the default recording schedule template to suit your needs or you can add new templates as required. For example, you can create one recording schedule template for the weekdays and another for the weekend.

Adding a Template

1. Right-click a server in the System Explorer and select **Setup** to open the server Setup dialog box. See Accessing the Server Setup for more information.
2. Click **Schedule**.
3. In the Schedule dialog box, click **Add Template** in the Templates pane.

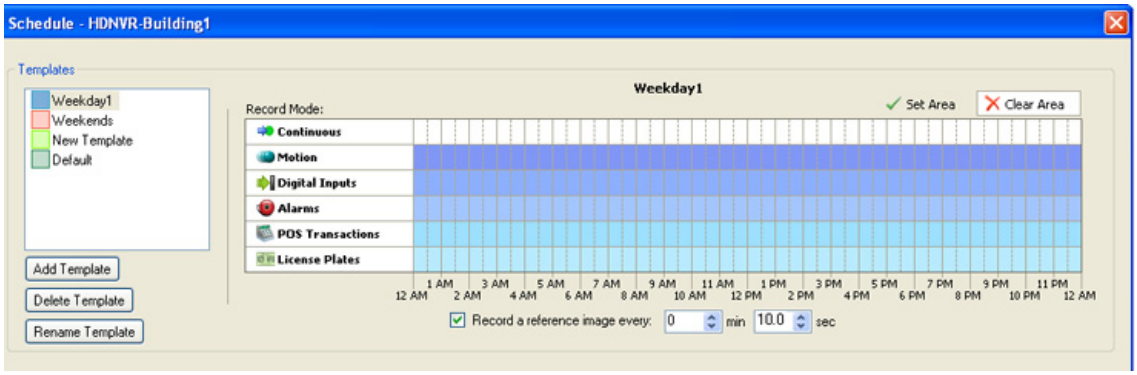


Figure A. Schedule dialog box

4. Enter a name for the template.
5. Click the **Set Area** button then click or drag the cursor across the **Record Mode** timeline to enable cameras to record during the specified hours for the highlighted events.

Record Mode	Definition
Continuous	Record image data continuously. Enable the continuous mode to record all image data.
Motion	Record image data only when motion is detected.
Digital Input	Record image data only when a digital input is activated.
POS Transactions	Record image data only when point of sale (POS) transactions are made.

6. To disable recording in parts of the template, click the **Clear Area** button then click or drag the cursor across the timeline until the required Record Modes and time ranges are blank.
7. If cameras are not recording in Continuous mode for the entire template period, you can configure cameras to record reference images between events in the recording schedule. Select the **Record a reference image every:** check box, and specify the time range between each reference image.

Editing and Deleting a Template

1. Right-click a server in the System Explorer and select **Setup** to open the server Setup dialog box. See Accessing the Server Setup for more information.
2. Click **Schedule**.
3. In the Schedule dialog box, select a template from the Templates pane and perform one of the following:
   - To edit a template, modify the schedule.
   - To rename a template, click **Rename Template** and enter a new name.

- To delete a template, click **Delete Template**.

4. Click **OK**.

Setting Up a Weekly Recording Schedule

You can setup a week's recording schedule by applying different templates to cameras for specific days of the week.

1. Right-click a server in the System Explorer and select **Setup** to open the server Setup dialog box. See Accessing the Server Setup for more information.
2. Click **Schedule**.
3. In the Schedule dialog box, select a template from the Templates pane.
4. In the Default Week area, select the days of the week to apply the template schedule for each camera.

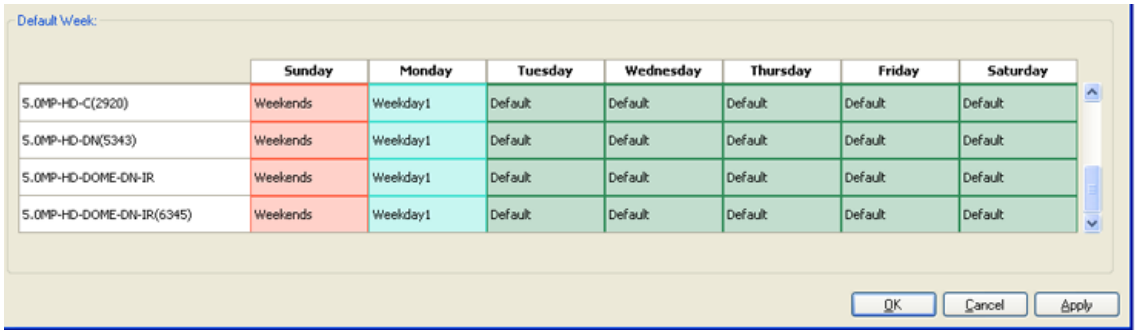


Figure A. Schedule dialog box: Default Week

5. Click **OK**.

Recording and Bandwidth

You can use the Recording and Bandwidth dialog box to change the server recording settings, and view the bandwidth used by each camera that is connected to the server.

Changing Recording Settings

1. Right-click a server in the System Explorer and select **Setup** to open the server Setup dialog box. See Accessing the Server Setup for more information.
2. Click **Recording and Bandwidth**. The Recording and Bandwidth dialog box appears.

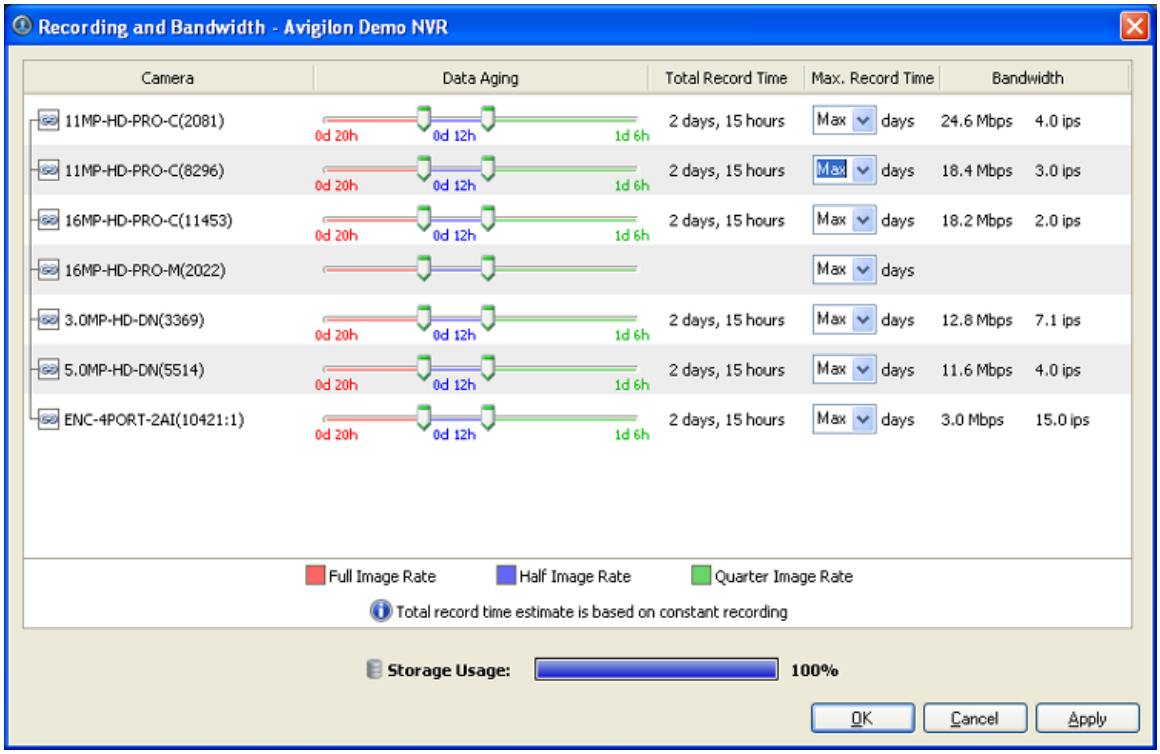


Figure A. Recording and Bandwidth dialog box

3. In the Data Aging area for each camera, move the sliders to adjust the amount of time video is stored at full, half, and quarter image rate.

   Note: Data Aging is only enabled for cameras using JPEG 2000 or JPEG compression.

   The settings for all linked cameras are changed at the same time. To control the settings for a single camera, break the camera's link by clicking the **Link** icon to the left of the camera's name and make the necessary adjustments.

4. In the **Max. Record Time** field, manually enter a maximum record time or select one of the options from the drop down list for each camera.

   If the auto-generated Total Record Time is shorter than the Max. Record Time setting, it may be an indication that your actual record time will be shorter than the Max. Record Time setting.

5. Click **OK**.

Users and Groups

When users are added to the Avigilon system, they are assigned to an access group that defines their access permissions on a server. Create and manage users and groups in the Users and Groups dialog box.

Adding a User

You can add users and manage their access permissions by assigning users to specific access groups.

1. Right-click a server in the System Explorer and select **Setup** to open the server Setup dialog box. See Accessing the Server Setup for more information.
2. Click **Users and Groups**.
3. In the User and Groups dialog box, click **Add User**.

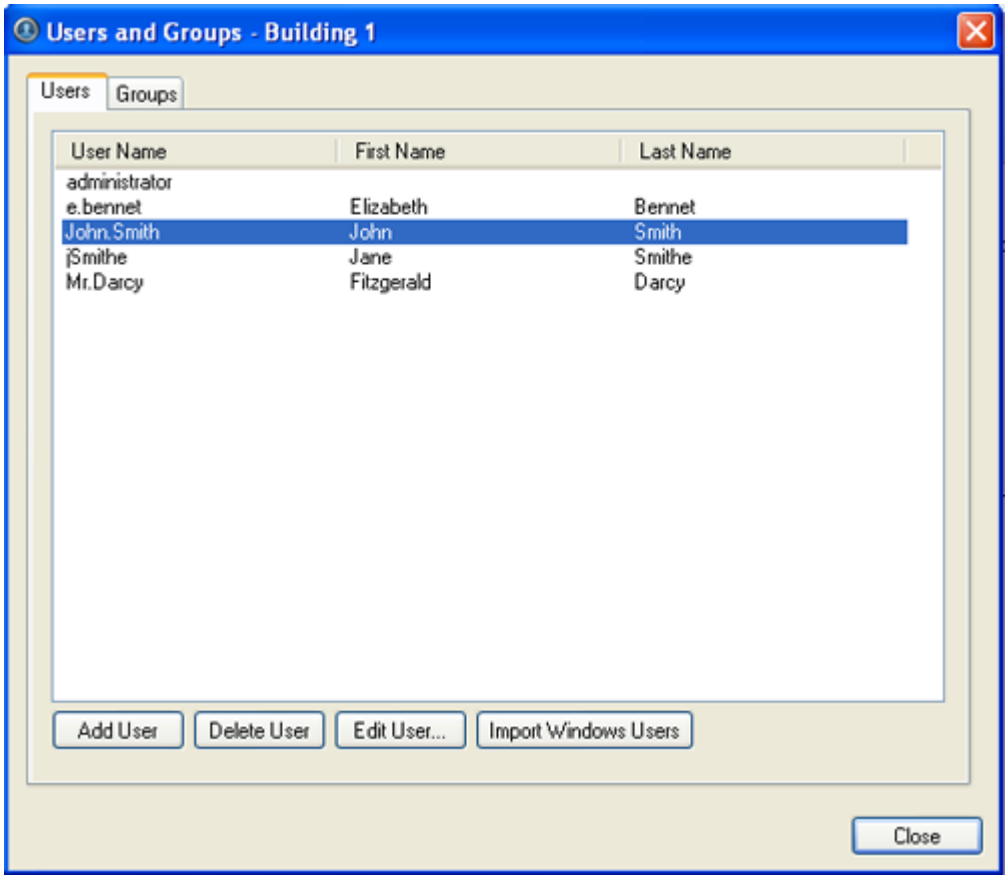


Figure A. User and Groups dialog box

4. When the Add User dialog box appears, complete the User Information area.

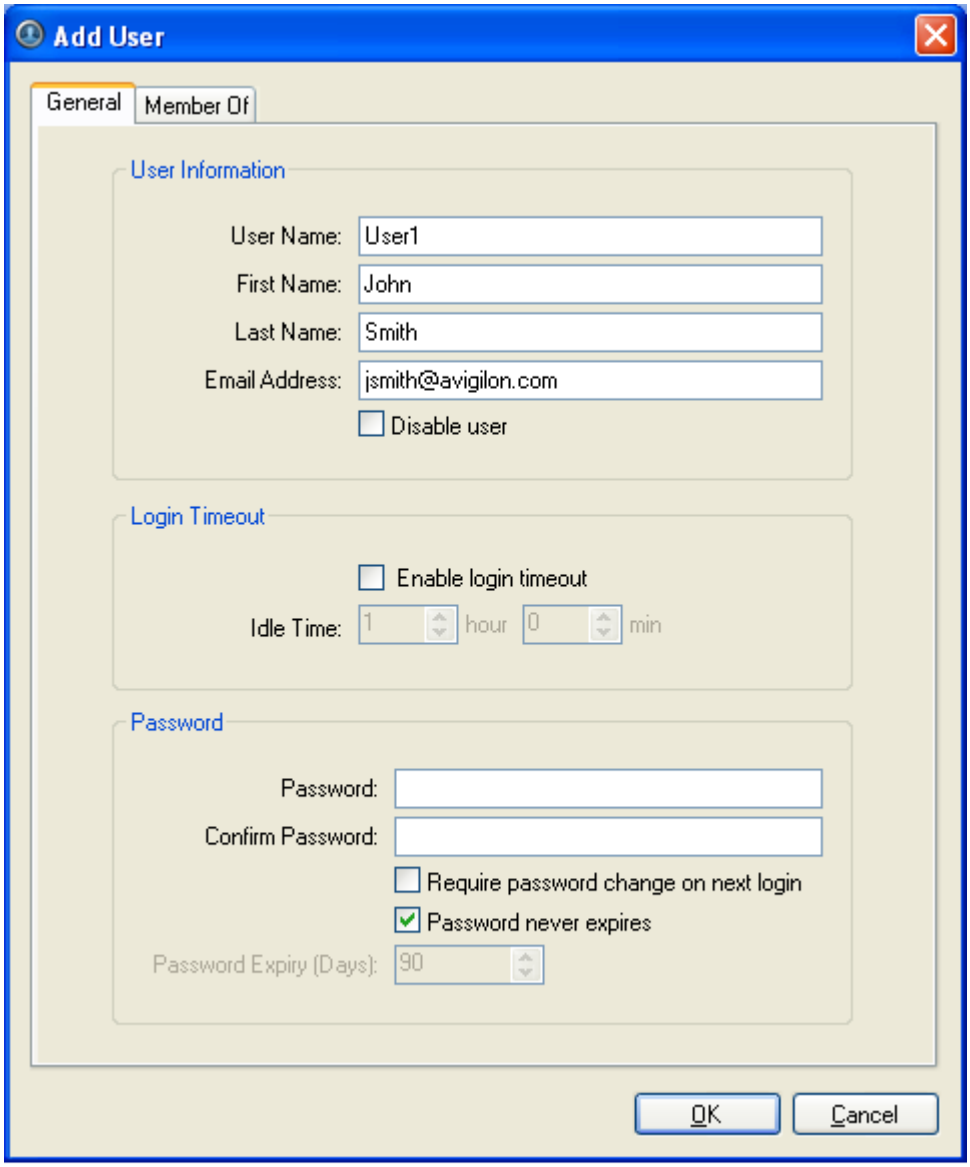


Figure B. Add User dialog box, General tab

5. If you don't want to make this user active yet, select the **Disable user** check box.
6. In the Login Timeout area, select the **Enable login timeout** check box to allow the application to log out the user after the application has been idle for the specified amount of time.
7. In the Password area, complete the following fields:
   - **Password:** enter a password for the user.
   - **Confirm Password:** re-enter the password.
   - **Require password change on next login:** select this check box if you want the user to personalize the password after their first login.

- **Password Expiry (Days):** specify the number of days before the password must be changed. This field is not required if the password never expires.
- **Password never expires:** select this check box if the password does not need to be changed.

8. Select the Member Of tab and assign the user to one or more access groups by selecting the appropriate check box in the Groups list.

   The other two columns display the permissions associated with the selected Groups.

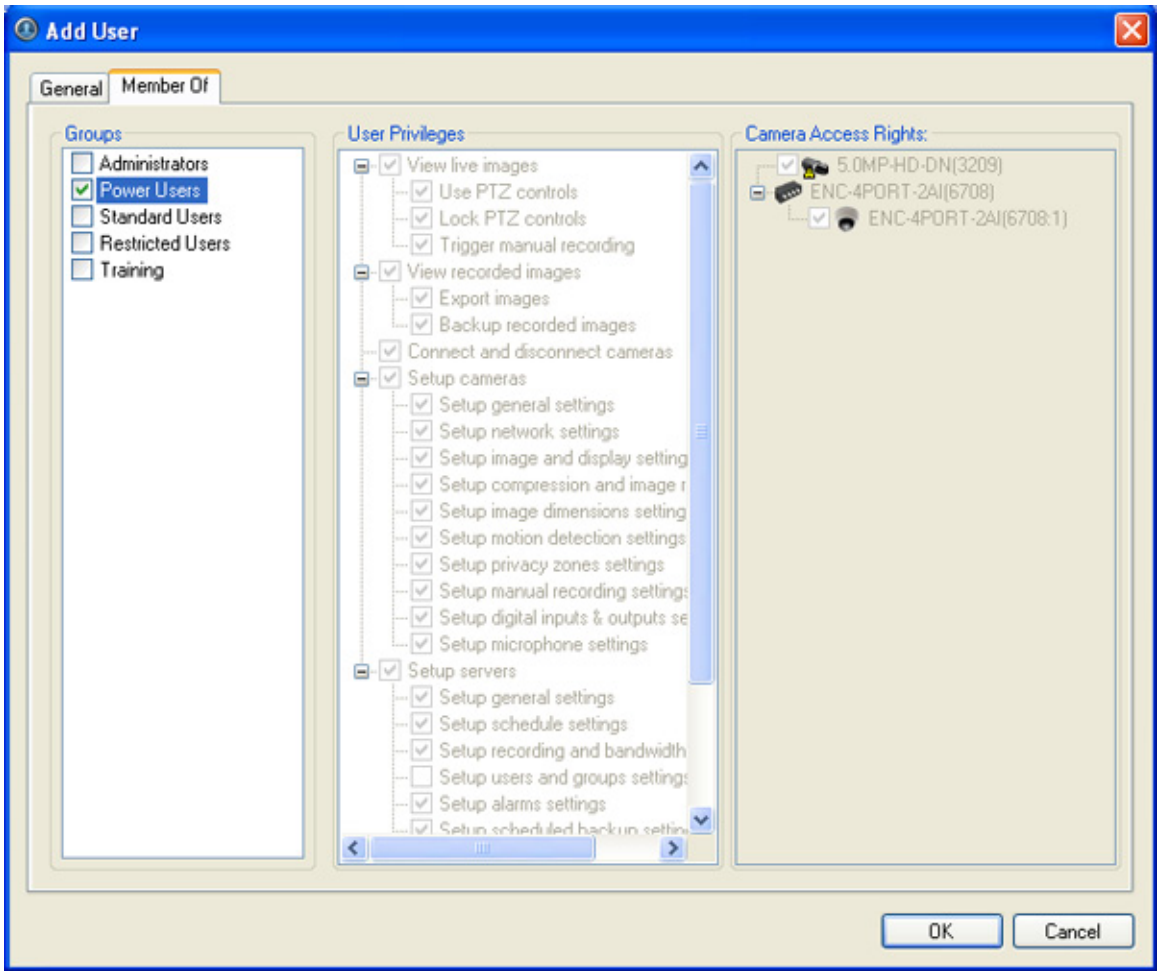


Figure C. Add User dialog box, Member Of tab

9. Click **OK**. The user is added to the server.

Editing and Deleting a User

You can edit the details of an existing user, or delete the user account that is no longer required.

Note: If a user has access to more than one server, the user needs to be removed from each server individually.

1. Right-click a server in the System Explorer and select **Setup** to open the server Setup dialog box. See Accessing the Server Setup for more information.
2. Click **Users and Groups**.
3. In the Users and Groups dialog box, select a user and perform one of the following:
    - Click **Edit User** to edit the user's information. Refer to Adding a User or details about the editable options.
    - Click **Delete User** to delete the user.

Importing Windows Users

You can import Windows user accounts on to the server to allow users to log in using their Windows credentials.

1. Right-click a server in the System Explorer and select **Setup** to open the server Setup dialog box. See Accessing the Server Setup for more information.
2. Click **Users and Groups**.
3. In the Users and Groups dialog box, click **Import Windows Users**.
4. In the Select Users or Groups dialog box, locate the Windows user you wish to add by performing one of the following:
    - In the Select Users or Groups dialog box, enter the name of a Windows user or group in the **Enter the object names to select field** and click **OK**.
    - In the Select Users or Groups dialog box, click the **Advanced** button and search for the users or groups to import.

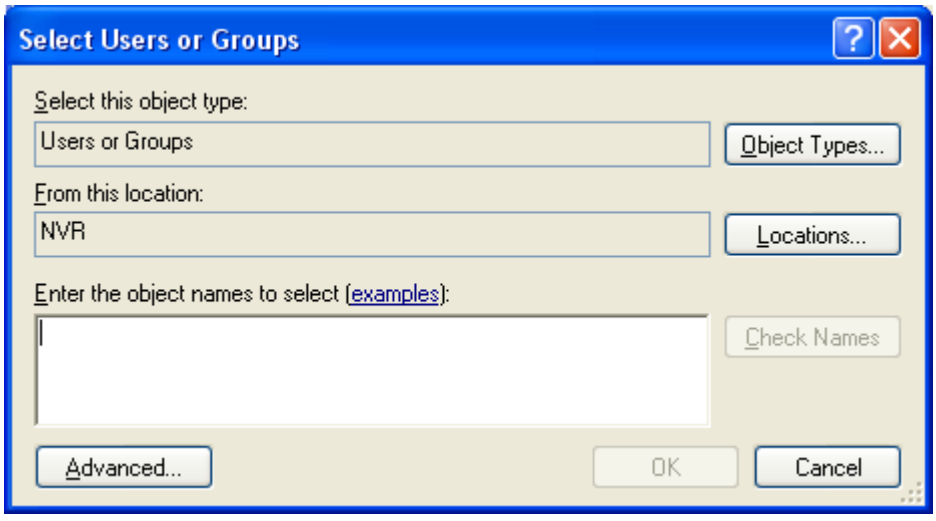


Figure A. Select Users or Groups dialog box

5. In the Import Windows Users dialog box, select the users you wish to import and assign the users to an access group by selecting the appropriate **Groups** check box.

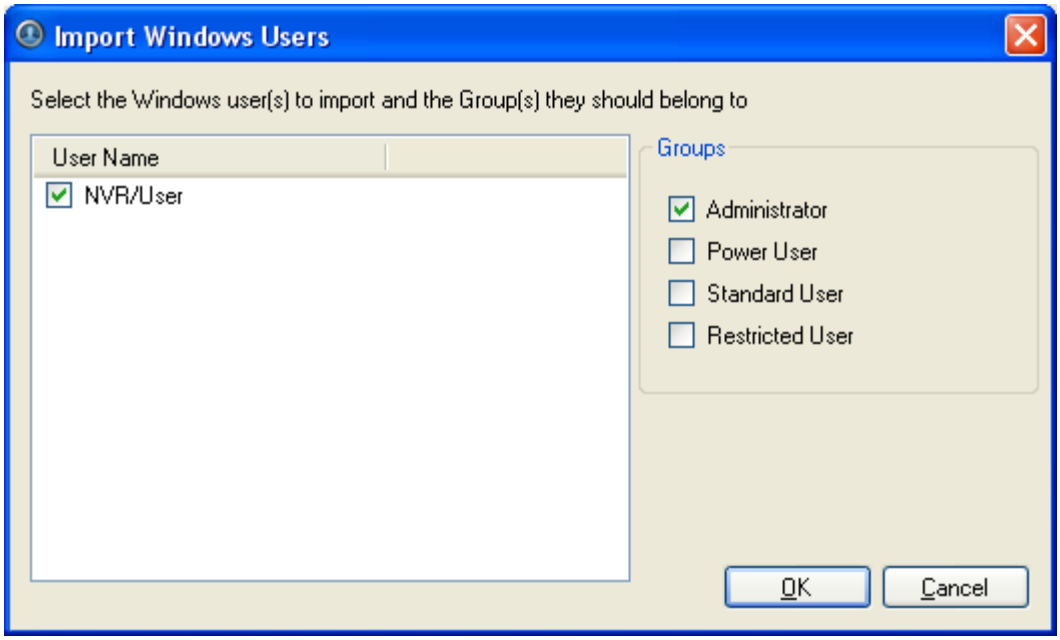


Figure B. Import Windows Users dialog box

Note: If you are importing multiple Windows users, be aware that you are assigning all selected users to the same access group.

6. Click **OK**.

Adding Groups

You can change users' access permissions by changing their access groups. Create new groups to define specific sets of access permissions.

Note: Access permissions for the Administrator group cannot be modified.

1. Right-click a server in the System Explorer and select **Setup** to open the server Setup dialog box. See Accessing the Server Setup for more information.
2. Click **Users and Groups**.
3. In the Users and Groups dialog box, select the Groups tab and click **Add Group**.

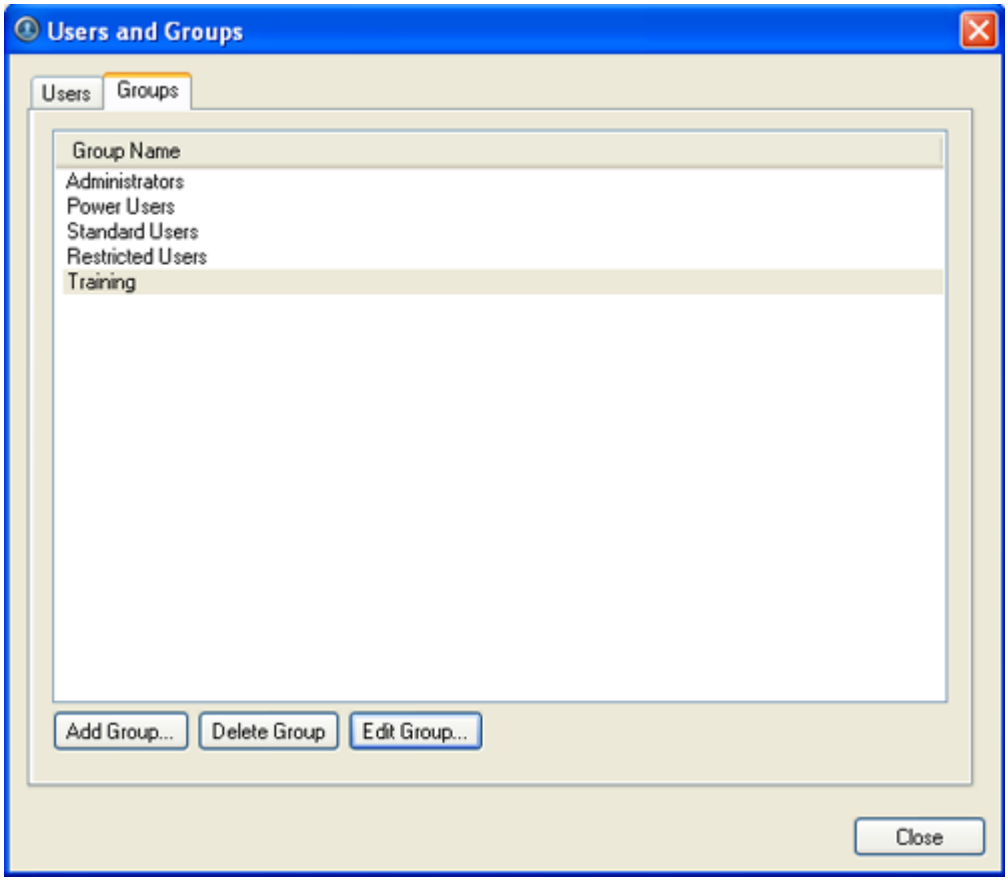


Figure A. User and Groups dialog box

4. In the Add Group dialog box, select a group to use as a template for your new group and click **OK**.

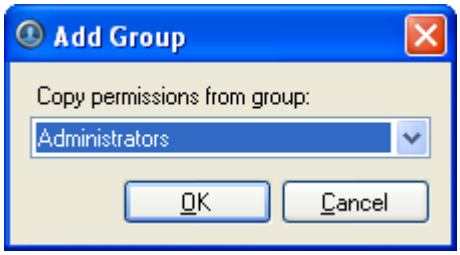


Figure B. Add Group dialog box

5. In the Edit Group dialog box, give the new group a name then select the permissions and camera access rights for the group.

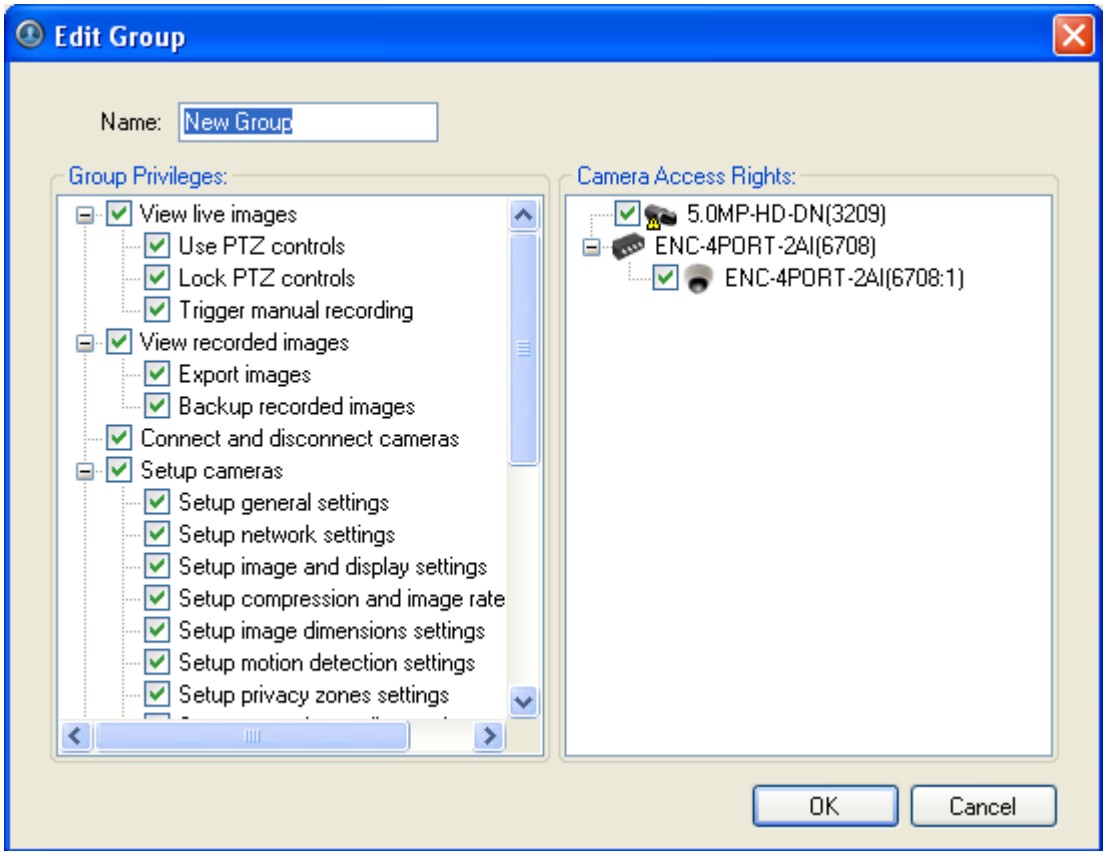


Figure C. Edit Group dialog box

6. Click **OK**.

Editing and Deleting a Group

You can change the access permissions for a set of users by editing their access group.

Note: The Administrators group cannot be edited or deleted.

1. Right-click a server in the System Explorer and select **Setup** to open the server Setup dialog box. See Accessing the Server Setup for more information.
2. Click **Users and Groups** and select the Groups tab.
3. Select a group and perform one of the following:
   - To edit the group, click **Edit Group**. In the Edit Group dialog box, change the permissions and camera access rights as required then click **OK**. Refer to Adding Groups for details about the editable options.
   - To delete the group, click **Delete Group**.

     Note: Default groups cannot be deleted.

POS Transactions

The Point of Sale (POS) Transaction Engine is a licensed feature that records video and raw data from POS transaction sources. POS transaction sources can be added to the Avigilon Control Center System and configured in the Client software.

Adding a POS Transaction Source

1. Right-click a server in the System Explorer and select **Setup** to open the server Setup dialog box. See Accessing the Server Setup for more information.
2. Click **POS Transactions**.
3. In the POS Transactions dialog box, click **Add**.
4. Enter the **Hostname/IP Address** and the **Port** for the POS Transaction Source device. Click **Next**.

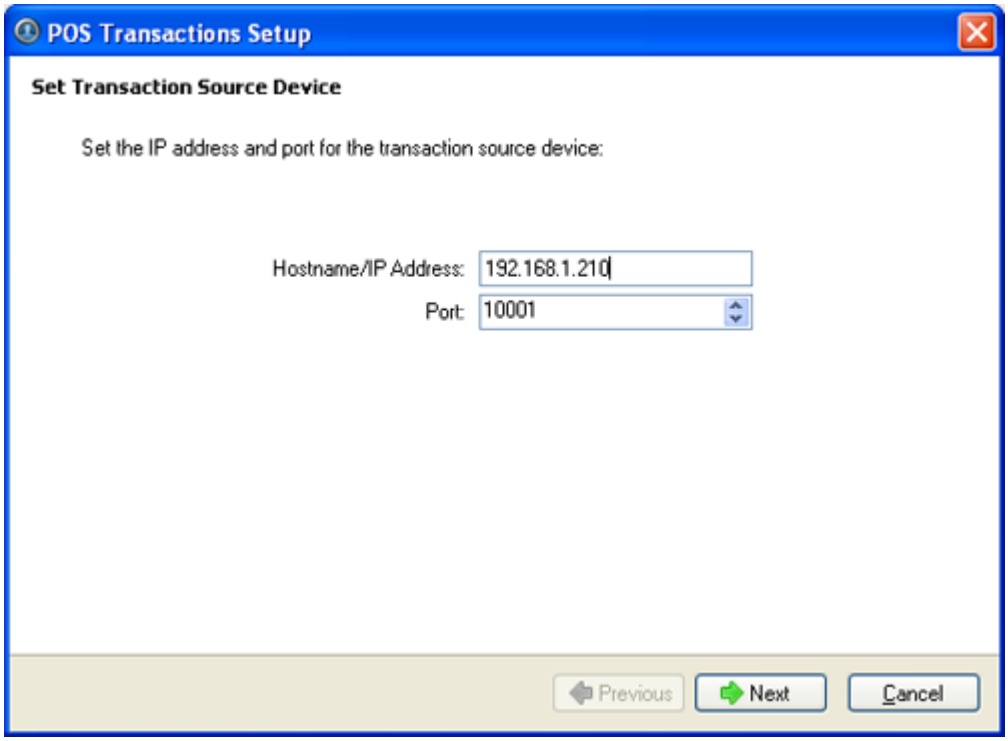


Figure A. Set Transaction Source Device page

5. Select a Transaction Source Data format and click **Next**.

   If the source data format needs to be added, click **Add**. Or, click **Copy From** to create a new data format based on the selected data format. See Adding a Transaction Source Data Format for more information.

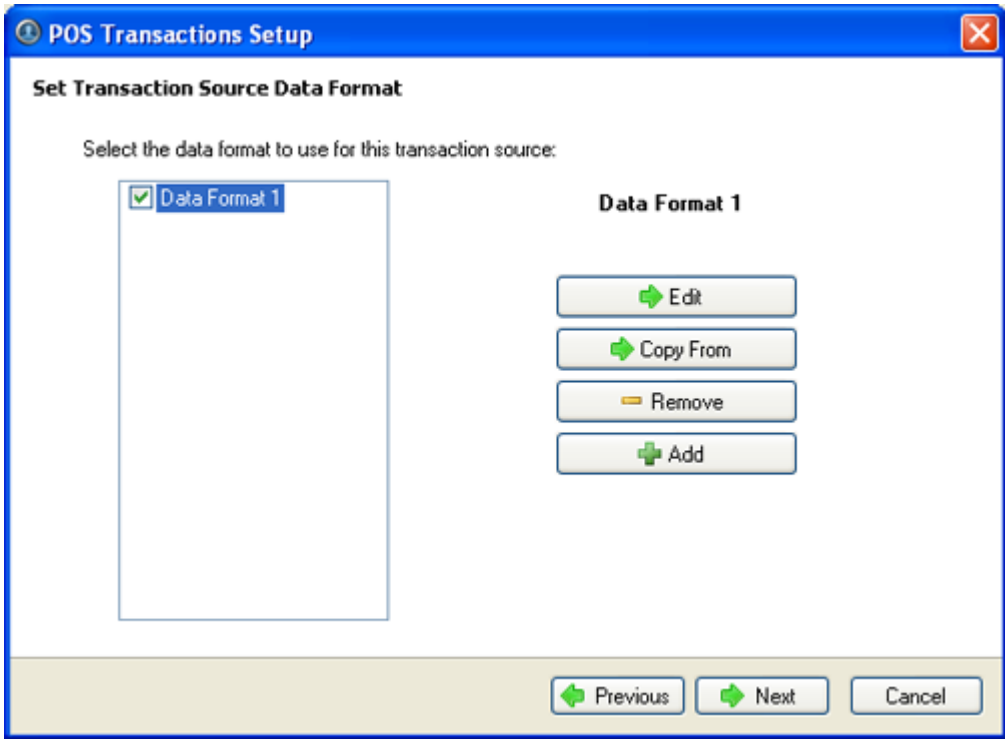


Figure B. Set POS Transaction Source Data Format page

6. On the Set Transaction Exceptions page, select any exceptions that should be monitored for on this transaction source and click **Next**. If no exceptions are required, just click **Next**.

   Click **Add** to add an exception. See Adding a Transaction Exception for more information.

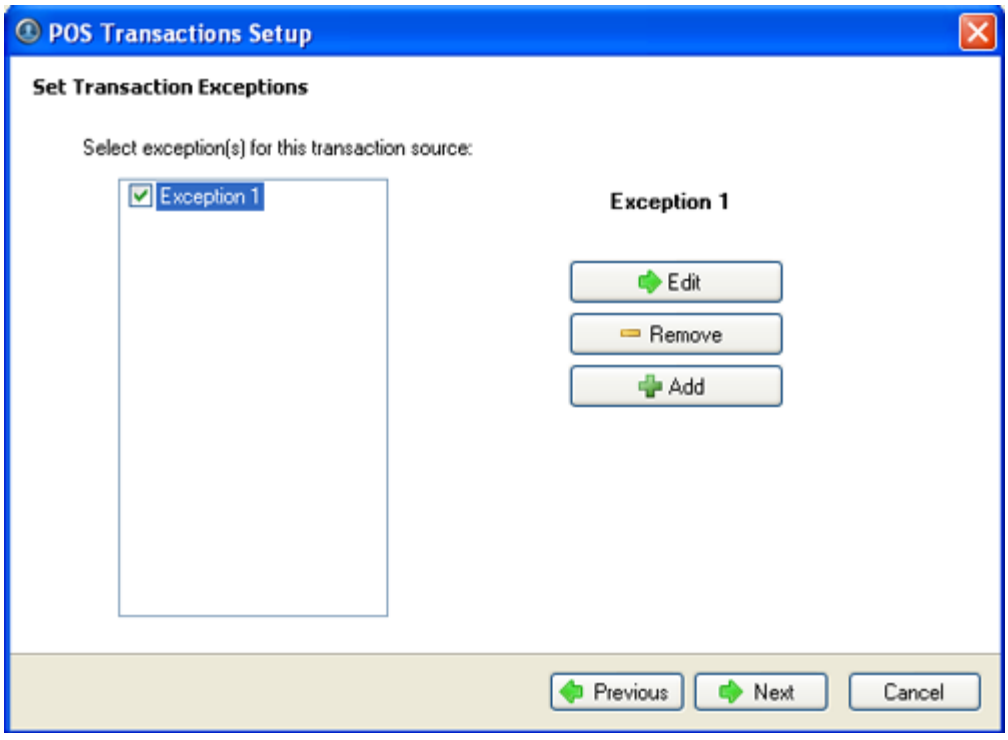


Figure C. Set Transaction Exceptions page

7. Select the cameras to link to the transaction source, and set the pre-transaction record time and post-transaction record time. Click **Next**.

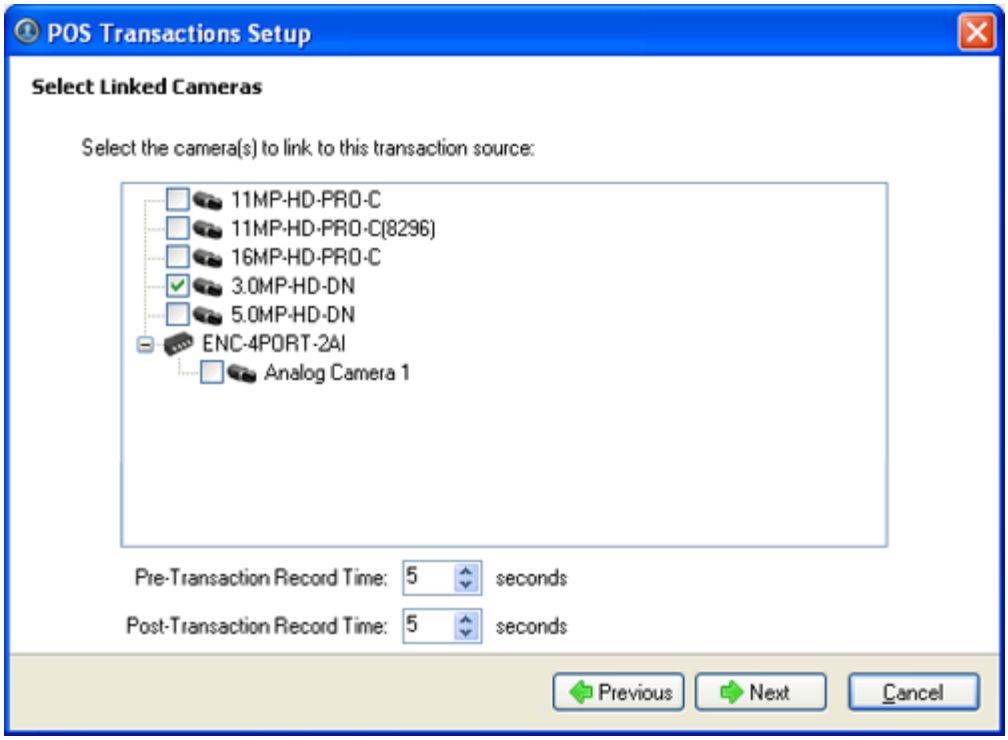


Figure D. Select Linked Cameras page

8. Enter a transaction source name and description, select **Enable transaction source**.

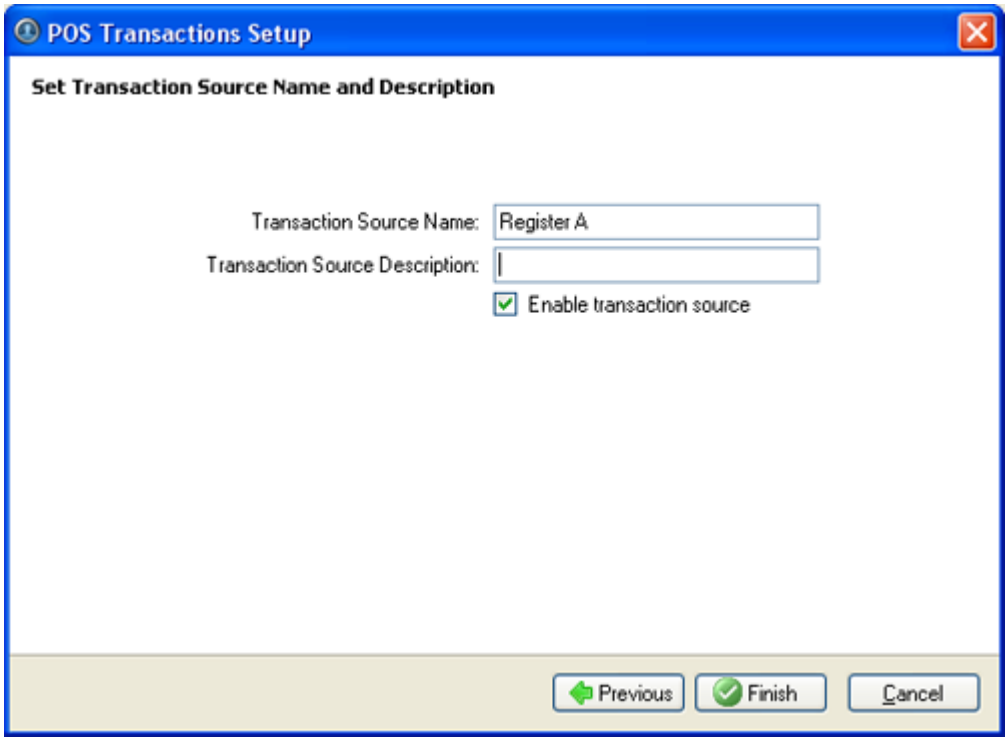


Figure E. Set Transaction Source Name and Description page

9. Click **Finish**.

Adding a Transaction Source Data Format

When you add a new POS transaction source, be aware that the transaction source must have a source data format.

In the POS Transaction Setup wizard, click **Add** when you arrive on the Set Transaction Source Data Format page. When the Configure Data Format dialog box appears, complete the following procedure:

1. In the Properties area, specify the following:

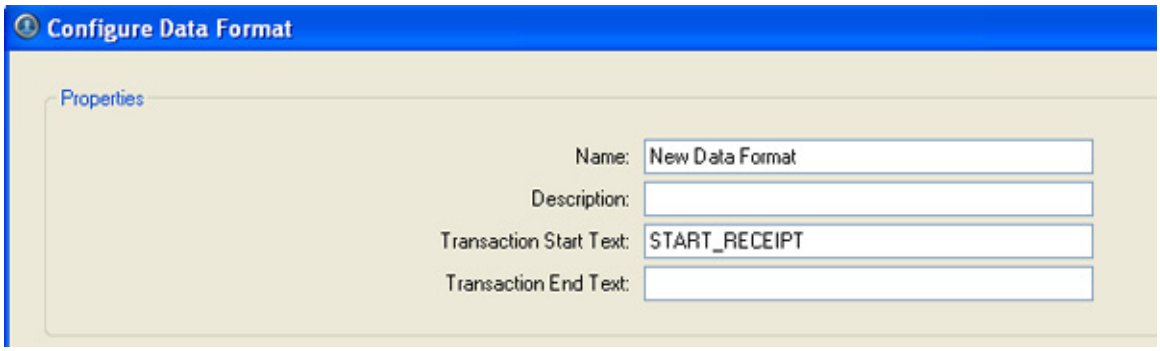


Figure A. Configure Data Format dialog box

- **Name:** enter a name for the data format.

- **Description:** enter a description of the data format if required.
- **Transaction Start Text:** (required) enter the text that identifies the start of each transaction from the POS transaction source.
- **Transaction End Text:** (optional) enter the text that identifies the end of each transaction.

2. The two boxes below show raw and filtered transaction data. Perform any of the following:

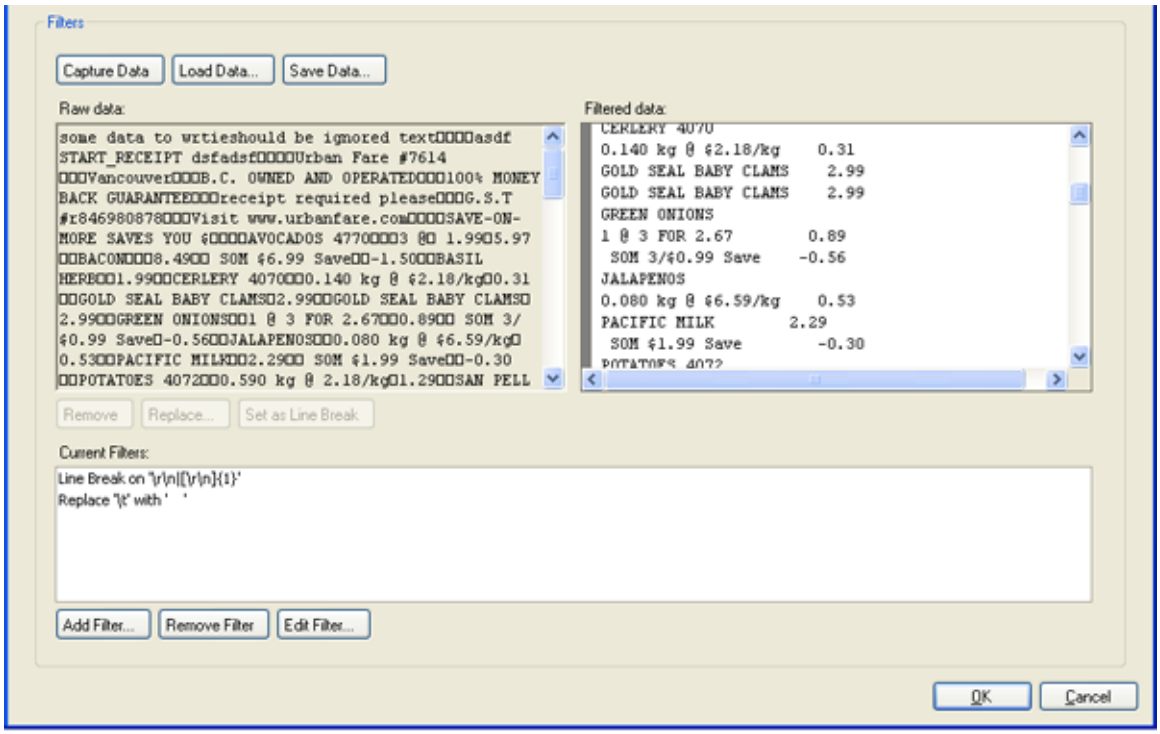


Figure B. Configure Data Format dialog box

- Click **Capture Data** to start capturing a raw transaction data sample.
- Click **Stop Capture** to stop capturing transaction data.
- Click **Load Data** to load raw transaction data from a file.
- Click **Save Data** to save transaction data.

3. (Optional) Click **Add Filter** to create a new filter for the raw transaction data file.

   There are several default filters for line breaks listed in the Current Filters area, if the default filters are sufficient for your needs, skip this step.

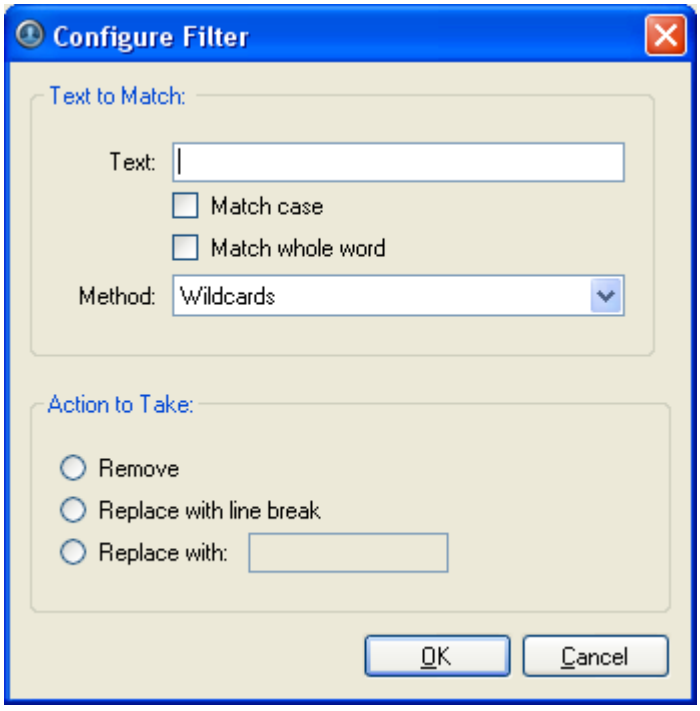


Figure C. Configure Filter dialog box

2.

a. In the **Text** field, enter text for the filter to search for.
b. Select **Match case** and/or **Match whole word** check box to focus the text filter to only find text with the same capitalization or match the text exactly.

c. Select a method from the **Method** drop down list.
d. In the Action to Take area, select which action to take when the filter finds a match to your text criteria.

e. Click **OK**.

3. On the Configure Data Format screen, click **OK** to add the new data format to the data format list.

Adding a Transaction Exception

In the POS Transaction Setup wizard, click **Add** when you arrive on the Set Transaction Exceptions page. When the Configure Exception dialog box appears, complete the following procedure:

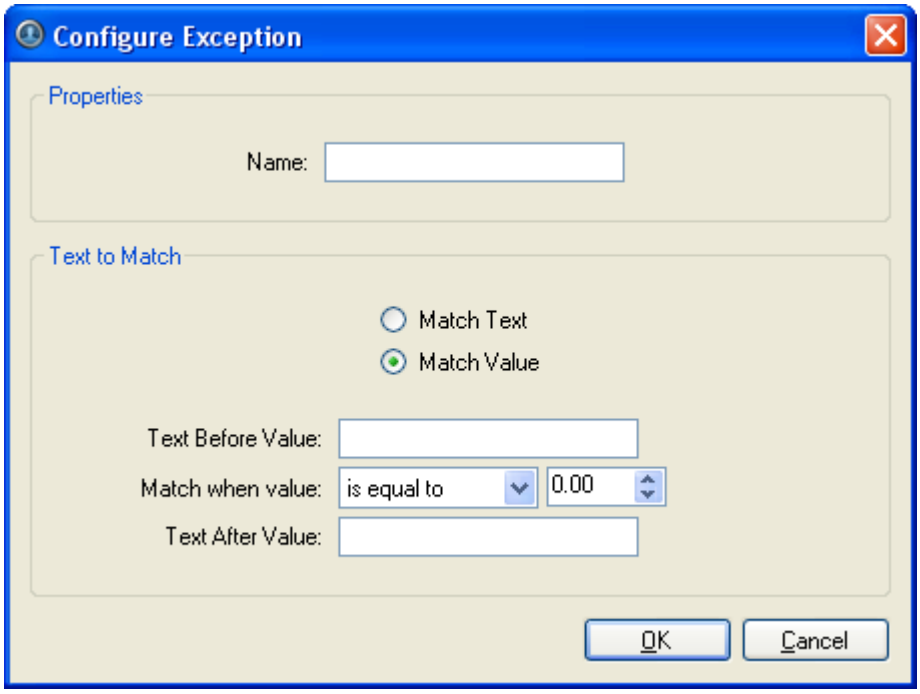


Figure A. Configure Exception dialog box

1. Enter a name.
2. Select one of the Text to Match options:

Select	And do this...
Match Text	Enter text for the exception to search for. The exception will search for instances that are an exact match to the text entered in the **Text to Match** field.
Match Value	Enter the value that triggers the exception, and enter the text that may appear around the value. The exception will search for values that match the values you enter in the **Text Before Value**, **Match When Value** and **Text After Value** fields

3. Click **OK.**

Editing and Deleting a POS Transaction Source

1. Right-click a server in the System Explorer and select **Setup** to open the server Setup dialog box. See Accessing the Server Setup for more information.
2. Click **POS Transactions**.

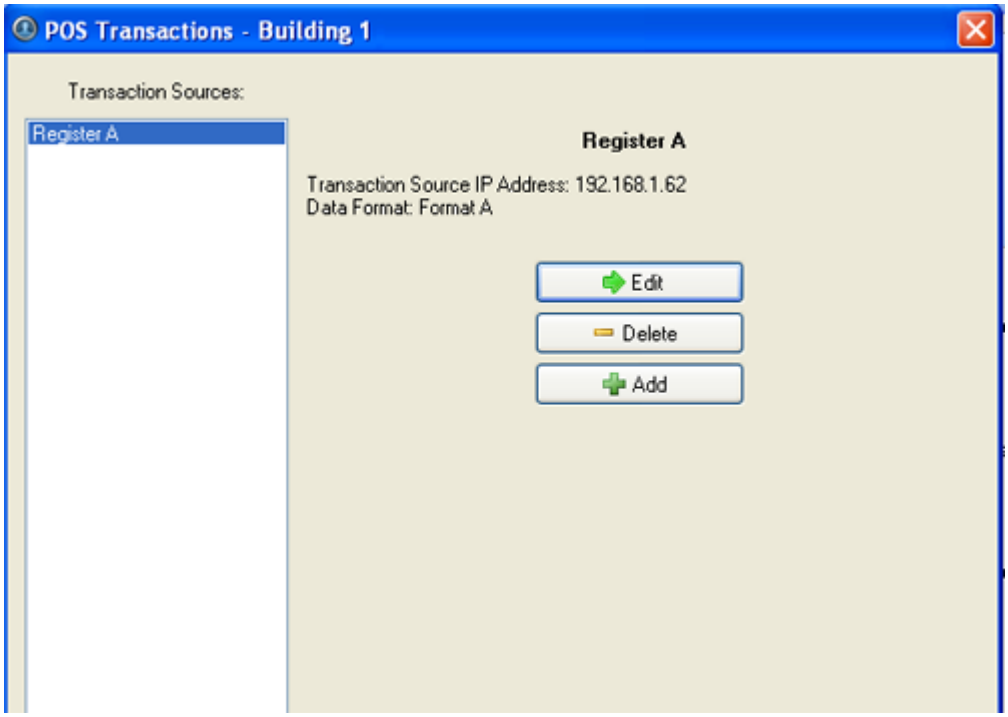


Figure A. POS Transactions dialog box

3. In the POS Transaction dialog box, select a POS transaction source then perform one of the following:
    - Click **Edit** to edit the POS transaction source. Go through the POS Transaction Setup wizard and make the required changes on each page. On the last page, click **Finish**. Refer to Adding a POS Transaction Source for details about the editable options.
    - Click **Delete** to delete the POS transaction source. When the confirmation dialog box appears, click **OK**.

Email Notification

Use the Email Notification dialog box to prepare the server for sending email messages in response to events. You can configure what events require email notification and who receives the emails.

Setting Up the Email Server

Before emails can be sent, the server must be set up to send emails.

1. Right-click a server in the System Explorer and select **Setup** to open the server Setup dialog box. See Accessing the Server Setup for more information.
2. Click **Email Notification**.
3. In the Email Notification dialog box, select the Email Server tab.

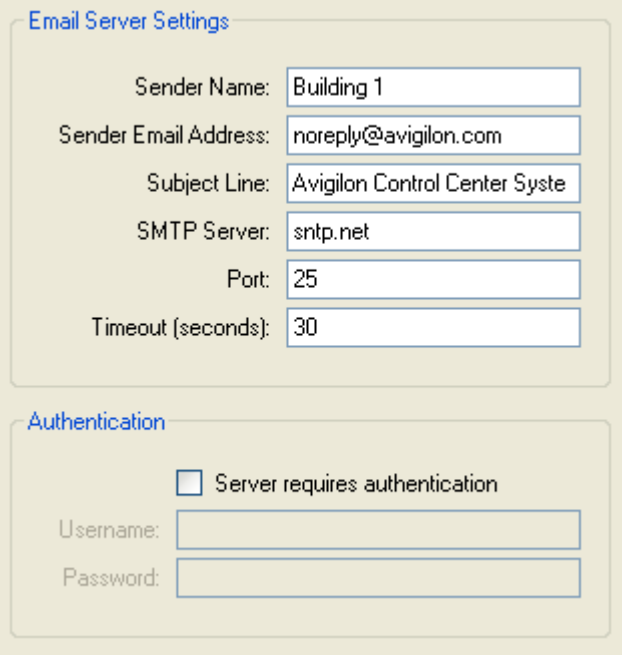


Figure A. Email Notifications dialog box: Email Server tab

4. In the Email Server Settings area, specify the following
    a. **Sender Name:** enter a name to represent the server sending out the email.
    b. **Sender Email Address:** enter an email address the server can use to send emails.
    c. **Subject Line:** enter a default subject line for all emails sent from this server.
    d. **SMTP Server:** enter the SMTP server address used by the server's email.
    e. **Port:** enter the SMTP port.
    f. **Timeout (seconds):** enter the maximum number of seconds the server will attempt to send the email before it stops.
5. (Optional) In the **Authentication** area, select the **Server requires authentication** check box.
    a. Enter the server **Username** and **Password**.
6. Click **OK**.

Configuring Email Notification

In the Email Notification dialog box, you can create email notification groups to specify who will receive email notifications when an event occurs.

1. Right-click a server in the System Explorer and select **Setup** to open the server Setup dialog box. See Accessing the Server Setup for more information.
2. Click **Email Notification**.

3. In the Email Notification dialog box, ensure the Email Notification tab is selected.
4. Click **Add**.

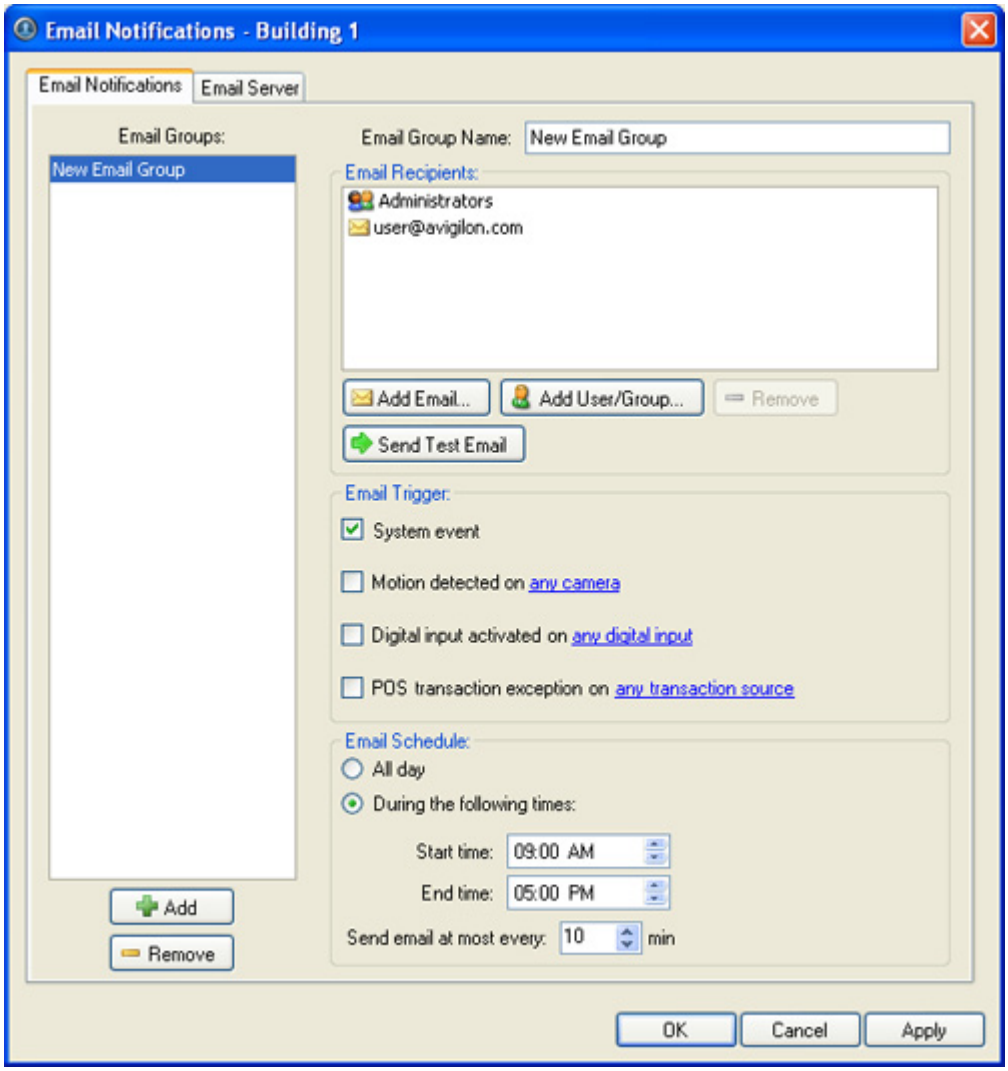


Figure A. Email Notifications dialog box

5. Enter a name for the new email group.
6. In the Email Recipients area, add all the users, groups and emails that are part of this email group. Perform any of the following:
   - Click **Add User/Group** to add an Avigilon Control Center user or access group. In the dialog box, select all the required users and groups then click **OK**.
   - Click **Add Email** to add individual emails. In the dialog box, enter the email address then click **OK**.

   Tip: Ensure the Avigilon users and groups added to the Email Recipient list have a valid email in their user profile.

7. Click **Send Test Email** to send a test email to everyone on the Email Recipients list.
8. In the Email Trigger area, select all the events that this email group will be notified of. Click the blue text to define the event requirements.
9. In the Email Schedule area, select when emails are sent.
    - Select **All day** to send email notifications whenever events occur.
    - Select **During the following times** to send email notifications only during the specified time range. You can limit the number of emails sent by setting the time interval between each email.
10. Click **OK**.

Editing and Deleting an Email Notification

You can edit the details of an email notification or delete the email notification when it is no longer required.

1. Right-click a server in the System Explorer and select **Setup** to open the server Setup dialog box. See Accessing the Server Setup for more information.
2. Click **Email Notification**.
3. In the Email Notification dialog box, ensure the Email Notification tab is selected then perform one of the following:
    - To edit the email notification, select the Email Group and make the required changes, then click **OK**. Refer to Configuring Email Notification for details about the editable options.
    - To delete the email notification, select the Email Group and click **Remove**.

System Log

The system log records events that occur in the Avigilon Control Center system. This can be useful for tracking system usage and diagnosing issues.

You can filter the items displayed in the log and save the log to a separate file for sending to Avigilon support.

Note: The system log maintains a record of system events for up to 90 days.

Viewing the System Log

1. Right-click a server in the System Explorer and select **Setup** to open the server Setup dialog box. See Accessing the Server Setup for more information.
2. Click **System Log**.
3. In the System Log dialog box, select the log events you want to display in the Event Types to Show area, then click **Start Search**.

   The search results are displayed in the left pane.

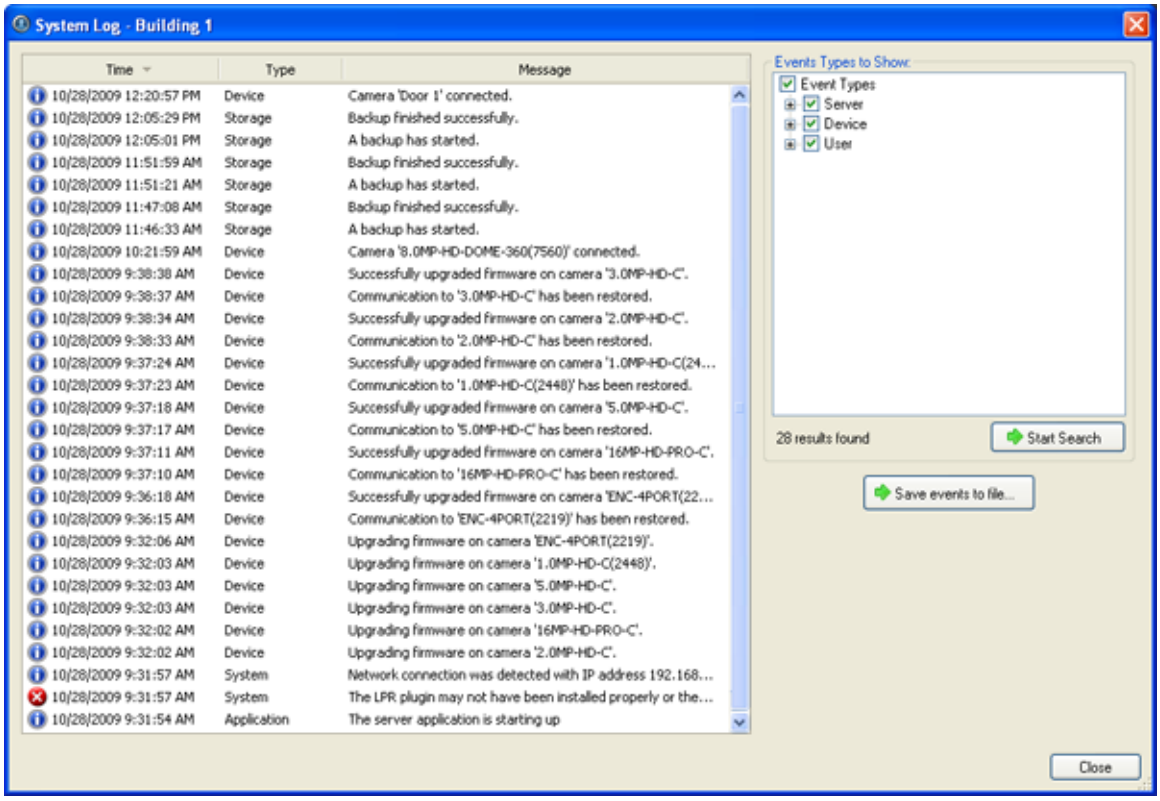


Figure A. System Log dialog box

4. Select a result to display the event details.
5. To save the log search results, click **Save events to file...** and save the file.
6. Click **Close**.

Camera Setup

In the Avigilon Control Center Client software, cameras are pre-configured for optimal image recording. If your surveillance location requires special recording or display settings, you can configure the camera to meet your needs in the camera Setup dialog box.

Note: Some features are not displayed if the server does not have the required license, or if you do not have the user permissions to access the feature.

Note: The dialog box may appear different depending on the camera. Some cameras do not offer the full set of configuration options.

Accessing the Camera Setup

Perform one of the following steps to open the camera Setup dialog box:

- Select **Tools > Setup...** then select the camera you want to setup from the left pane.
- In the System Explorer pane, right-click the camera and select **Setup**.

Note: Some features are not displayed if the server does not have the required license, or if you do not have the user permissions to access the feature.

Note: The dialog box may appear different depending on the camera. Some cameras do not offer the full set of configuration options.

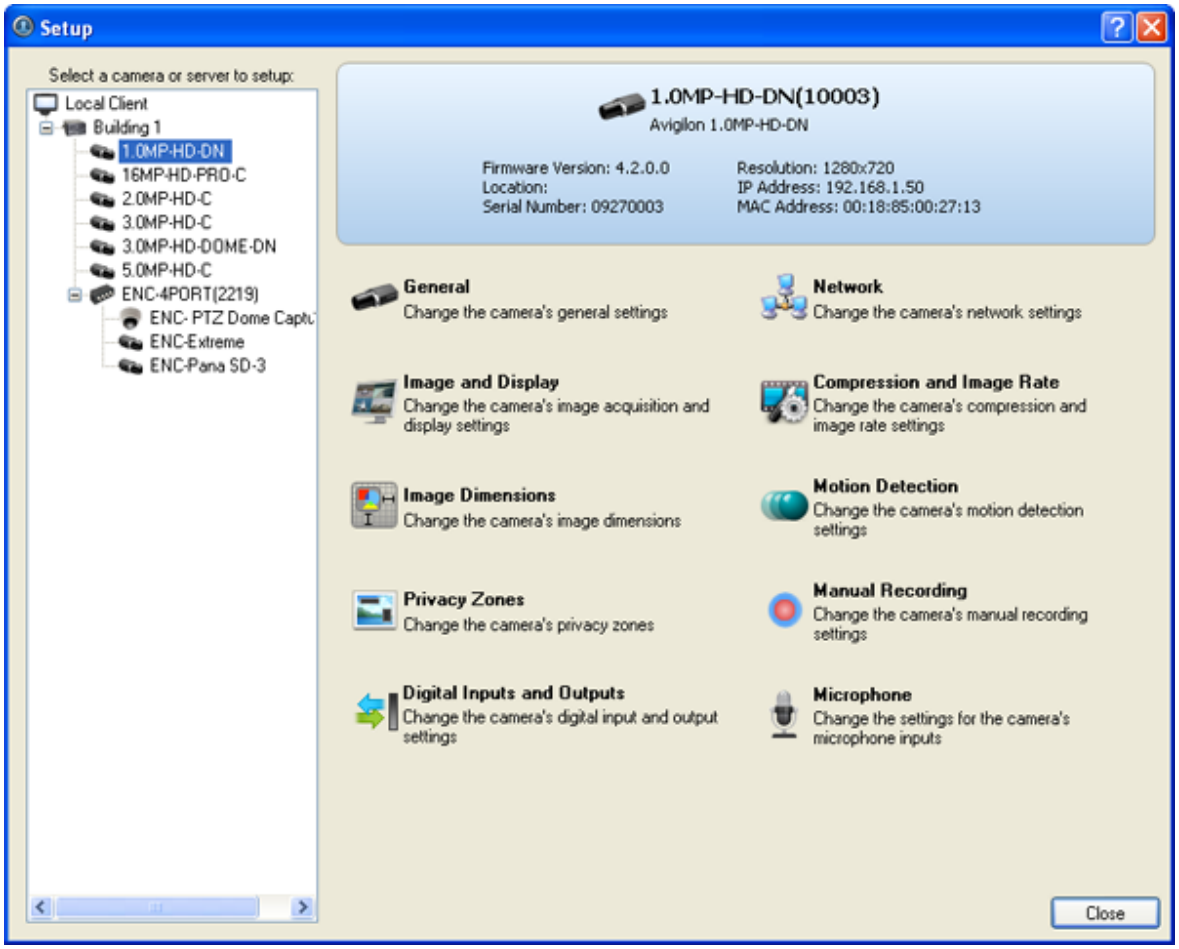


Figure A. Camera Setup dialog box

General

The camera General dialog box allow you to define the camera's name, the camera's location, configure the camera's PTZ settings and disable the camera's status LEDs.

Note: The dialog box may appear different depending on the camera. Some cameras do not offer the full set of configuration options.

Changing General Camera Settings

1. Right-click the camera in the System Explorer and select **Setup** to open the camera Setup dialog box.
   See Accessing the Camera Setup for more information.
2. Click **General**.
3. In the General dialog box, complete the following fields as required:

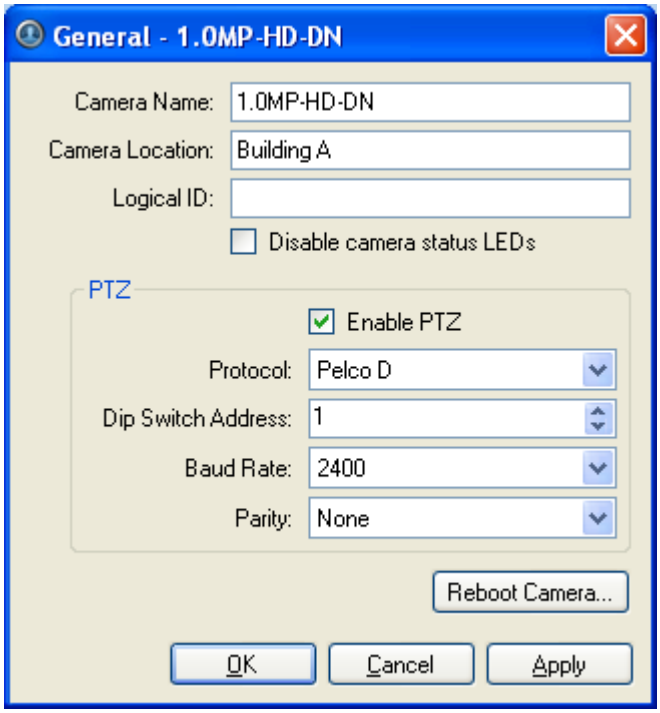


Figure A. General dialog box

- **Camera Name:** enter a camera name. Give the camera a meaningful name to help you identify the camera.
- **Camera Location:** describe the camera's location.
- **Logical ID:** enter a number to allow the Client software to identify this camera.

  The logical ID is used to call up the camera video when using the select camera keyboard command.
- **Disable camera status LEDs:** select this check box to disable the LEDs located on the back of the camera.
- **Enable PTZ:** select this check box to enable the camera's pan, tilt and zoom (PTZ) functions. The PTZ device is controlled from the RS-485 inputs on the camera.

  Select the appropriate **Protocol**, **Dip Switch Address**, **Baud Rate** and **Parity** settings.

  Tip: PTZ enabled cameras are given the dome camera icon in the System Explorer.

4. If required, click **Reboot Camera** to restart the camera.
5. Click **OK**.

Network

Use the camera Network dialog box to modify how a camera connects to the server network, and specify the IP address used by the camera.

Note: The dialog box may appear different depending on the camera. Some cameras do not offer the full set of configuration options.

Changing Camera Network Settings

1. Right-click the camera and select **Setup** to open the camera Setup dialog box.
2. Click **Network**.
3. In the Network dialog box, select the required options and complete the related fields:

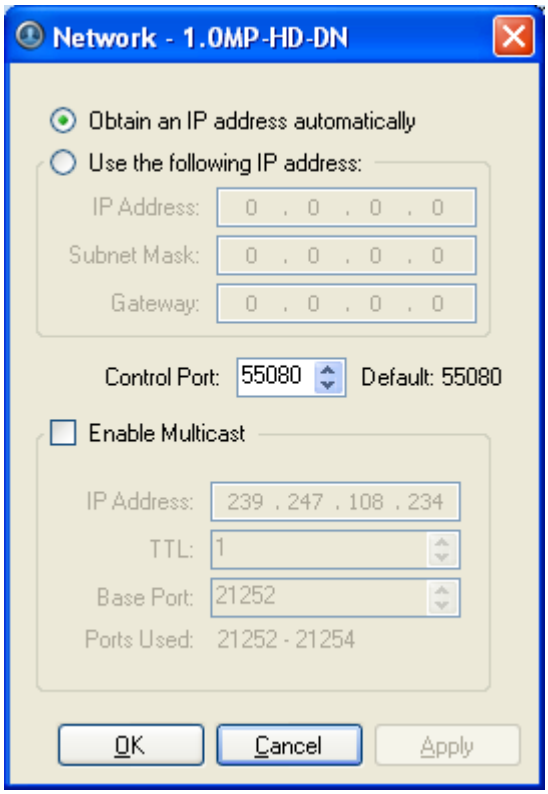


Figure A. Network dialog box

- **Obtain an IP address automatically:** select this option to enable the camera to connect to the network through an automatically assigned IP address.

  The camera will attempt to obtain an address from a DHCP server, if it cannot find one it will default to addresses in the 169.254.x.x range.

- **Use the following IP address:** select this option to enable the camera to connect to the network through a static IP address.

  Enter the **IP Address**, **Subnet Mask** and **Gateway**.

- **Control Port:** select the network port for connecting to the camera. This port is also used for manually discovering cameras on the network.

- **Enable Multicast:** select this check box to enable multicast streaming from the camera. You must enable multicast if you are setting up redundant connections to multiple servers.

  Use the default generated **IP Address**, **TTL** and **Base Port**, or enter your own values.

4. Click **OK**.

Image and Display

Use the Image and Display dialog box to control a camera's display settings for live and recorded images.

Changing Image and Display Settings

Note: The dialog box may appear different depending on the camera. Some cameras do not offer the full set of configuration options.

1. Right-click the camera in the System Explorer and select **Setup** to open the camera Setup dialog box.
   See Accessing the Camera Setup for more information.

2. Click **Image and Display**.

3. In the Image and Display dialog box, make the required changes to adjust the camera's image settings.

   Tip: Use the **Maximum Exposure**, **Maximum Gain** and **Priority** options to control low light behavior.

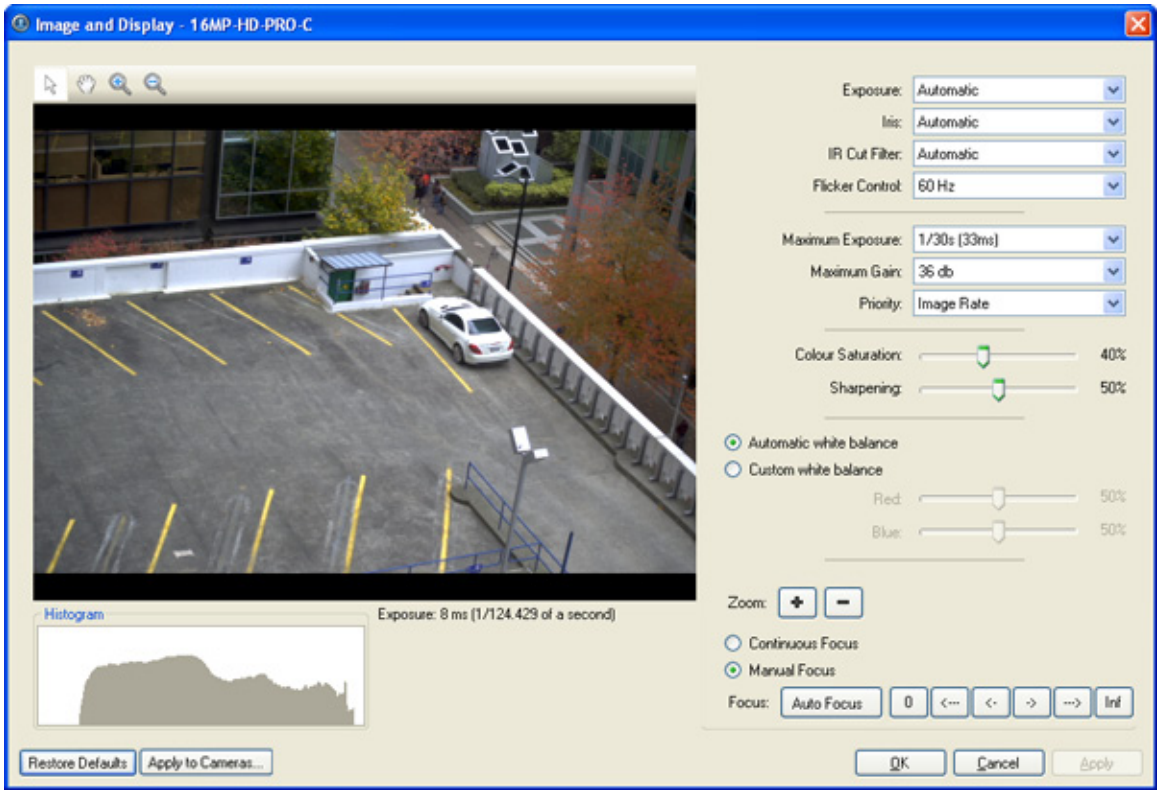


Figure A. Image and Display dialog box

Option	Description
Exposure	You can allow the camera to control the exposure automatically or you can manually set the exposure. ▪ Select **Automatic** for the camera to automatically control the exposure. ▪ Select an exposure rate to manually set the exposure. **Note:** Increasing the manual exposure time may affect the image rate.
Iris	If your camera has a lens with an auto iris, you can allow the camera to control the iris automatically or you can manually set it as open or closed. ▪ From the **Iris** drop down list, select one of the following: ▪ **Automatic** ▪ **Open** ▪ **Close**
IR Cut Filter	If your camera has a removable infrared cut filter, you can allow the camera to control it automatically or you can manually set the camera to color or monochrome mode.

	▪ From the **IR Cut Filter** drop down list, select one of the following: ▪ **Automatic** ▪ **Color** ▪ **Monochrome**
Flicker Control	If your video image flickers because of the fluorescent lights around the camera, you can reduce the effects of the flicker by setting the **Flicker Control** to the same power frequency as your lights. For example, for Europe 50Hz or for North America 60Hz. ▪ In the **Flicker Control** drop down list, select a frequency.
Backlight Compensation	If your scene has small areas of intense light that are causing the overall image to be too dark, backlight compensation can be used to achieve a well exposed image. ▪ Move the **Backlight Compensation** slider until the video image meets your requirements.
Maximum Exposure	You can limit the automatic exposure setting by setting a maximum exposure level. By setting a maximum exposure level for low light situations, you can control the camera's exposure time to let in the maximum amount of light without creating blurry images. ▪ Select an exposure rate from the **Maximum Exposure** drop down list.
Maximum Gain	You can limit the automatic gain setting in the camera by setting a maximum gain level. By setting a maximum gain level for low light situations, you can maximize the detail of an image without creating excessive noise in the images. ▪ Select a gain level from the **Maximum Gain** drop down list.
Priority	You can set **Image Rate** or **Exposure** as the priority. When set to **Image Rate**, the camera will maintain the set image rate as the priority, and will not adjust the exposure beyond what can be recorded for the set Image Rate. See Changing Compression and Image Rate Settings to set the Image Rate. When set to **Exposure** the camera will maintain the exposure setting as the priority, and will override the set image rate to achieve the best image possible. ▪ In the **Priority** drop down list, select either **Image Rate** or **Exposure**.
Saturation	You can adjust the video's color intensity. ▪ Move the **Color Saturation** slider until the video image meets

	your requirements.
Sharpening	If the video image is blurry, you can adjust the video sharpness to make the edges of objects more visible. ▪ Move the **Sharpening** slider until the video image meets your requirements.
White Balance	You can control white balance settings to account for different scene illuminations. ▪ Select one of the following: ▪ **Automatic white balance** ▪ **Custom white balance** Move the corresponding sliders to manually modify the color balance.

4. To focus the camera, see Focusing the Camera Lens.
5. Click **Apply to Cameras...** to apply the same settings to other cameras of the same model.
6. Click **OK**.

Zooming and Focusing the Camera Lens

If you have a camera with a lens capable of electronic zoom and focus, you can zoom or focus the camera through the Avigilon Control Center Client software.

Note: The dialog box may appear different depending on the camera. Some cameras do not offer the full set of configuration options.

1. Right-click the camera in the System Explorer and select **Setup** to open the camera Setup dialog box.
   See Accessing the Camera Setup for more information.
2. Click **Image and Display**. The Image and Display dialog box appears.
3. If the camera has a built-in auto focus feature, you can choose one of the following:
   - **Continuous Focus:** the camera will automatically focus itself whenever the scene changes. Skip the following step.
   - **Manual Focus:** you can manually focus the camera through the Image and Display **Focus** buttons. Once the focus is manually set, it will not change.
4. While you view the camera image panel, complete the following steps to zoom and focus the camera:

Tip: For Avigilon HD Professional cameras, the lens must be set to auto-focus (AF) mode on the camera. If the camera does not detect the lens, the **Focus** buttons are not displayed.

3.

a. Use the **Zoom** buttons to zoom in to the distance you want to focus.

b. In the **Iris** drop down list, select **Open**. When the camera iris is fully open, the depth of field is the shortest.

c. Use the **Focus** buttons until the image becomes clear.

Button	Description
Auto Focus	The camera will automatically focus once.
0	Focused as close to zero as possible
<---	Large step toward zero
<-	Small step toward zero
->	Small step toward infinity
--->	Large step toward infinity
Inf	Infinity

4. Click **Apply to Cameras...** to apply the same settings to other cameras of the same model.

5. Click **OK**.

Compression and Image Rate

Use the camera Compression and Image Rate dialog box to modify the camera's compression and image quality settings for sending image data over the network.

Note: The dialog box may appear different depending on the camera. Some cameras do not offer the full set of configuration options.

Changing Compression and Image Rate Settings

1. Right-click the camera in the System Explorer and select **Setup** to open the camera setup dialog box.

2. Click **Compression and Image Rate**. The Compression and Image Rate dialog box appears.

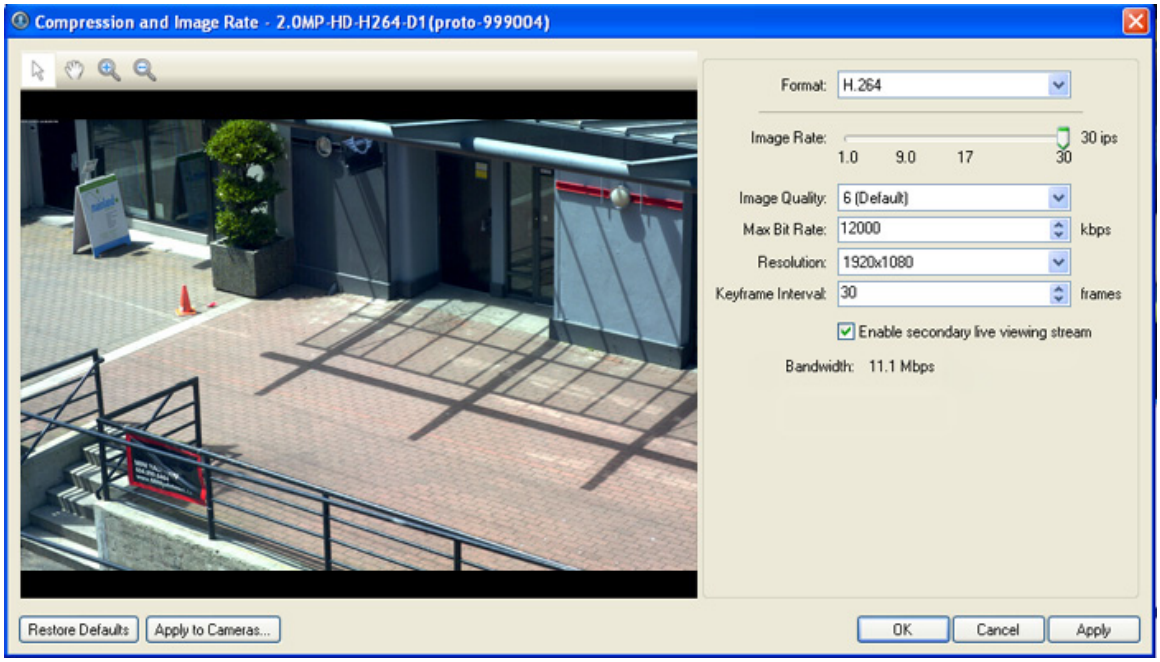


Figure A. Compression and Image Rate dialog box.

The Bandwidth area gives an estimate of the amount of bandwidth the camera would be using given the configured compression and image rate. Adjust the settings as required.

3. In the **Format** drop down list, select the preferred streaming format.

4. In the **Image Rate** bar, move the slider to select the desired image rate.

5. In the **Image Quality** drop down list, select the desired image quality number.

   Image quality setting of **1** will produce the highest quality video and require the most bandwidth.

6. In the **Max Bit Rate** drop down list, select the maximum bandwidth the camera can use.

7. In the **Resolution** drop down list, select the preferred image resolution.

8. In the Keyframe Interval drop down list, select the preferred number of frames between each keyframe.

9. If your camera supports multiple video streams, select the **Enable secondary live viewing stream** check box to enable the secondary stream.

   A secondary video stream allows you to view video at a lower image rate to reduce bandwidth usage, while still recording at a high image rate in the primary stream.

10. Click **Apply to Cameras...** to apply the same settings to other cameras of the same model.
11. Click **OK**.

Image Dimensions

Use the Image Dimension dialog box to set the image dimensions for the camera. This can help reduce bandwidth and increase the maximum image rate.

Changing Image Dimensions Settings

1. Right-click the camera in the System Explorer and select **Setup** to open the camera Setup dialog box.
   See Accessing the Camera Setup for more information.
2. Click **Image Dimensions**.
3. In the Image Dimensions dialog box, adjust the image dimensions by performing one of the following:
   - Drag the edges of the image until you achieve the required size.
   - Change the values for the **Top**, **Left**, **Width**, and **Height** field.

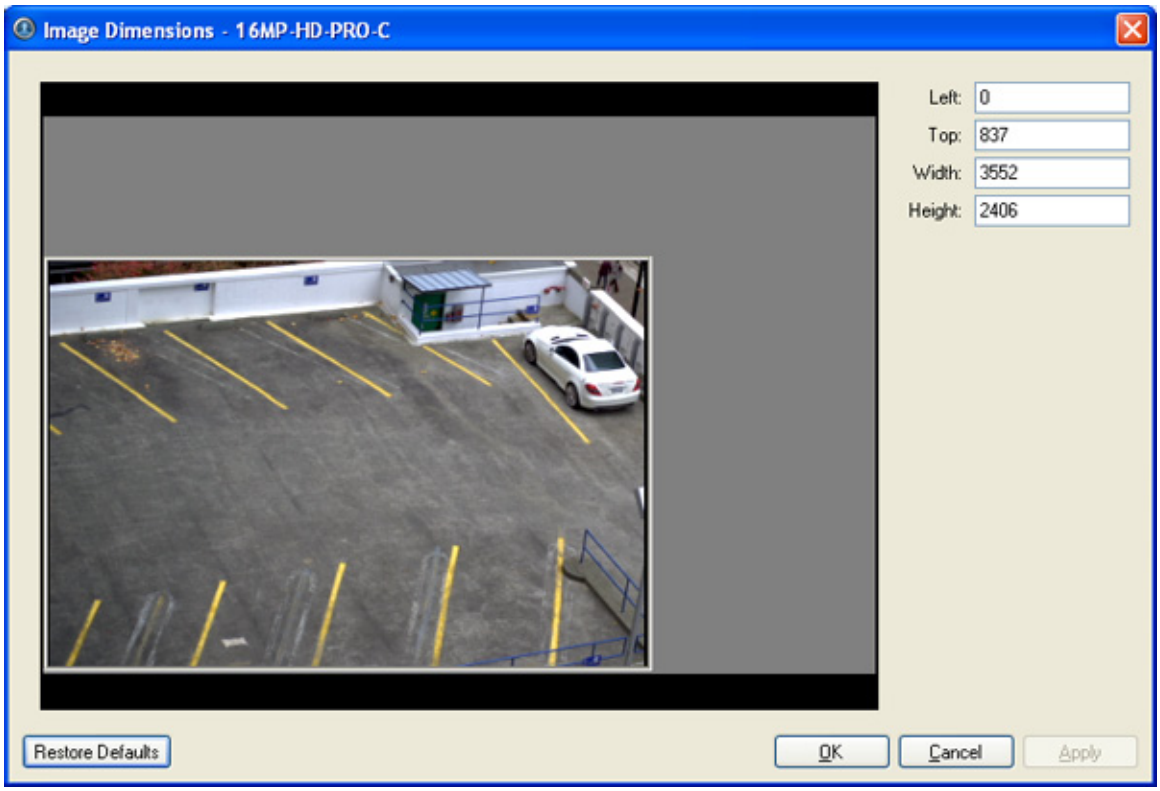


Figure A. Image Dimensions dialog box

4. Click **OK**.

Motion Detection

In the Motion Detection dialog box, you can define specific areas where motion is detected and configure the sensitivity and threshold for motion detection.

Selecting an Area to Detect Motion

In the Motion Detection dialog box, define the green motion detection area of a camera image. Motion detection is ignored in the areas not highlighted in green.

1. Right-click the camera in the System Explorer and select **Setup** to open the camera Setup dialog box.
   See Accessing the Camera Setup for more information.
2. Click **Motion Detection**.
3. In the Motion Detection dialog box, select the buttons above the image panel and use your mouse to define the green motion detection area. The motion detection area must be defined before motion is detected:
   - **Set Area:** select this button then draw green rectangles to define motion detection areas. If necessary, draw multiple rectangles to create your motion detection area.
   - **Clear Area:** select this button and draw rectangles to erase sections from the motion detection area.
   - **Draw:** select this button and manually draw motion detection area. This tool allows you to be very specific and highlight unusual shapes.
   - **Set All:** select this button to highlight the entire image for motion detection.
   - **Clear All:** select this button to clear the image of motion detection areas.

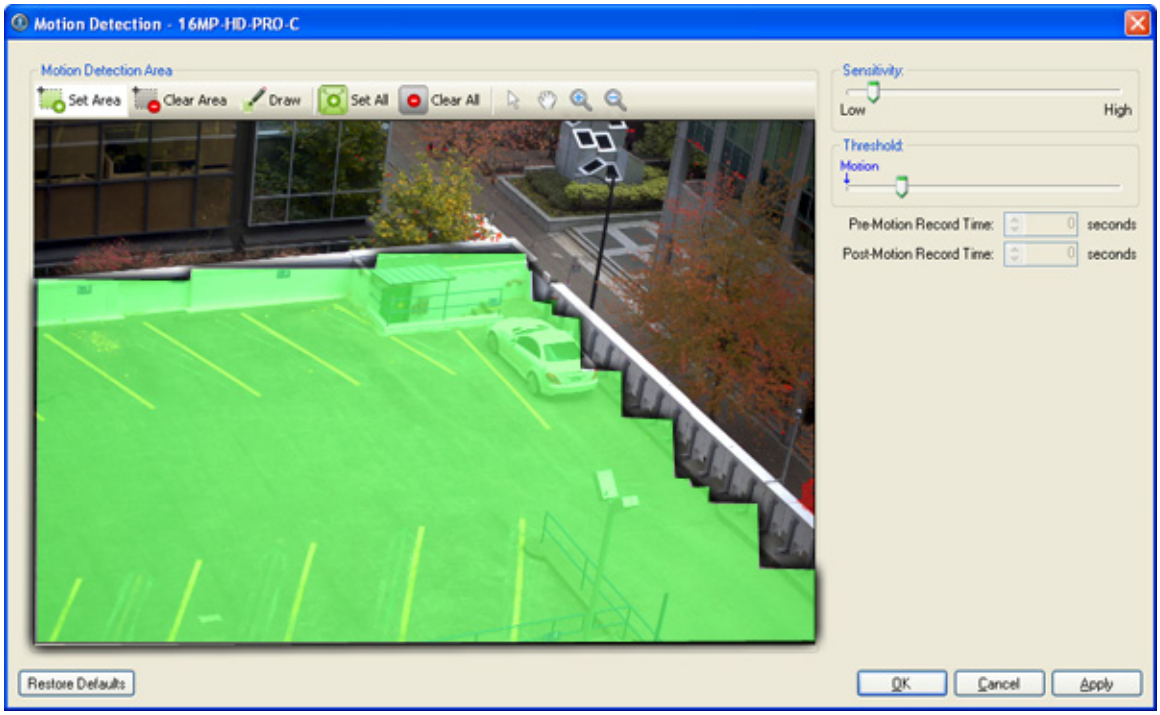


Figure A. Motion Detection dialog box

4. Click **OK**.

To define the sensitivity and threshold for the motion detection area, see Controlling Motion Sensitivity and Threshold.

Controlling Motion Sensitivity and Threshold

In the Motion Detection dialog box, you can control the camera's sensitivity threshold for motion. You can also define how much time should be recorded before and after the motion event.

1. Right-click the camera in the System Explorer and select **Setup** to open the camera Setup dialog box.
   See Accessing the Camera Setup for more information.
2. Click **Motion Detection**. The Motion Detection dialog box appears.
3. Move the **Sensitivity** slider to adjust how much each pixel must change before it is considered in motion.

   The higher the sensitivity, the smaller the amount of pixel change is required before a motion is detected.
4. Move the **Threshold** slider to adjust how many pixels must change before the image is considered to have motion.

   The higher the threshold, the higher the number of pixels must change before the image is considered to have motion.

Tip: The **Motion** indicator above the Threshold slider will move to indicate how much motion is occurring in the current scene.

5. In the **Pre-Motion Record Time** and **Post-Motion Record Time** boxes, specify how much time you want the camera to record before and after the motion event.
6. Click **OK**.

Privacy Zones

You can set privacy zones in the camera's field of view to block out regions of the camera image that you do not want to view or record.

Adding a Privacy Zone

1. Right-click the camera in the System Explorer and select **Setup** to open the camera Setup dialog box.
   See Accessing the Camera Setup for more information.
2. Click **Privacy Zones**.
3. In the Privacy Zones dialog box, click **Add** and a green box will appear on the image.

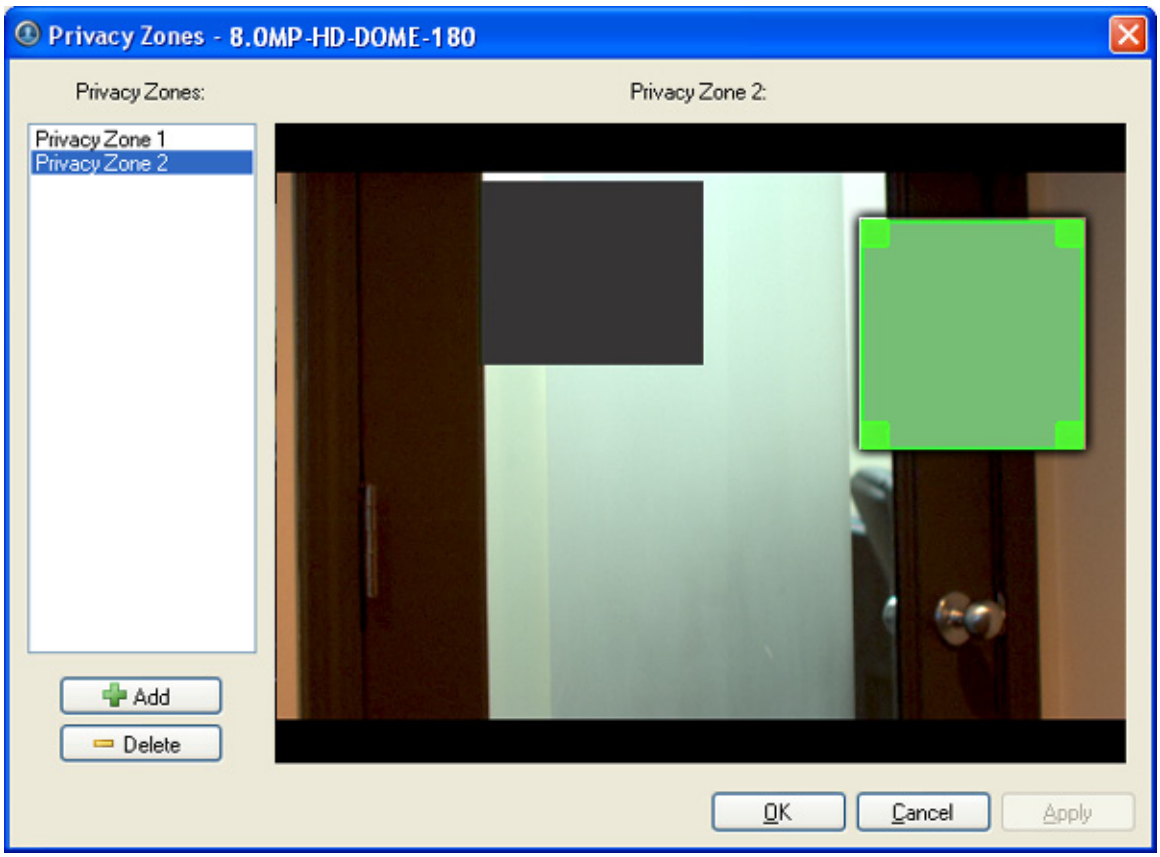


Figure A. Privacy Zones dialog box

4. Move and resize the green box until it covers the area you want to block out.
5. Click **OK**.

Editing and Deleting a Privacy Zone

1. Right-click the camera in the System Explorer and select **Setup** to open the camera Setup dialog box.
   See Accessing the Camera Setup for more information.
2. Click **Privacy Zones**.
3. In the Privacy Zones dialog box, select a privacy zone from Privacy Zone list and perform one of the following:
   - To edit the privacy zone, adjust the green box on the image.
   - To delete the privacy zone, click **Delete**.
4. Click **OK**.

Manual Recording

Manual recording allows you to control video recording outside a camera's recording schedule. Manual recording can only be activated when viewing live camera images. See Triggering Manual Recording for more information.

In the Manual Recording dialog box, you can define the maximum recording duration and the pre-trigger recording time for each camera.

Changing Manual Recording Settings

1. Right-click the camera in the System Explorer and select **Setup** to open the camera Setup dialog box.
   See Accessing the Camera Setup for more information.
2. Click **Manual Recording**. The Manual Recording dialog box appears.

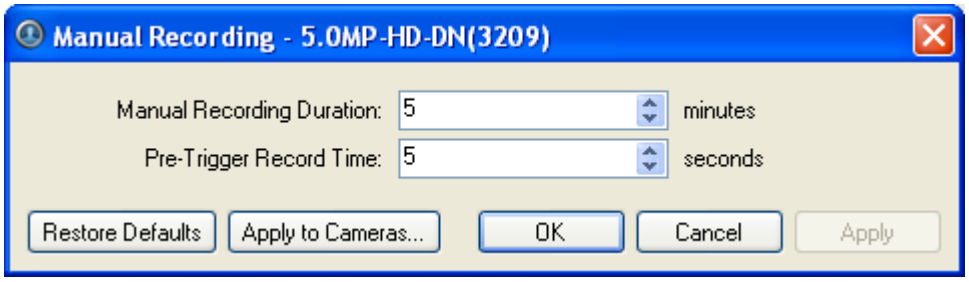


Figure A. Manual Recording dialog box

3. Specify the following:
    - **Manual Recording Duration:** enter the maximum duration of a manual recording if it is not manually stopped.
    - **Pre-Trigger Record Time:** enter the amount of time the camera's images are recorded before manual recording is activated.
4. Click **Apply to Cameras...** to apply the same settings to other cameras of the same model.
5. Click **OK**.

Digital Inputs and Outputs

In the Digital Inputs and Outputs dialog box, set up the external digital inputs and outputs that are connected to the camera.

Setting Up Digital Inputs

1. Right-click the camera in the System Explorer and select **Setup** to open the camera Setup dialog box.
   See Accessing the Camera Setup for more information.
2. Click **Digital Inputs and Outputs**.
3. In the Digital Inputs area, select an input.

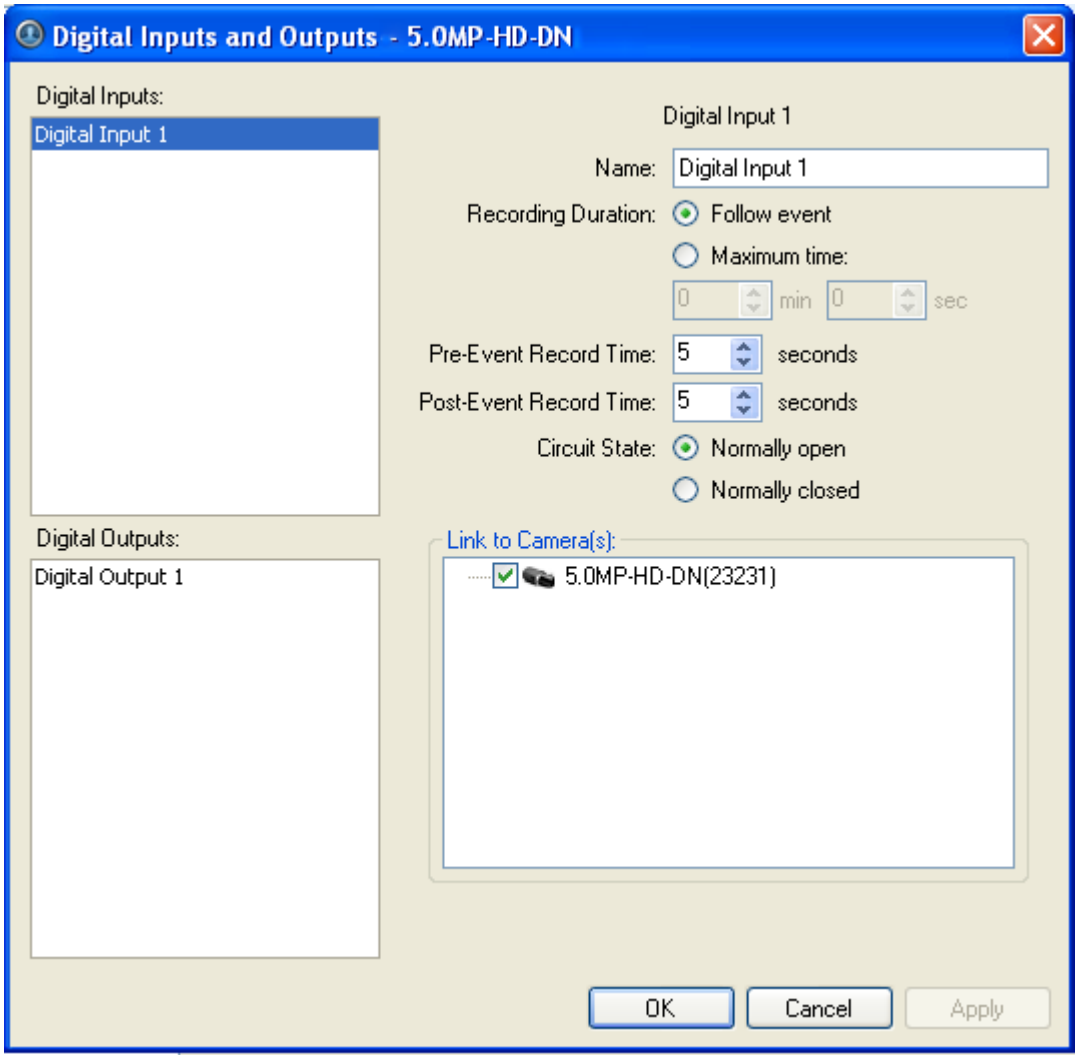


Figure A. Digital Inputs and Outputs dialog box: Digital Inputs Settings

4. Specify the following:
    - **Name:** enter a name to identify the digital input.
    - **Recording Duration:** select **Follow Event** to record the entire digital input event. Or, select **Maximum Time** to limit the recording time.
    - **Pre-Event Record Time:** enter the amount of time to record before the digital input is triggered.
    - **Post-Event Record Time:** enter the amount of time to continue recording after the digital input returns to its normal state.
    - **Circuit State:** select the digital input's default circuit state.
    - **Link to Camera(s):** select the cameras that need to be linked to this input for recording.

If the Recording Schedule is configured to record digital inputs, the cameras selected in the Link to Camera(s) area are used to record this digital input.

5. Click **OK**.

Setting Up Digital Outputs

Note: The dialog box may appear different depending on the camera. Some cameras do not offer the full set of configuration options.

1. Right-click the camera in the System Explorer and select **Setup** to open the camera Setup dialog box.
   See Accessing the Camera Setup for more information.
2. Click **Digital Inputs and Outputs**.
3. In the Digital Outputs area, select an output.

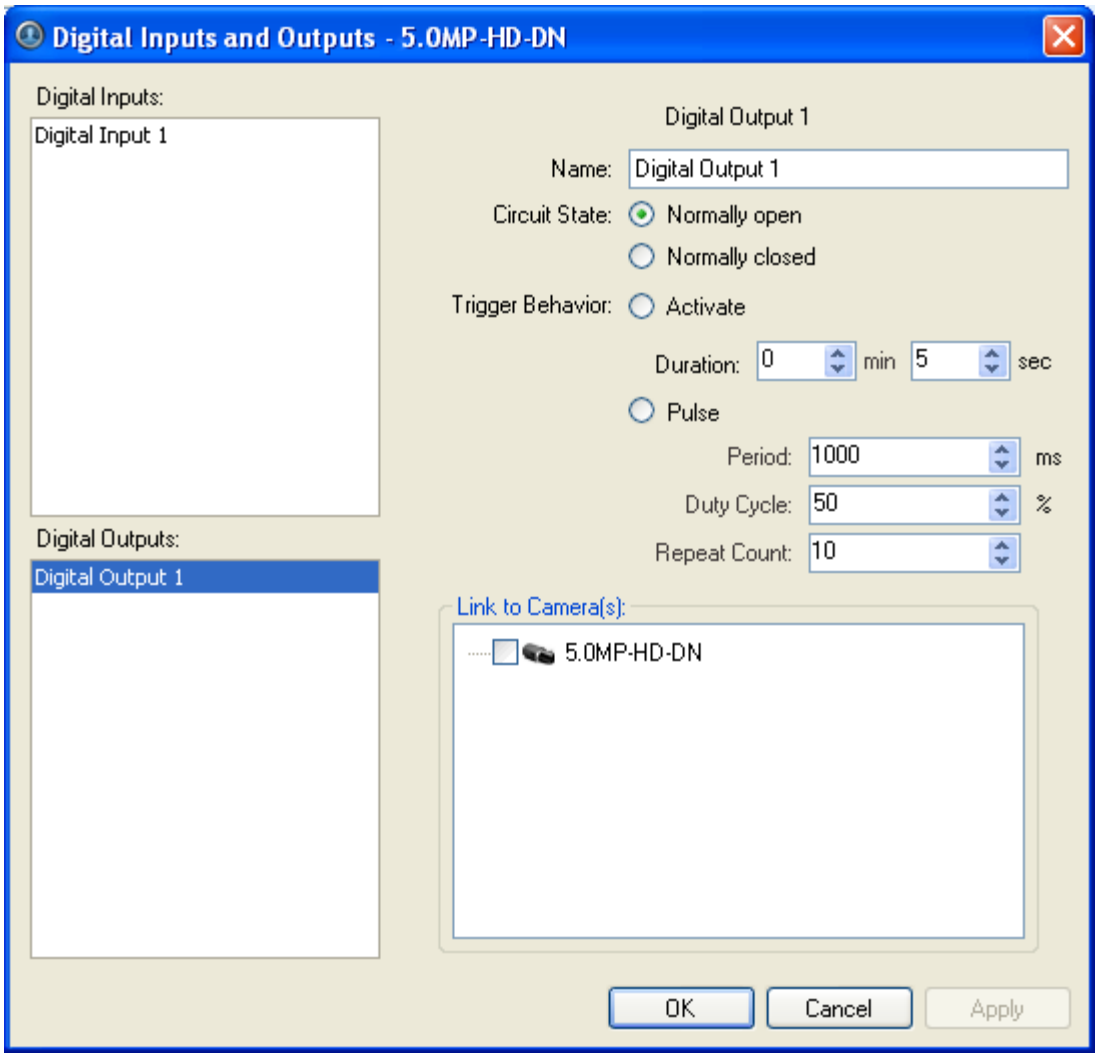


Figure A. Digital Inputs and Outputs dialog box: Digital Output Settings

4. Enter a name to identify the digital output.
5. Select one of the Circuit State options to define the digital output's default circuit state.
6. The Trigger Behavior options define what occurs when the output activated.
    - Select **Activate** to enable the digital output in continuous mode. The **Duration** fields allow you to specify how long the digital output should be active for.
    - Select **Pulse** to enable the digital output in pulse mode. Specify the **Period**, **Duty Cycle**, and **Repeat Count** for the pulse.
7. Select the cameras this digital output should be linked to.

    When you view the live video from the selected cameras, you can manually trigger this digital output. See Triggering Digital Output for more information.
8. Click **OK**.

Microphone

Note: Audio recording requires an Audio Channel License.

Use the Microphone dialog box to change the settings for the microphone input on a supported device. You can link the audio with any camera connected to the server.

Note: The dialog box may appear different depending on the camera. Some cameras do not offer the full set of configuration options.

Changing Microphone Settings

1. Right-click the camera in the System Explorer and select **Setup** to open the camera Setup dialog box.
   See Accessing the Camera Setup for more information.
2. Click **Microphone**. The Microphone dialog box appears.

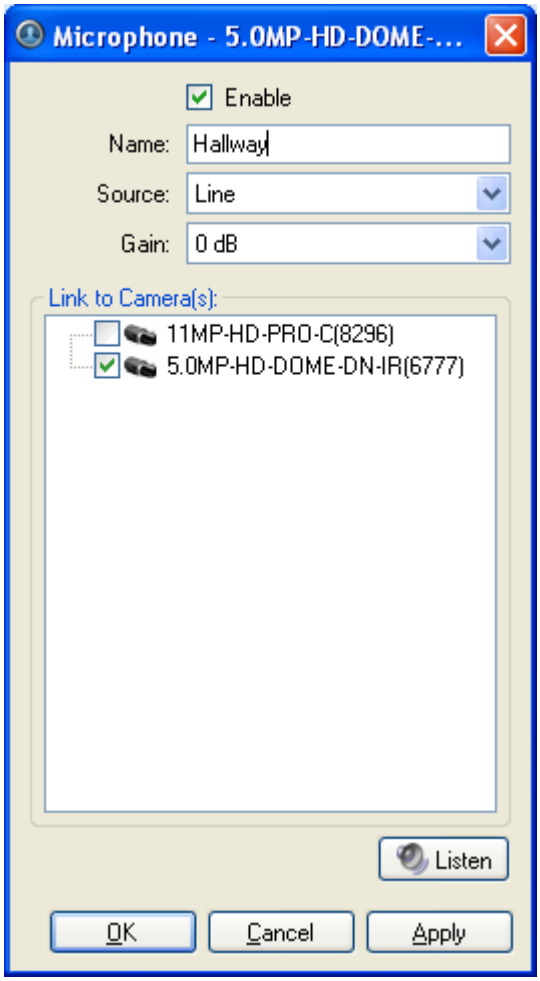


Figure A. Microphone dialog box

3. Complete the following fields:
    - **Enable:** select this check box to enable audio recording from this input.

      Note: An error message will appear if you do not have an Audio Channel License.
    - **Name:** enter a name for the audio input.
    - **Source:** select either line or microphone depending on the type of audio source.
    - **Gain:** select the amount of analog gain to be applied to the audio in the device.

      Values above **0 dB** will increase the volume of the audio source and negative values will decrease the volume.
4. Click **Listen** to test the settings and listen to the audio source.
5. In the Link to Camera(s) area, select the camera video that is linked with the audio.
6. Click **OK**.

Client Setup

You can modify the local client properties in the client Setup dialog box. The client Setup includes configuring the following settings:

Accessing the Client Setup

Perform one of the following steps to open the client Setup dialog box in the Avigilon Control Center Client software.

- Select **Tools > Setup...** and select the local client from the left pane.
- In the System Explorer, right-click the local client and select **Setup**.

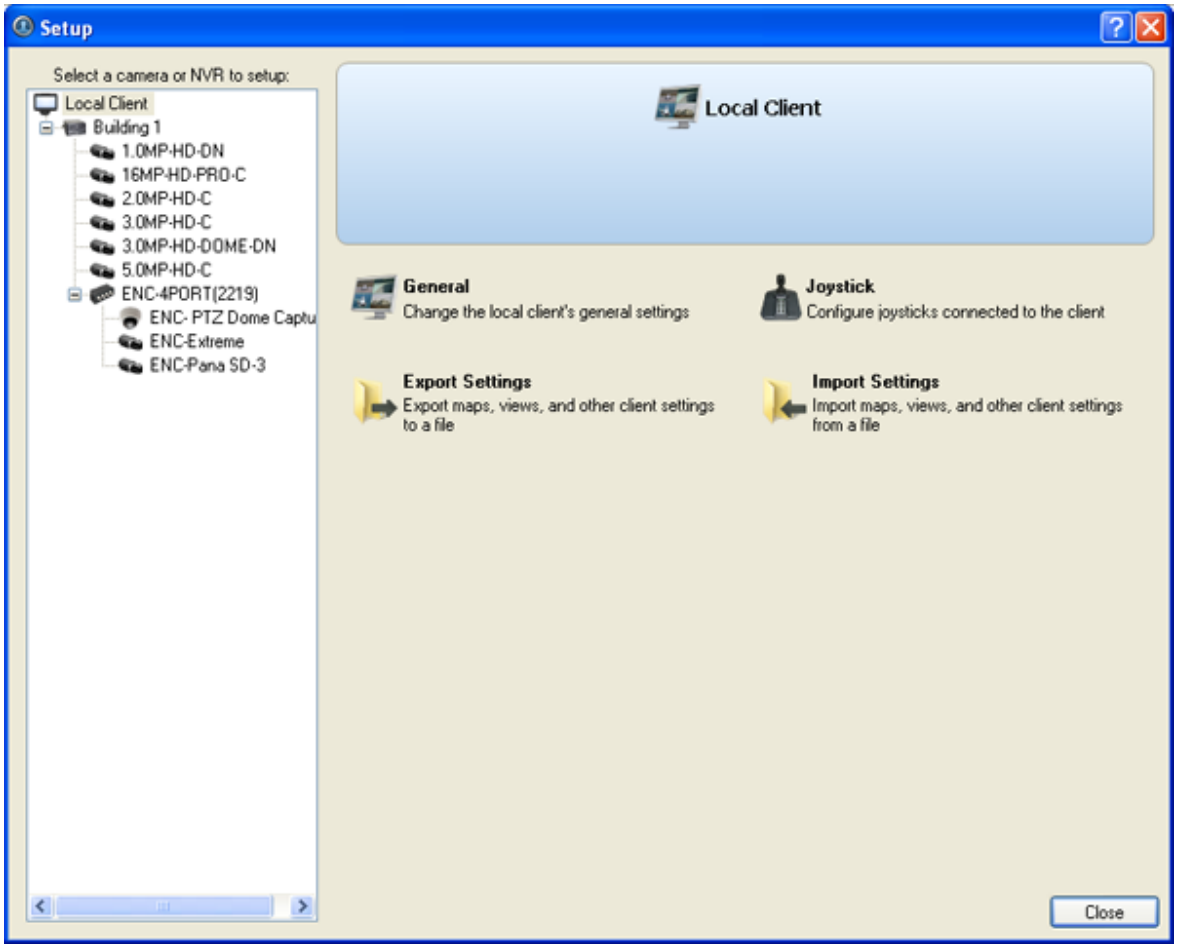


Figure A. Setup Local Client dialog box

General

Use the client General dialog box to change the local client's log in preferences and connection speed.

The client's connection speed can be changed to match the available incoming network bandwidth. This is useful when streaming video over the internet.

Changing General Client Settings

1. Right-click the local client in the System Explorer and select **Setup** to open the client Setup dialog box.
   For more information, see Accessing the Client Setup.
2. Click **General**.
3. In the General dialog box, complete the following fields as required:

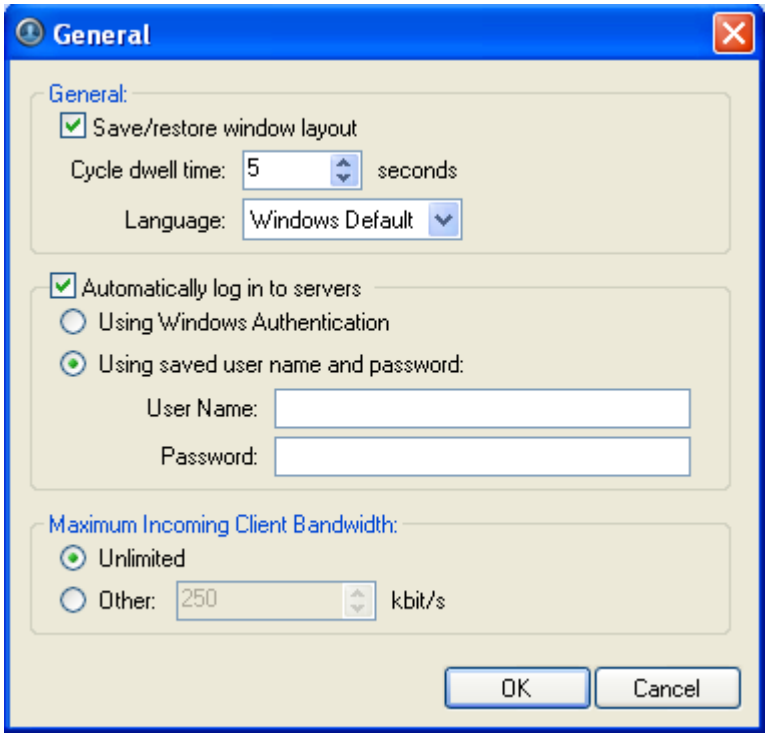


Figure A. General dialog box

- **Save/restore window layout:** select this check box if you want the application to remember your layout preferences.
- **Cycle dwell time:** enter the number of seconds the application waits before it cycles to a different View. See Cycling Through Views for more information.

- **Language:** select a language from the drop down list to change the application language. Select **Windows Default** for the application to automatically display the same language as the local client.
- **Automatically log in to servers:** select this check box to enable the application to automatically log you into all servers that are available on the network. Select the type of login you use: **Windows Authentication** — your Windows login; or **saved user name and password** — your Avigilon Control Center username and password.
- In the Maximum Incoming Client Bandwidth area, select **Unlimited**, or select **Other** and specify the maximum kilobits per second (kbit/s) you want to allow.

4. Click **OK**.

Joystick

The Avigilon Control Center Client software supports two types of joysticks: standard Microsoft DirectX USB Joysticks and the Avigilon Professional Joystick Keyboard.

Use the Joystick dialog box to configure joystick settings.

Configuring a Standard USB Joystick

Use the Joystick dialog box to configure the buttons used in your standard Microsoft DirectX USB joystick.

1. Connect the joystick.
2. Right-click the local client in the System Explorer and select **Setup** to open the client Setup dialog box.
   For more information, see Accessing the Client Setup.
3. Click **Joystick**.
4. If the joystick is not automatically detected, an error message will appear. Click **Scan for Joysticks...**.

   Note: The error message will not appear if the joystick was detected.

   When the joystick is detected, the Joystick dialog box appears.

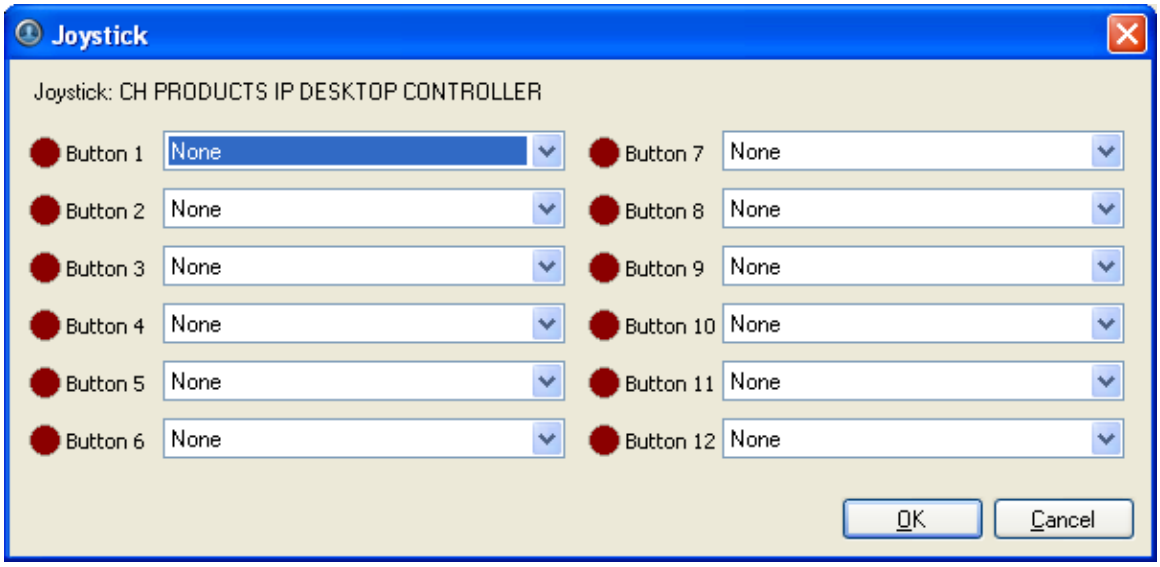


Figure A. Joystick dialog box

5. Set up an action for each button on the joystick:
    a. Press a button on the joystick. The button label is highlighted in the Joystick dialog box.
    b. Select an action for the button from the drop down list.
    c. Repeat this procedure for each button on the joystick.
6. Click **OK**.

Configuring an Avigilon Professional Joystick Keyboard

The Avigilon Professional Joystick Keyboard is a USB add-on that contains a joystick for controlling zoom and pan within image panels, a jog shuttle for controlling the Timeline, and a keypad programmed with the Client software keyboard commands.

By default, the keyboard is installed in right-hand mode. Use the Joystick dialog box to configure left-hand mode.

1. Connect the keyboard.
2. Right-click the local client in the System Explorer and select **Setup** to open the client Setup dialog box.
   For more information, see Accessing the Client Setup.
3. Click **Joystick**.
4. If the keyboard is not automatically detected, an error message will appear. Click **Scan for Joysticks...**.

Note: The error message will not appear if the keyboard was detected.

When the keyboard is detected, the Joystick dialog box appears.

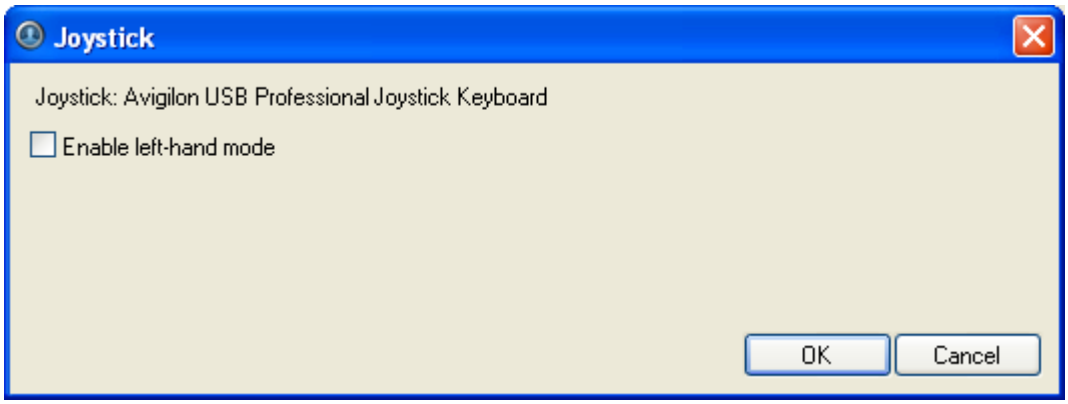


Figure A. Joystick dialog box

5. Select the **Enable left-hand mode** check box.
6. Click **OK**.

The keyboard is now configured for left-hand mode.

Rotate the keyboard until the joystick is on the left and the jog shuttle is on the right. Reinstall the keypad cover with the View button labels at the top.

Exporting Settings

You can export your personalized settings for the Client software so that the settings can be backed up or used on a different computer.

To export server settings like Recording Schedules, Users & Groups, Device, POS Source, and Device Connection settings, see the *Avigilon Control Center Server User Guide*.

Note: Some features are not displayed if the server does not have the required license, or if you do not have the user permissions to access the feature.

Exporting client settings

1. Right-click the local client in the System Explorer and select **Setup** to open the client Setup dialog box.
   For more information, see Accessing the Client Setup.
2. Click **Export Settings**.
3. Select the items you want to export.

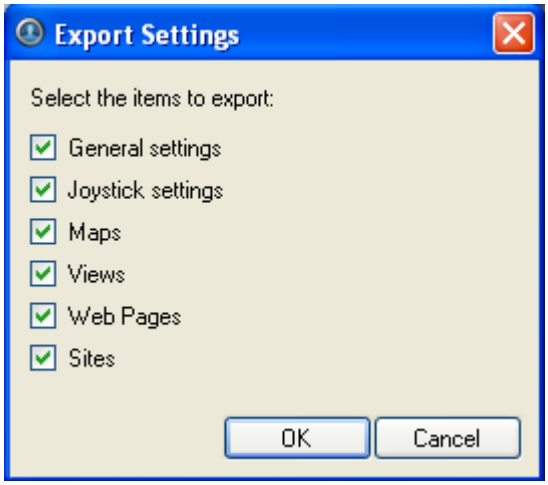


Figure A. Export Settings dialog box

The **General settings** include display quality, deinterlacing, manually added servers, image overlays, and client connection speed.

4. Click **OK**.
5. In the Save As dialog box, name and save the file.

   Exported client settings can only be saved in Avigilon Client Settings File (AVC) format.

Import Settings

Import and use settings that were previously exported from the local client, or from a different computer.

Importing client settings

1. Right-click the local client in the System Explorer and select **Setup** to open the client Setup dialog box.
   For more information, see Accessing the Client Setup.
2. Click **Import Settings**.
3. In the Select File to Import From dialog box, browse to the settings file you want to import, and click **Open**.
4. Select the specific settings you want to import.

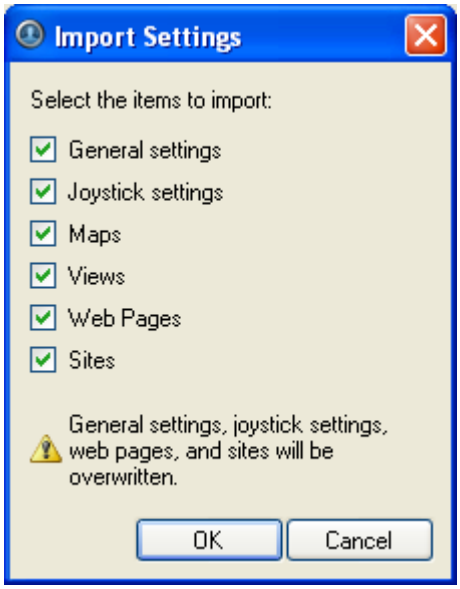


Figure A. Import Settings dialog box

5. Click **OK**.

Views

What are Views?

A View is a tab composed of image panels that allow you to organize how video is monitored.

For example, you can choose to monitor video from multiple cameras simultaneously by using different layouts.

Adding and Removing a View

Views allow you to customize how you monitor video. You can add a new View to an existing window or open a new View in its own window to make use of multiple monitors. Views can also be removed as required.

Adding a New View to the Application Window

Perform one of the following to open a new View in the application window:

- Select **File > New View**.
- From the toolbar, click the  **New View** button.

Adding a View to a New Window

Perform one of the following to open a new View window.

- Select **File > New Window**.
- From the toolbar, click the  **New Window** button.

A new window appears. You can now position this window to make use of multiple monitors.

Closing a View from the Application Window

Perform one of the following to remove a View from the application window:

- Select **File > Close View**.
- On the View tab, click the red **Close View** button.

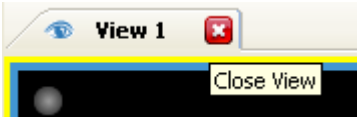


Figure A. Close View button

Closing a Window

- Select **File > Close Window**.

Selecting a Layout for a View

You can organize how video from multiple cameras are displayed by selecting a View layout.

- Select **View > Layouts > # Division**.
- On the toolbar, select one of the layout options.

Figure A. Layouts on the Toolbar

Making a View Full Screen

You can enlarge a View to maximize the use of the monitor.

Making a View Full Screen

- On the toolbar, click  **Full Screen**.

Ending Full Screen

- On the toolbar at the top left of the screen, click 

.

Tip: The toolbar is hidden when the application is idle. Move your mouse to display the toolbar.

Cycling Through Views

Once you have multiple Views setup, you can cycle through the Views by displaying each for a few seconds. This is useful when monitoring a large number of cameras.

1. Activate the Cycle Tab function by performing one of the following:
    - From the View menu, select **Cycle Views**.
    - On the toolbar, click  **Cycle Views**.

If required, the cycle dwell time can be changed, see Changing General Client Settings for more information.

Saving a View

Once you have set up a particular View, you can save the View for use again in the future. A saved View records the View layout, the cameras displayed in each image panel, and the image panel display settings.

Saving a View

1. Select **File > Save View**.
2. In the Save As dialog box, name the View and click **OK**.

Your saved view will appear in the System Explorer.

Figure A. Saved Views

Opening a saved View

Perform one of the following

- In the System Explorer, right-click the saved View and select **Open**.
- Drag the saved View from the System Explorer to the current View in the application or new window.

Renaming a saved View

1. In the System Explorer, right-click the saved View and select **Rename**.
2. In the Rename View dialog box, enter a new name and click **OK**.

Deleting a saved View

1. In the System Explorer, right-click the saved View and select **Delete**.
2. In the confirmation dialog box, click **Yes**.

Video

The Avigilon Control Center Client software allows you to view multiple live and recorded video streams in a View, while giving you control of PTZ cameras, digital zoom, audio, manual recording, digital outputs, and other playback settings.

To watch a video of the application's video features, see *Module 1 - Introduction to Avigilon Control Center Client and Viewing Live Video* and *Module 2 - Identifying, Bookmarking, Searching and Exporting Video* in the Avigilon University - End User Stream.

Note: Some features are not displayed if the server does not have the required license, or if you do not have the user permissions to access the feature.

Viewing Live Video

While viewing live video, you can perform any of the following procedures.

Adding and Removing Cameras in a View

To view a camera's video, display the camera in a View. The video can be removed from the View when it is no longer needed.

Adding a Camera to a View

Perform one of the following:

- Drag the camera from the System Explorer pane to an empty image panel in a View.
- In the System Explorer, right-click the camera and select **Add to View**.

  The camera is added to the next empty image panel in the View layout.

Tip: You can drag the same camera to multiple image panels to view the images at different zoom levels or with different video adjustment properties.

Removing a Camera From a View

Perform one of the following:

- Right-click the image panel, and select **Close**.
- Inside the image panel, click  **Close**.

Displaying Live Video

Once a camera video has been added to an image panel, you can choose to view the live video stream. You can set the entire View to display live video, or only set specific image panels to display live video.

Live video is indicated by a blue border around the image panel.

- To display live video in a View, perform one of the following:
  - Select **View > Live**.
  - On the toolbar, select 

.
- To switch an individual image panel to view live video, right-click the image panel and select **Live**.

Zooming and Panning a Video

The zoom and pan tools allow you to focus on specific regions in a camera video.

Using the Zoom Tools

You can rotate the scroll wheel on your mouse to zoom in and out of a video image. Or you can use the Zoom tools in the application:

1. Select a Zoom tool:
   - From the **Tools** menu, select **Zoom In Tool** or **Zoom Out Tool**.
   - On the toolbar, click  **Zoom In Tool** or  **Zoom Out Tool**.
2. Click the image panel until you reach the desired zoom depth.

Using the Pan Tools

You can right-click and drag inside an image panel to pan the video image, or you can perform the following:

1. Select the Pan tool:
    - From the Tools menu, select **Pan Tool**.
    - On the toolbar, click the **Pan Tool**.
2. Drag the video image in any direction inside the image panel.

Controlling PTZ Cameras

Pan, Tilt, Zoom (PTZ) controls allow you to control cameras with PTZ functionality. You can control a PTZ camera by using the onscreen controls or by using the tools in the PTZ Controls pane.

1. To display the PTZ Controls pane, perform one of the following:
    - From the **Tools** menu, select **PTZ Controls**.
    - On the toolbar, click **PTZ Controls**.

    The PTZ Controls pane is displayed on the left, below the System Explorer.

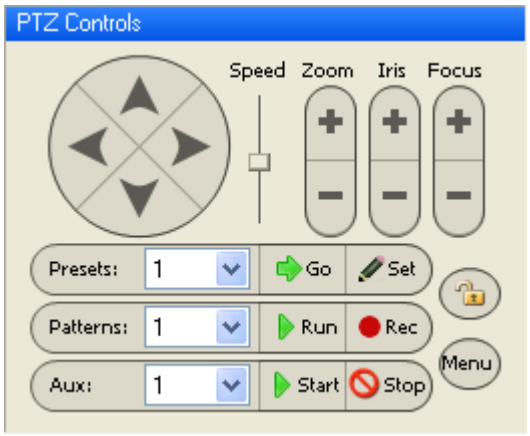


Figure A. PTZ Controls

2. Display the video from a PTZ camera in the current View.
3. To pan or tilt, perform one of the following:
    - Drag the mouse pointer in the direction that you want to move the camera. The further the mouse is from the center of the image panel, the faster the camera will move.

- Click the **Pan/Tilt** arrow buttons in the PTZ Controls pane. The speed for all pan/tilt movements can be adjusted using the **Speed** slider.

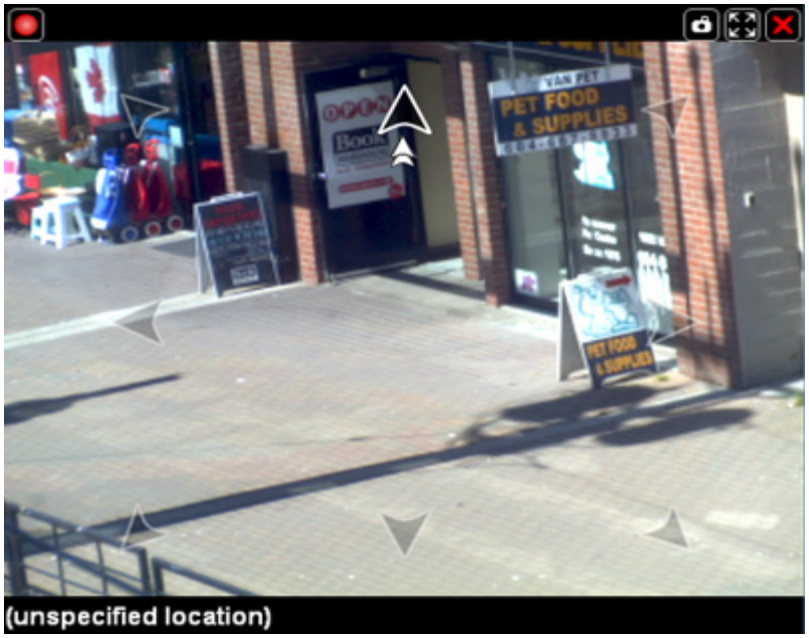
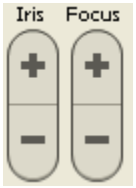


Figure B. PTZ On-Screen Controls

4. Use the other PTZ controls to perform any of the following:

Action	Control	Procedure
To zoom		Perform one of the following: • Click on the zoom controls in the PTZ Controls area. • Click the image panel and use the mouse scroll wheel to zoom in and out.
To control the **Iris** or **Focus**		Click the **+** and **-** buttons.
To program a PTZ preset		1. Use the PTZ buttons to move the camera field-of-view to the desired position. 2. In the PTZ Controls pane, select a preset number and click **Set**.

To activate a PTZ preset		Select a preset number and click **Go**.
To program a PTZ pattern		1. In the PTZ Controls pane, select a pattern number and click **Rec**. 2. Use the PTZ controls to initiate a series of camera movements. 3. In the PTZ Controls pane, click **Stop**.
To activate a PTZ pattern		In the PTZ Controls pane, select a pattern number and click **Run**. The pattern will repeat until the pattern is stopped or another pattern is set.
To activate an auxiliary command		1. Select an command number and click **Start** to initiate the auxiliary output. 2. Click **Stop** to turn off the auxiliary output.
To display the PTZ camera onscreen menu		1. Click the **Menu** button. 2. In the PTZ Controls pane, use the pan/tilt controls to navigate the menu. Use the **Pan/Tilt** buttons to navigate the menu. Use the **Zoom** buttons to modify your selection choices. Use the **Focus** buttons to confirm or cancel your selections.
To lock the PTZ controls		Click the **Lock** button. No other user will be able to use the PTZ controls for the selected camera until you unlock the

		controls or log out.

Listening to Audio in a View

If there is a microphone linked to a camera, the Audio bar is displayed in the image panel when you view the camera's video.

Note: This feature is only available if there is a microphone and a Audio Channel License installed.

To control the audio settings, perform any of the following:

- In the lower-right corner of the image panel, click the **Speaker** icon to mute or activate the audio.
- Move the slider to change the volume level.

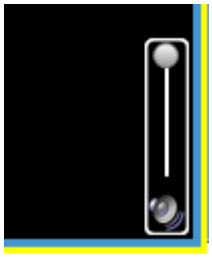
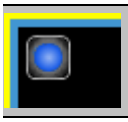
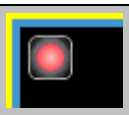
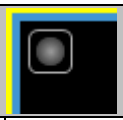


Figure A. Audio bar

Triggering Manual Recording

When viewing live video, you can click the **Manual Recording** icon to force the camera to record the current video stream regardless of the camera's recording schedule.

The **Recorder Indicator** overlay must be enabled for manual recording to function. See Overlaying Information on the Image Panel for more information.

		
If the icon is blue, it is in Continuous Recording mode.	If the icon is red, an event has caused the camera to begin recording.	If the icon is grey, the camera is not recording.

Starting Manual Recording

- In the top-left corner of the image panel, click the record indicator to start manual recording.

Figure A. Manual Recording indicator

The record indicator is highlighted in blue to indicate that the camera is recording. Manual recording continues until it is stopped, or until the maximum recording duration is reached. The maximum duration is configured in the Manual Recording dialog box, see Manual Recording Settings for more information.

Stopping Manual Recording

- In the top-left corner of the image panel, click the record indicator to stop manual recording.

Figure B. Manual Recording indicator

Triggering Digital Output

While you view live video in an image panel, you can manually trigger any digital output that is linked to the camera.

The digital output is configured in the Digital Inputs and Outputs dialog box, see Setting Up Digital Outputs for more information.

1. Open the camera's live video in an image panel.
2. In the image panel, click  **Trigger Digital Output**.
3. If you have more than one digital output linked to the camera, you will be prompted to select the digital output you want to trigger.

Viewing Recorded Video

While viewing recorded video, you can perform any of the following procedures:

Adding and Removing Cameras in a View

To view a camera's video, display the camera in a View. The video can be removed from the View when it is no longer needed.

Adding a Camera to a View

Perform one of the following:

- Drag the camera from the System Explorer pane to an empty image panel in a View.
- In the System Explorer, right-click the camera and select **Add to View**.

  The camera is added to the next empty image panel in the View layout.

Tip: You can drag the same camera to multiple image panels to view the images at different zoom levels or with different video adjustment properties.

Removing a Camera From a View

Perform one of the following:

- Right-click the image panel, and select **Close**.
- Inside the image panel, click  **Close**.

Displaying Recorded Video

Once a camera video has been added to an image panel, you can choose to view the camera's recorded video. You can set the entire View to display recorded video, or only set specific image panels to display recorded video.

Recorded video is indicated by a green border around the image panel.

- To display recorded video in a View, perform one of the following:
  - Select **View > Recorded**.
  - On the toolbar, select 

.
- To switch an individual image panel to view recorded video, right-click the image panel and select **Recorded**.

Zooming and Panning a Video

The zoom and pan tools allow you to focus on specific regions in a camera video.

Using the Zoom Tools

You can rotate the scroll wheel on your mouse to zoom in and out of a video image. Or you can use the Zoom tools in the application:

1. Select a Zoom tool:
    - From the **Tools** menu, select **Zoom In Tool** or **Zoom Out Tool**.
    - On the toolbar, click  **Zoom In Tool** or  **Zoom Out Tool**.
2. Click the image panel until you reach the desired zoom depth.

Using the Pan Tools

You can right-click and drag inside an image panel to pan the video image, or you can perform the following:

1. Select the Pan tool:
    - From the Tools menu, select **Pan Tool**.
    - On the toolbar, click the  **Pan Tool**.
2. Drag the video image in any direction inside the image panel.

Listening to Audio in a View

If there is a microphone linked to a camera, the Audio bar is displayed in the image panel when you view the camera's video.

Note: This feature is only available if there is a microphone and a Audio Channel License installed.

To control the audio settings, perform any of the following:

- In the lower-right corner of the image panel, click the **Speaker** icon to mute or activate the audio.
- Move the slider to change the volume level.

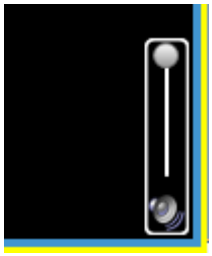


Figure A. Audio bar

Playing Back Recorded Video

The Timeline displays the time period when video were recorded and provides several controls for playing back the recordings.

The colored bars on the Timeline display a camera's recording history:

- A red bar indicates the camera recorded an event.
- A blue bar indicates the camera recorded video, but not in response to any event.
- White areas indicate that the camera did not record any video.
- An orange bar indicates a bookmark in the camera's recording history.

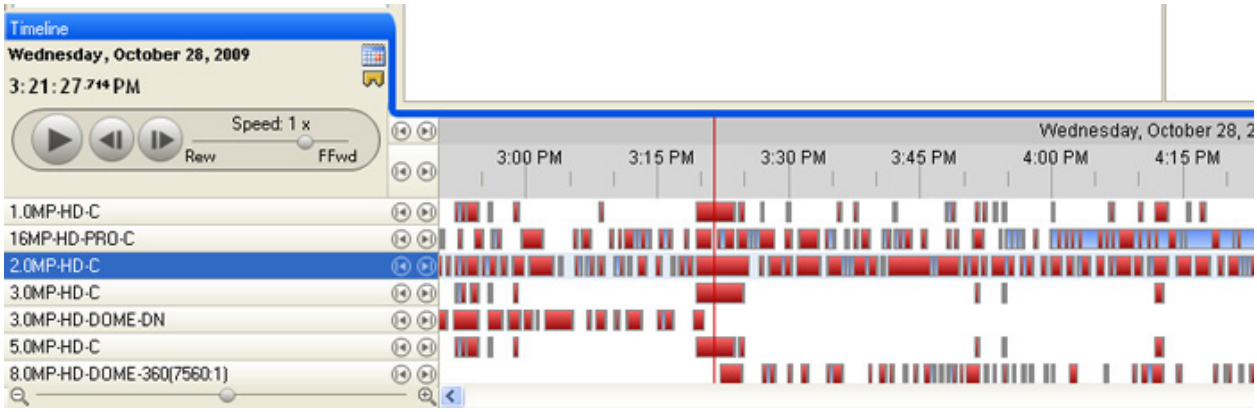
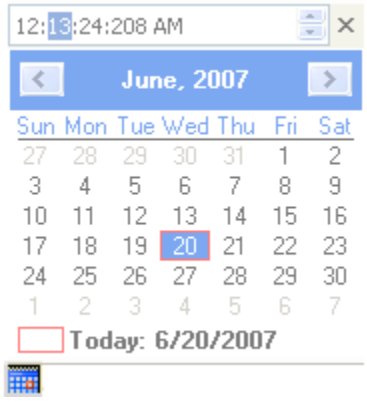
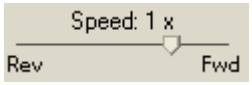
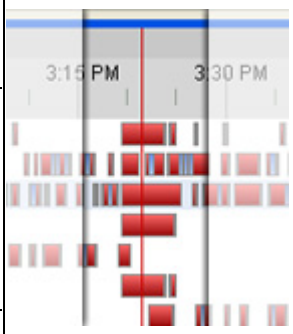


Figure A. Playback tools on the Timeline

Perform any of the following actions to control the playback of recorded video files:

Action	Tool	Procedure
To select a playback time		Perform one of the following: • Click the calendar and select a date and time. • On the Timeline, click on an area with recorded data indicated by a colored bar.
To add a		Click **Add Bookmark** to add a bookmark on the

bookmark		Timeline. See Bookmarking Recorded Video for more information.
To start playback		Click **Play**.
To stop playback		Click **Pause**.
To move forward a frame		Click **Step Forward**.
To move back a frame		Click **Step Backward**.
To control the playback direction and speed		Click and drag the slider to the right to move the video forward, or to the left to move the video in reverse. The further the slider is away from the center the faster the playback speed.
To jump forward or back on the Timeline		On the Timeline, click one of the **Go Forward** or **Go Back** buttons to move to different points on the Timeline.
To expand the Timeline to a specific moment in time		Perform one of the following: • Move the slider to zoom in or zoom out on the Timeline. • You can also use the mouse scroll wheel to zoom in or zoom out on the Timeline.
To center the Timeline on the time marker		Right-click the Timeline, and select **Center on Marker.**
To move through the Timeline quickly with the time marker		Drag the time marker through the Timeline.
To pan the Timeline		Perform one of the following:

		• Move the Timeline horizontal scroll bar at the bottom of the application window. • Right-click and drag the Timeline.

Bookmarking Recorded Video

You can add bookmarks to help identify segments of recorded video. Bookmarked video can be protected against scheduled data cleanup so the video is never deleted.

Adding a bookmark

1. To open the Edit Bookmark dialog box, perform one of the following:
   - On the Timeline, click **Add Bookmark**.
   - Drag the time marker to the beginning of the time you want to bookmark, then right-click and select **Add Bookmark**.

   The Edit Bookmark dialog box appears, and the bookmark time range is highlighted on the Timeline

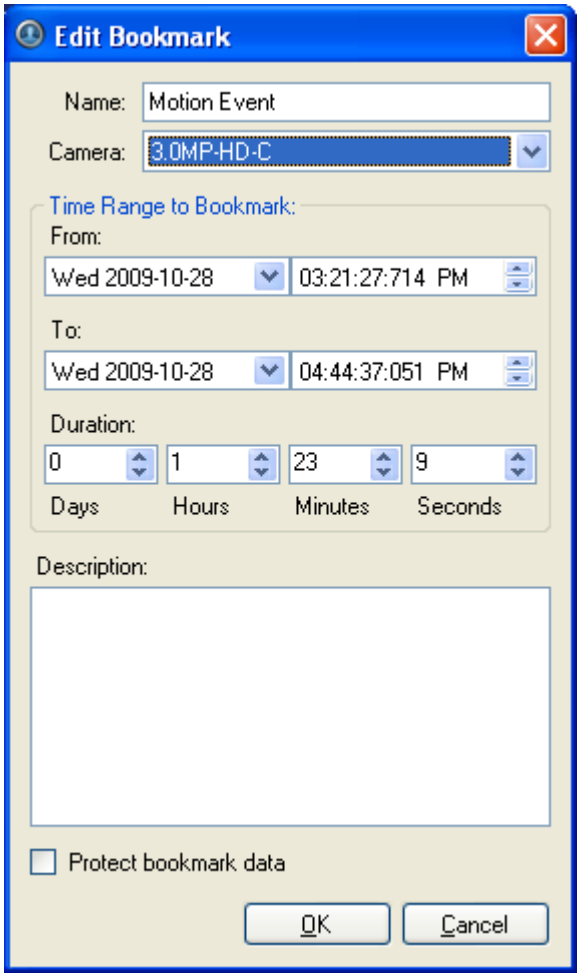


Figure A. Add Bookmark dialog box

2. In the **Name** field, enter a name for the bookmark.
3. In the **Camera** drop down list, select the camera the bookmark is attached to.
4. In the Time Range to Bookmark area, enter the time period you want to bookmark.

   You can also move the black time range markers on the Timeline to adjust the time range.
5. In the **Description** field, enter any required information about the bookmark.
6. To protect the bookmark data from deletion select the **Protect bookmark data** check box.

   Note: Protected bookmarks are never deleted. Be aware that bookmarked video occupy space on the server and become the oldest stored video.
7. Click **OK**.

Editing, deleting or exporting a bookmark

1. Click the bookmark on the Timeline then perform one of the following:

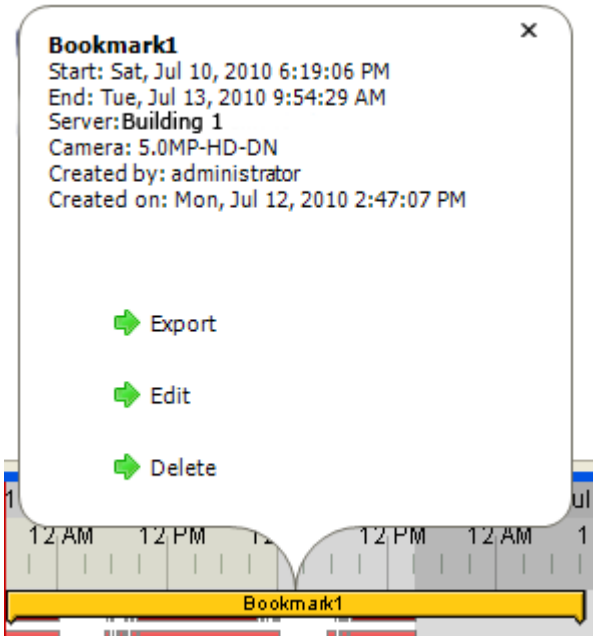


Figure B. Bookmark properties

To	Do this...
Edit a bookmark	Click **Edit** then make the necessary changes to the Edit Bookmark dialog box and click **OK**. Refer to the Adding a Bookmark procedure for details about the Edit Bookmark dialog box.
Delete a bookmark	Click **Delete**. When the confirmation dialog box appears, click **Yes**.
Export a bookmark	Click **Export** then complete the Export tab. See Exporting Recorded Video and Images for more information.

Adjusting Video Display in Image Panels

You can adjust the image panel display settings to enhance the video display on your monitor.

Maximizing an Image Panel

You can enlarge an image panel to help magnify the video displayed.

Maximizing an Image Panel

Perform one of the following:

- Right-click an image panel and select **Maximize**.
- Inside the image panel, click  **Maximize**.
- Double-click the image panel.

Restoring an Image Panel

Perform one of the following:

- Right-click the maximized image panel, and select **Restore Down**.
- Inside the image panel, click  **Restore Down**.
- Double-click the image panel.

Displaying Video Overlays

When you monitor video in a View, you can select the type of information that is displayed over the video in each image panel.

- Select **View > Image Overlays**, then select one or more of the following:

Option	Description
Camera Name	Displays the name given to the camera.
Camera Location	Displays the location given to the camera.
Timestamp	Displays the exposure timestamp of the video. The timestamp only appears when viewing recorded video.
Record Indicator	Displays the recording status of a camera. The recording status is indicated by the round **Record Indicator** icon on the top left corner of the image panel. The Record Indicator only appears when viewing live video. The color of the icon indicates the camera's recording status. ▪ Red: recording because an event occurred ▪ Blue: recording ▪ Grey: not recording Select the **Record Indicator** icon at any time to begin manual recording.
PTZ Controls	Displays the controls for controlling PTZ cameras on the video image.

Motion Activity	Highlights detected motion events in red.

Changing the Display Quality

If you do not have sufficient network bandwidth or processing power, you may not be able to view video at the full image rate and full quality. You can bias the image panels to display video in high quality/low frame rate or low quality/high frame rate.

The Change Display Quality settings only affect the image panel display and does not affect the actual video quality or image rate transmitted between the camera and the server. To modify the camera's display settings, see Compression and Image Rate settings.

1. Open the Change Display Quality dialog box:
   - Select **Tools > Change Display Quality...**.
   - In the toolbar, click  **Change Display Quality**.
2. In the Change Display Quality dialog box, select one of the following:

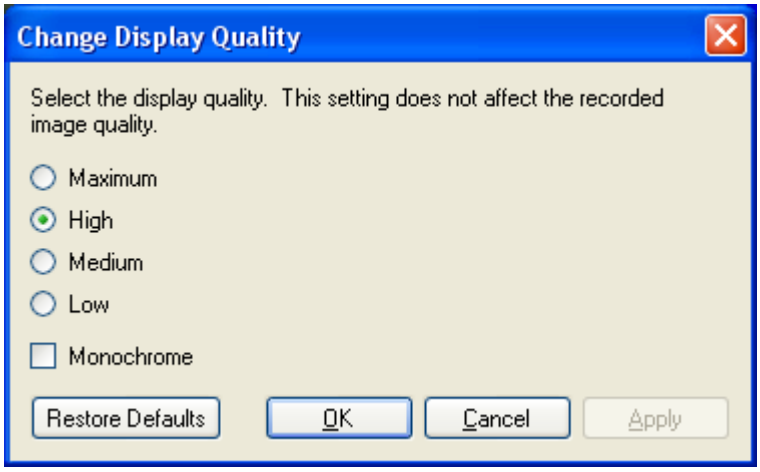


Figure A. Change Display Quality dialog box

   - **Maximum:** displays the full video quality and results in lowest displayed image rate.
   - **High:** displays 1/4 of the full video resolution.
   - **Medium:** displays 1/16 of the full video resolution.
   - **Low:** displays 1/64 of the full video resolution and results in the highest displayed image rate.
3. Select the **Monochrome** check box to display the video in black and white.
4. Click **OK**.

Changing the Image Panel Display Settings

You can change the image panel display settings to bring out video details that are hard to see with the image panel's default settings.

Note: These settings only affect the image panel display and do not affect the camera's actual configuration.

1. Right-click an image panel and select **Display Adjustments...**.

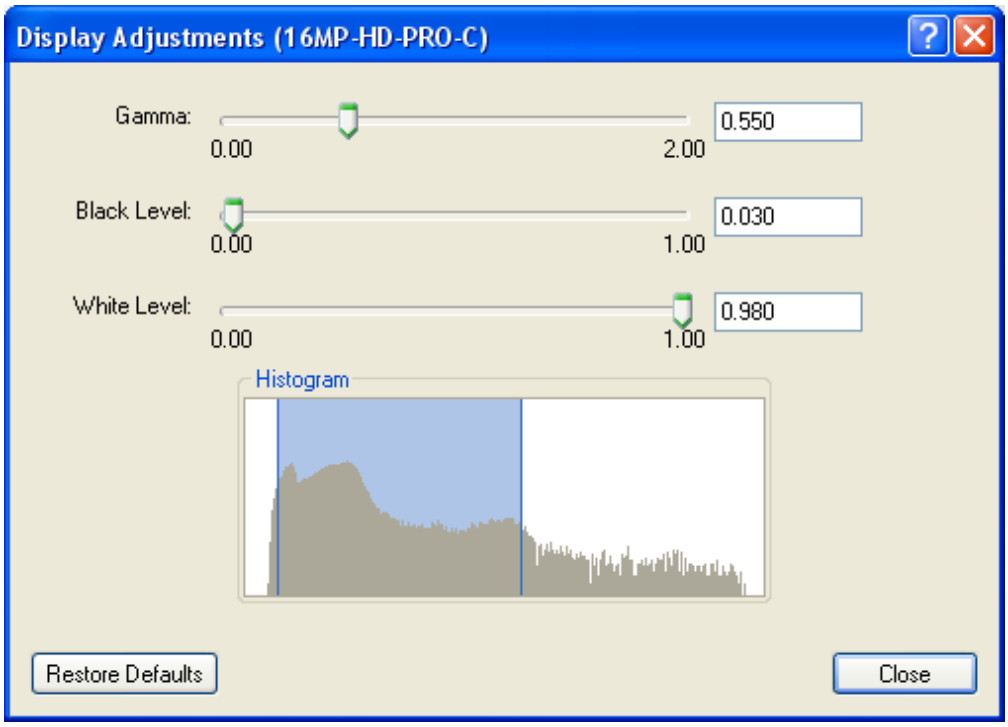


Figure A. Display Adjustments dialog box

2. Move the sliders to adjust the **Gamma**, **Black Level** and **White Level**.

   The image panel displays a preview of your adjustments.

3. Click **Restore Defaults** to clear your changes.

4. Click **Close**.

Viewing Analog Video in Deinterlaced Mode

If there are visible interlacing artifacts in the analog camera video, you can enable the deinterlacing filter to help improve the video image.

- To enable the deinterlacing filter, select **View > Display Deinterlaced Images**.

Search

You can search for recorded video by events, thumbnails or POS transactions.

To watch a video overview of the Search features, see *Module 2 - Identifying, Bookmarking, Searching and Exporting Video* in the Avigilon University - End User Stream.

Note: Some features are not displayed if the server does not have the required license, or if you do not have the user permissions to access the feature.

Performing an Event Search

The Event Search allows you to search for a specific motion or digital input event by time range for the selected cameras.

1. Click 

to open the Search tab.
2. In the Search tab, select **Event Search**.

   The Search:Event tab is displayed.

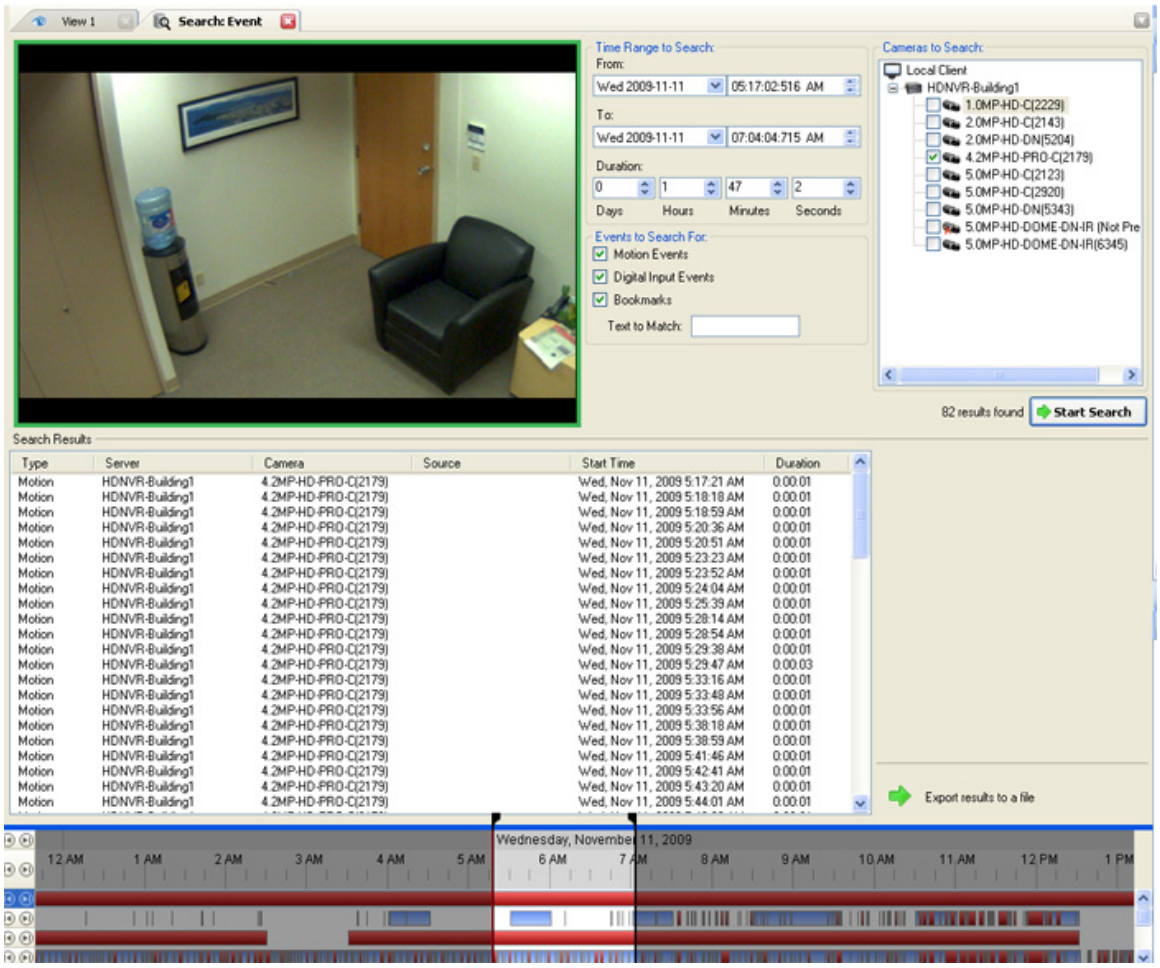


Figure A. Search: Event tab

3. In the Camera to Search area, select all the cameras you want to include in the search.
4. In the Time Range to Search area, set the date and time range of your search. The time range is highlighted on the Timeline by the black time range markers. You can also drag the time range markers to modify the time range.
5. In the Events to Search For area, select the types of events or bookmarks to include in the search.
6. In the Text to Match area, enter text to search for in the titles and descriptions of bookmarks.
7. Click **Start Search**.

Viewing Event Search Results

1. In the Search Results area, select a search result. The event timeline is highlighted and the related video is displayed in the search image panel.

2. Use the Timeline controls to review the event. See Playing Back Recorded Video for more information.
3. If you want to further refine your search, click **Perform a pixel search on this event** to perform a pixel search on the selected result. See Performing a Pixel Search for more information.
4. Click **Export this event** to export the selected event video. See Exporting Recorded Video and Images for more information about the available export settings.
5. To export all listed results, click **Export results to a file** and save the file.

Performing a Pixel Search

The Pixel Search allows you to search for motion events in specific areas of the camera's field of view.

1. Click 

to open the Search tab.
2. In the Search tab, select **Pixel Search**.

   The Search:Pixel tab displays.

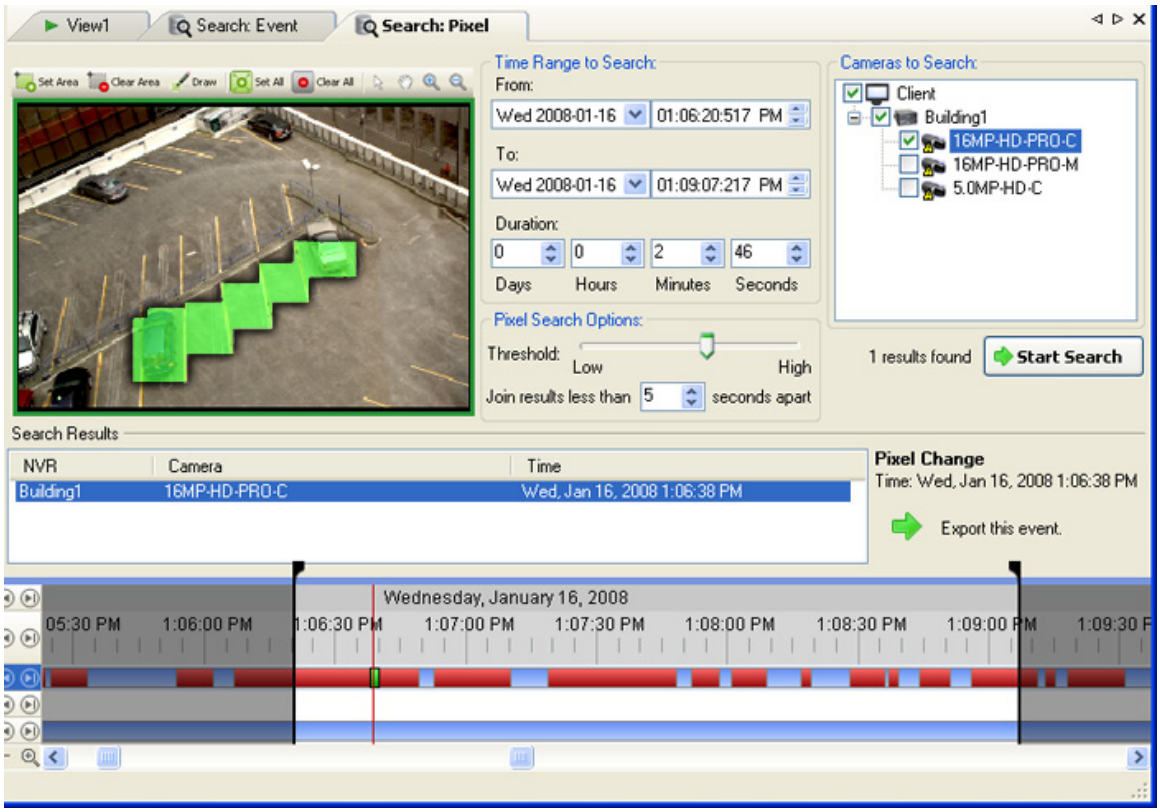


Figure A. Search:Pixel tab

By default, the entire video image is highlighted in green.

3. In the Camera to Search area, select a camera.
4. In the Time Range to Search area, set the date and time range of your search. The time range is highlighted on the Timeline by the black time range markers. You can also drag the time range markers to modify the time range.
5. Define the pixel search region by using the motion detection selection tools above the image panel. The pixel search will be performed in all areas highlighted in green.
6. In the Pixel Search Options area, drag the **Threshold** slider to select the amount of motion required to return a search result.

   The higher the threshold, the greater number of pixels must change before a result is returned.
7. Enter a number in the **Join results less than** field to define the minimum number of seconds between motion events before they are considered separate search results.
8. Click **Start Search**.

Viewing Pixel Search Results

1. In the Search Results area, select a search result. The event timeline is highlighted and the related video is displayed in the search image panel.
2. Use the Timeline controls to review the event. See Playing Back Recorded Video for more information.
3. Click **Export this event** to export the selected event video. See Exporting Recorded Video and Images for more information about the available export settings.
4. To export all listed results, click **Export results to a file** and save the file.

Performing a Thumbnail Search

The Thumbnail Search allows you to search through a specific period of time by viewing a series of thumbnail images.

1. Click 

to open the Search tab.
2. In the Search tab, select **Thumbnail Search**.

   The Search:Thumbnails tab displays.

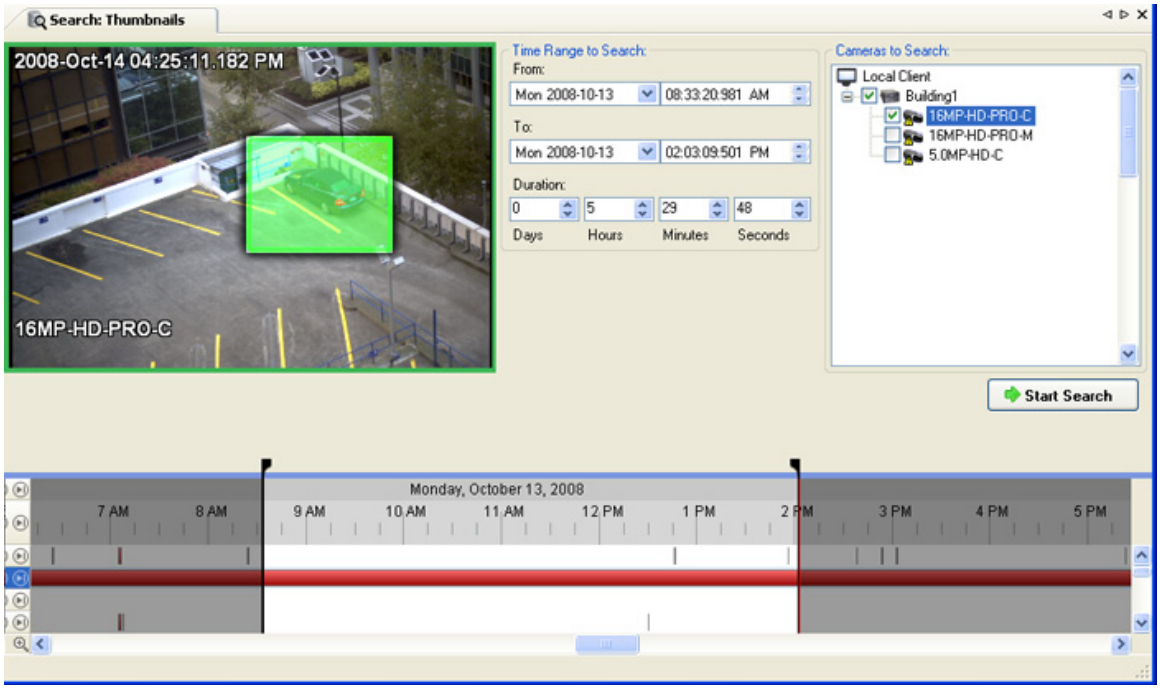


Figure A. Search:Thumbnails tab

3. In the Camera to Search area, select a camera.
4. In the Time Range to Search area, set the date and time range of your search. The time range is highlighted on the Timeline by the black time range markers. You can also drag the time range markers to modify the time range.
5. In the image panel, define the search region by moving the edges of the green overlay. Use this feature if you only want to see thumbnails for a region of the video image instead of the whole field of view.

   The thumbnail search will only be performed on the area highlighted in green.
6. Click **Start Search**.

Viewing Thumbnail Search Results

The search results display thumbnails at equal intervals on the Timeline.

1. To change the size of the search result thumbnails, select **Large Thumbnails**, **Medium Thumbnails**, or **Small Thumbnails** from the drop-down menu above the search results and click **Search Again**.

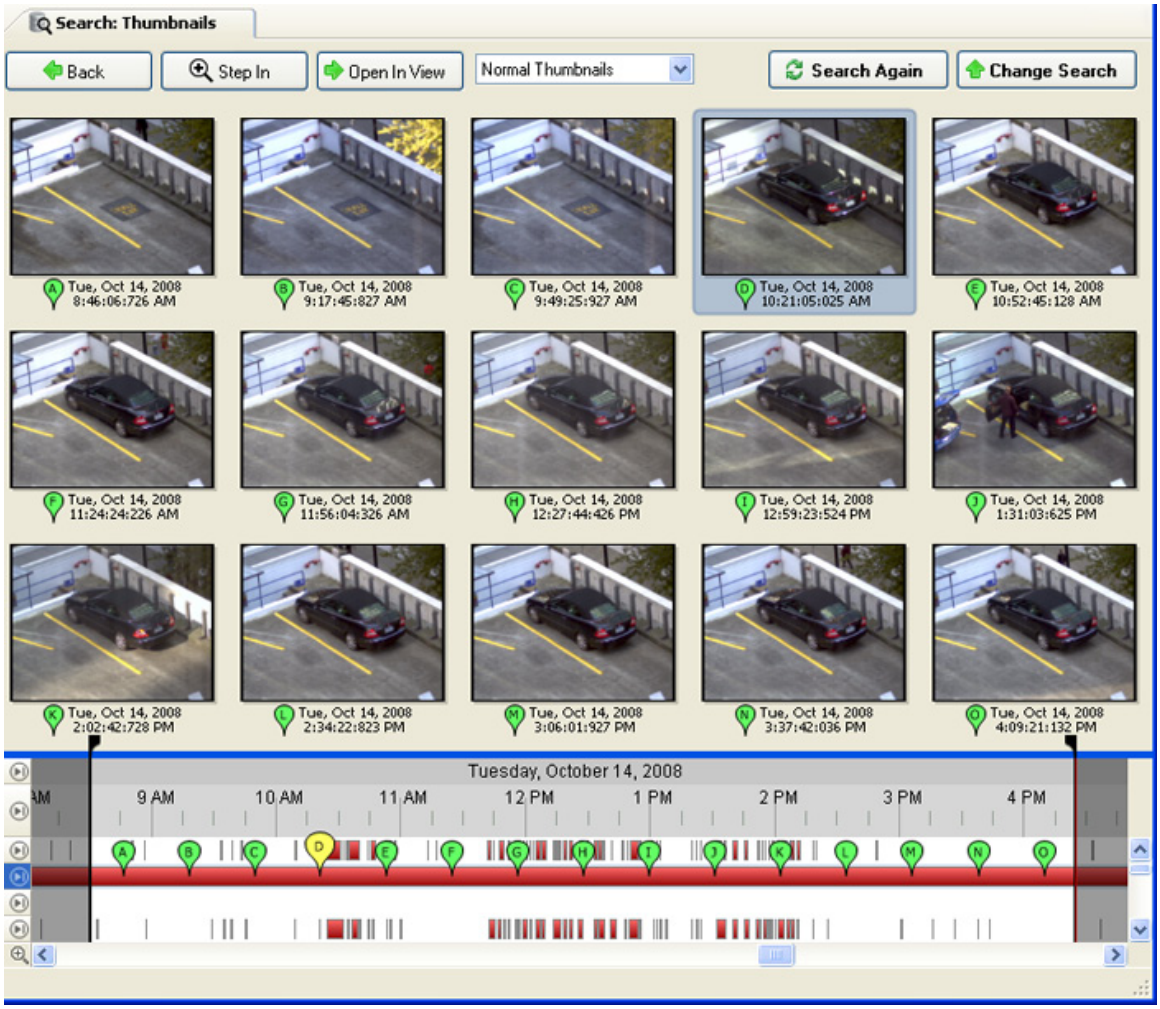


Figure B. Search:Thumbnail results tab

2. Select a thumbnail to highlight the image on the Timeline.
3. Click **Step In**, or double-click the thumbnail to perform another search around the thumbnail.

   Click **Back** to return to the previous results page.
4. Click **Open In View** to open the recorded video in a new View.

Performing a POS Transaction Search

The POS Transaction Search allows you to search for POS transactions by transaction data source, content in the raw transaction data, and time range.

1. Click 

to open the Search tab.

2. In the Search tab, select **POS Transactions Search**.

   The Search: POS Transactions tab is displayed.

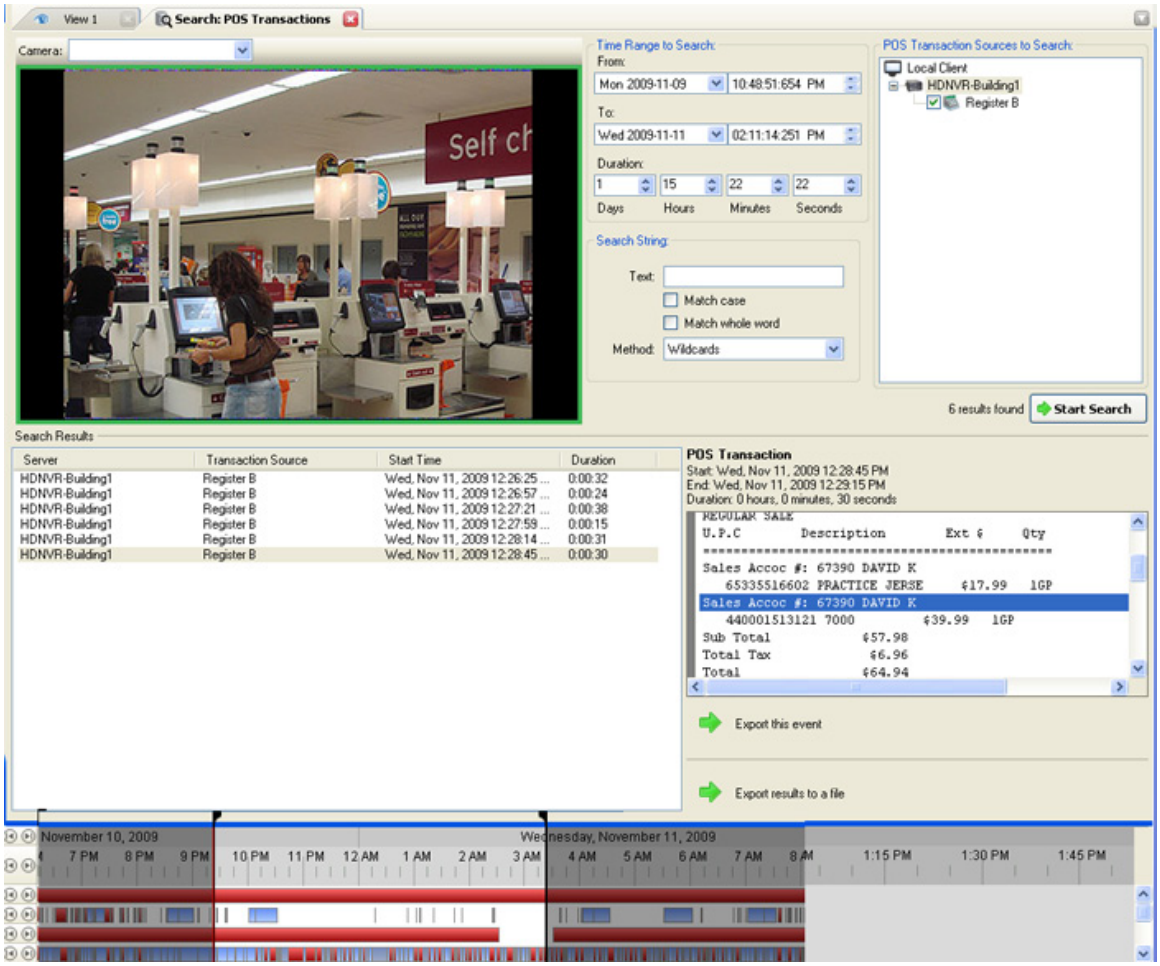


Figure A. Search:POS Transactions tab

3. In the POS Transaction Sources to Search area, select all the POS transaction sources you would like to include in the search.

4. In the Time Range to Search area, set the date and time range of your search. The time range is highlighted on the Timeline by the black time range markers. You can also drag the time range markers to modify the time range.

5. In the Search Text area, enter any text you want to search for, then select **Match case** and/or **Match whole word**, and choose a search method.

   Leave the **Text** field blank to find all transactions.

6. Click **Start Search**.

Viewing POS Transaction Search Results

1. In the Search Results area, select a search result. The event timeline is highlighted and the related video is displayed in the search image panel.
2. Use the Timeline controls to review the event. See Playing Back Recorded Video for more information.
3. If the event is linked to multiple cameras, select a camera from the **Camera** drop down list to change the video displayed in the image panel.
4. Click **Export this event** to export the selected event video. See Exporting Recorded Video and Images for more information about the available export settings.
5. To export all listed results, click **Export results to a file** and save the file.

Export

You can export video and still images. You can specify a number of options to ensure the exported files are appropriate for your needs.

To watch a video overview of the Export features, see *Module 2 - Identifying, Bookmarking, Searching and Exporting Video* in the Avigilon University - End User Stream.

Note: Some features are not displayed if the server does not have the required license, or if you do not have the user permissions to access the feature.

Saving a Snapshot of an Image

A Snapshot allows you to export a single frame in a video. You can specify the file format and various options, like overlays and resolution.

1. Open the snapshot Export tab:

   - In the image panel, click the  **Save Snapshot** icon.
   - Right-click the image panel and select **Save Snapshot**.

   The snapshot Export tab is displayed.

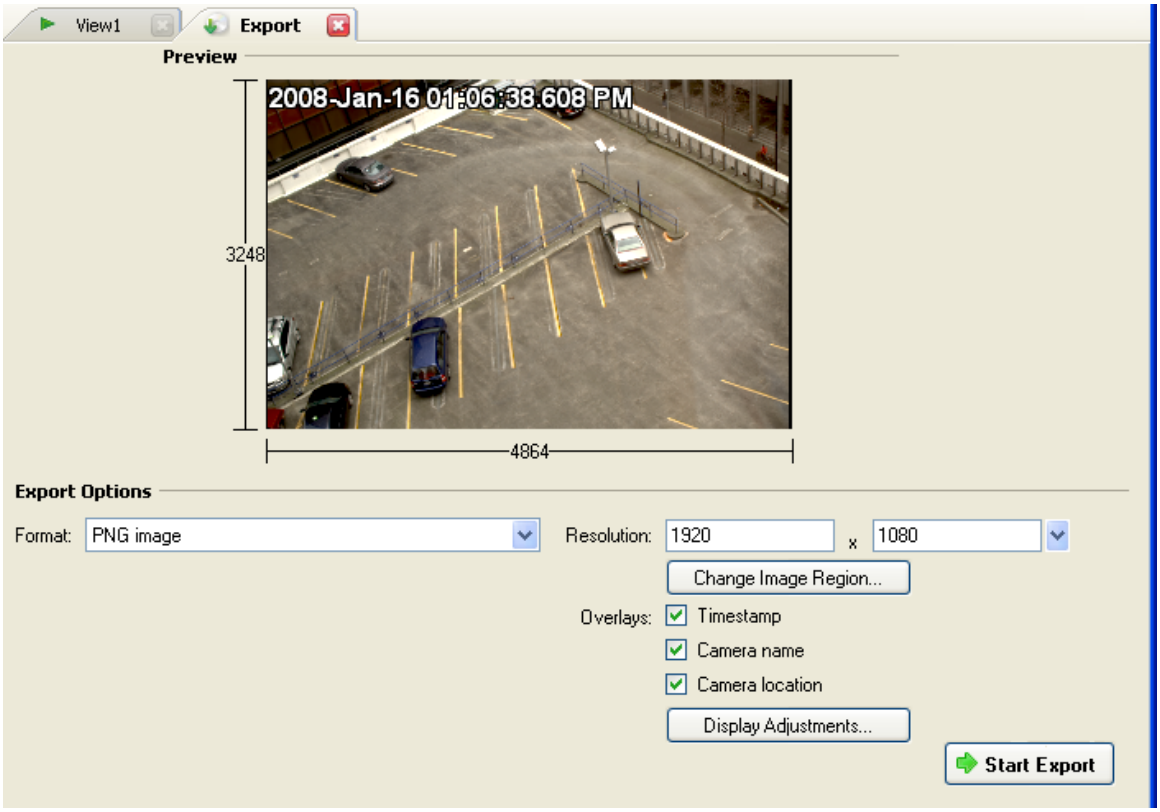


Figure A. Export tab for Snapshot export

2. In the Export Options area, select the image export format from the **Format** drop down list: **PNG**, **JPEG**, **TIFF**, **PDF**, **Print**, or **Native** format.

3. For the selected export image format, define your preferences:

Format	Image options
Native **Note:** The Native format requires the Avigilon Control Center Player to view.	This is the recommended export format because the exported image maintains original compression and can be authenticated against tampering in the Avigilon Control Center Player. ▪ Select the **Export the Control Center Player Installer** check box if you want a copy of the Avigilon Control Center Player to be distributed with your native image file.
PNG	1. In the **Resolution** field, select a resolution for the video image. You can manually enter the resolution or click the drop down arrow to select a standard resolution. **Note:** The **Resolution** field automatically maintains the image aspect ratio. 2. Click **Change Image Region...** to change the region of the video image that is exported.

	In the Change Image Region dialog box, modify the size and position of the green overlay, then click **OK**. The Preview image panel will show the modified image region. 3. Select the required image overlays: **Timestamp**, **Camera name**, and **Camera location**. 4. Click **Display Adjustments** to adjust the Gamma, Black Level and/or White Level.
JPEG	1. In the **Compression** field, select a compression level. 2. Set the image **Resolution**. 3. Click **Change Image Region** to only export a specific region of the image. 4. Select the required image overlays. 5. Click **Display Adjustments** to modify the image quality.
TIFF	1. Set the image **Resolution**. 2. Click **Change Image Region** to only export a specific region of the image. 3. Select the required image overlays. 4. Click **Display Adjustments** to modify the image quality.
Print	1. Click **Change Image Region** to only export a specific region of the image. 2. Click **Printer Settings...** to change the selected printer and paper size. 3. Select the required image overlays. 4. Click **Add Export Notes...** to add notes about the exported image. The notes are printed below the exported image. 5. Click **Display Adjustments** to modify the image quality.
PDF	1. Click **Change Image Region** to only export a specific region of the image. 2. Select the required image overlays.

	3. Click **Add Export Notes...** to add notes about the exported image. 4. Click **Display Adjustments** to modify the image quality.

4. Click **Start Export**.
5. In the Save As dialog box, name the export file and click **Save**.

   The Preview area displays the video stream you are exporting.
6. When the export is complete, click **OK**.

Exporting Recorded Video and Images

You can export recorded video and still images that are stored on the server.

Note: Only recorded video can be exported in video format.

Accessing the Export Tab

The Export tab can be accessed in any of the following ways:

- Select **File > Export**.
- On the toolbar, click 

.
- When searching for a specific video image, select a search result and click **Export this event**.
- When viewing bookmarked video, right-click a bookmark on the Timeline and select **Export**.

Exporting Native Video

When you export video files, you can choose to export the video in the Native (AVE) format.

The AVE format is the recommended format for exporting video because you can export video from multiple cameras in a single file, and the video maintains its original compression. AVE video can be played in the Avigilon Control Center Player, where the video can be authenticated against tampering and be re-exported to other formats.

1. Click 

to open the Export tab. For more information, see Accessing the Export Tab.

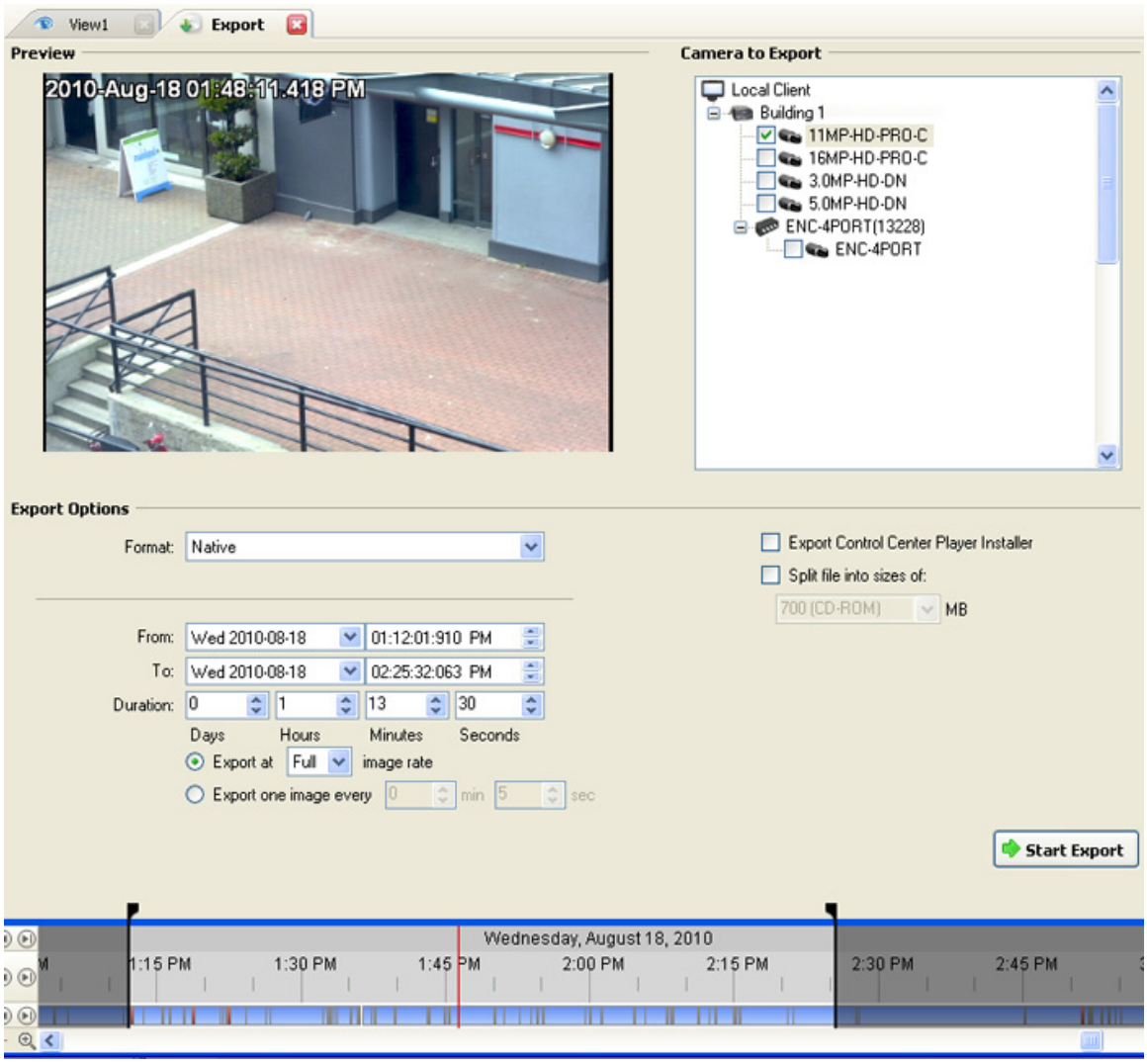


Figure A. Export tab for recorded video export

2. In the **Format** drop down list, select **Native**.
3. In the Camera to Export list, select all the camera video you want to export.
4. Enter the time range in the **From**, **To**, **Duration** fields. The time range is highlighted on the Timeline by black time range markers. You can also drag the time range markers to modify the time range.
5. Set the export image rate:

Option	Description
Export at __ image rate	Select this option to control how many images per second are exported. For example, the video is streaming at 30 images per second. If you select **1/2**, only 15 images for that second will be exported.

Export one image every __ min __sec	Select this option to control the time interval between each exported video image. For example, if you enter *5* min. *0* sec., only one image will be exported every 5 minutes.

6. Select the **Export the Control Center Player Installer** if you want a copy of the Avigilon Control Center Player to distribute with the AVE video file.
7. Select the **Split file into sizes of:** check box to split the exported file into smaller files so the exported files can be stored on optical media, like a CD or DVD.
8. Click **Start Export**.
9. In the Save As dialog box, name the export file and click **Save**.

   The Preview area displays the video stream you are exporting.
10. When the export is complete, click **OK**.

Exporting AVI Video

When you export video files, you can choose to export the video in Audio Video Interleave (AVI) format.

1. Click 

to open the Export tab. For more information, see Accessing the Export Tab.

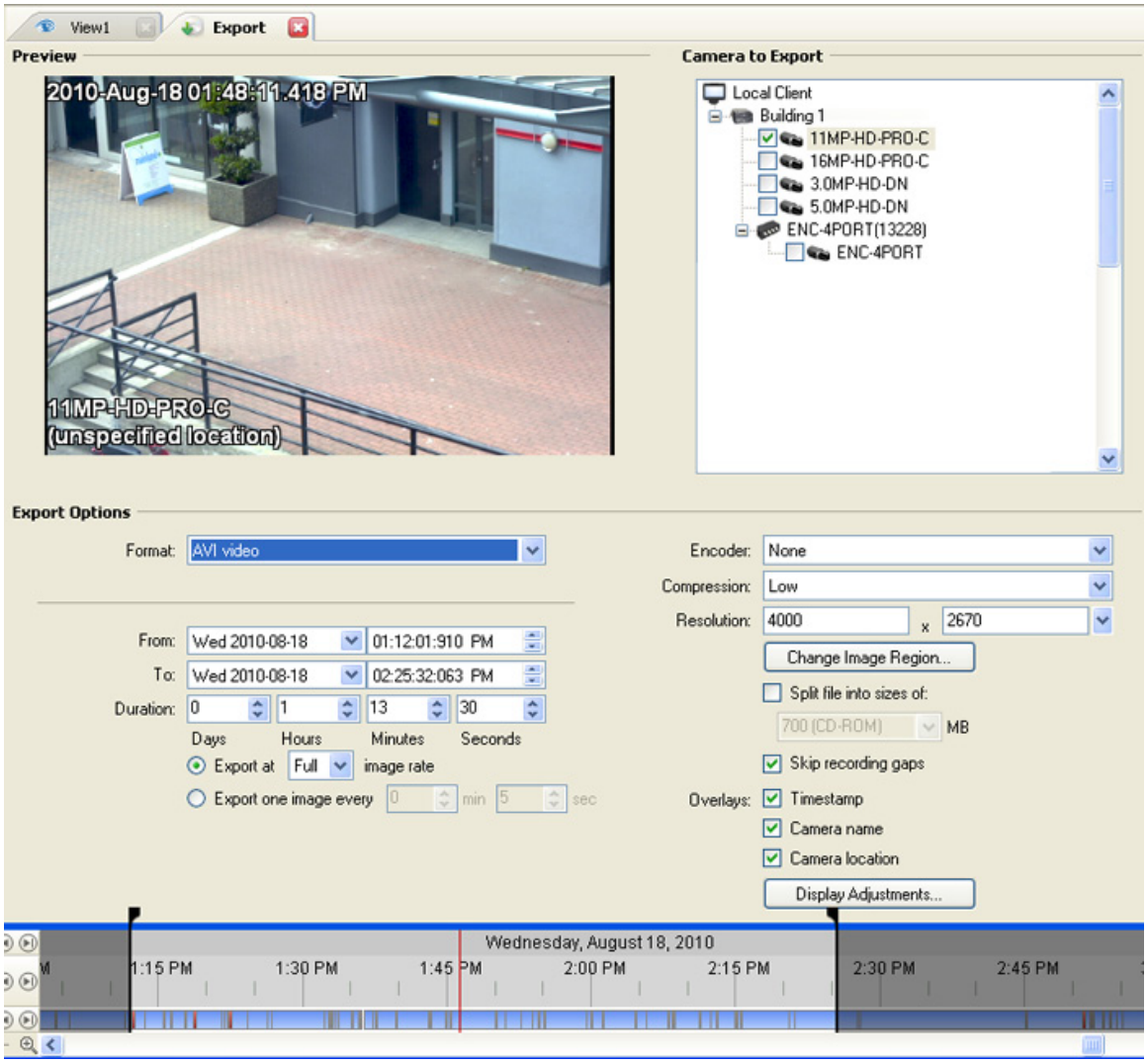


Figure A. Export tab for recorded video export

2. In the **Format** drop down list, select **AVI video**.
3. In the Camera to Export list, select all the camera video you want to export.
4. Enter the time range in the **From**, **To**, **Duration** fields. The time range is highlighted on the Timeline by black time range markers. You can also drag the time range markers to modify the time range.
5. Set the export image rate:

Option	Description
Export at __ image rate	Select this option to control how many images per second are exported. For example, the video is streaming at 30 images per second. If you select **1/2**, only 15 images for that second will be exported.

Export one image every __ min __sec	Select this option to control the time interval between each exported video image. For example, if you enter *5* min. *0* sec., only one image will be exported every 5 minutes.

6. In the **Encoder** field, select the compression used. The **VC-1 (Windows Media Video)** compression is included by default because it is tailored for high-resolution AVI encoding.
7. In the **Compression** field, select a compression level.
8. In the **Resolution** field, select a resolution for the video image. You can manually enter the resolution or click the drop down arrow to select a standard resolution.

   Note: The **Resolution** field automatically maintains the image aspect ratio.

   For high resolution video (11MP or 16MP) the greatest resolution option will be less than the camera's actual resolution because most media players cannot play high resolution AVI files.
9. Select the **Split file into sizes of:** check box to split the exported file into smaller files so the exported files can be stored on optical media, like a CD or DVD.
10. Click **Change Image Region...** to change the region of the video image that is exported.

    In the Change Image Region dialog box, modify the size and position of the green overlay, then click **OK**. The Preview image panel will show the modified image region.
11. Select the **Skips recording gaps** check box to avoid pauses in the video caused by gaps in the recorded video file.
12. Select the required image overlays: **Timestamp**, **Camera name**, and **Camera location**.
13. Click **Display Adjustments** to adjust the Gamma, Black Level and/or White Level.
14. Click **Start Export**.
15. In the Save As dialog box, name the export file and click **Save**.

    The Preview area displays the video stream you are exporting.
16. When the export is complete, click **OK**.

Exporting PNG, JPEG or TIFF Images

When you export recorded video, you can choose to export the video as still images in PNG, JPEG, or TIFF format.

1. Click 

to open the Export tab. For more information, see Accessing the Export Tab.

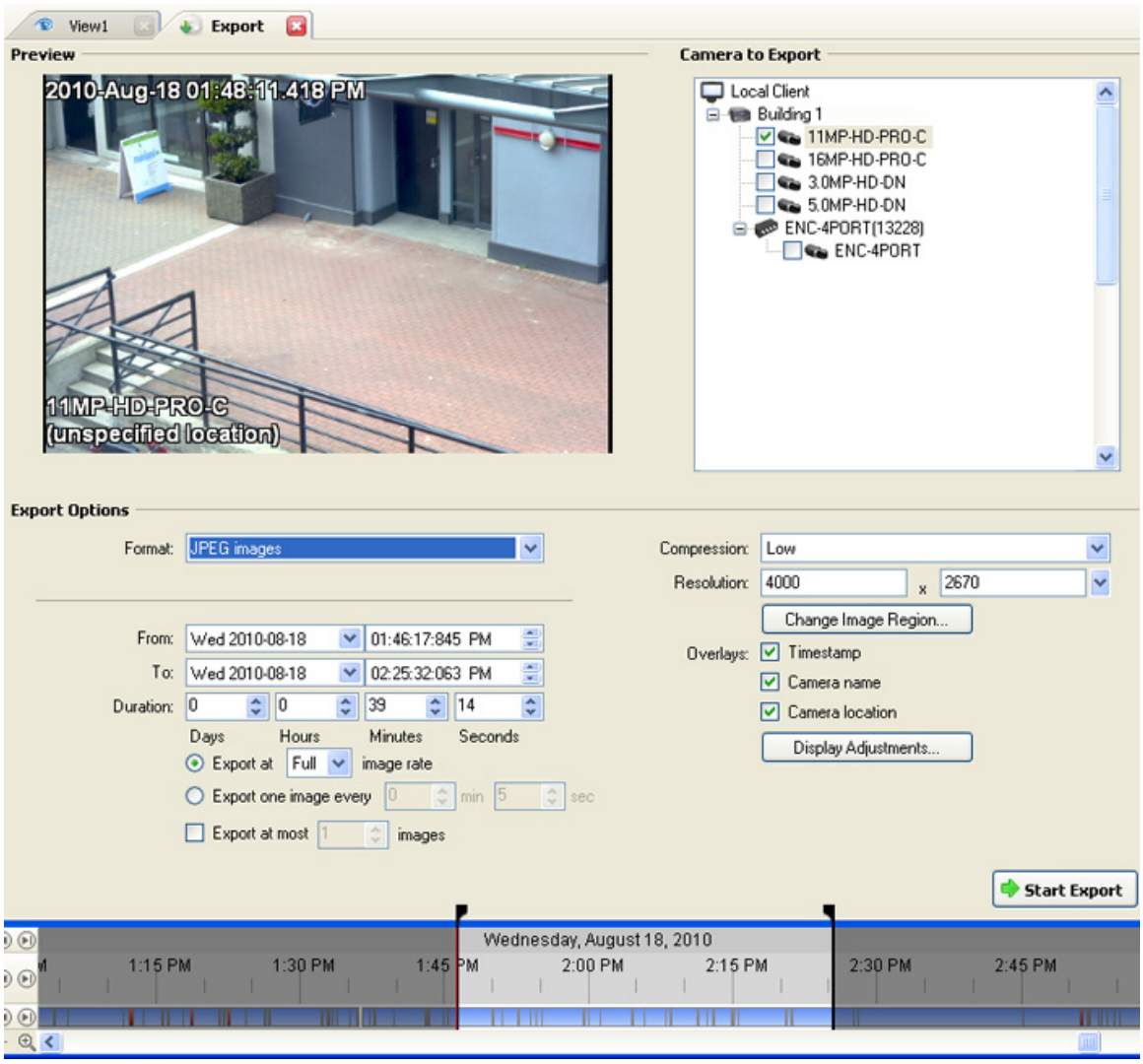


Figure A. Export tab for still image export

2. In the **Format** drop down list, select one of the following export formats: **PNG Images**, **JPEG Images**, or **TIFF Images**.
3. In the Camera to Export list, select all the camera video you want to export.
4. Enter the time range in the **From**, **To**, **Duration** fields. The time range is highlighted on the Timeline by black time range markers. You can also drag the time range markers to modify the time range.
5. Set the export image rate:

Option	Description
Export at __ image rate	Select this option to control how many images per second are exported. For example, the video is streaming at 30 images per second. If you select **1/2**, only 15

	images for that second will be exported.
Export one image every __ min __sec	Select this option to control the time interval between each exported video image. For example, if you enter *5* min. *0* sec., only one image will be exported every 5 minutes.

6. Select the **Export at most __ images** check box to limit the number of images that is exported. Enter the number of images you want exported.

   If this option is selected, the export will stop either when the number of specified images has been exported or when the specified time range has been reached.

7. (JPEG only)

   In the **Compression** field, select a compression level.

8. In the **Resolution** field, select a resolution for the video image. You can manually enter the resolution or click the drop down arrow to select a standard resolution.

   Note: The **Resolution** field automatically maintains the image aspect ratio.

9. Click **Change Image Region...** to change the region of the video image that is exported.

   In the Change Image Region dialog box, modify the size and position of the green overlay, then click **OK**. The Preview image panel will show the modified image region.

10. Select the required image overlays: **Timestamp**, **Camera name**, and **Camera location**.

11. Click **Display Adjustments** to adjust the Gamma, Black Level and/or White Level.

12. Click **Start Export**.

13. In the Save As dialog box, name the export file and click **Save**.

    The Preview area displays the video stream you are exporting.

14. When the export is complete, click **OK**.

Exporting PDF and Print Images

When you export recorded video, you can choose to export the video as still images for printing or in PDF format.

1. Click 

to open the Export tab. For more information, see Accessing the Export Tab.

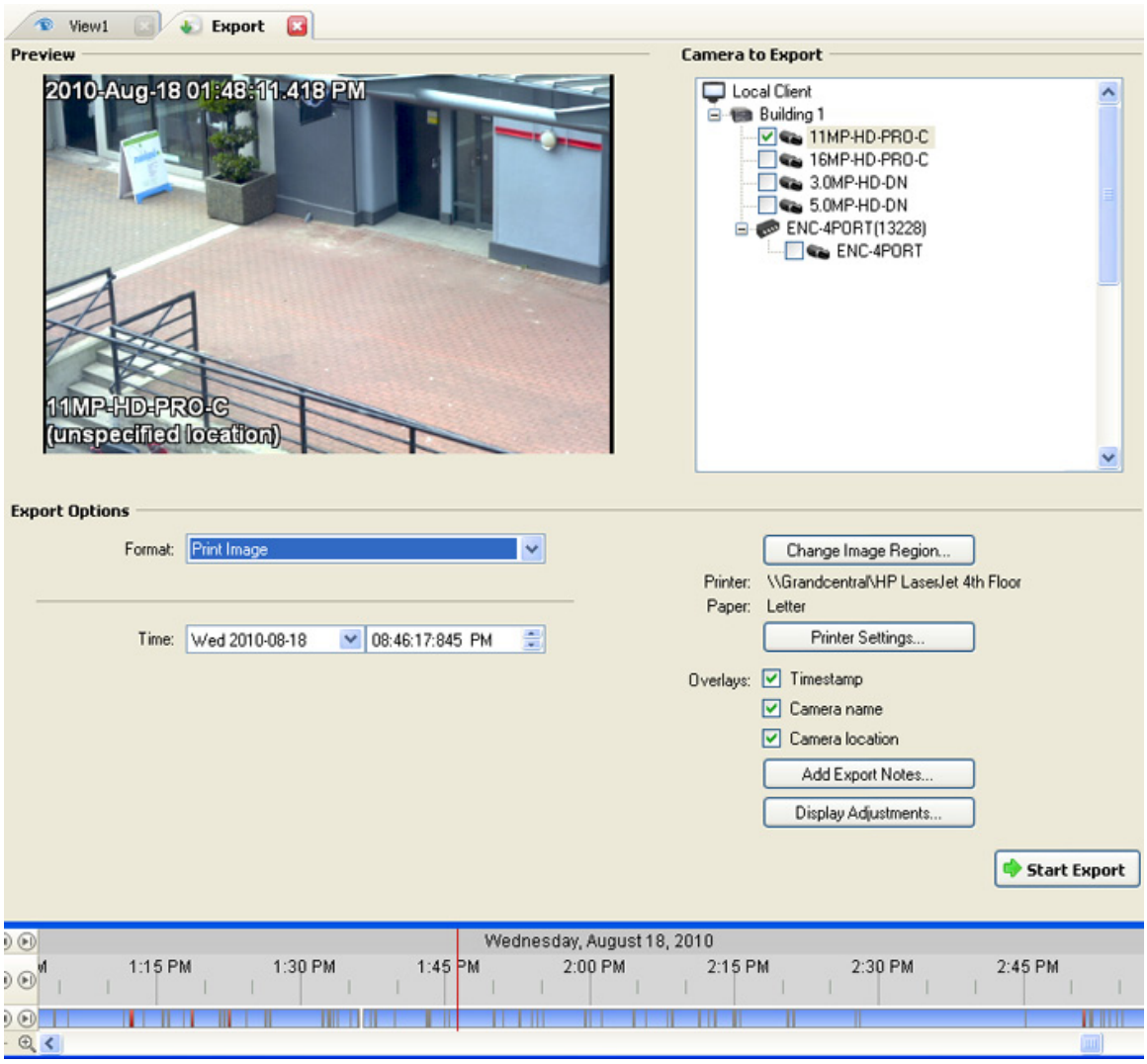


Figure A. Export tab for still image export

2. In the **Format** drop down list, select one of the following export formats: **Print Image** or **PDF File**.
3. In the Camera to Export list, select all the camera video you want to export.
4. In the **Time** field, enter the exact date and time of the video image you want to export.
5. Click **Change Image Region...** to change the region of the video image that is exported.

   In the Change Image Region dialog box, modify the size and position of the green overlay, then click **OK**. The Preview image panel will show the modified image region.
6. (Print Image only) Click **Print Settings** to change the printer and paper size that the image is printed on.
7. Select the required image overlays: **Timestamp**, **Camera name**, and **Camera location**.
8. Click **Add Export Notes** to add notes about the exported image. The notes are added below the image.

9. Click **Display Adjustments** to adjust the Gamma, Black Level and/or White Level.
10. Click **Start Export**.
11. In the Save As dialog box, name the export file and click **Save**.

    The Preview area displays the video stream you are exporting.
12. When the export is complete, click **OK**.

Exporting WAV Audio

If a video contains audio, the audio is exported with the video. If required, you can choose to only export the audio file.

Note: Audio recording requires an Audio Channel License. Without an audio license, no audio would have been recorded with the video.

1. Click 

to open the Export tab. For more information, see Accessing the Export Tab.

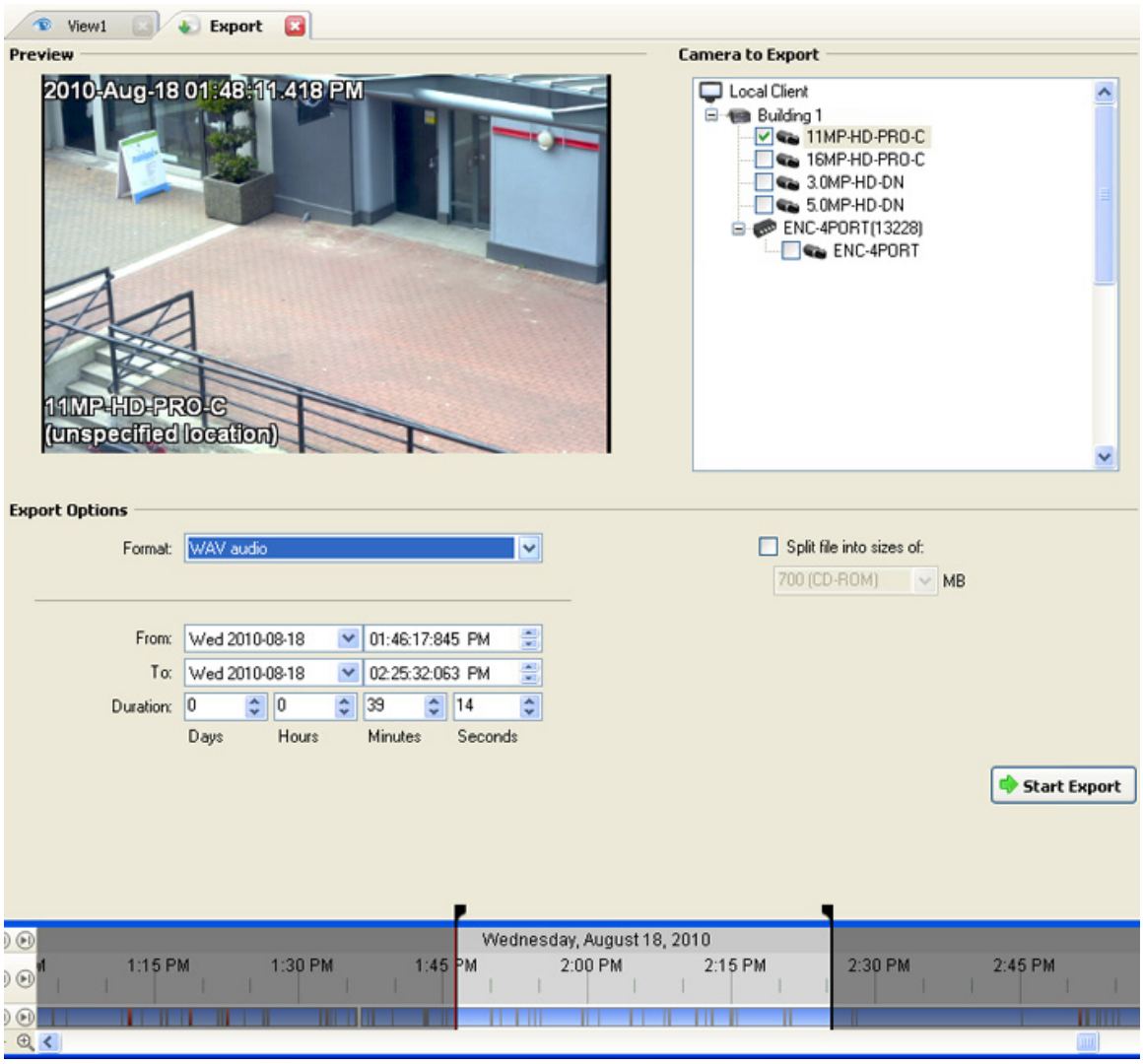


Figure A. Export tab for audio export

2. In the **Format** drop down list, select **WAV**.
3. In the Camera to Export list, select all the camera video you want to export.
4. Enter the time range in the **From**, **To**, **Duration** fields. The time range is highlighted on the Timeline by black time range markers. You can also drag the time range markers to modify the time range.
5. Click **Start Export**.
6. In the Save As dialog box, name the export file and click **Save**.

   The Preview area displays the video linked with the audio you are exporting.
7. When the export is complete, click **OK**.

Appendix

Accessing the Web Client

You can access your Avigilon High Definition Surveillance System through the Web Client. The Web Client is a simplified version of the Client software. It allows you to monitor your surveillance system, search for video events and export recorded video outside the Client software. Be aware that you cannot modify any system settings through the Web Client.

You can access the Web Client through the Internet Explorer web browser.

Note: The Web Client is only compatible with Internet Explorer.

To access the Web Client, you need the Avigilon server's IP address and port number. This information is available in the Avigilon Control Center Admin Tool installed on the server. See the *Avigilon Control Center Server User Guide* for more information.

1. To access the Web Client, open Internet Explorer and enter the following address: http://<*server ip address*>:<*port number*>/ (For example, http://192.168.2.62:50083/)

   If you have not accessed the Web Client before, you may be prompted to install the required software before the Web Client will open.

2. When the login screen appears, enter your username and password for the server.

The Web Client is opened in your browser, and you can access the video and cameras connected to the server.

Note: You can only access one server at a time through the Web Client.

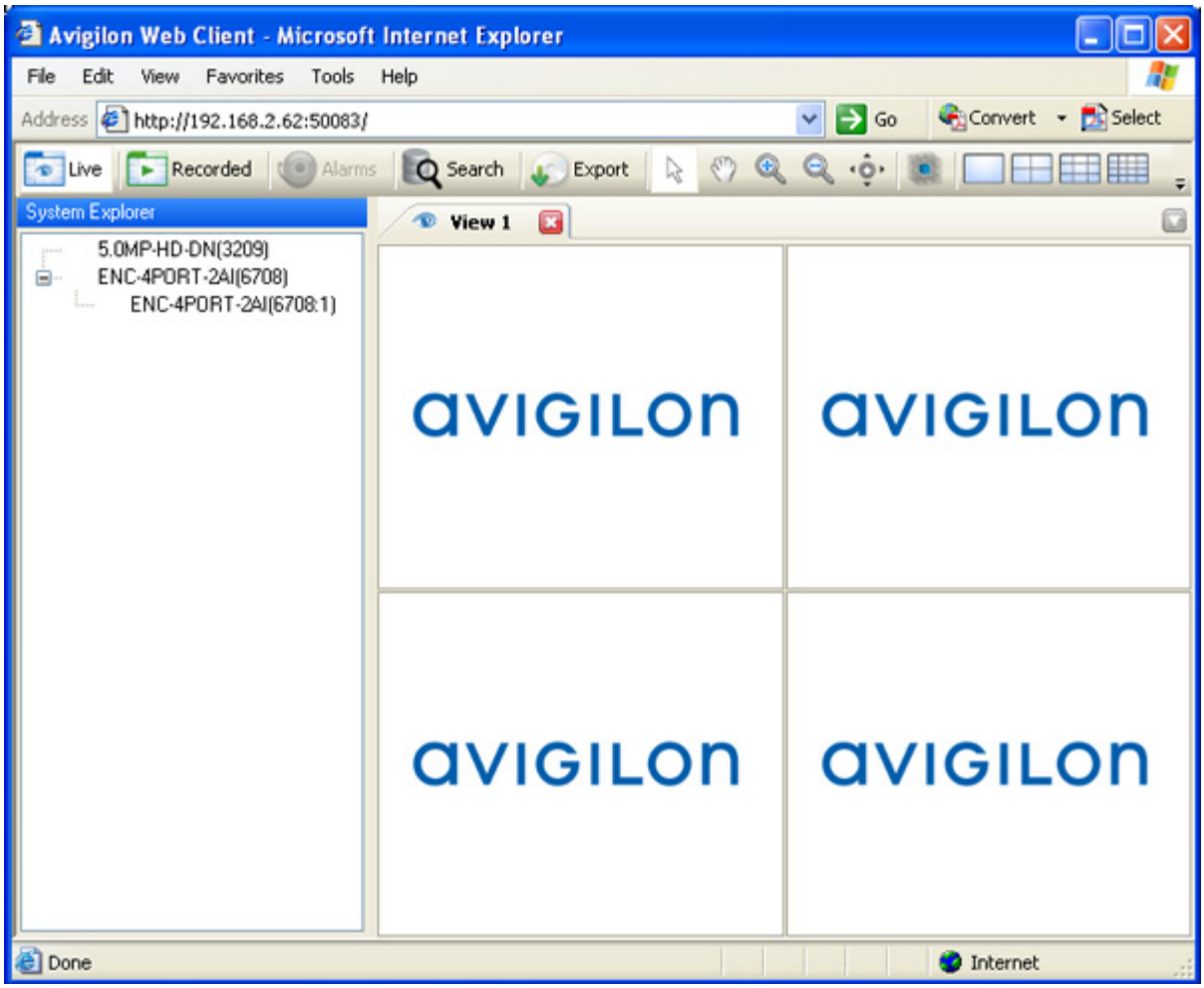


Figure A. Avigilon Control Center Web Client

Reporting Bugs

If an error occurs in the Avigilon Control Center System, you can contact Avigilon Support at support@avigilon.com or +1.888.281.5182.

To help diagnose your problem, the Avigilon Support team may ask you to provide a System Bug Report. The System Bug Report is a zip file generated by the Avigilon Control Center Client software that contains the system log and error reports for each of the servers you have access to.

1. Select **Help > System Bug Report...**.
2. When the Download System Bug Report dialog box appears, click **Download**.
3. In the Save As dialog box, name the file and click **Save**.
4. Once the System Bug Report has downloaded successfully, click **Close**.

Keyboard Commands

Use any of the keyboard commands below to help you navigate the Avigilon Control Center Client software.

The Key Combination column show the commands used on a standard keyboard, while the Keypad Combination column show the commands used on an Avigilon USB Professional Joystick Keyboard.

Image Panel & Camera Commands

Command	Key Combination	Keypad Combination (Image Panel buttons)
Select image panel Image panel # are displayed after pressing the first key.	* + <*image panel #*> + Enter	 + <*image panel #*> + ENTER
Select camera Cameras are selected using their *logical ID*.	/ + <*Logical ID*> + Enter	 + <*Logical ID*> + ENTER
Select the next panel	Tab	
Select the previous panel	Shift + Tab	
Clear panel selection	* + 0 + Enter	
Remove camera from selected panel	Backspace	
Expand/Collapse selected panel	Ctrl + E	
Add bookmark for selected camera **Note:** For recorded	Ctrl + B	

video only.		
Start/Stop audio for selected camera	Ctrl + A	
Snapshot image of selected camera video	F4	
Enable digital output		

View Commands

Command	Key Combination	Keypad Combination (View buttons)
Select the next view	Ctrl + Tab	
Select the previous view	Ctrl + Shift + Tab	
Jump to view	Ctrl + 1 to 9	
Start/Stop cycle views	Ctrl + Y	
Create new view	Ctrl + T	
Close current view	Ctrl + W	
Create new window	Ctrl + N	
Switch current view to live view mode	Ctrl + L	

Switch current view to recorded view mode	Ctrl + P	
Remove all cameras from current view	Ctrl + Backspace	
Enable/Disable full screen mode for current view	F11	
Open saved View The saved View number is displayed in the System Explorer after pressing the first button.		OPEN 3 + <Saved View #> + ENTER

Playback Commands

Command	Key Combination	Keypad Combination (Timeline buttons)
Play/Pause	Spacebar	
Increase playback speed	Page Up	
Decrease playback speed	Page Down	
Step to next frame	Shift + →	
Step to previous frame	Shift + ←	
Go to next event	Alt + →	
Go to previous event	Alt + ←	

Go forward one second	Ctrl + →	
Go forward five seconds	Ctrl + Shift + →	
Go back one second	Ctrl + ←	
Go back five seconds	Ctrl + Shift + ←	
Zoom in on the Timeline	Ctrl + Alt + +	
Zoom out on the Timeline	Ctrl + Alt + -	
Scroll forward on the Timeline	Ctrl + Alt + →	
Scroll backward on the Timeline	Ctrl + Alt + ←	
Go to start of the Timeline	Ctrl + Alt + Home	
Go to end of the Timeline	Ctrl + Alt + End	
Center the Timeline on marker	Ctrl + C	

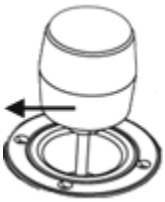
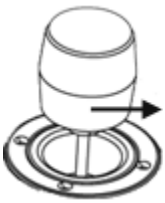
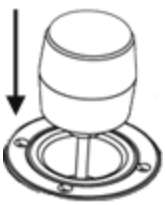
Layout Commands

Command	Key Combination	Keypad Combination

		(View buttons)
Change to 1 Division layout	Alt + 1	LAYOUT 4 + PREV 1
Change to 4 Division layout	Alt + 2	LAYOUT 4 + NEXT 2
Change to 9 Division layout	Alt + 3	LAYOUT 4 + OPEN 3
Change to 16 Division layout	Alt + 4	LAYOUT 4 + LAYOUT 4
Change to 25 Division layout	Alt + 5	LAYOUT 4 + 5
Change to 36 Division layout	Alt + 6	LAYOUT 4 + CLOSE 6
Change to 6 Division (1 + 5) layout	Alt + 7	LAYOUT 4 + 7
Change to 8 Division (1 + 7) layout	Alt + 8	LAYOUT 4 + 8
Change to 13 Division (1 + 12) layout	Alt + 9	LAYOUT 4 + 9
Change to 10 Division (2 + 8) layout	Alt + 0	LAYOUT 4 + 0
Change to next layout	Alt +]	
Change to previous layout	Alt + [	

PTZ Commands (Digital and Mechanical)

Command	Key	Keypad Combination

	Combination	(PTZ buttons)
Toggle PTZ controls	Ctrl + D	
Zoom in	+	
Zoom out	-	
Pan left	←	
Pan right	→	
Tilt up	↑	
Tilt down	↓	

Increase PTZ speed	Shift + ↑	The further the joystick is from center, the faster the speed.
Decrease PTZ speed	Shift + ↓	The closer the joystick is to center, the slower the speed.
Open iris	Home	
Close iris	End	
Focus near	Insert	
Focus far	Delete	
PTZ menu left	←	
PTZ menu right	→	
PTZ menu up	↑	
PTZ menu down	↓	
Activate preset		PRESET + <*Preset #*> + ENTER
Run pattern		PATTERN + <*Pattern #*> + ENTER
Start auxiliary		 + <*Aux #*> + ENTER

Stop auxiliary		 + <*Aux #*> + **ENTER**

Index

This Page Left Intentionally Blank

Avigilon Control Center Client User Guide

Version: 4.6 Enterprise

OLH-CLIENT-E-B-Rev2

Avigilon
Tel +1.604.629.5182
Fax +1.604.629.5183
http://www.avigilon.com

Revised 2010-11-22

Table of Contents

Introduction

What is the Avigilon Control Center Client?

The Avigilon Control Center Client is the application that works with the Avigilon Control Center Server software to give you access and control of the Avigilon High Definition Surveillance System.

The Client software allows you to view live and recorded video, monitor alarms and events, and control user access to the Avigilon Control Center System. The Client software also gives you the ability to configure the server, cameras and other external devices that are part of your surveillance system.

The Client software can run on the same computer as the Server software, or run on a remote computer that connects with the Server software through a local area network (LAN) or a wireless area network (WAN).

The Client software features available to you are dependant on the Server software edition. There are two editions of the Server software available: Standard and Enterprise. The Standard edition allows you to monitor video but not alarms, and contains all the essential Client features. The Enterprise edition gives you access to the full suite of Client software features, including alarms, rules, Site View, Web Pages, Maps and system backup. Visit the Avigilon website for an overview of the features available in each edition: http://avigilon.com/products/controlcenter/overview/

A copy of the Client software can be downloaded from the Avigilon website, or installed with the Server software.

System Requirements

A copy of the Client software can be downloaded from the Avigilon website, or installed with the Server software.

You do not need a license to use the Client software, but the features available in the Client software are dependant on the Server software license.

Minimum requirements	Recommended requirements

Monitor resolution	1280 x 1024	1280 x 1024
OS	Windows XP with Service Pack (SP) 2 or later, Windows Vista, or Windows 7	Windows XP with Service Pack (SP) 2 or later, Windows Vista, or Windows 7
CPU	Intel Single Core 2.4 GHz processor	Intel Dual Core 2.0 GHz processor
System RAM	1 GB	2 GB
Video card	PCI Express, DirectX 9.0c compliant with 128 MB RAM (Intel GMA 900 or better, NVIDIA 6600 or better, ATI X1300 or better)	PCI Express, DirectX 10.0 compliant with 256 MB RAM (NVIDIA GeForce 8000 series or better)
Network card	100 Mbps	1 Gbps
Hard disk space	500 MB	500 MB

For More Information

Visit Avigilon at http://www.avigilon.com/ for additional product documentation.

Avigilon University

The Avigilon University provides free online training videos that demonstrate how to set up and use the Avigilon Surveillance System. Register online at the Avigilon Partner site to begin: http://avigilon.com/partners/

Support

For additional support information, visit http://www.avigilon.com/support/.

Regular Avigilon Customer Support Center hours of operation are from 6:00 a.m. to 6:00 p.m. Pacific Standard Time (PST) and can be reached by calling the toll-free number: +1.888.281.5182.

E-mails can be sent to: support@avigilon.com.

For emergency technical support 24 hours a day, 7 days a week, please call the Avigilon Emergency Technical Support Hotline at +1.604.506.3117.

Upgrades

Software and firmware upgrades will be made available for download as they become available. Check http://www.avigilon.com/support/software for available upgrades.

Feedback

We value your feedback. Visit our feedback page to comment on our products and services: http://avigilon.com/feedback/

Getting Started

Once the Avigilon Control Center Client software has been installed, you can start using the Avigilon High Definition Surveillance System immediately. Refer to any of the following procedures to help you get started.

To watch a video overview of the application, see *Module 1 - Introduction to Avigilon Control Center Client and Viewing Live Video* in the Avigilon University - End User Stream.

Starting and Shutting Down the Avigilon Control Center Client

The Avigilon Control Center Client software can be started or shut down at anytime. The Avigilon Control Center Server software is a Windows service and will continue to run in the background even when the Client software is shut down.

Starting the Control Center Client

Perform one of the following:

- From the Windows Start menu, select **All Programs > Avigilon > Avigilon Control Center Client > Avigilon Control Center Client**.
- Double-click the  **Avigilon Control Center Client** shortcut icon on the desktop.
- From the Avigilon Control Center Admin Tool, click **Launch Control Center Client**. See the *Avigilon Control Center Server User Guide* for more information.

Log in to the appropriate server when the Log In dialog box appears. See Logging_In for more information.

Shutting down the Control Center Client

1. In the Avigilon Control Center Client software, select **File > Exit**.
2. In the confirmation dialog box, click **Yes**.

Locating Servers

The Avigilon Control Center Client software must communicate with the Avigilon Control Center Server software to access and configure your surveillance system. If the server is on the same network segment (subnet) as the computer running the Client software, the server will be automatically discovered by the Client software and will appear in the System Explorer on the left side of the application window.

If the server is on a different subnet, the server must be manually discovered. There is no limit to the number of servers that could be discovered by the Client software.

Discovering and Managing Server Connections

1. Open the Find Server dialog box.
    - In the Log In dialog box, click **Find Server...**.
    - In the application window, select **File > Manage Server Connections**. In the Manage Servers dialog box, click **Find Server...**

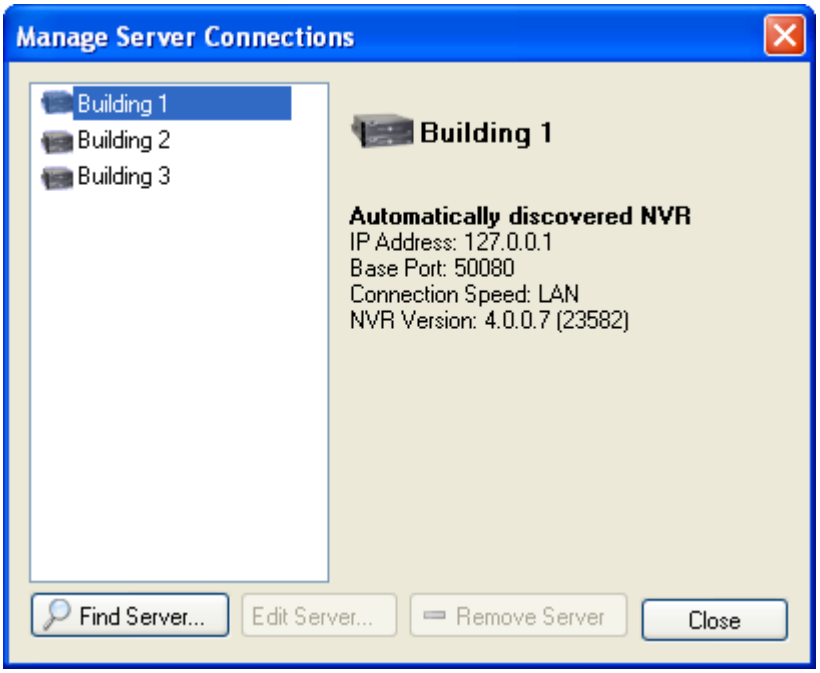


Figure A. Manage Server Connections dialog box

2. In the Find Server dialog box, enter the **Hostname/IP Address**, the **Base Port**, and the **Connection Speed** of the server you want to discover.

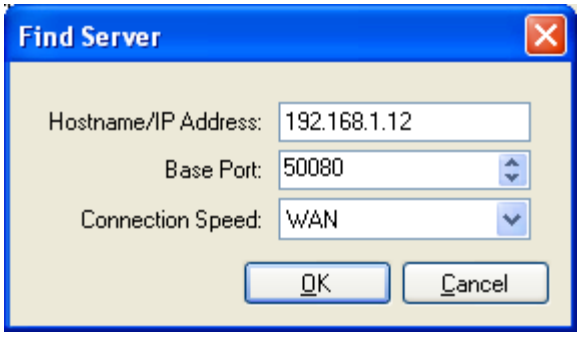


Figure B. Find Server dialog box

The base port is 50080 by default. You can change the base port number in the Avigilon Control Center Admin Tool. See the *Avigilon Control Center Server User Guide* for more information.

> **Tip:** Set the **Connection Speed** to WAN if you are on a low bandwidth network (i.e. internet or wireless network), and select LAN if you are on a high bandwidth connection (i.e. office or home network). This enables the Avigilon Control Center to better manage your bandwidth and image rate.

3. Click **OK.**

If the server is found, the server will appear in the Manage Server Connections dialog box.

If the server is not found, ensure the network settings are configured correctly, the firewall is not blocking the application, and the Avigilon Control Center Server software is running on the server, then try again.

Logging Into and Out of Servers

To access your Avigilon High Definition Surveillance System through the Client software, you must log in to the servers running the Avigilon Control Center Server software. Whenever the Client software detects a server with the Server software installed, you are prompted to log in.

The default administrator access uses *administrator* as the username and no password. To maintain the security of the administrator account, it is recommended that your system administrator immediately create a password for this account after the first login. Your system administrator can then create user accounts for other users.

If the Client software does not detect any servers, click **Find Server...** and enter the server IP address in the dialog box. See Locating Servers for more information.

Logging In

Be aware that the number of servers you can log into at one time is determined by the type of server you can access. Standard edition servers only allow you to be logged into three servers simultaneously, while Enterprise edition servers allow you to be logged into an unlimited number of servers.

Note: You cannot access Standard edition servers and Enterprise edition servers at the same time.

1. Open the Log In dialog box. The Log In dialog box automatically appears when a server is detected by the Client software.

   To manually access the Log In dialog box, perform one of the following:

   - From the **File** menu, select **Log In** to log in to all available servers
   - In the System Explorer, right-click a server and select **Log In**.

2. In the Log In dialog box, select a specific server or select **All Servers** from the **Log in to** drop down list.

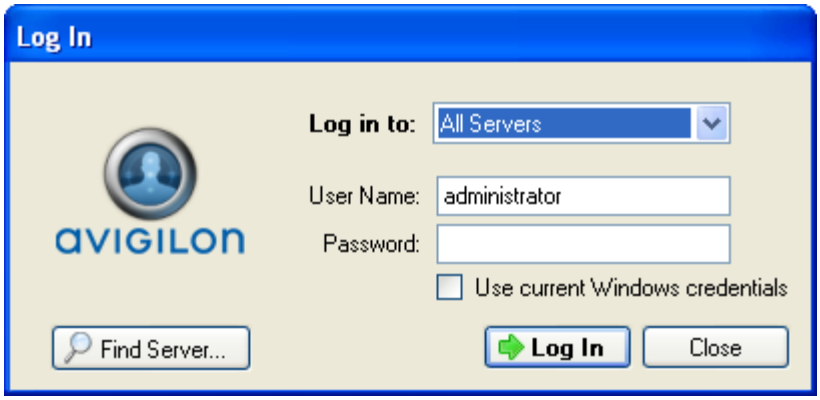


Figure A. Log In dialog box

   Tip: If you accessed the Log In dialog box from a specific server, you will not have the option of logging into All Servers.

   If the server you want to log into is not shown, click **Find Server...** to attempt to locate the server.

3. Enter your **User Name** and **Password**, or select the **Use current Windows credentials** check box if your system administrator has imported your Windows account information into the server.

4. Click **Log In**.

After logging in the first time, you can configure automatic login from the client Setup dialog box. See General for more information.

Logging Out

You can log out of one or all servers at any time in the Client software.

To	Do this
Log out of an individual server	1. Right-click the server in the System Explorer and select **Log Out**.
Log out of all servers	1. Select **File > Log out**. 2. When the Log Out dialog box appears, click **Yes**.

Navigating the Application

Once you log in, the Avigilon Control Center Client application window is where you setup your surveillance system, monitor video, and view, search, and export recorded video.

Note: Some features are not displayed if the server does not have the required license, or if you do not have the user permissions to access the feature.

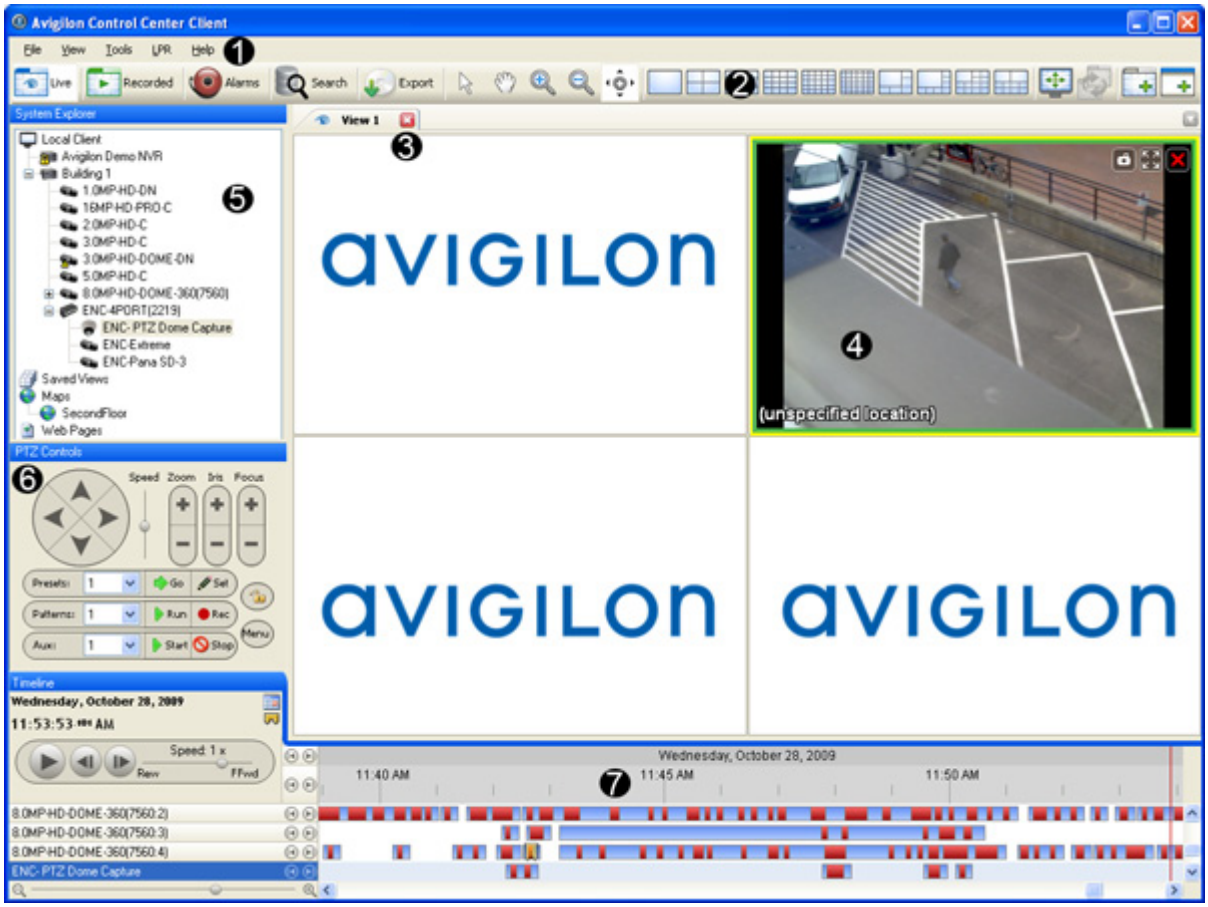


Figure A. Avigilon Control Center Client application window.

	Area	Description
	Workspace	The right pane where the feature tabs appear.
1	Menu bar	A standard Windows application menu that provides access to application features not available on the Toolbar.
2	Toolbar	Provides quick access to commonly used tools. If any buttons are missing from your toolbar, click the small down arrow on the right-edge of the toolbar to display the hidden buttons.
3	View	Provides a way to organize image panels. You can have multiple Views open at once. This is the most common tab in the Workspace.
4	Image panel	Displays live or recorded video from a single camera.
5	System Explorer	Displays surveillance system components such as servers,

		cameras, views, and maps.
6	PTZ Controls	Provides a way to control pan and tilt and zoom (PTZ) cameras.
7	Timeline	Displays the timeline for a recorded video, and contains color-coded events. This tool allows you to select a date and time for playback, and controls the playback rate. **Note:** The Timeline only appears when displaying recorded video.

Viewing Live and Recorded Video

Live and recorded video are displayed in Views. A View is a tab composed of image panels. Views allow you to organize how video is monitored, while image panels allow you to control the video image display quality and other features that are directly related to the video. To customize the way video is displayed, refer to the *Video* section of this guide.

Note: Some features are not displayed if the server does not have the required license, or if you do not have the user permissions to access the feature.

Tip: You can choose to simultaneously watch live video in some panels and recorded video in other panels, or only view one type of video per View.

1. Drag a camera from the System Explorer pane to an empty image panel in the View.

   The video from the camera is displayed. By default, live video is displayed when you first add a camera to an image panel.

2. To switch the View between live and recorded video, perform one of the following:

   - Select **View > Live** or **Recorded**.
   - On the toolbar, select either 

or 

.

3. To switch individual panels between live and recorded, right-click the image panel and select either **Live** or **Recorded**.

Image panels displaying live video appear with a blue border, while image panels displaying recorded video appear with a green border.

Setup

The default settings configured in the Avigilon Control Center Client software allows you to start working with the application immediately after installation.

If you have special requirements, refer to the following sections to configure your settings:

Note: Some features are not displayed if the server does not have the required license, or if you do not have the user permissions to access the feature.

Connect/Disconnect Cameras

You can connect and disconnect cameras to servers using the Connect/Disconnect Cameras dialog box.

A camera's connection status is indicated by the status icon beside the camera name in the System Explorer.

Icon	Definition
 **Camera Connected**	The camera is connected to the server.
 **Camera Connection Error**	The camera cannot connect to a server. This may be because the camera is no longer on the network or there is a network conflict
 **Camera Disconnected**	The camera is disconnected from the server but there is recorded video for the camera remaining on the server.
No icon	The camera is disconnected from the server and there is no recorded video remaining on the server.

Discovering a Camera

When cameras are connected to the Avigilon HD Surveillance System, they should be automatically discovered by the Avigilon Control Center Client software.

If a camera is not automatically discovered, you can attempt to manually discover the camera on the network.

1. From the **Tools** menu, select **Connect/Disconnect Cameras**.

   In the Connect/Disconnect Cameras window, all Avigilon cameras located on the same subnet as the computer running the Avigilon Control Center Server software are automatically detected and appear in the Discovered Cameras area.

If the camera you want to connect to is on a different subnet, or is manufactured by a third party, perform the following:

1. At the top of the Connect/Disconnect Cameras dialog box, click **Find Camera...**.
2. In the Find Camera dialog box, complete the following fields:

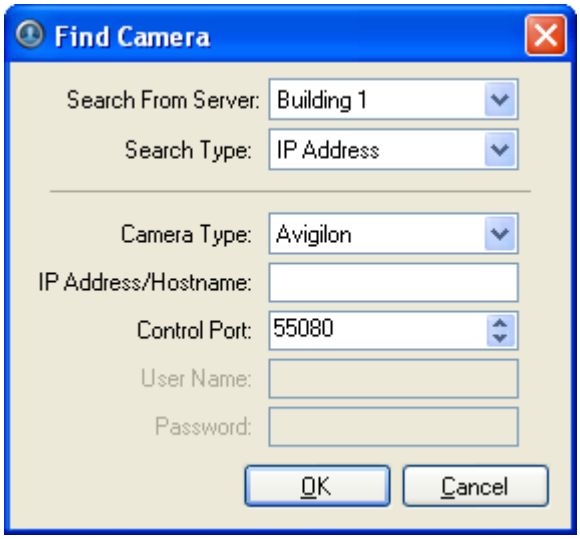


Figure A. Find Camera dialog box: IP Address

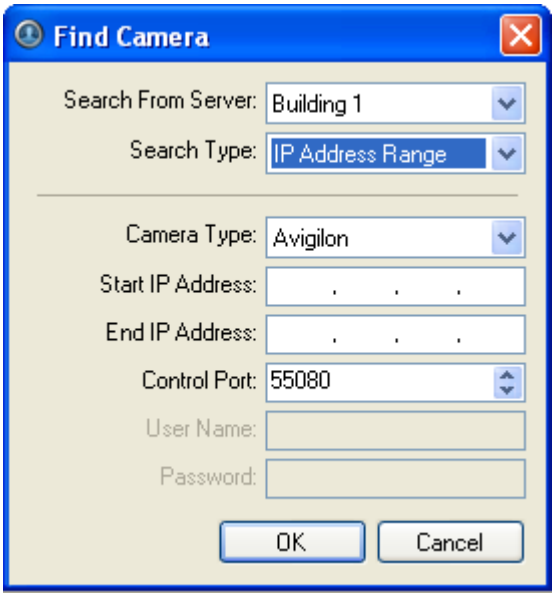


Figure B. Find Camera dialog box: IP Address Range

- **Search From Server:** select the server that you want the camera to connect to.
- **Search Type:** select a search type.
- **Camera Type:** select the camera's brand name.

  Tip: Select ONVIF to discover cameras that are ONVIF complaint.

- **IP Address/Hostname:** (For IP Address search only) enter the camera's IP address or hostname. The camera and server's gateway IP address must be set correctly for the camera to be found.
- **Start IP Address** and **End IP Address:** (For IP Address Range search only) enter the start and end IP addresses. Only addresses in that range will be searched for the selected camera type.
- **Control Port:** enter the camera control port number.
- Provide the **User Name** and **Password** for the camera if required by the camera manufacturer .

3. Click **OK**.

If the camera is discovered, it will appear in the Discovered Cameras area.

Connecting a Camera to a Server

Once the camera has been discovered on the network, it can be connected to the server.

1. From the **Tools** menu, select **Connect/Disconnect Cameras**. The Connect/Discover Cameras dialog box appears.

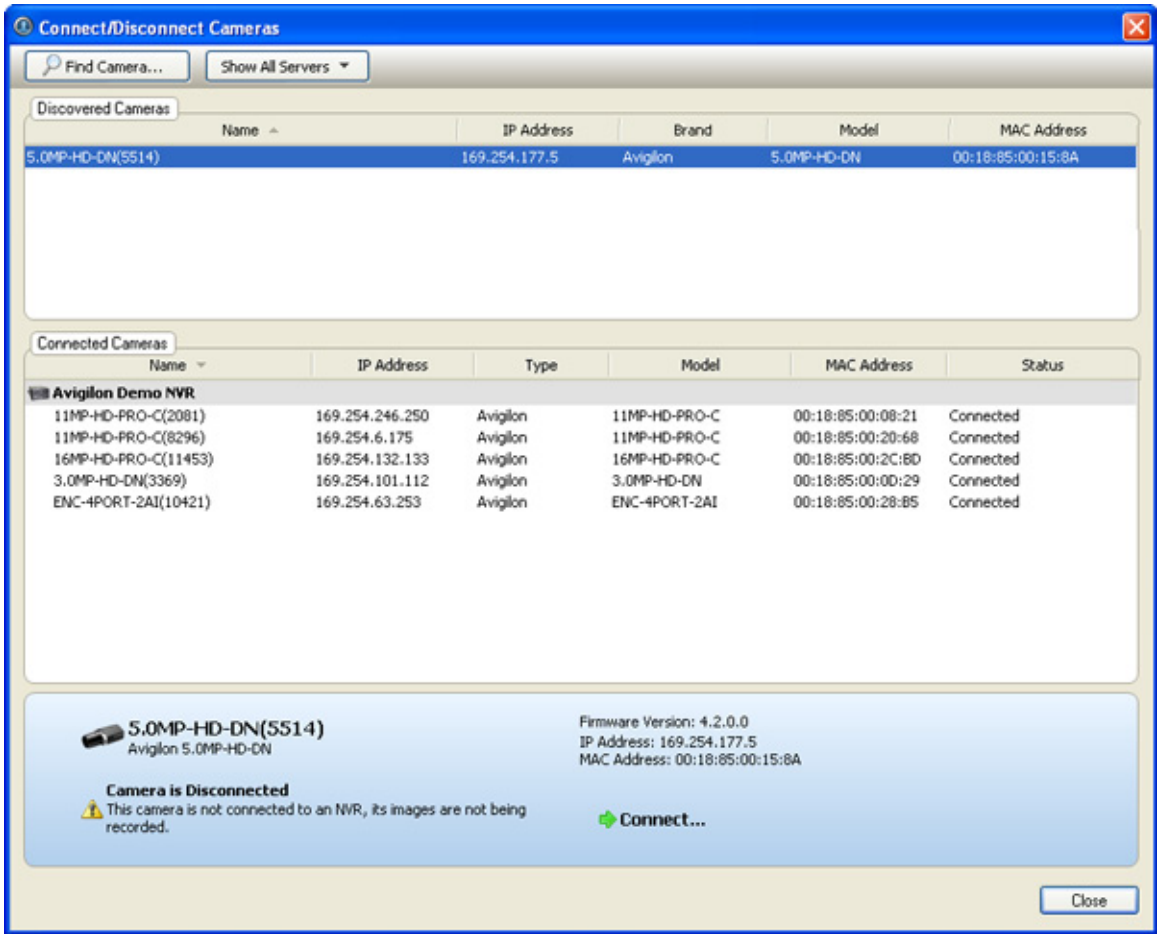


Figure A. Connect/Disconnect Cameras dialog box

2. In the Discovered Cameras area, select a camera then click **Connect...**.

   Tip: You can also drag the camera to a server on the Connected Cameras list, then you can skip the following step.

3. In the Connect Camera dialog box, select the server you want the camera to connect to.

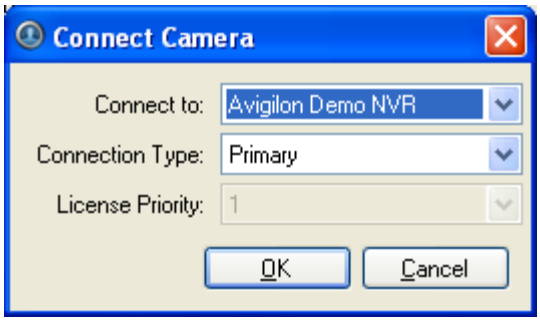


Figure B. Connect Camera dialog box

4. In the **Connection Type** drop down list, select one of the following:

- **Primary:** the camera will automatically connect to this server if they are on the same network.
- **Secondary:** the camera will attempt to connect to this server if they are on the same network, and the primary server is not available.
- **Tertiary:** the camera will attempt to connect to this server if they are on the same network, and the primary and secondary servers are not available.

5. In the **License Priority** drop down list, select the appropriate license priority. **1** is the highest priority and **5** is the lowest.

   Note: This option is only available if you are connecting to a secondary or tertiary server.

   The license priority setting determines the order that cameras are connected to the server. The server will attempt to connect cameras with a higher license priority before cameras with lower priority. If the server does not have enough camera channel licenses, low priority cameras may not be connected. A camera channel license is only used when the camera actually connects to the server.

6. Click **OK**.
7. If the camera is password protected, the Camera Authentication dialog box appears. Enter the camera's username and password, then click **OK**.
8. Close the Connect/Disconnect Camera dialog box.

Editing the Camera Connection to the Server

1. From the **Tools** menu, select **Connect/Disconnect Cameras**.
2. In the Connect/Disconnect Cameras dialog box, select the camera connection you want to edit from the Connected Cameras list.
3. Click **Edit** and make the required changes to the Connection Settings dialog box.
4. Click **OK**.

Disconnecting a Camera from a Server

1. From the **Tools** menu, select **Connect/Disconnect Cameras**.
2. In the Connect/Disconnect Cameras dialog box, select the camera you want to disconnect from the Connected Cameras list.
3. To disconnect the camera from the server perform, one of the following:

- Click **Disconnect**.
  The camera is disconnected from the server and moved to the Discovered Cameras list.
- Drag the camera into the Discovered Cameras list.

Server Setup

The Avigilon Control Center Server is setup by default to only record image data when events occur. In the Client software, you can use the server Setup dialog box to configure the server to record continuously, or schedule cameras to only record at specific times.

The server Setup dialog box also allows you to create alarms, schedule automatic backup of image data, set user access permissions, configure email notifications, and add POS transaction engines.

Note: Some features are not displayed if the server does not have the required license, or if you do not have the user permissions to access the feature.

Accessing the Server Setup

Perform one of the following steps to open the server Setup dialog box:

- Select **Tools > Setup...** then select the server you want to setup from the left pane.
- In the System Explorer pane, right-click the server and select **Setup**.

Note: Some features are not displayed if the server does not have the required license, or if you do not have the user permissions to access the feature.

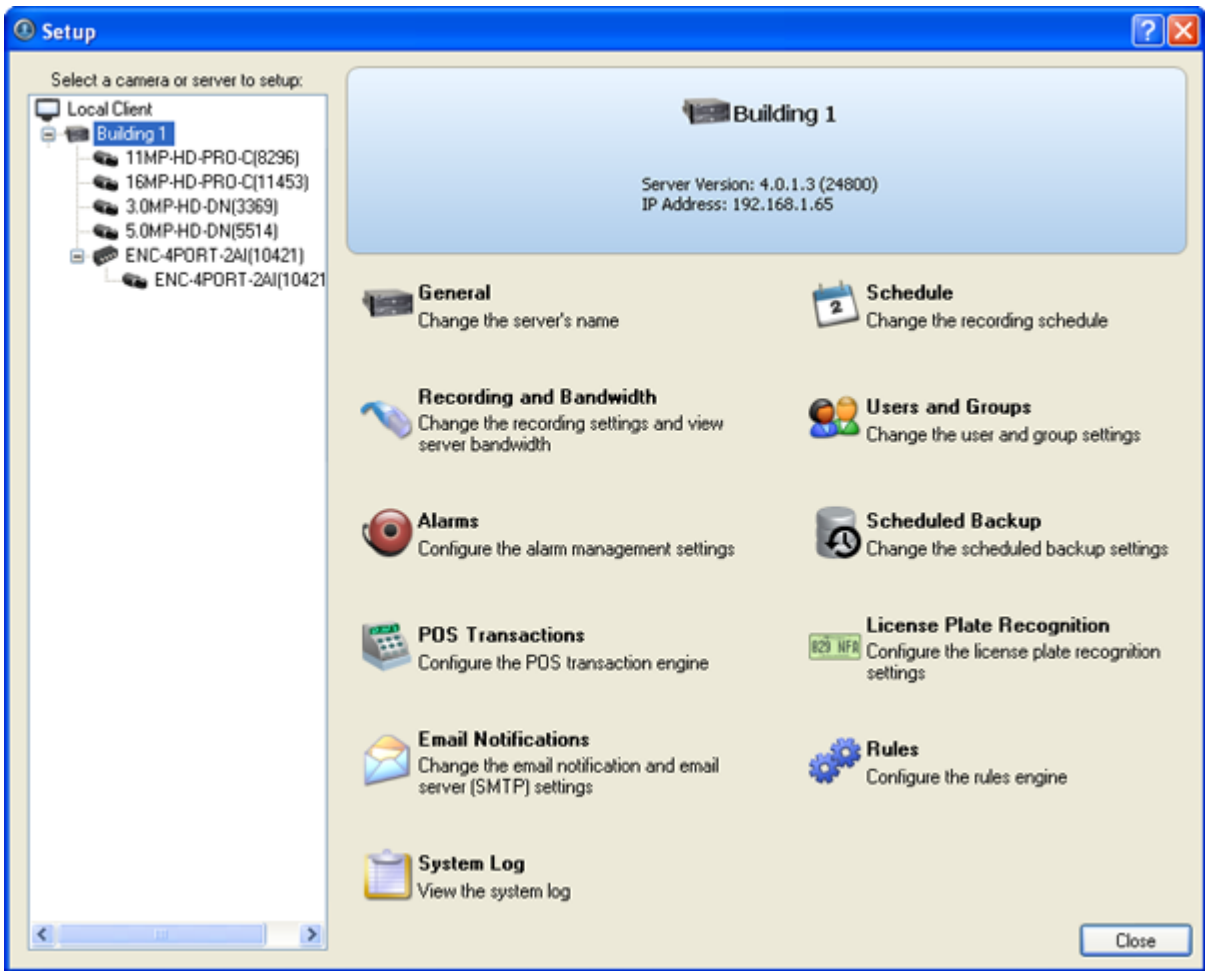


Figure A. Server Setup dialog box

General

Use the General dialog box to customize the identity of each server.

Changing the Server's Name

The default name for the server may not be useful for your purposes. Use the General dialog box to change the server's name to something more appropriate to your needs.

1. Right-click a server in the System Explorer and select **Setup** to open the server Setup dialog box. See Accessing the Server Setup for more information.
2. Click **General**.
3. In the General dialog box, enter a new server name.

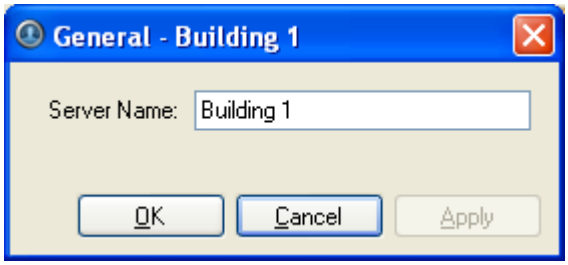


Figure A. General dialog box

4. Click **OK**.

Schedule

Use the Schedule dialog box to customize the recording schedule for the cameras connected to the server. All Avigilon High Definition Surveillance Systems are set to record whenever motion or events occur by default .

Once the recording schedule is set, camera recordings are made automatically.

Using Templates to Modify the Recording Schedule

You can modify the default recording schedule template to suit your needs or you can add new templates as required. For example, you can create one recording schedule template for the weekdays and another for the weekend.

Adding a Template

1. Right-click a server in the System Explorer and select **Setup** to open the server Setup dialog box. See Accessing the Server Setup for more information.
2. Click **Schedule**.
3. In the Schedule dialog box, click **Add Template** in the Templates pane.

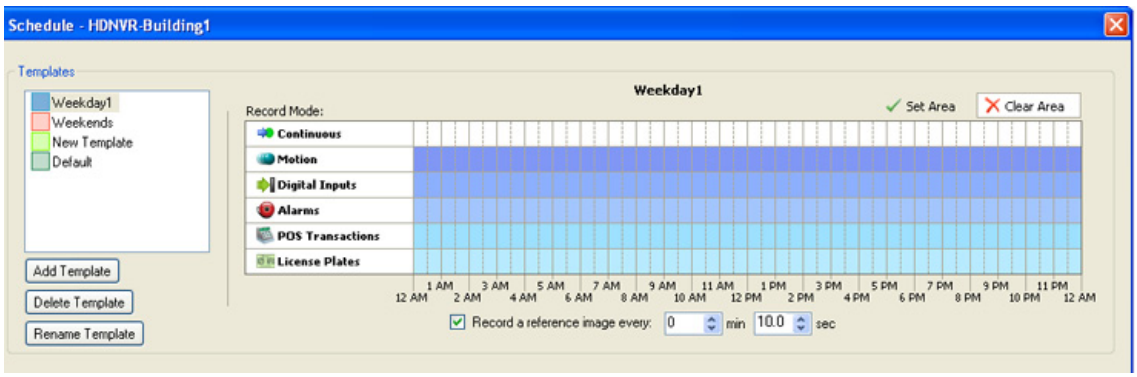


Figure A. Schedule dialog box

4. Enter a name for the template.
5. Click the **Set Area** button then click or drag the cursor across the **Record Mode** timeline to enable cameras to record during the specified hours for the highlighted events.

Record Mode	Definition
Continuous	Record image data continuously. Enable the continuous mode to record all image data.
Motion	Record image data only when motion is detected.
Digital Input	Record image data only when a digital input is activated.
Alarms	Record image data only when an alarm has been activated.
POS Transactions	Record image data only when point of sale (POS) transactions are made.
License Plates	Record image data only when a license plate is detected.

6. To disable recording in parts of the template, click the **Clear Area** button then click or drag the cursor across the timeline until the required Record Modes and time ranges are blank.
7. If cameras are not recording in Continuous mode for the entire template period, you can configure cameras to record reference images between events in the recording schedule. Select the **Record a reference image every:** check box, and specify the time range between each reference image.

Editing and Deleting a Template

1. Right-click a server in the System Explorer and select **Setup** to open the server Setup dialog box. See Accessing the Server Setup for more information.
2. Click **Schedule**.
3. In the Schedule dialog box, select a template from the Templates pane and perform one of the following:
   - To edit a template, modify the schedule.
   - To rename a template, click **Rename Template** and enter a new name.
   - To delete a template, click **Delete Template**.
4. Click **OK**.

Setting Up a Weekly Recording Schedule

You can setup a week's recording schedule by applying different templates to cameras for specific days of the week.

1. Right-click a server in the System Explorer and select **Setup** to open the server Setup dialog box. See Accessing the Server Setup for more information.
2. Click **Schedule**.
3. In the Schedule dialog box, select a template from the Templates pane.
4. In the Default Week area, select the days of the week to apply the template schedule for each camera.

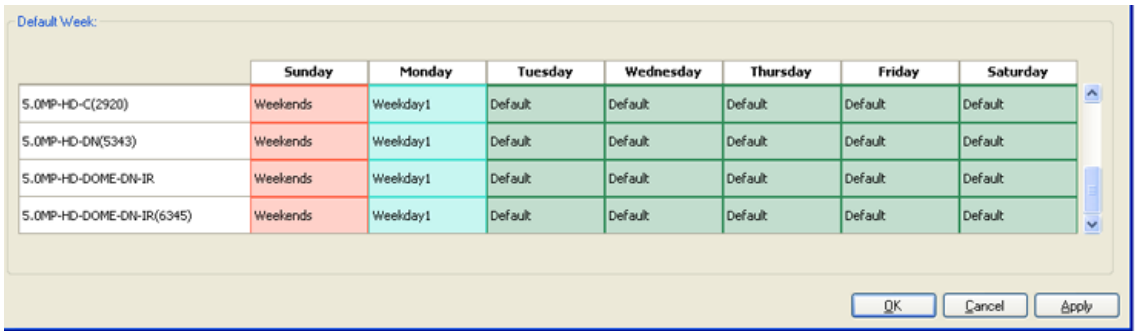


Figure A. Schedule dialog box: Default Week

5. Click **OK**.

Recording and Bandwidth

You can use the Recording and Bandwidth dialog box to change the server recording settings, and view the bandwidth used by each camera that is connected to the server.

Changing Recording Settings

1. Right-click a server in the System Explorer and select **Setup** to open the server Setup dialog box. See Accessing the Server Setup for more information.
2. Click **Recording and Bandwidth**. The Recording and Bandwidth dialog box appears.

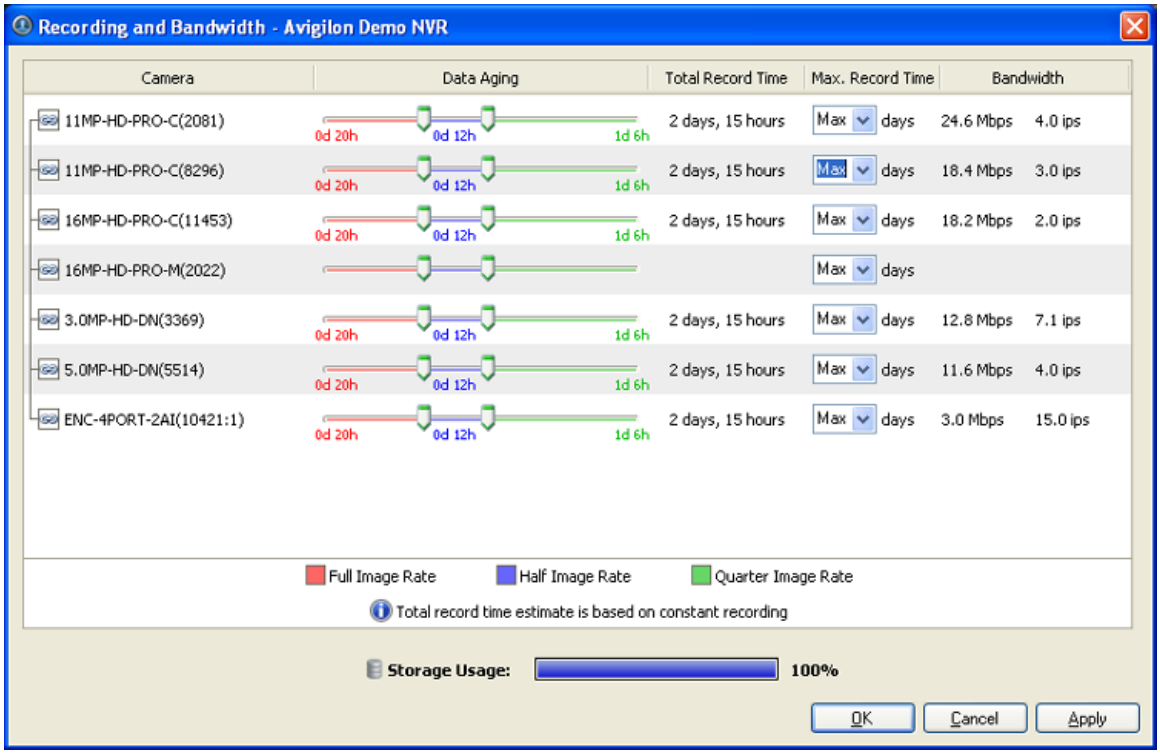


Figure A. Recording and Bandwidth dialog box

3. In the Data Aging area for each camera, move the sliders to adjust the amount of time video is stored at full, half, and quarter image rate.

   Note: Data Aging is only enabled for cameras using JPEG 2000 or JPEG compression.

   The settings for all linked cameras are changed at the same time. To control the settings for a single camera, break the camera's link by clicking the **Link** icon to the left of the camera's name and make the necessary adjustments.

4. In the **Max. Record Time** field, manually enter a maximum record time or select one of the options from the drop down list for each camera.

   If the auto-generated Total Record Time is shorter than the Max. Record Time setting, it may be an indication that your actual record time will be shorter than the Max. Record Time setting.

5. Click **OK**.

Users and Groups

When users are added to the Avigilon system, they are assigned to an access group that defines their access permissions on a server. Create and manage users and groups in the Users and Groups dialog box.

Adding a User

You can add users and manage their access permissions by assigning users to specific access groups.

1. Right-click a server in the System Explorer and select **Setup** to open the server Setup dialog box. See Accessing the Server Setup for more information.
2. Click **Users and Groups**.
3. In the User and Groups dialog box, click **Add User**.

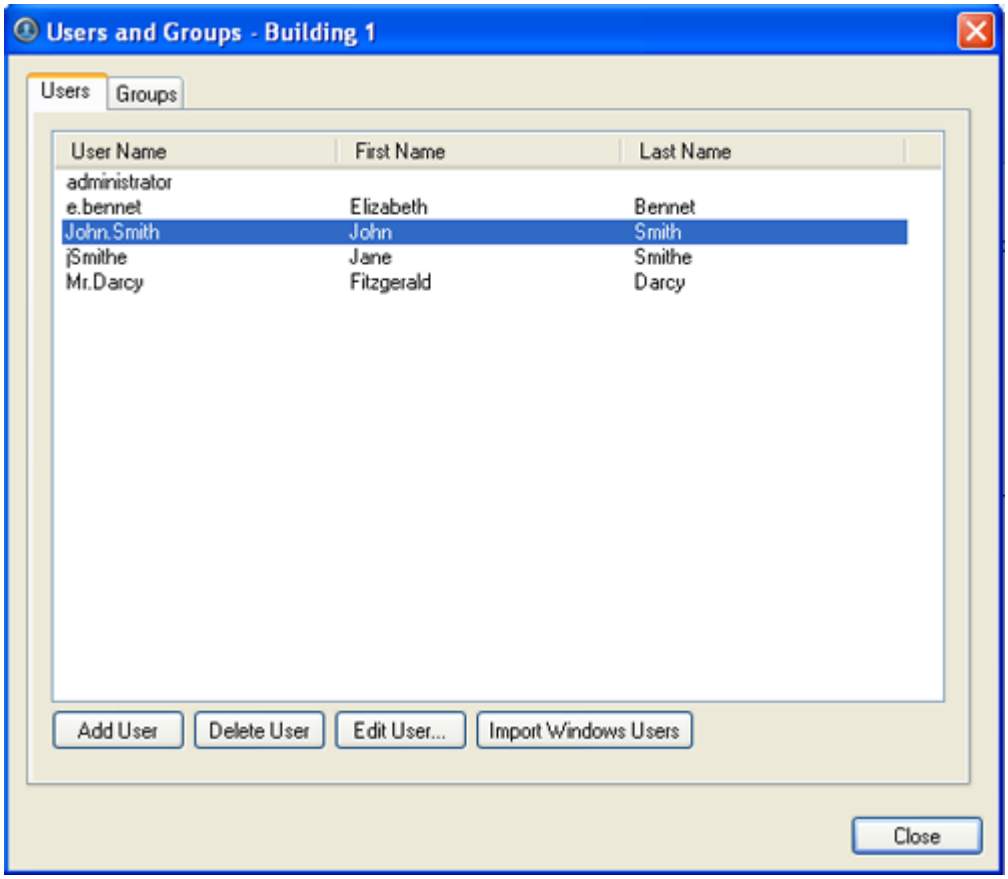


Figure A. User and Groups dialog box

4. When the Add User dialog box appears, complete the User Information area.

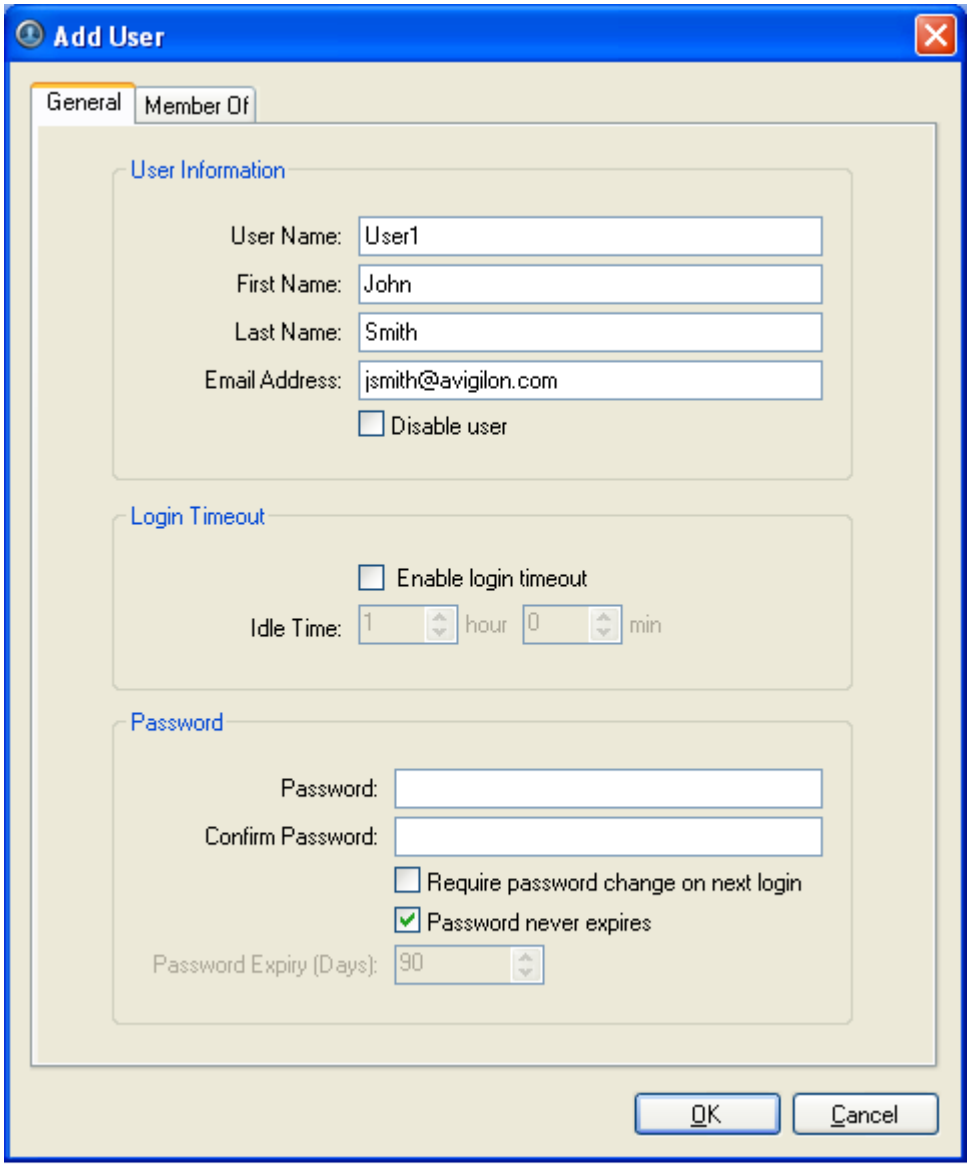


Figure B. Add User dialog box, General tab

5. If you don't want to make this user active yet, select the **Disable user** check box.
6. In the Login Timeout area, select the **Enable login timeout** check box to allow the application to log out the user after the application has been idle for the specified amount of time.
7. In the Password area, complete the following fields:
    - **Password:** enter a password for the user.
    - **Confirm Password:** re-enter the password.
    - **Require password change on next login:** select this check box if you want the user to personalize the password after their first login.

- **Password Expiry (Days):** specify the number of days before the password must be changed. This field is not required if the password never expires.
- **Password never expires:** select this check box if the password does not need to be changed.

8. Select the Member Of tab and assign the user to one or more access groups by selecting the appropriate check box in the Groups list.

   The other two columns display the permissions associated with the selected Groups.

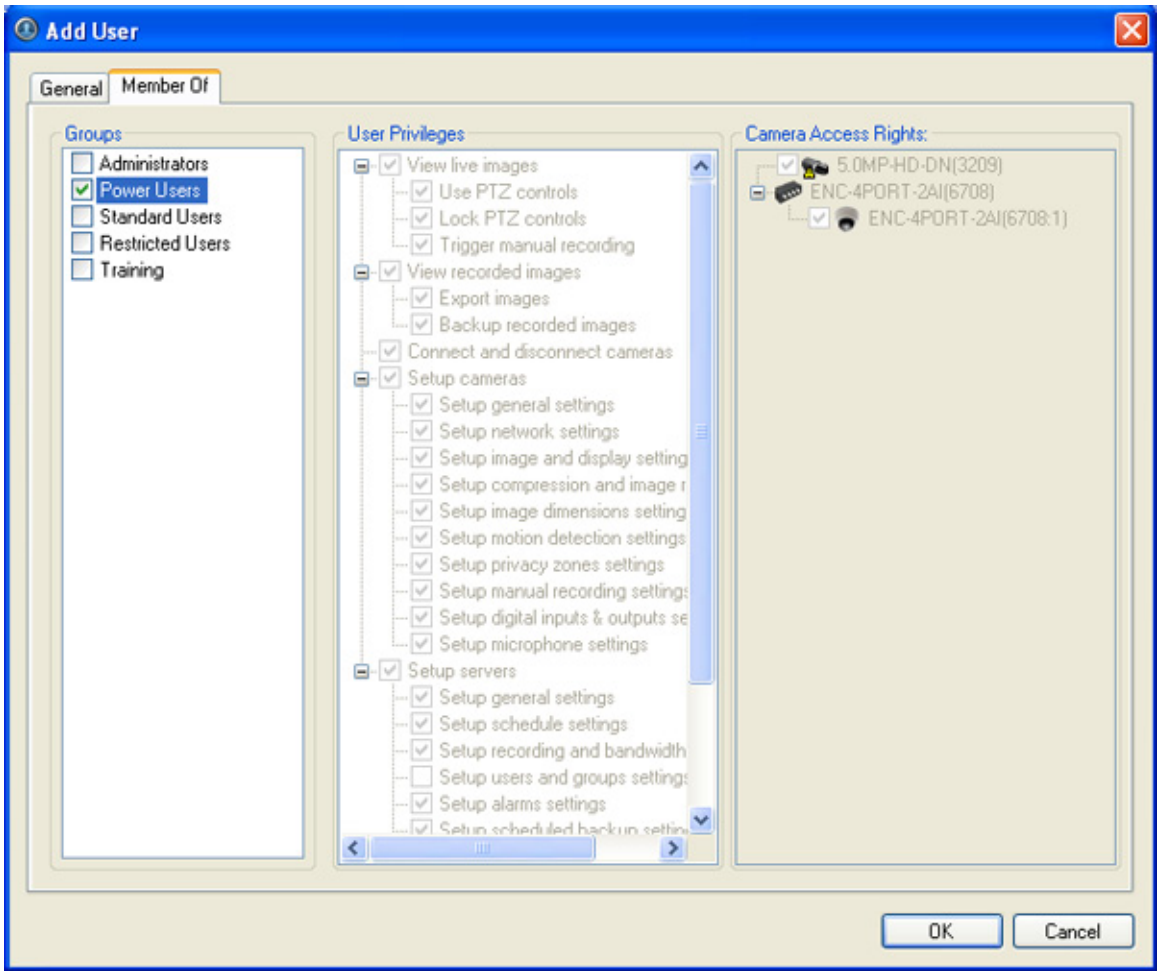


Figure C. Add User dialog box, Member Of tab

9. Click **OK**. The user is added to the server.

Editing and Deleting a User

You can edit the details of an existing user, or delete the user account that is no longer required.

Note: If a user has access to more than one server, the user needs to be removed from each server individually.

1. Right-click a server in the System Explorer and select **Setup** to open the server Setup dialog box. See Accessing the Server Setup for more information.
2. Click **Users and Groups**.
3. In the Users and Groups dialog box, select a user and perform one of the following:
    - Click **Edit User** to edit the user's information. Refer to Adding a User or details about the editable options.
    - Click **Delete User** to delete the user.

Importing Windows Users

You can import Windows user accounts on to the server to allow users to log in using their Windows credentials.

1. Right-click a server in the System Explorer and select **Setup** to open the server Setup dialog box. See Accessing the Server Setup for more information.
2. Click **Users and Groups**.
3. In the Users and Groups dialog box, click **Import Windows Users**.
4. In the Select Users or Groups dialog box, locate the Windows user you wish to add by performing one of the following:
    - In the Select Users or Groups dialog box, enter the name of a Windows user or group in the **Enter the object names to select field** and click **OK**.
    - In the Select Users or Groups dialog box, click the **Advanced** button and search for the users or groups to import.

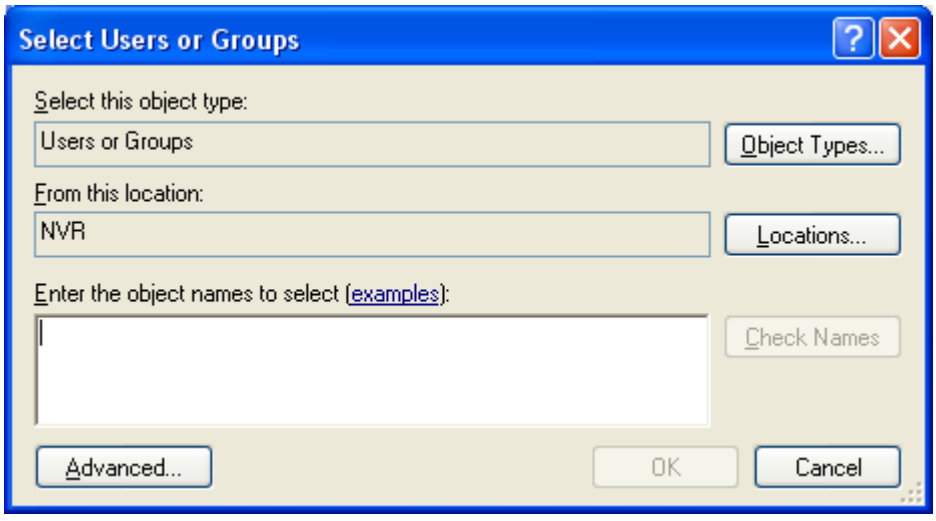


Figure A. Select Users or Groups dialog box

5. In the Import Windows Users dialog box, select the users you wish to import and assign the users to an access group by selecting the appropriate **Groups** check box.

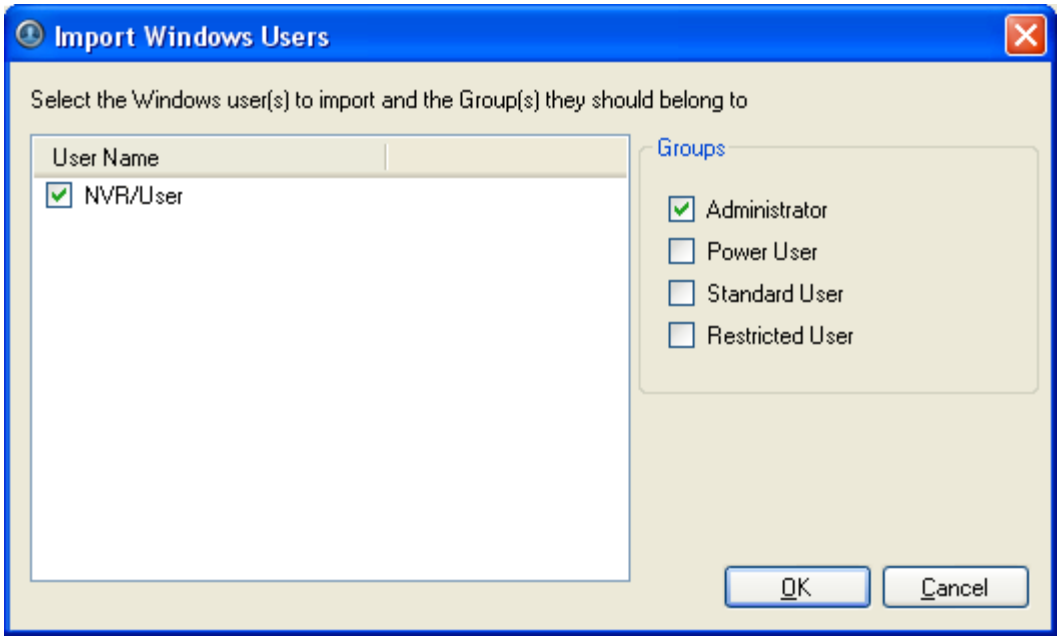


Figure B. Import Windows Users dialog box

Note: If you are importing multiple Windows users, be aware that you are assigning all selected users to the same access group.

6. Click **OK**.

Adding Groups

You can change users' access permissions by changing their access groups. Create new groups to define specific sets of access permissions.

Note: Access permissions for the Administrator group cannot be modified.

1. Right-click a server in the System Explorer and select **Setup** to open the server Setup dialog box. See Accessing the Server Setup for more information.
2. Click **Users and Groups**.
3. In the Users and Groups dialog box, select the Groups tab and click **Add Group**.

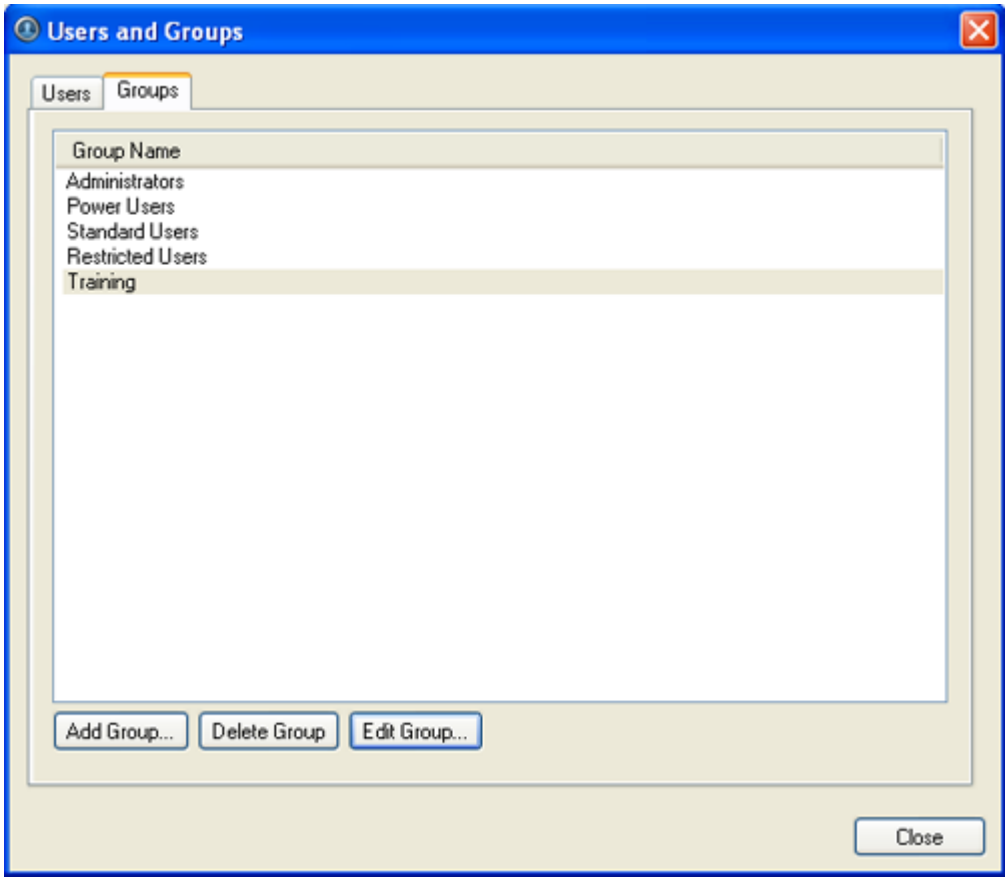


Figure A. User and Groups dialog box

4. In the Add Group dialog box, select a group to use as a template for your new group and click **OK**.

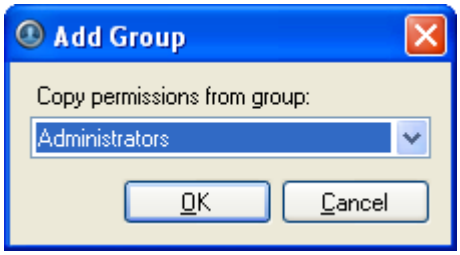


Figure B. Add Group dialog box

5. In the Edit Group dialog box, give the new group a name then select the permissions and camera access rights for the group.

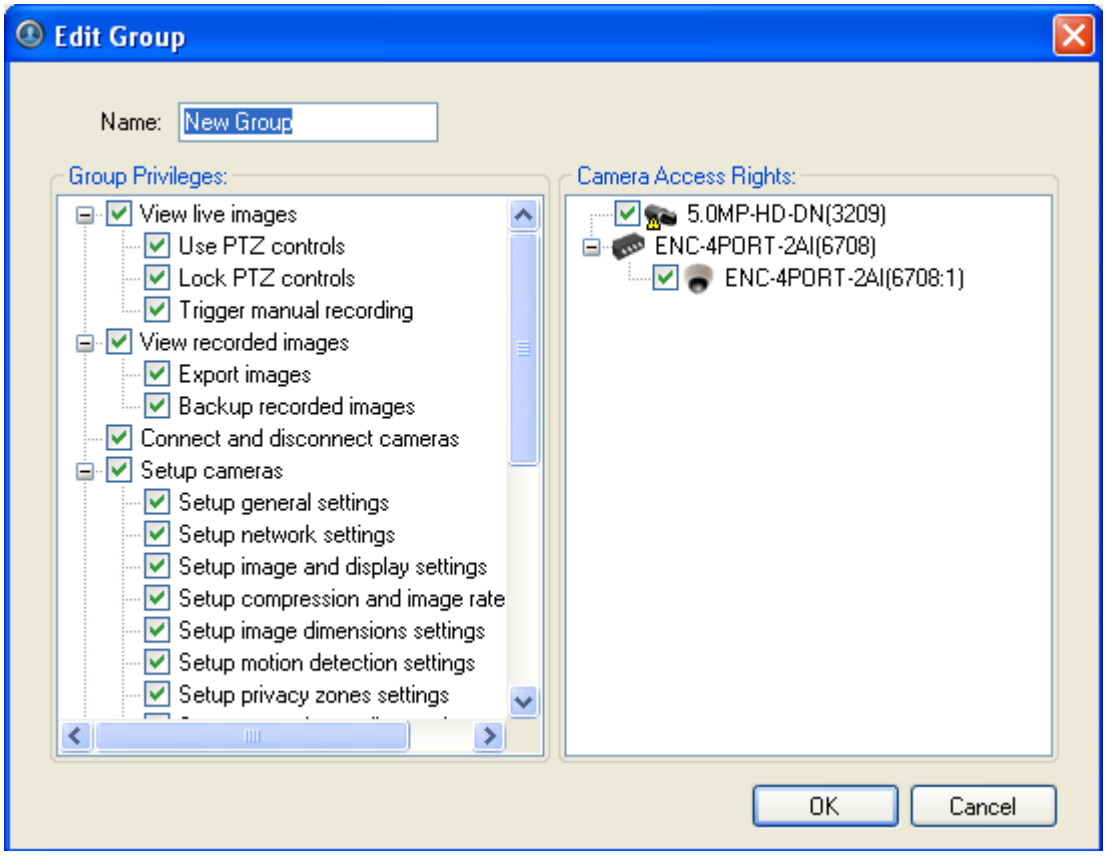


Figure C. Edit Group dialog box

6. Click **OK**.

Editing and Deleting a Group

You can change the access permissions for a set of users by editing their access group.

Note: The Administrators group cannot be edited or deleted.

1. Right-click a server in the System Explorer and select **Setup** to open the server Setup dialog box. See Accessing the Server Setup for more information.
2. Click **Users and Groups** and select the Groups tab.
3. Select a group and perform one of the following:
   - To edit the group, click **Edit Group**. In the Edit Group dialog box, change the permissions and camera access rights as required then click **OK**. Refer to Adding Groups for details about the editable options.
   - To delete the group, click **Delete Group**.

     Note: Default groups cannot be deleted.

Alarms

The Alarms dialog box allows you to create and configure alarms. Alarm triggers can include Motion Detection, Digital Input Activation, License Plate Watchlist match, POS Transaction Exception, Camera Error, System Error and External Software Event.

Adding a New Alarm

Alarms need to be added to the server Setup before they can be monitored in the Alarms tab.

1. Right-click a server in the System Explorer and select **Setup** to open the server Setup dialog box. See Accessing the Server Setup for more information.
2. Click **Alarms**.
3. In the Alarms dialog box, click **Add**.
4. Select the **Alarm Trigger Source** then select the required features for the alarm. Click **Next**.

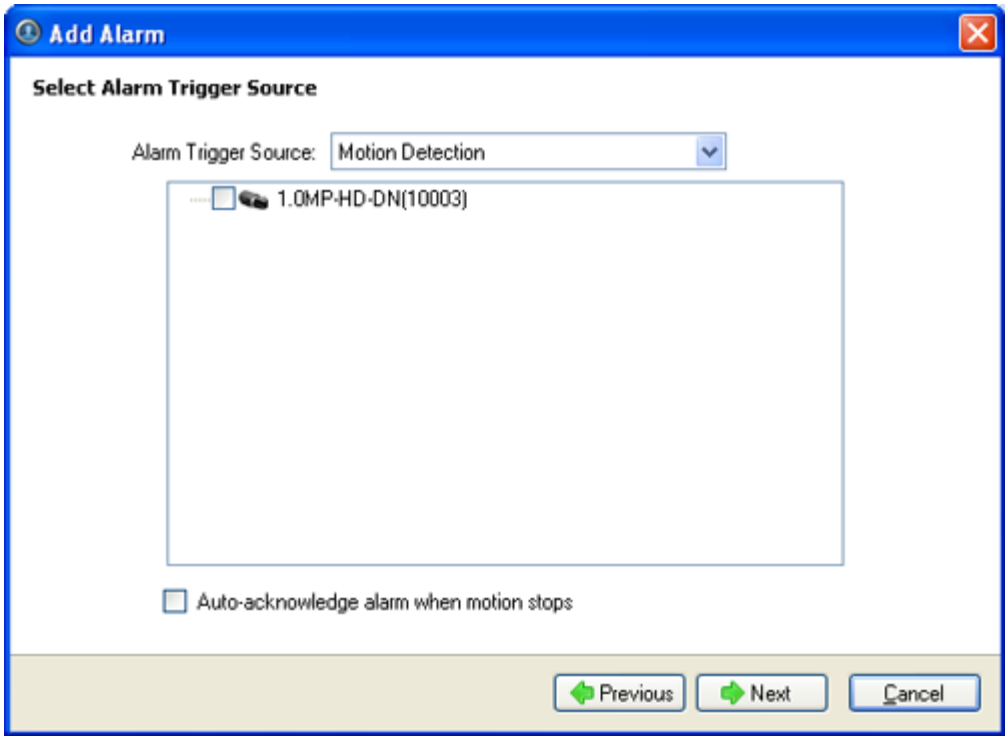


Figure A. Select Alarm Trigger Source page

5. Select the cameras to link to this alarm then complete the following:

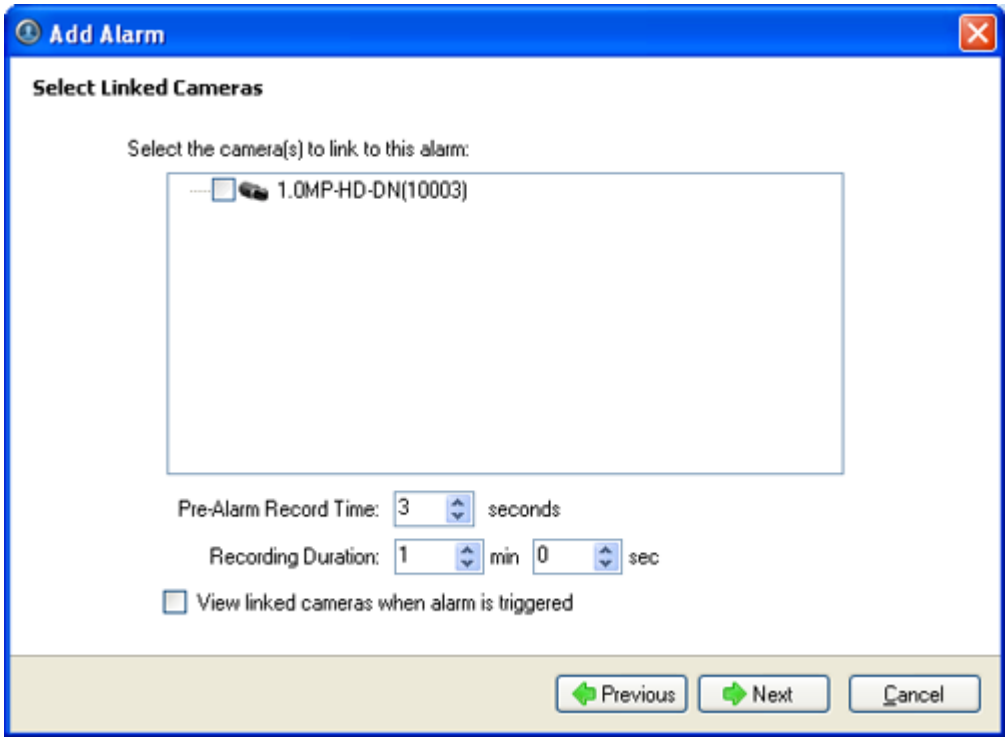


Figure B. Select Linked Cameras page

a. Set the **Pre-Alarm Record Time** and the **Recording Duration**.

b. Select the **View linked cameras when alarm is triggered** check box to automatically display the alarm video in a View when the alarm is triggered.

c. Click **Next**.

6. Select the groups or users who should receive alarm notifications, and decide if the alarm should play a sound. Then click **Next**.

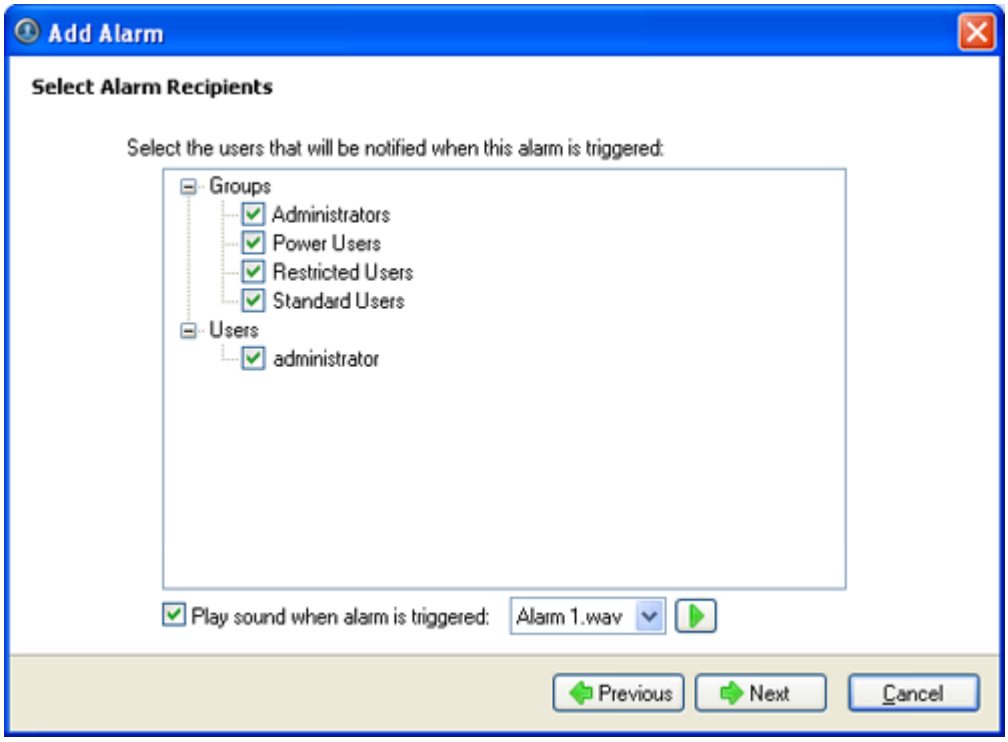


Figure C. Select Alarm Recipients page

7. (Optional) If you would like to trigger an action when an alarm is acknowledged, select the **Activate selected digital output(s) on alarm acknowledgement** check box.

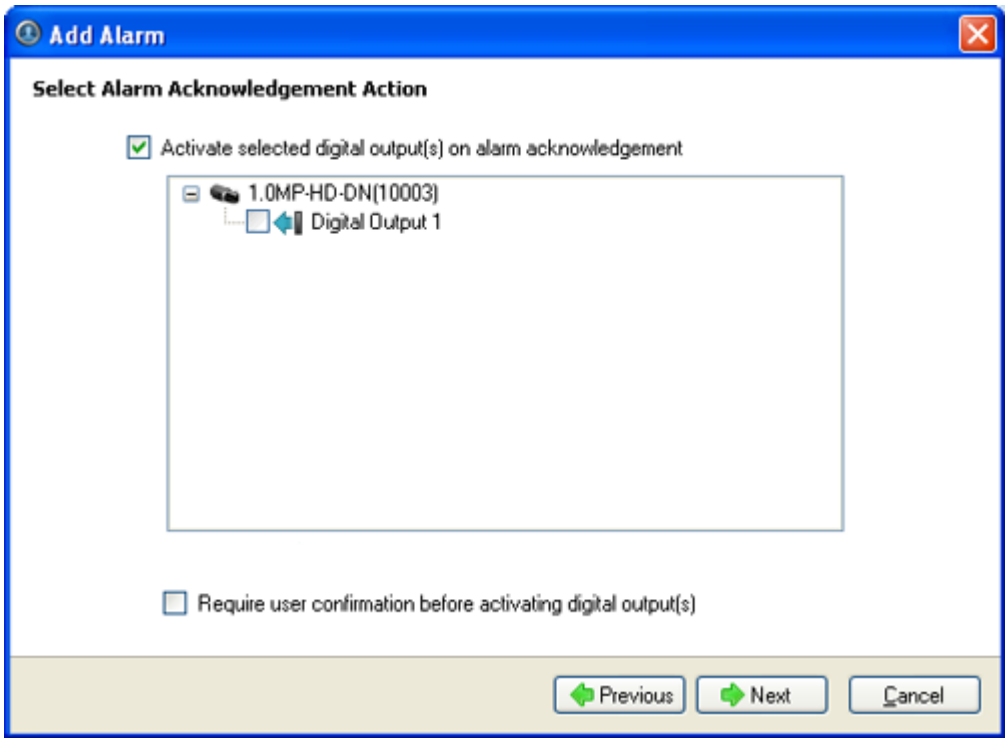


Figure D. Select Alarm Acknowledgement Action page

a. Select the digital outputs to be activated and specify the duration.

b. If the digital output should only be activated by user confirmation after an alarm has been acknowledged, select the **Require user confirmation before activating digital output(s)** check box.

c. Click **Next**.

8. On the Select Alarm Properties page, enter a name and select a priority number for the alarm. **Priority: 1** represents the highest alarm priority.

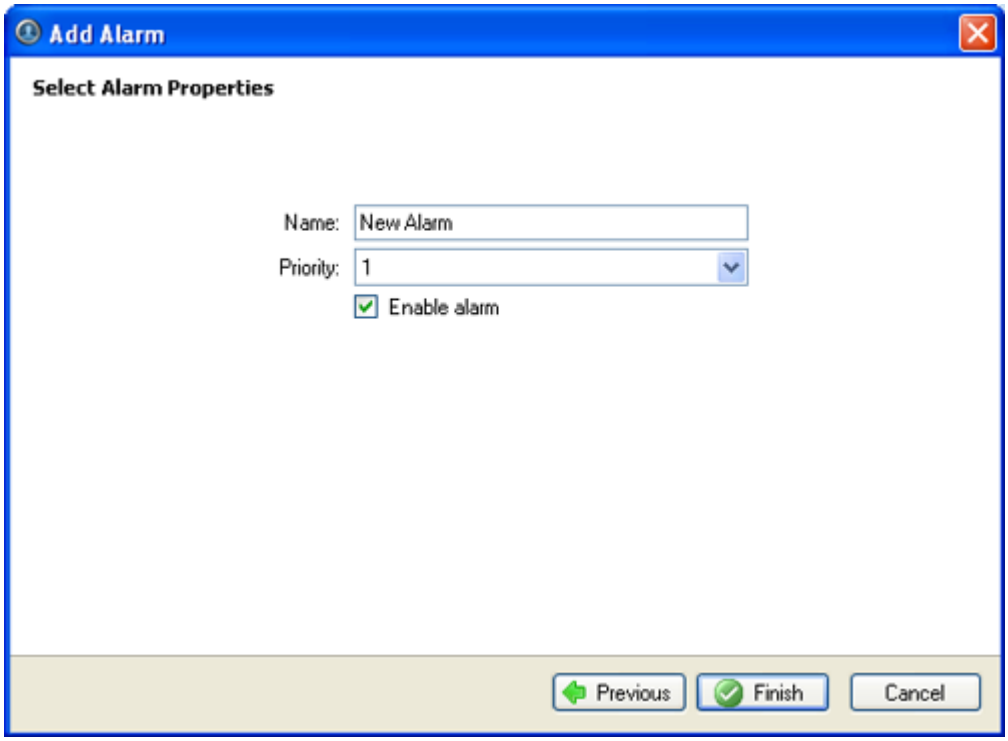


Figure E. Select Alarm Properties page

9. Click **Finish**.

Editing and Deleting Alarms

1. Right-click a server in the System Explorer and select **Setup** to open the server Setup dialog box. See Accessing the Server Setup for more information.

2. Click **Alarms**.

3. In the Alarms dialog box, select the alarm you want to modify.

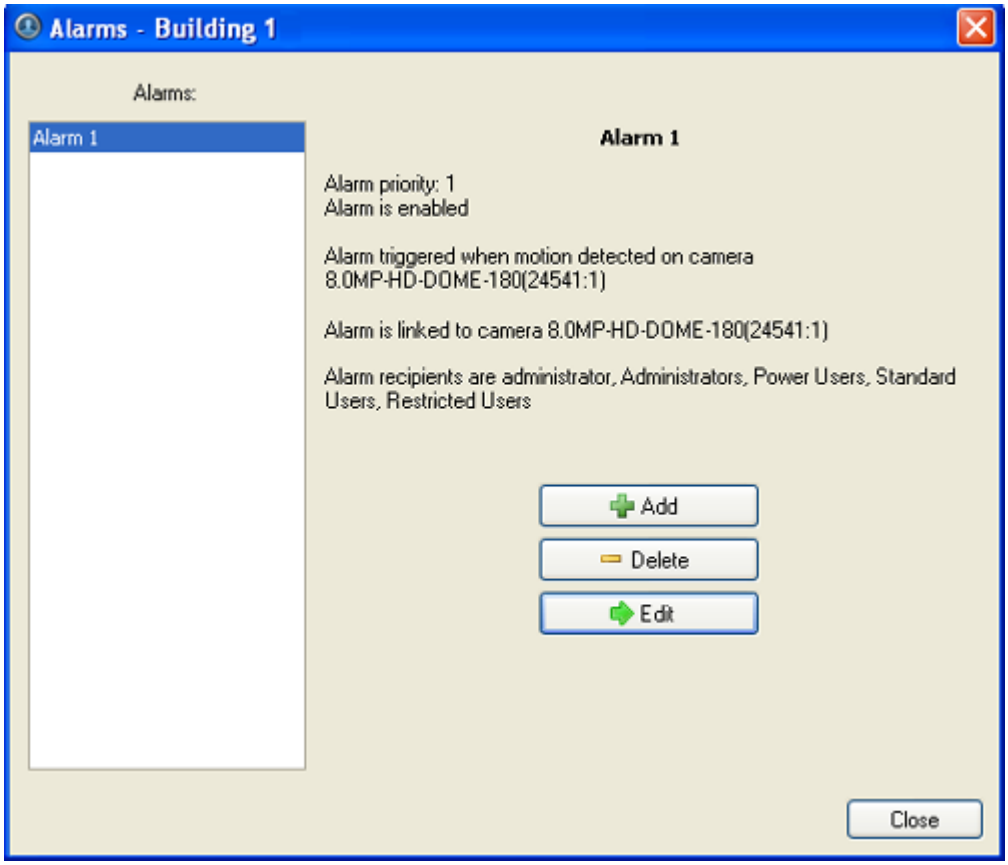


Figure A. Alarms dialog box: alarm properties

4. Perform one of the following:
    - Click **Edit** to edit the alarm. Go through the Add Alarm wizard and make the required changes on each page. On the last page, click **Finish**. Refer to Adding a New Alarm for details about the editable options.
    - Click **Delete** to delete the alarm.

Scheduled Backup

Data backup must be enabled on the server before scheduled backup settings can be modified in the Avigilon Control Center Client software.

See the *Avigilon Control Center Server User Guide* for more information about enabling backup on the server through the Avigilon Control Center Admin Tool.

Files are always backed up in the Avigilon Backup (AVK) format. You can review backed up video in the Avigilon Control Center Player.

Changing Scheduled Backup Settings

In the Scheduled Backup dialog box, configure when image data is backed up on the server.

Note: The video backup location is configured in the Avigilon Control Center Admin Tool. See the *Avigilon Control Center Server User Guide* for more information.

1. Right-click a server in the System Explorer and select **Setup** to open the server Setup dialog box. See Accessing the Server Setup for more information.
2. Click **Scheduled Backup**.

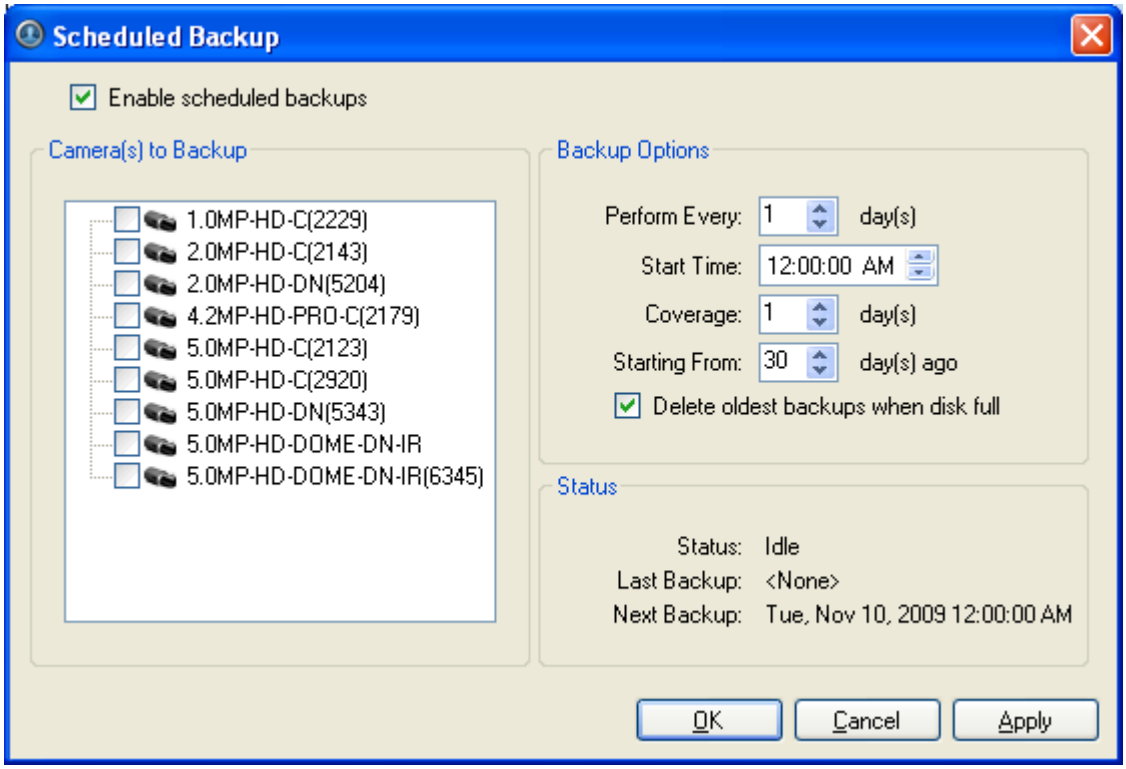


Figure A. Scheduled Backup dialog box

3. Select the **Enable scheduled backups** check box.
4. In the Camera(s) to Backup area select all the cameras to backup.
5. In the Backup Options area, complete the following:
   - **Perform Every <X> day(s):** specify the number of days between backups
   - **Start Time:** the time when backup occurs
   - **Coverage:** the amount of recorded image data that is backed up
   - **Starting From:** starting point for the backup

- **Delete oldest backups when disk full:** select this check box to automatically delete the oldest backups when the target disk is full

For example in the image above, the Scheduled Backup is configured to occur every day at 12a.m. The image data starting from 30 days ago is backed up and the back up only covers 1 day, so only the 30th day is backed up to the remote server.

6. Click **OK**.

   The Status area displays when the next backup will be.

POS Transactions

The Point of Sale (POS) Transaction Engine is a licensed feature that records video and raw data from POS transaction sources. POS transaction sources can be added to the Avigilon Control Center System and configured in the Client software.

Adding a POS Transaction Source

1. Right-click a server in the System Explorer and select **Setup** to open the server Setup dialog box. See Accessing the Server Setup for more information.
2. Click **POS Transactions**.
3. In the POS Transactions dialog box, click **Add**.
4. Enter the **Hostname/IP Address** and the **Port** for the POS Transaction Source device. Click **Next**.

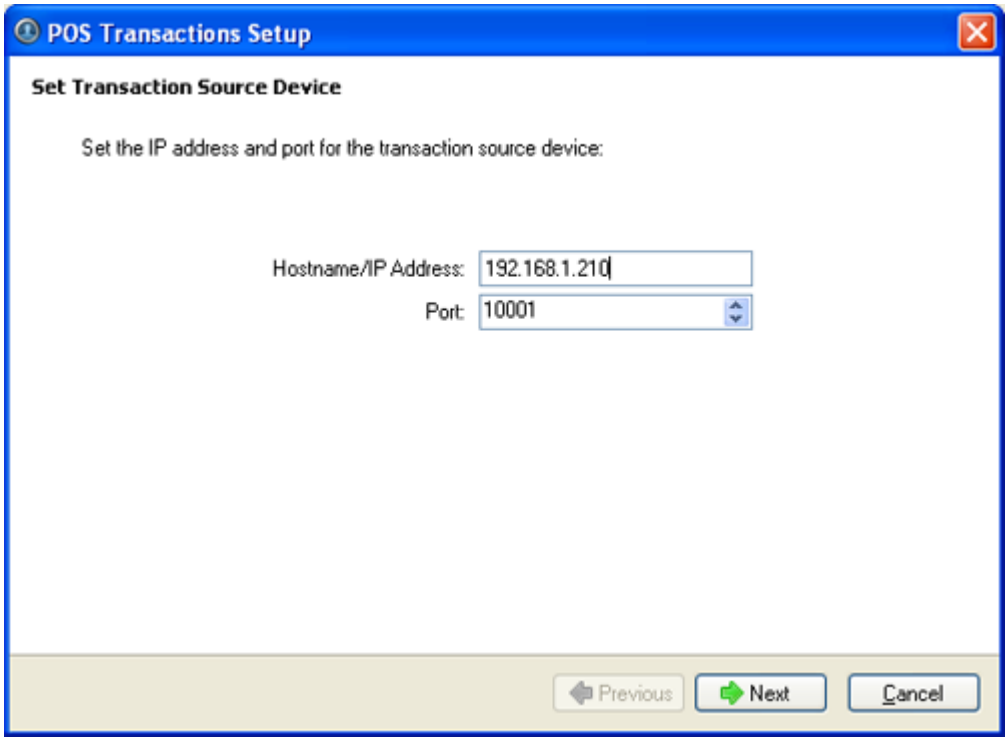


Figure A. Set Transaction Source Device page

5. Select a Transaction Source Data format and click **Next**.

   If the source data format needs to be added, click **Add**. Or, click **Copy From** to create a new data format based on the selected data format. See Adding a Transaction Source Data Format for more information.

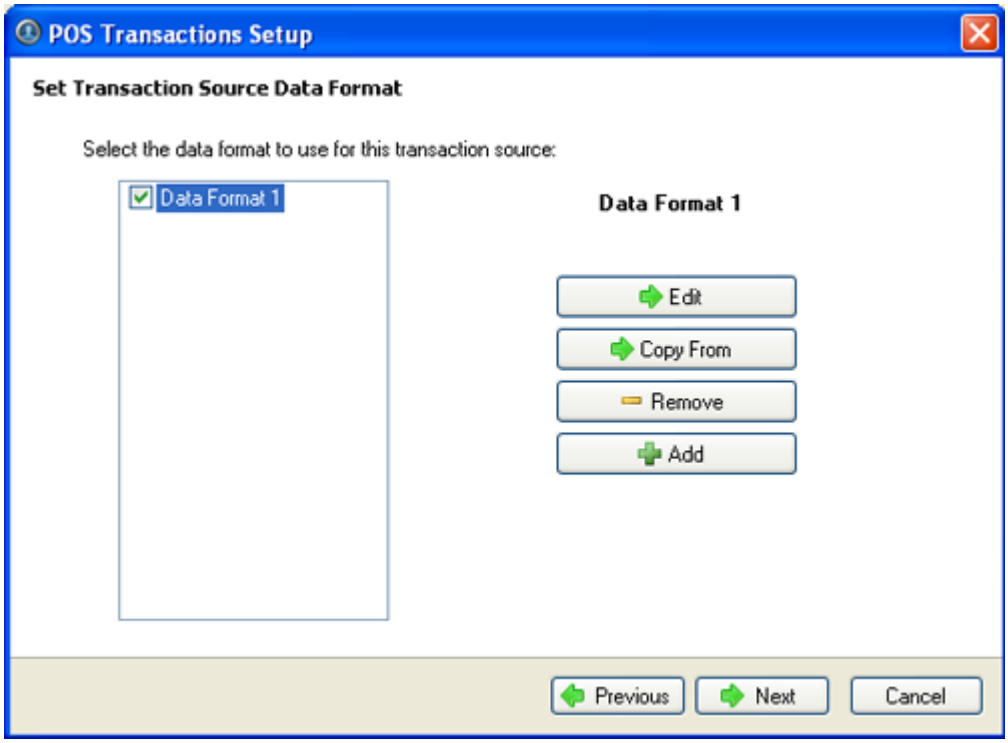


Figure B. Set POS Transaction Source Data Format page

6. On the Set Transaction Exceptions page, select any exceptions that should be monitored for on this transaction source and click **Next**. If no exceptions are required, just click **Next**.

   Click **Add** to add an exception. See Adding a Transaction Exception for more information.

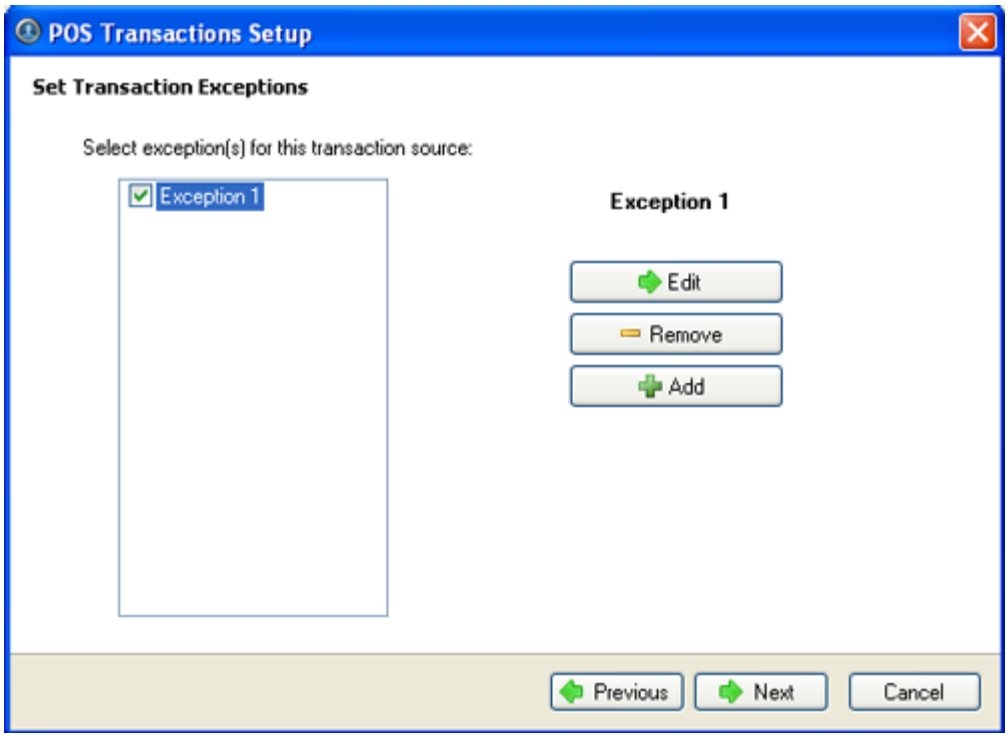


Figure C. Set Transaction Exceptions page

7. Select the cameras to link to the transaction source, and set the pre-transaction record time and post-transaction record time. Click **Next**.

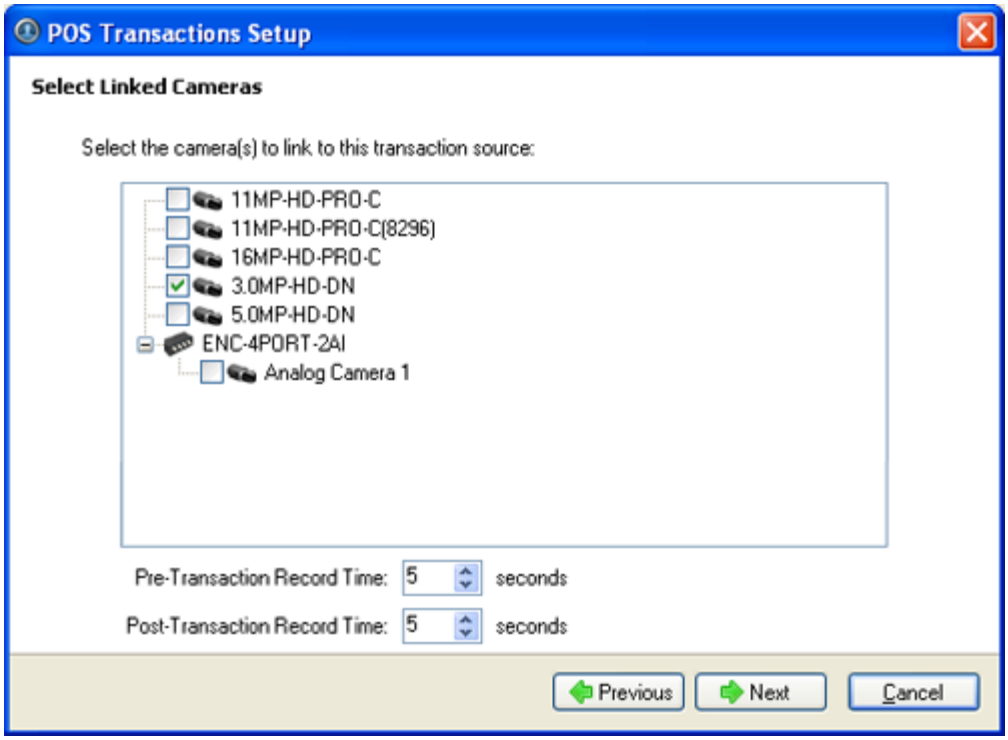


Figure D. Select Linked Cameras page

8. Enter a transaction source name and description, select **Enable transaction source**.

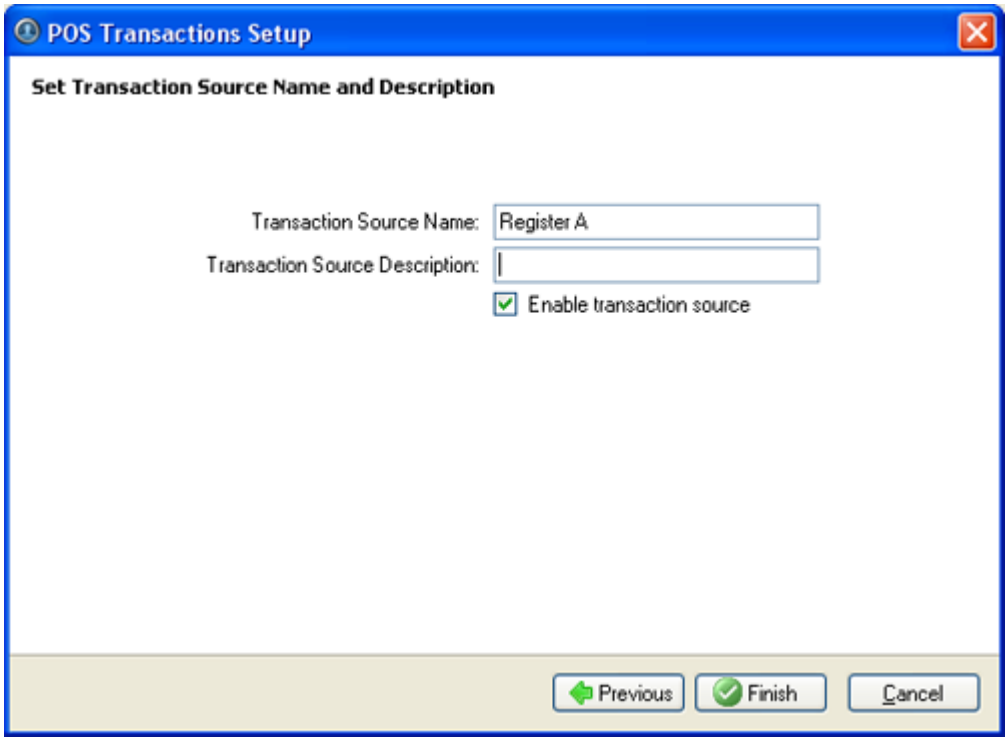


Figure E. Set Transaction Source Name and Description page

9. Click **Finish**.

Adding a Transaction Source Data Format

When you add a new POS transaction source, be aware that the transaction source must have a source data format.

In the POS Transaction Setup wizard, click **Add** when you arrive on the Set Transaction Source Data Format page. When the Configure Data Format dialog box appears, complete the following procedure:

1. In the Properties area, specify the following:

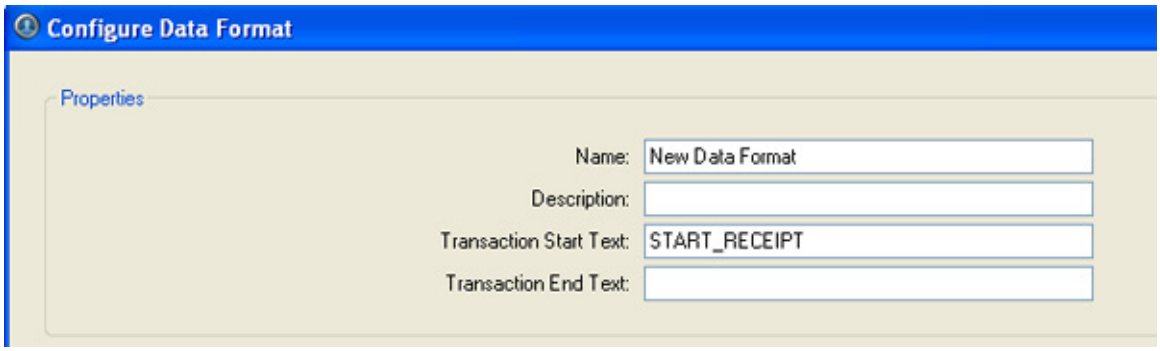


Figure A. Configure Data Format dialog box

- **Name:** enter a name for the data format.

- **Description:** enter a description of the data format if required.
- **Transaction Start Text:** (required) enter the text that identifies the start of each transaction from the POS transaction source.
- **Transaction End Text:** (optional) enter the text that identifies the end of each transaction.

2. The two boxes below show raw and filtered transaction data. Perform any of the following:

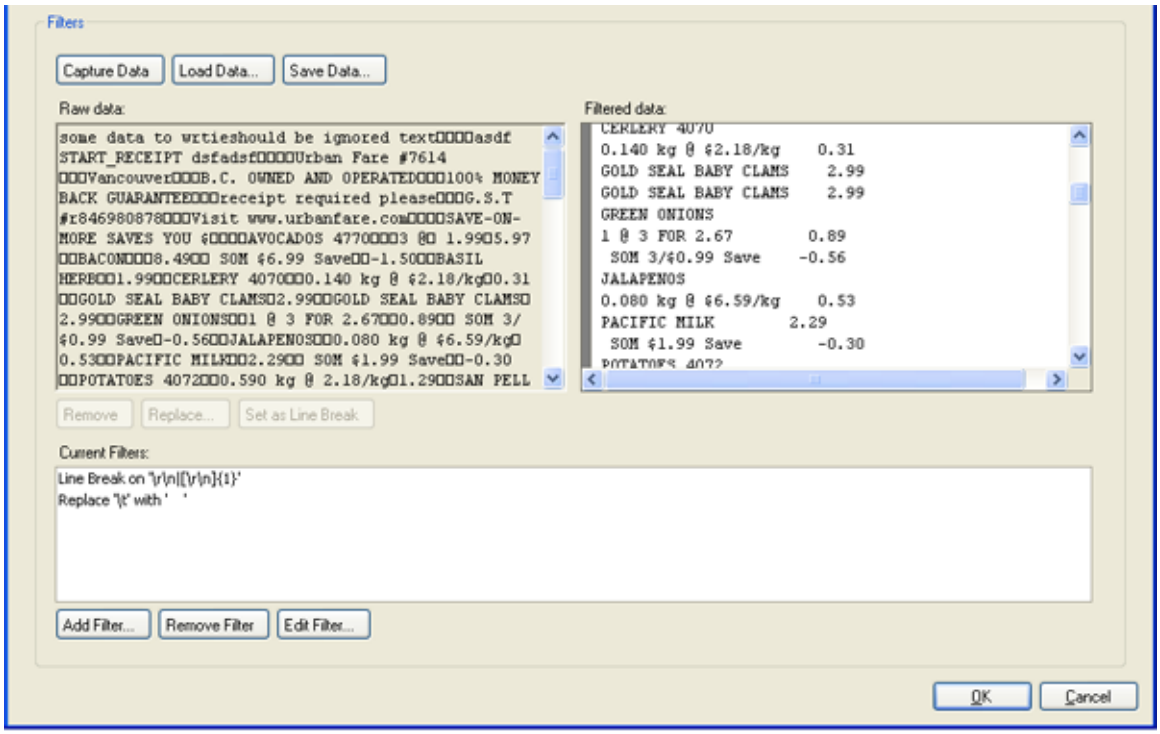


Figure B. Configure Data Format dialog box

- Click **Capture Data** to start capturing a raw transaction data sample.
- Click **Stop Capture** to stop capturing transaction data.
- Click **Load Data** to load raw transaction data from a file.
- Click **Save Data** to save transaction data.

3. (Optional) Click **Add Filter** to create a new filter for the raw transaction data file.

   There are several default filters for line breaks listed in the Current Filters area, if the default filters are sufficient for your needs, skip this step.

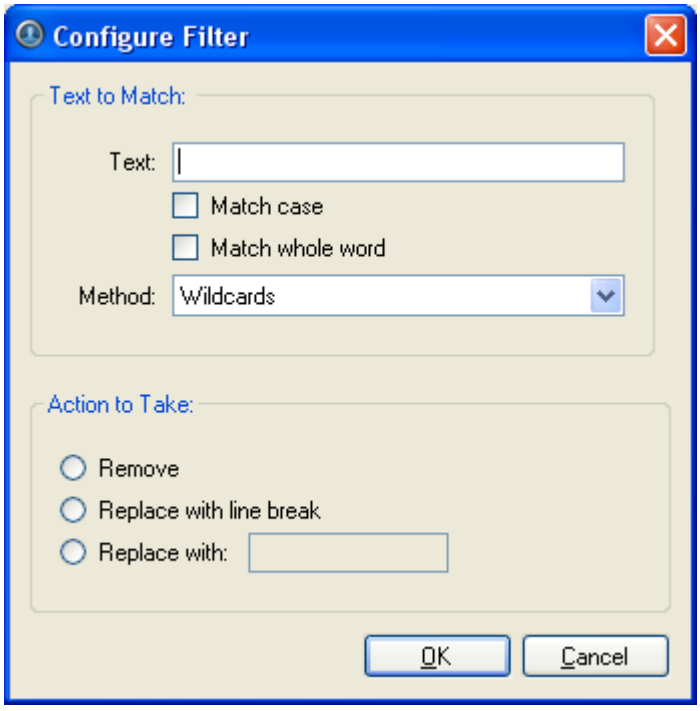


Figure C. Configure Filter dialog box

2.

a. In the **Text** field, enter text for the filter to search for.
b. Select **Match case** and/or **Match whole word** check box to focus the text filter to only find text with the same capitalization or match the text exactly.

c. Select a method from the **Method** drop down list.
d. In the Action to Take area, select which action to take when the filter finds a match to your text criteria.

e. Click **OK**.

3. On the Configure Data Format screen, click **OK** to add the new data format to the data format list.

Adding a Transaction Exception

In the POS Transaction Setup wizard, click **Add** when you arrive on the Set Transaction Exceptions page. When the Configure Exception dialog box appears, complete the following procedure:

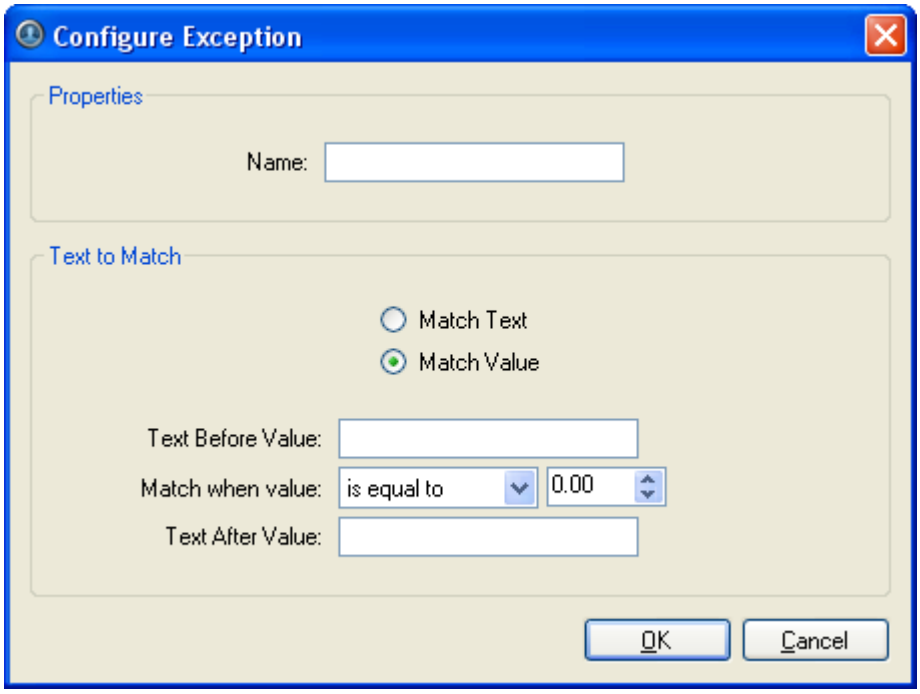


Figure A. Configure Exception dialog box

1. Enter a name.
2. Select one of the Text to Match options:

Select	And do this...
Match Text	Enter text for the exception to search for. The exception will search for instances that are an exact match to the text entered in the **Text to Match** field.
Match Value	Enter the value that triggers the exception, and enter the text that may appear around the value. The exception will search for values that match the values you enter in the **Text Before Value**, **Match When Value** and **Text After Value** fields

3. Click **OK.**

Editing and Deleting a POS Transaction Source

1. Right-click a server in the System Explorer and select **Setup** to open the server Setup dialog box. See Accessing the Server Setup for more information.
2. Click **POS Transactions**.

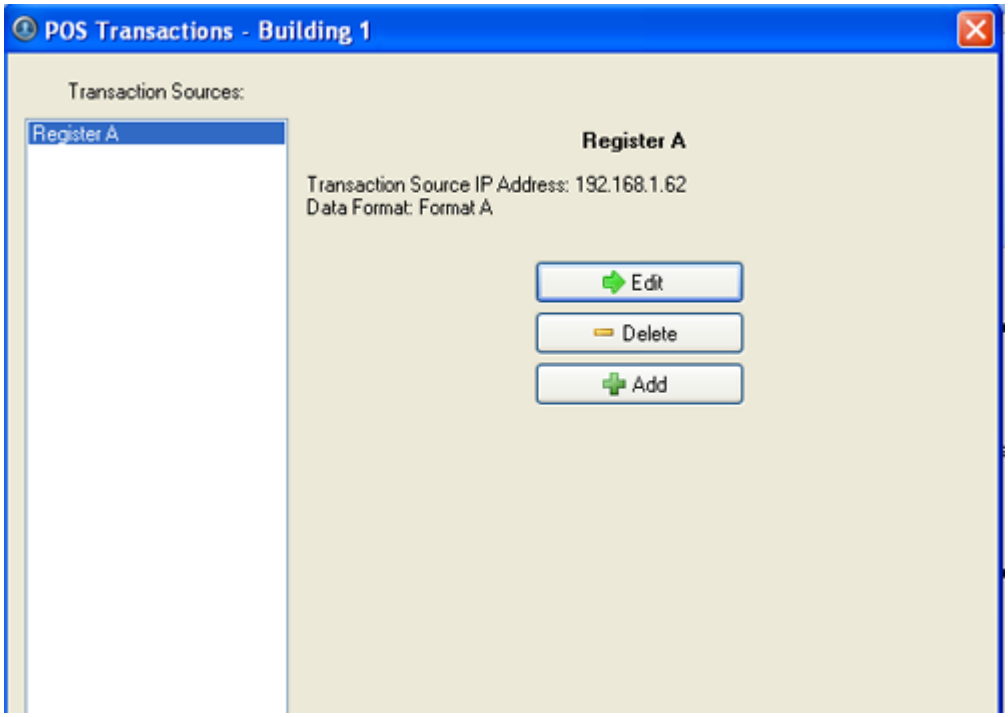


Figure A. POS Transactions dialog box

3. In the POS Transaction dialog box, select a POS transaction source then perform one of the following:
    - Click **Edit** to edit the POS transaction source. Go through the POS Transaction Setup wizard and make the required changes on each page. On the last page, click **Finish**. Refer to Adding a POS Transaction Source for details about the editable options.
    - Click **Delete** to delete the POS transaction source. When the confirmation dialog box appears, click **OK**.

Email Notification

Use the Email Notification dialog box to prepare the server for sending email messages in response to events. You can configure what events require email notification and who receives the emails.

Setting Up the Email Server

Before emails can be sent, the server must be set up to send emails.

1. Right-click a server in the System Explorer and select **Setup** to open the server Setup dialog box. See Accessing the Server Setup for more information.
2. Click **Email Notification**.
3. In the Email Notification dialog box, select the Email Server tab.

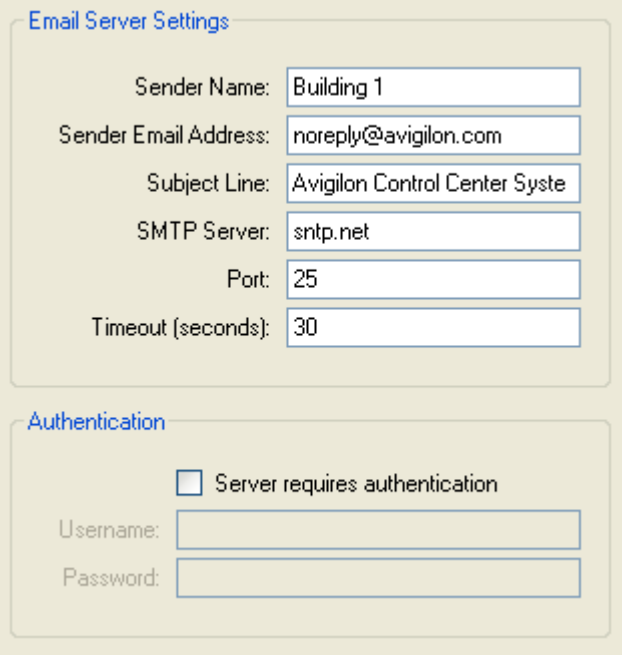


Figure A. Email Notifications dialog box: Email Server tab

4. In the Email Server Settings area, specify the following
    a. **Sender Name:** enter a name to represent the server sending out the email.
    b. **Sender Email Address:** enter an email address the server can use to send emails.
    c. **Subject Line:** enter a default subject line for all emails sent from this server.
    d. **SMTP Server:** enter the SMTP server address used by the server's email.
    e. **Port:** enter the SMTP port.
    f. **Timeout (seconds):** enter the maximum number of seconds the server will attempt to send the email before it stops.
5. (Optional) In the **Authentication** area, select the **Server requires authentication** check box.
    a. Enter the server **Username** and **Password**.
6. Click **OK**.

Configuring Email Notification

In the Email Notification dialog box, you can create email notification groups to specify who will receive email notifications when an event occurs.

1. Right-click a server in the System Explorer and select **Setup** to open the server Setup dialog box. See Accessing the Server Setup for more information.
2. Click **Email Notification**.

3. In the Email Notification dialog box, ensure the Email Notification tab is selected.
4. Click **Add**.

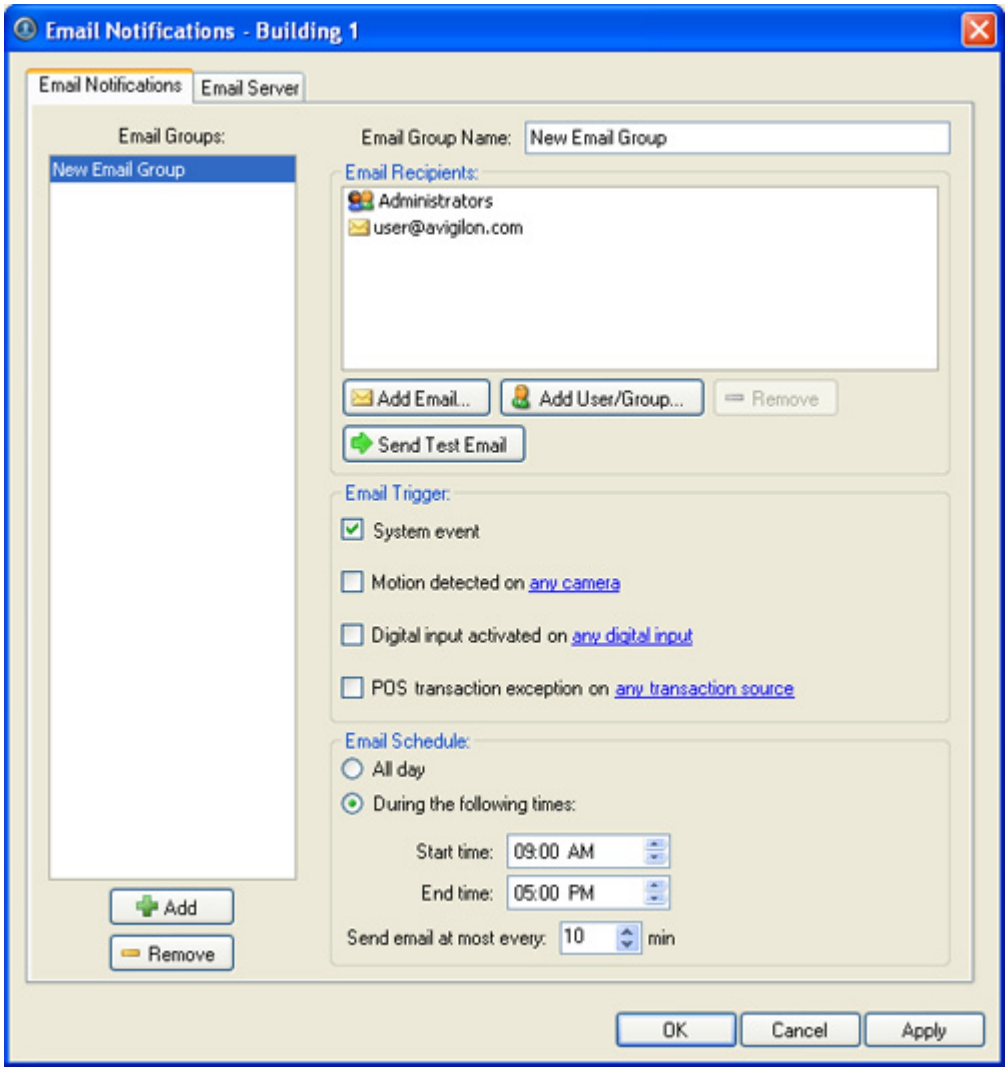


Figure A. Email Notifications dialog box

5. Enter a name for the new email group.
6. In the Email Recipients area, add all the users, groups and emails that are part of this email group. Perform any of the following:
   - Click **Add User/Group** to add an Avigilon Control Center user or access group. In the dialog box, select all the required users and groups then click **OK**.
   - Click **Add Email** to add individual emails. In the dialog box, enter the email address then click **OK**.

   Tip: Ensure the Avigilon users and groups added to the Email Recipient list have a valid email in their user profile.

7. Click **Send Test Email** to send a test email to everyone on the Email Recipients list.
8. In the Email Trigger area, select all the events that this email group will be notified of. Click the blue text to define the event requirements.

   If you require other events or more specific requirements, you can also configure email notification in the rules engine. See Rules for more information.
9. In the Email Schedule area, select when emails are sent.
   - Select **All day** to send email notifications whenever events occur.
   - Select **During the following times** to send email notifications only during the specified time range. You can limit the number of emails sent by setting the time interval between each email.
10. Click **OK**.

Editing and Deleting an Email Notification

You can edit the details of an email notification or delete the email notification when it is no longer required.

1. Right-click a server in the System Explorer and select **Setup** to open the server Setup dialog box. See Accessing the Server Setup for more information.
2. Click **Email Notification**.
3. In the Email Notification dialog box, ensure the Email Notification tab is selected then perform one of the following:
   - To edit the email notification, select the Email Group and make the required changes, then click **OK**. Refer to Configuring Email Notification for details about the editable options.
   - To delete the email notification, select the Email Group and click **Remove**.

Rules

The rules engine allows you to trigger specific actions when certain events occur.

For example, starting a live stream when a digital input is triggered, or sending an email to an administrator when a camera is disconnected.

Adding a Rule

1. Right-click a server in the System Explorer and select **Setup** to open the server Setup dialog box. See Accessing the Server Setup for more information.

2. Click **Rules**.
3. In the Rules dialog box, click **Add**.
4. Select the events that will trigger the rule. If blue underlined text appear in the rule description, click on the link to further define the event.

   For example, in the image below, you can define the specific camera that triggers the **connection has failed** rule by clicking the blue link.

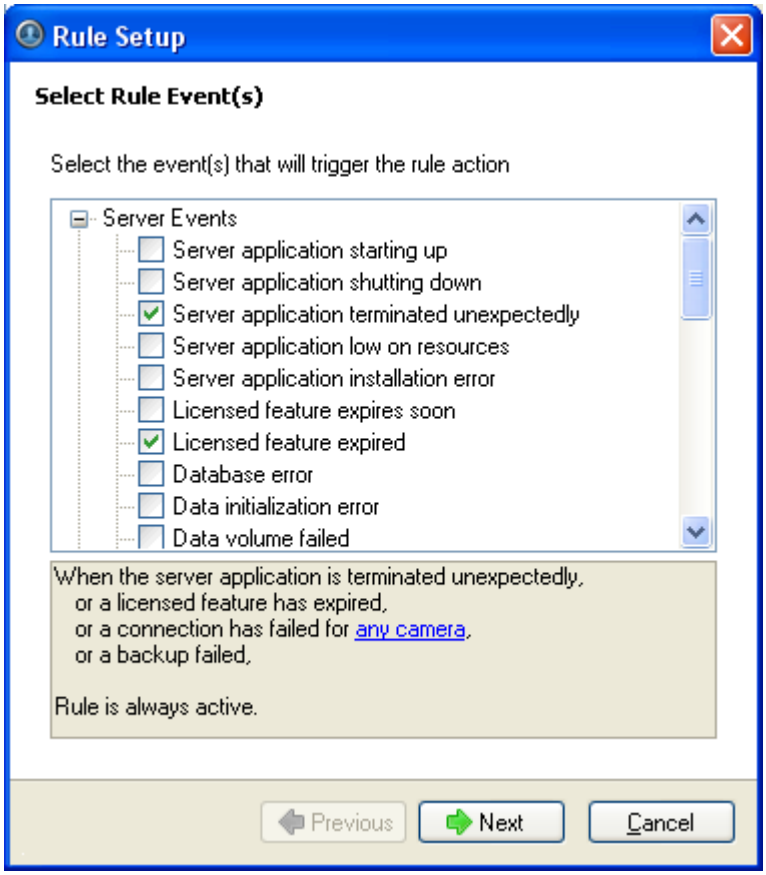


Figure A. Select Rule Event(s) page

5. When the trigger event is defined, click **Next**.
6. Select the actions that will occur when the rule is triggered. If any blue underlined text appear in the rule description, click on the link to further define the action. When the action is defined, click **Next**.

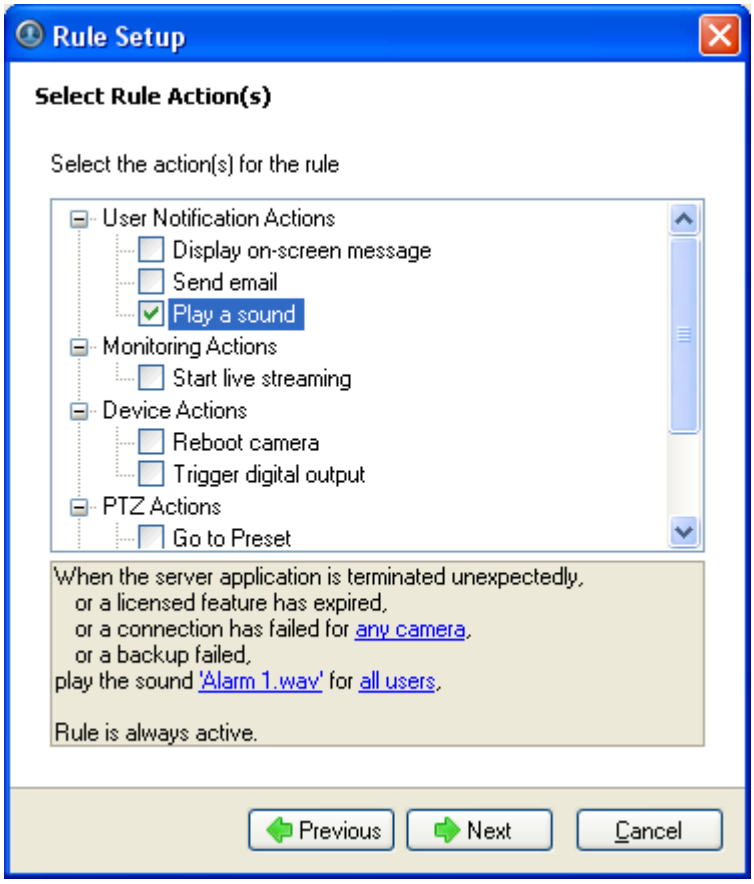


Figure B. Select Rule Action(s) page

7. Select when the rule should be active then click **Next**.

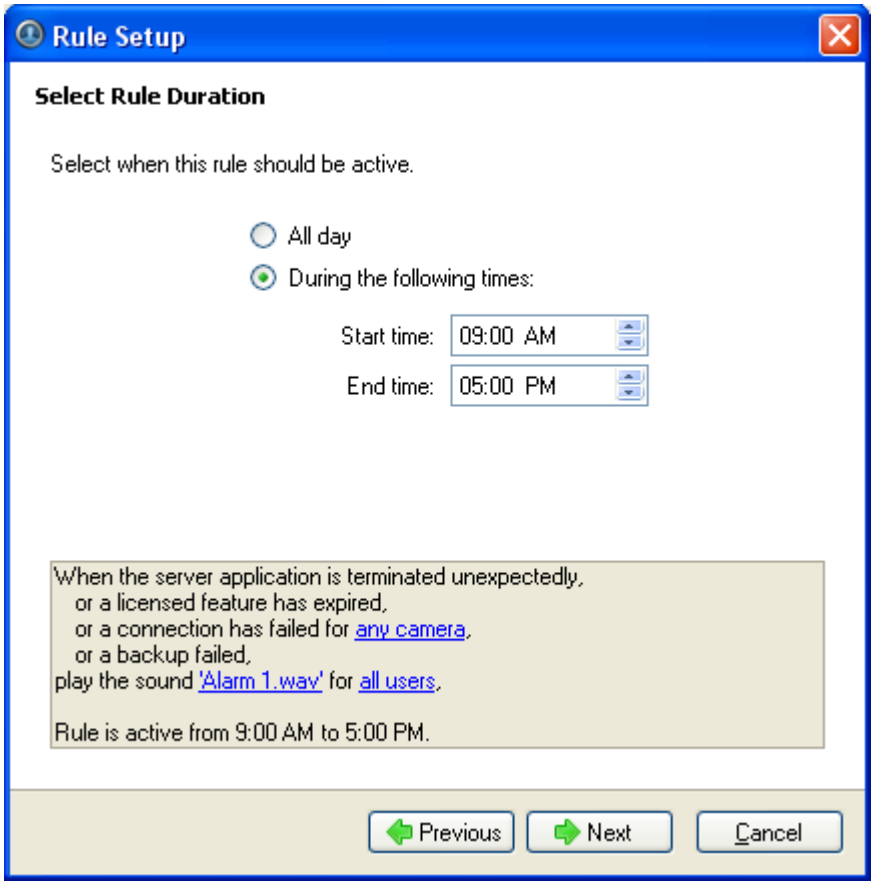


Figure C. Select Rule Duration page

8. Give the rule a name and description. Ensure the **Rule is enabled** check box is selected to enable the rule.

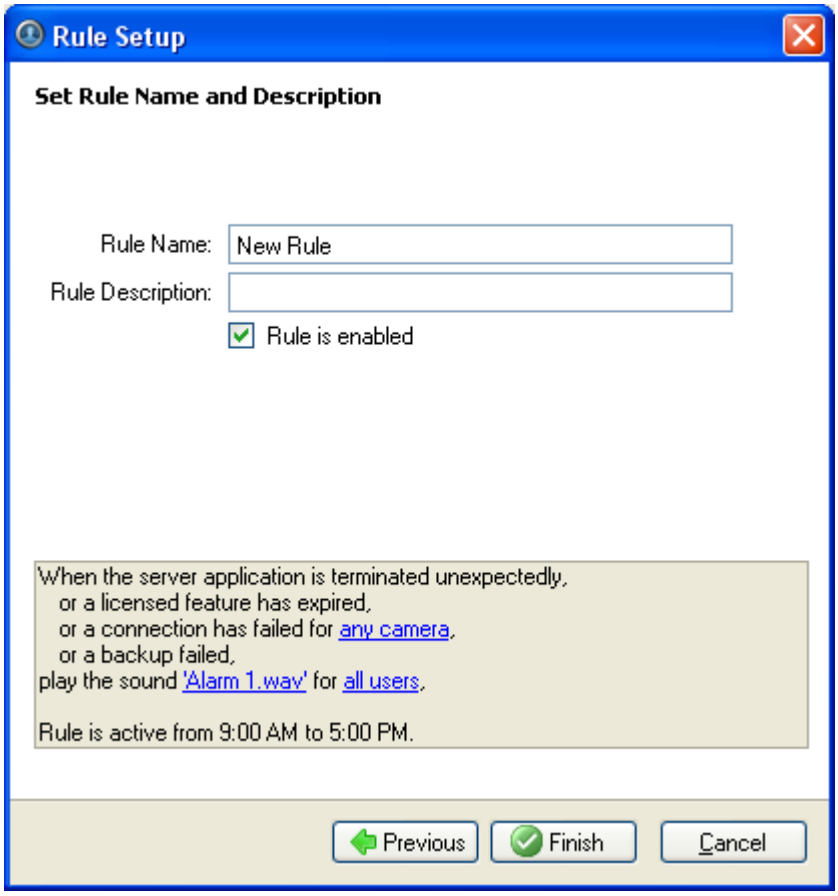


Figure D. Set Rule Name and Description page

9. Click **Finish**.

Editing and Deleting a Rule

1. Right-click a server in the System Explorer and select **Setup** to open the server Setup dialog box. See Accessing the Server Setup for more information.
2. Click **Rules**.
3. In the Rules dialog box, select a rule and perform one of the following:

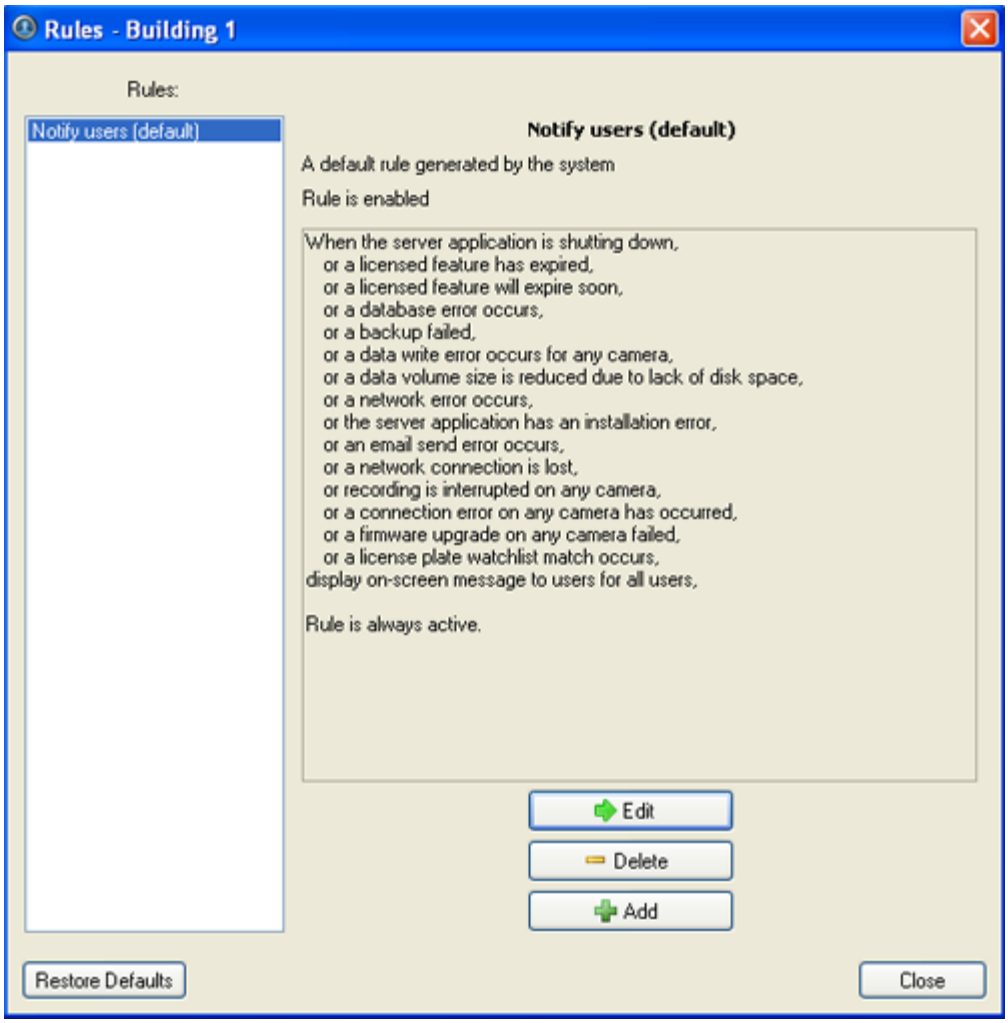


Figure A. Rules dialog box

- Click **Edit** to edit the rule. Go through the Rules Setup wizard and make the required changes on each page. On the last page, click **Finish**. Refer to Adding a Rule for details about the editable options.
- To delete a rule, click **Delete**. When the confirmation dialog box appears, click **OK**.

System Log

The system log records events that occur in the Avigilon Control Center system. This can be useful for tracking system usage and diagnosing issues.

You can filter the items displayed in the log and save the log to a separate file for sending to Avigilon support.

Note: The system log maintains a record of system events for up to 90 days.

Viewing the System Log

1. Right-click a server in the System Explorer and select **Setup** to open the server Setup dialog box. See Accessing the Server Setup for more information.
2. Click **System Log**.
3. In the System Log dialog box, select the log events you want to display in the Event Types to Show area, then click **Start Search**.

   The search results are displayed in the left pane.

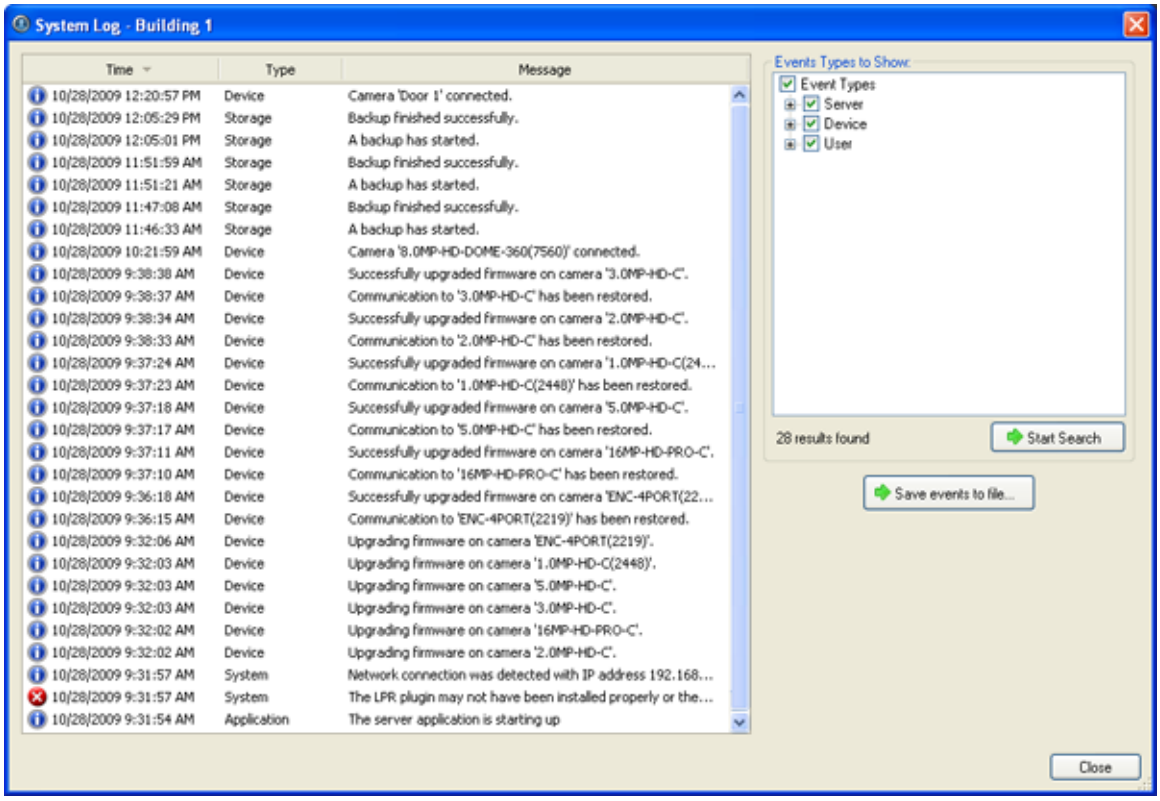


Figure A. System Log dialog box

4. Select a result to display the event details.
5. To save the log search results, click **Save events to file...** and save the file.
6. Click **Close**.

License Plate Recognition

License Plate Recognition is a licensed feature that allows users to read and store vehicle license plate numbers from any image streamed through the Avigilon Control Center Server software.

The License Plate Recognition options will only appear if you have the feature licensed and installed on the server.

Setting Up License Plate Recognition

1. Right-click a server in the System Explorer and select **Setup** to open the server Setup dialog box. See Accessing the Server Setup for more information.
2. Click **License Plate Recognition**.
3. When the License Plate Recognition dialog box appears, select a lane from the left pane.

   The number of lanes listed is determined by the number of LPR channels licensed on the server.

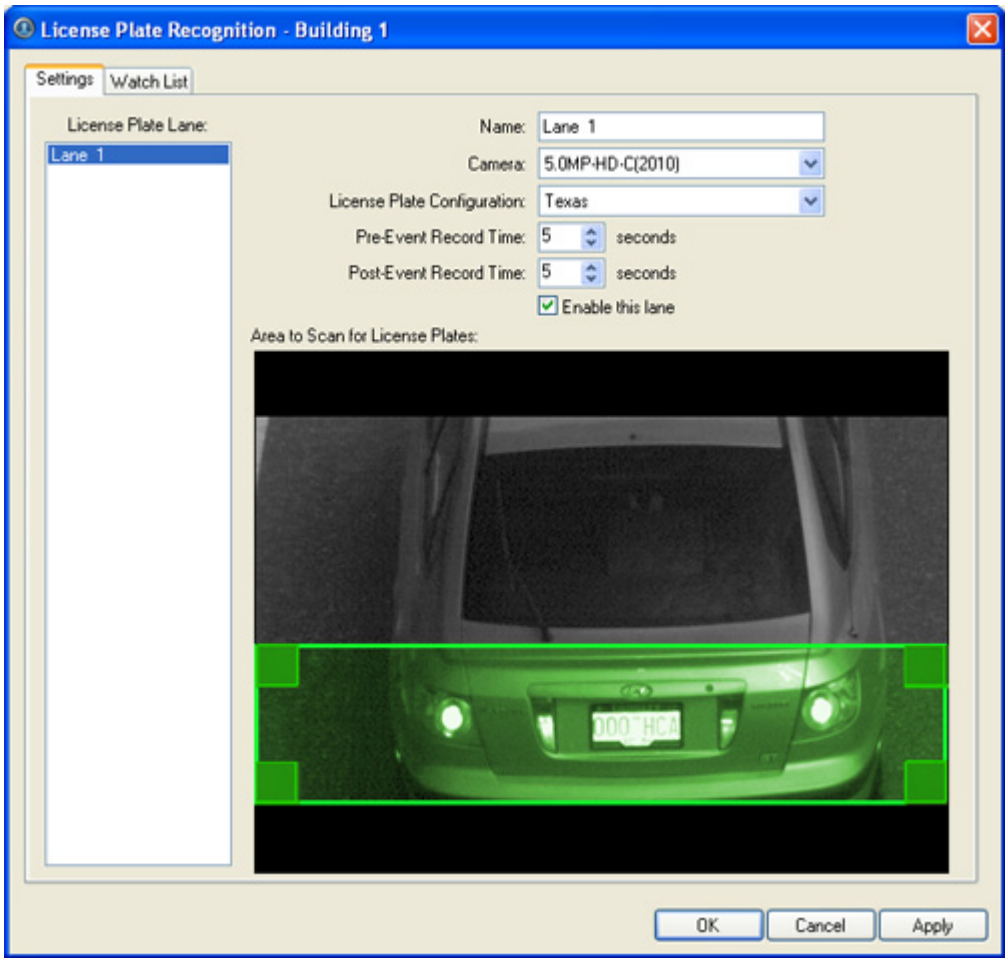


Figure A. License Plate Recognition dialog box, Settings tab

4. Complete the following fields:
   - **Name:** enter a name for the lane.
   - **Camera:** select the camera that will perform the license plate recognition. One camera can be used for multiple lanes.

- **License Plate Configuration:** select the regional license plate format that needs to be recognized by the camera.
- **Pre-Event Record Time:** enter the amount of time the camera should record before the license plate is recognized.
- **Post-Event Record Time:** enter the amount of time the camera should record after the license plate is recognized.
- **Enable this lane:** select this check box to enable the License Plate Recognition feature on this lane.

5. Move and adjust the size of the green overlay to define the area where license plates are detected by the camera.

   Note: The maximum size of the license plate recognition area is one megapixel. The green overlay automatically adjusts itself to meet the size limits.

6. Click **OK**.

Configuring the Watch List

The License Plate Recognition Watch List identifies license plates that may be of special interest. When a license plate on the Watch List is detected, an event is generated to notify the user and can be used to trigger a specific action in the Rules engine.

You can manually add each license plate that needs to be recognized, or import a list of licenses into the Client software.

Adding Licenses to the Watch List

1. Right-click a server in the System Explorer and select **Setup** to open the server Setup dialog box. See Accessing the Server Setup for more information.
2. Click **License Plate Recognition**.
3. When the License Plate Recognition dialog box appears, select the Watch List tab.

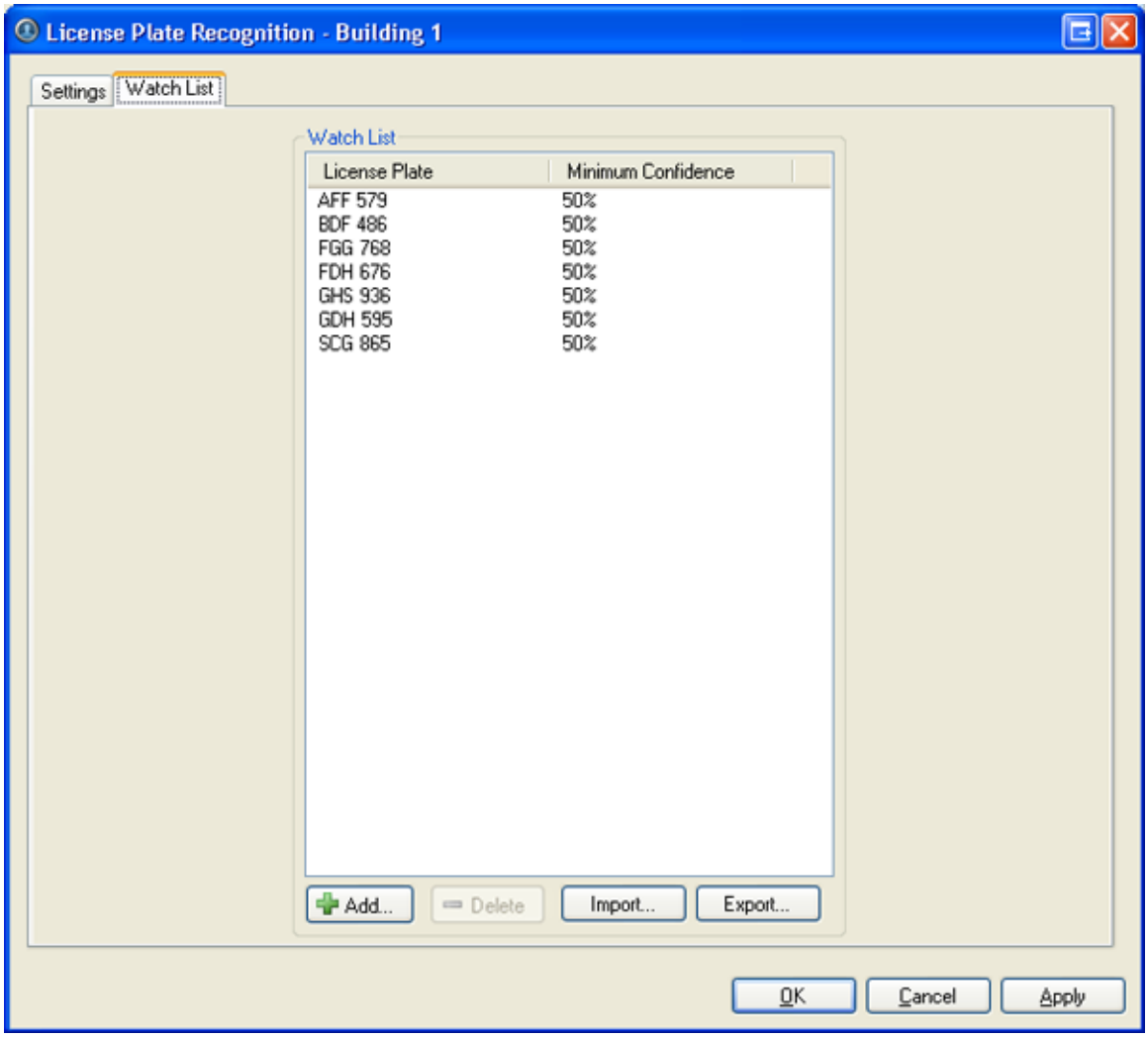


Figure A. License Plate Recognition dialog box: Watch List tab

4. Click **Add**. The Add License Plate dialog box appears.

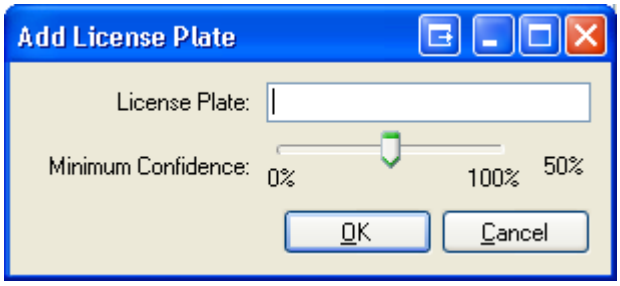


Figure B. Add License Plate dialog box

5. Enter the license plate number.
6. Move the **Minimum Confidence** slider to determine how similar the detected license plates must be before it is considered a match.

For example, if a license plate on your watch list is ABC 123 and Avigilon detects an ABC 789 license plate, the system will be 50% confident that it has found a match. If the system detects ABC 129, it will be 83% confident that it has found a match.

7. Click **OK**.

Deleting a License Plate from the Watch List

1. In the License Plate Recognition dialog box, select the Watch List tab.
2. Select the license from the Watch List, and click **Delete**.

Exporting a Watch List

1. In the License Plate Recognition dialog box, select the Watch List tab.
2. Click **Export**.
3. In the Save As dialog box, name the file and click **Save**.

The Watch List can be exported as a text file or a comma-separated values (CSV) file.

Importing a Watch List

1. In the License Plate Recognition dialog box, select the Watch List tab.
2. Click **Import**.
3. In the Import dialog box, locate the Watch List file and click **Open**.

Camera Setup

In the Avigilon Control Center Client software, cameras are pre-configured for optimal image recording. If your surveillance location requires special recording or display settings, you can configure the camera to meet your needs in the camera Setup dialog box.

Note: Some features are not displayed if the server does not have the required license, or if you do not have the user permissions to access the feature.

Note: The dialog box may appear different depending on the camera. Some cameras do not offer the full set of configuration options.

Accessing the Camera Setup

Perform one of the following steps to open the camera Setup dialog box:

- Select **Tools > Setup...** then select the camera you want to setup from the left pane.

- In the System Explorer pane, right-click the camera and select **Setup**.

Note: Some features are not displayed if the server does not have the required license, or if you do not have the user permissions to access the feature.

Note: The dialog box may appear different depending on the camera. Some cameras do not offer the full set of configuration options.

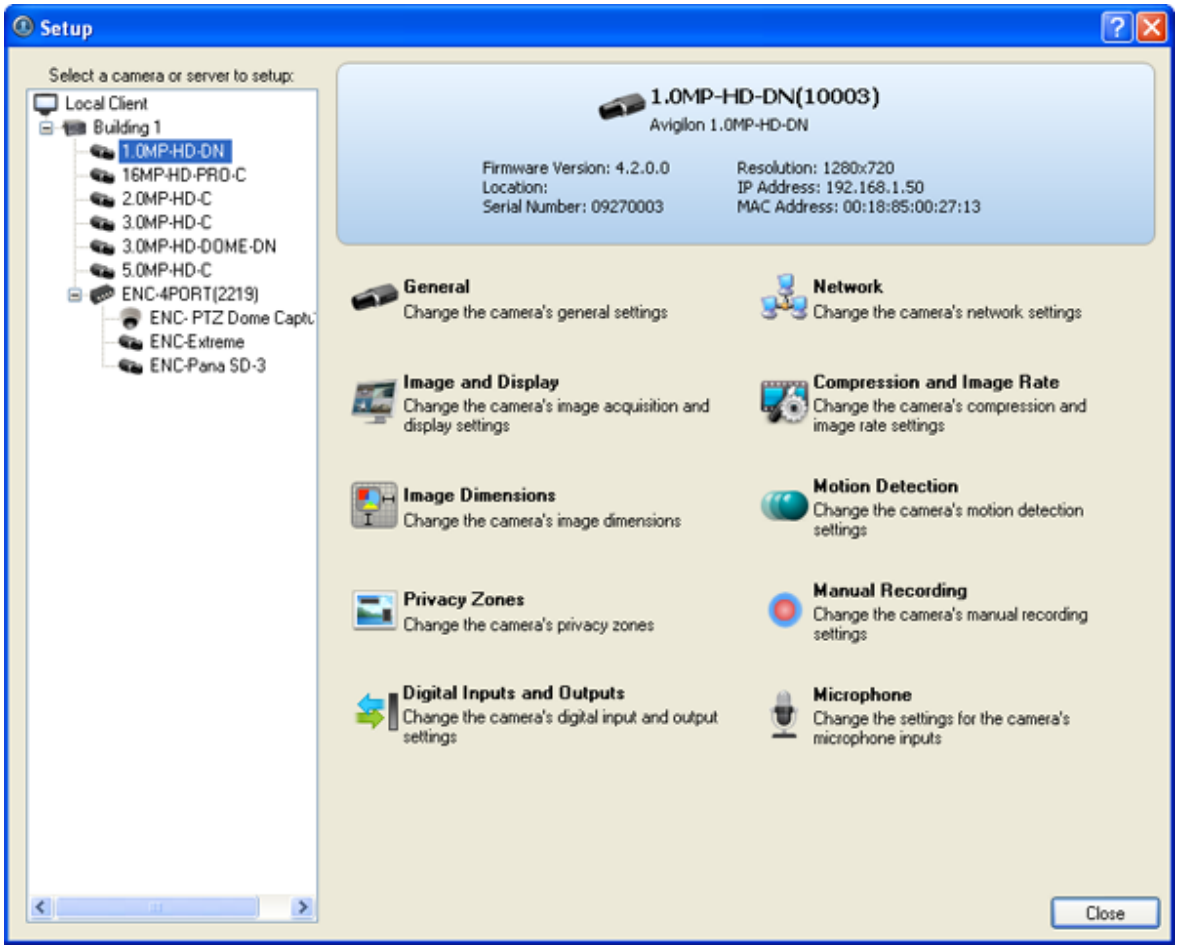


Figure A. Camera Setup dialog box

General

The camera General dialog box allow you to define the camera's name, the camera's location, configure the camera's PTZ settings and disable the camera's status LEDs.

Note: The dialog box may appear different depending on the camera. Some cameras do not offer the full set of configuration options.

Changing General Camera Settings

1. Right-click the camera in the System Explorer and select **Setup** to open the camera Setup dialog box.
   See Accessing the Camera Setup for more information.
2. Click **General**.
3. In the General dialog box, complete the following fields as required:

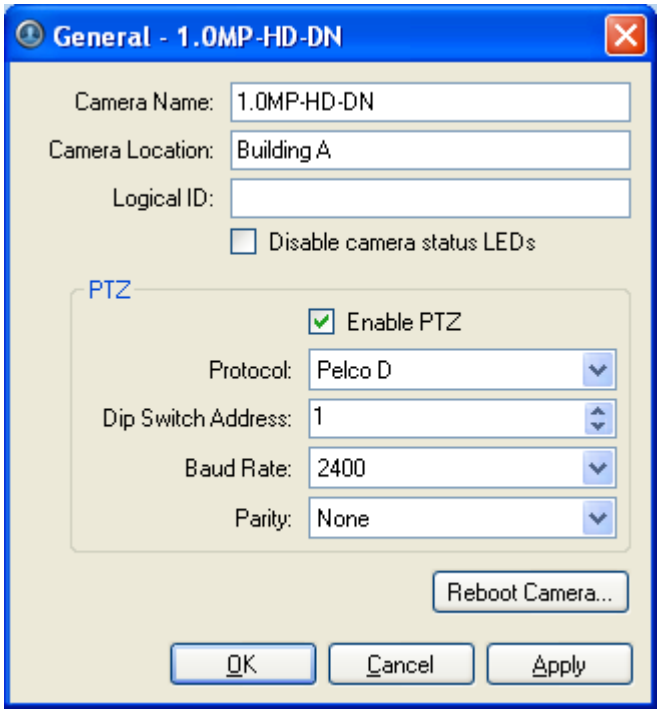


Figure A. General dialog box

- **Camera Name:** enter a camera name. Give the camera a meaningful name to help you identify the camera.
- **Camera Location:** describe the camera's location.
- **Logical ID:** enter a number to allow the Client software to identify this camera.

  The logical ID is used to call up the camera video when using the select camera keyboard command.
- **Disable camera status LEDs:** select this check box to disable the LEDs located on the back of the camera.
- **Enable PTZ:** select this check box to enable the camera's pan, tilt and zoom (PTZ) functions. The PTZ device is controlled from the RS-485 inputs on the camera.

  Select the appropriate **Protocol**, **Dip Switch Address**, **Baud Rate** and **Parity** settings.

Tip: PTZ enabled cameras are given the dome camera icon in the System Explorer.

4. If required, click **Reboot Camera** to restart the camera.
5. Click **OK**.

Network

Use the camera Network dialog box to modify how a camera connects to the server network, and specify the IP address used by the camera.

Note: The dialog box may appear different depending on the camera. Some cameras do not offer the full set of configuration options.

Changing Camera Network Settings

1. Right-click the camera and select **Setup** to open the camera Setup dialog box.
2. Click **Network**.
3. In the Network dialog box, select the required options and complete the related fields:

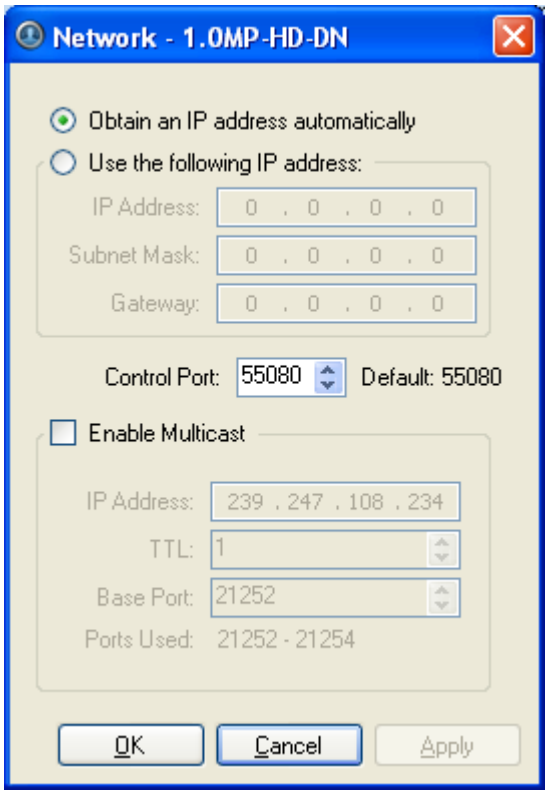


Figure A. Network dialog box

- **Obtain an IP address automatically:** select this option to enable the camera to connect to the network through an automatically assigned IP address.

  The camera will attempt to obtain an address from a DHCP server, if it cannot find one it will default to addresses in the 169.254.x.x range.

- **Use the following IP address:** select this option to enable the camera to connect to the network through a static IP address.

  Enter the **IP Address**, **Subnet Mask** and **Gateway**.

- **Control Port:** select the network port for connecting to the camera. This port is also used for manually discovering cameras on the network.

- **Enable Multicast:** select this check box to enable multicast streaming from the camera. You must enable multicast if you are setting up redundant connections to multiple servers.

  Use the default generated **IP Address**, **TTL** and **Base Port**, or enter your own values.

4. Click **OK**.

Image and Display

Use the Image and Display dialog box to control a camera's display settings for live and recorded images.

Changing Image and Display Settings

Note: The dialog box may appear different depending on the camera. Some cameras do not offer the full set of configuration options.

1. Right-click the camera in the System Explorer and select **Setup** to open the camera Setup dialog box.
   See Accessing the Camera Setup for more information.
2. Click **Image and Display**.
3. In the Image and Display dialog box, make the required changes to adjust the camera's image settings.

   Tip: Use the **Maximum Exposure**, **Maximum Gain** and **Priority** options to control low light behavior.

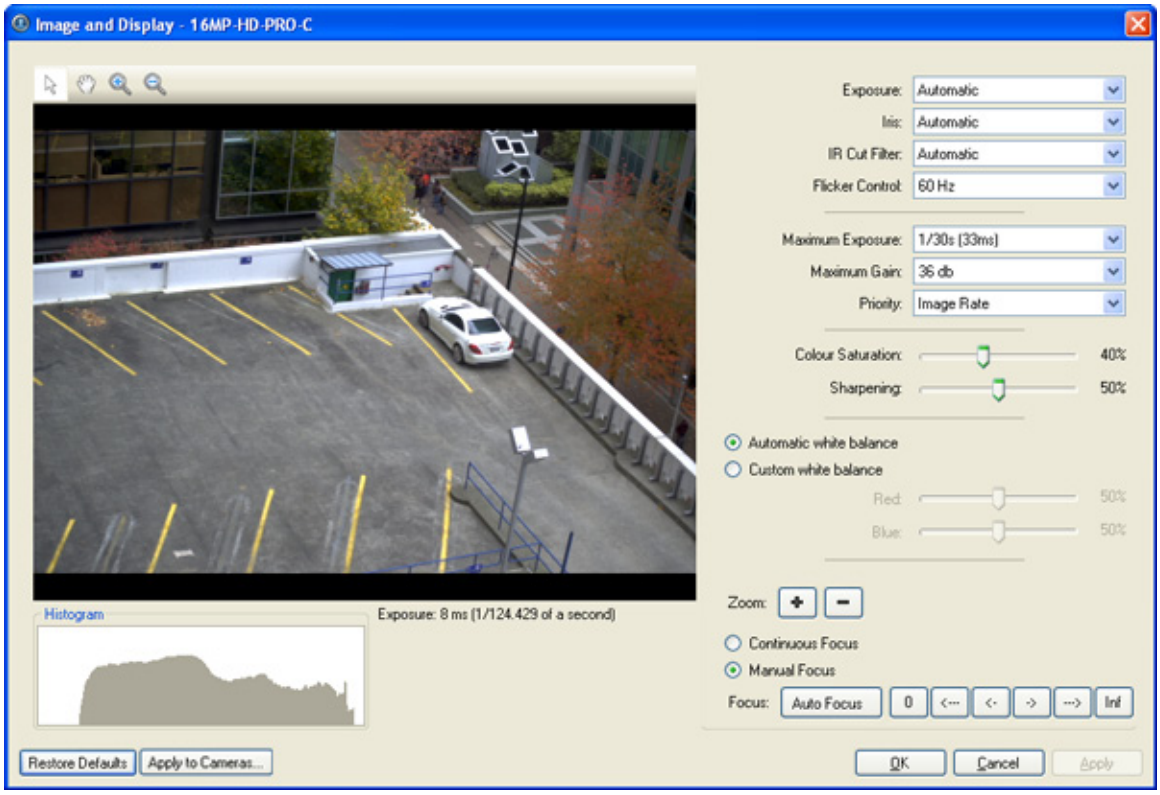


Figure A. Image and Display dialog box

Option	Description
Exposure	You can allow the camera to control the exposure automatically or you can manually set the exposure. ▪ Select **Automatic** for the camera to automatically control the exposure. ▪ Select an exposure rate to manually set the exposure. **Note:** Increasing the manual exposure time may affect the image rate.
Iris	If your camera has a lens with an auto iris, you can allow the camera to control the iris automatically or you can manually set it as open or closed. ▪ From the **Iris** drop down list, select one of the following: ▪ **Automatic** ▪ **Open** ▪ **Close**
IR Cut Filter	If your camera has a removable infrared cut filter, you can allow the camera to control it automatically or you can manually set the camera to color or monochrome mode.

	▪ From the **IR Cut Filter** drop down list, select one of the following: ▪ **Automatic** ▪ **Color** ▪ **Monochrome**
Flicker Control	If your video image flickers because of the fluorescent lights around the camera, you can reduce the effects of the flicker by setting the **Flicker Control** to the same power frequency as your lights. For example, for Europe 50Hz or for North America 60Hz. ▪ In the **Flicker Control** drop down list, select a frequency.
Backlight Compensation	If your scene has small areas of intense light that are causing the overall image to be too dark, backlight compensation can be used to achieve a well exposed image. ▪ Move the **Backlight Compensation** slider until the video image meets your requirements.
Maximum Exposure	You can limit the automatic exposure setting by setting a maximum exposure level. By setting a maximum exposure level for low light situations, you can control the camera's exposure time to let in the maximum amount of light without creating blurry images. ▪ Select an exposure rate from the **Maximum Exposure** drop down list.
Maximum Gain	You can limit the automatic gain setting in the camera by setting a maximum gain level. By setting a maximum gain level for low light situations, you can maximize the detail of an image without creating excessive noise in the images. ▪ Select a gain level from the **Maximum Gain** drop down list.
Priority	You can set **Image Rate** or **Exposure** as the priority. When set to **Image Rate**, the camera will maintain the set image rate as the priority, and will not adjust the exposure beyond what can be recorded for the set Image Rate. See Changing Compression and Image Rate Settings to set the Image Rate. When set to **Exposure** the camera will maintain the exposure setting as the priority, and will override the set image rate to achieve the best image possible. ▪ In the **Priority** drop down list, select either **Image Rate** or **Exposure**.
Saturation	You can adjust the video's color intensity. ▪ Move the **Color Saturation** slider until the video image meets

	your requirements.
Sharpening	If the video image is blurry, you can adjust the video sharpness to make the edges of objects more visible. ▪ Move the **Sharpening** slider until the video image meets your requirements.
White Balance	You can control white balance settings to account for different scene illuminations. ▪ Select one of the following: ▪ **Automatic white balance** ▪ **Custom white balance** Move the corresponding sliders to manually modify the color balance.

4. To focus the camera, see Focusing the Camera Lens.
5. Click **Apply to Cameras...** to apply the same settings to other cameras of the same model.
6. Click **OK**.

Zooming and Focusing the Camera Lens

If you have a camera with a lens capable of electronic zoom and focus, you can zoom or focus the camera through the Avigilon Control Center Client software.

Note: The dialog box may appear different depending on the camera. Some cameras do not offer the full set of configuration options.

1. Right-click the camera in the System Explorer and select **Setup** to open the camera Setup dialog box.
   See Accessing the Camera Setup for more information.
2. Click **Image and Display**. The Image and Display dialog box appears.
3. If the camera has a built-in auto focus feature, you can choose one of the following:
   - **Continuous Focus:** the camera will automatically focus itself whenever the scene changes. Skip the following step.
   - **Manual Focus:** you can manually focus the camera through the Image and Display **Focus** buttons. Once the focus is manually set, it will not change.
4. While you view the camera image panel, complete the following steps to zoom and focus the camera:

Tip: For Avigilon HD Professional cameras, the lens must be set to auto-focus (AF) mode on the camera. If the camera does not detect the lens, the **Focus** buttons are not displayed.

3.

a. Use the **Zoom** buttons to zoom in to the distance you want to focus.

b. In the **Iris** drop down list, select **Open**. When the camera iris is fully open, the depth of field is the shortest.

c. Use the **Focus** buttons until the image becomes clear.

Button	Description
Auto Focus	The camera will automatically focus once.
0	Focused as close to zero as possible
<---	Large step toward zero
<-	Small step toward zero
->	Small step toward infinity
--->	Large step toward infinity
Inf	Infinity

4. Click **Apply to Cameras...** to apply the same settings to other cameras of the same model.

5. Click **OK**.

Compression and Image Rate

Use the camera Compression and Image Rate dialog box to modify the camera's compression and image quality settings for sending image data over the network.

Note: The dialog box may appear different depending on the camera. Some cameras do not offer the full set of configuration options.

Changing Compression and Image Rate Settings

1. Right-click the camera in the System Explorer and select **Setup** to open the camera setup dialog box.
2. Click **Compression and Image Rate**. The Compression and Image Rate dialog box appears.

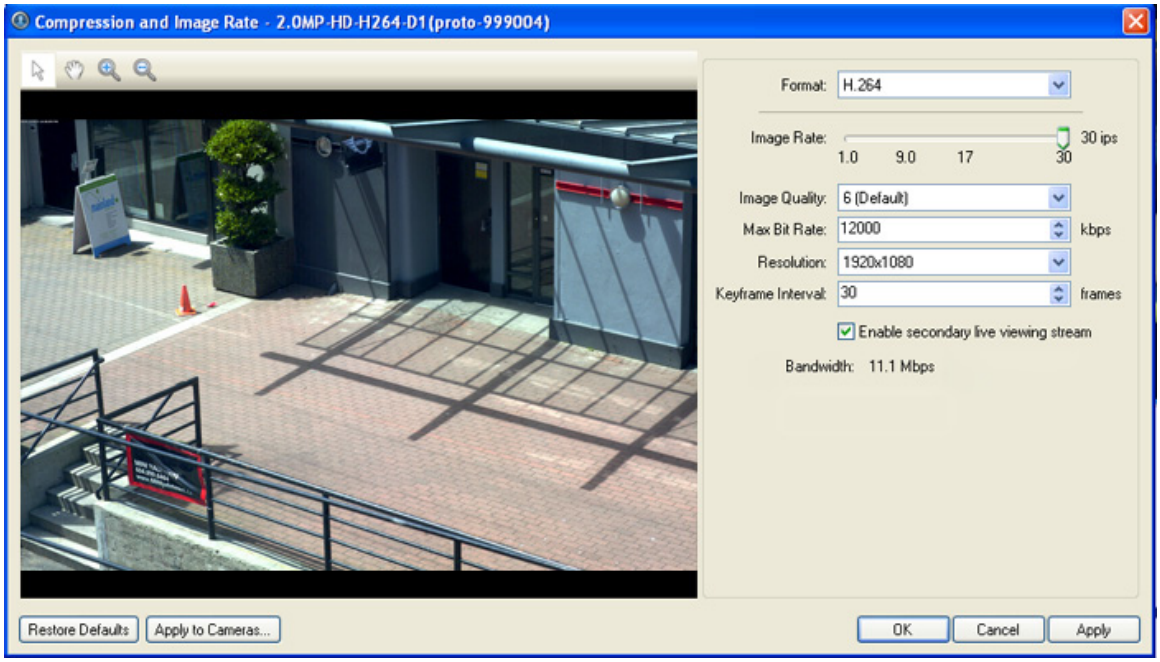


Figure A. Compression and Image Rate dialog box.

The Bandwidth area gives an estimate of the amount of bandwidth the camera would be using given the configured compression and image rate. Adjust the settings as required.

3. In the **Format** drop down list, select the preferred streaming format.
4. In the **Image Rate** bar, move the slider to select the desired image rate.
5. In the **Image Quality** drop down list, select the desired image quality number.

   Image quality setting of **1** will produce the highest quality video and require the most bandwidth.
6. In the **Max Bit Rate** drop down list, select the maximum bandwidth the camera can use.
7. In the **Resolution** drop down list, select the preferred image resolution.
8. In the Keyframe Interval drop down list, select the preferred number of frames between each keyframe.
9. If your camera supports multiple video streams, select the **Enable secondary live viewing stream** check box to enable the secondary stream.

   A secondary video stream allows you to view video at a lower image rate to reduce bandwidth usage, while still recording at a high image rate in the primary stream.

10. Click **Apply to Cameras...** to apply the same settings to other cameras of the same model.
11. Click **OK**.

Image Dimensions

Use the Image Dimension dialog box to set the image dimensions for the camera. This can help reduce bandwidth and increase the maximum image rate.

Changing Image Dimensions Settings

1. Right-click the camera in the System Explorer and select **Setup** to open the camera Setup dialog box.
   See Accessing the Camera Setup for more information.
2. Click **Image Dimensions**.
3. In the Image Dimensions dialog box, adjust the image dimensions by performing one of the following:
   - Drag the edges of the image until you achieve the required size.
   - Change the values for the **Top**, **Left**, **Width**, and **Height** field.

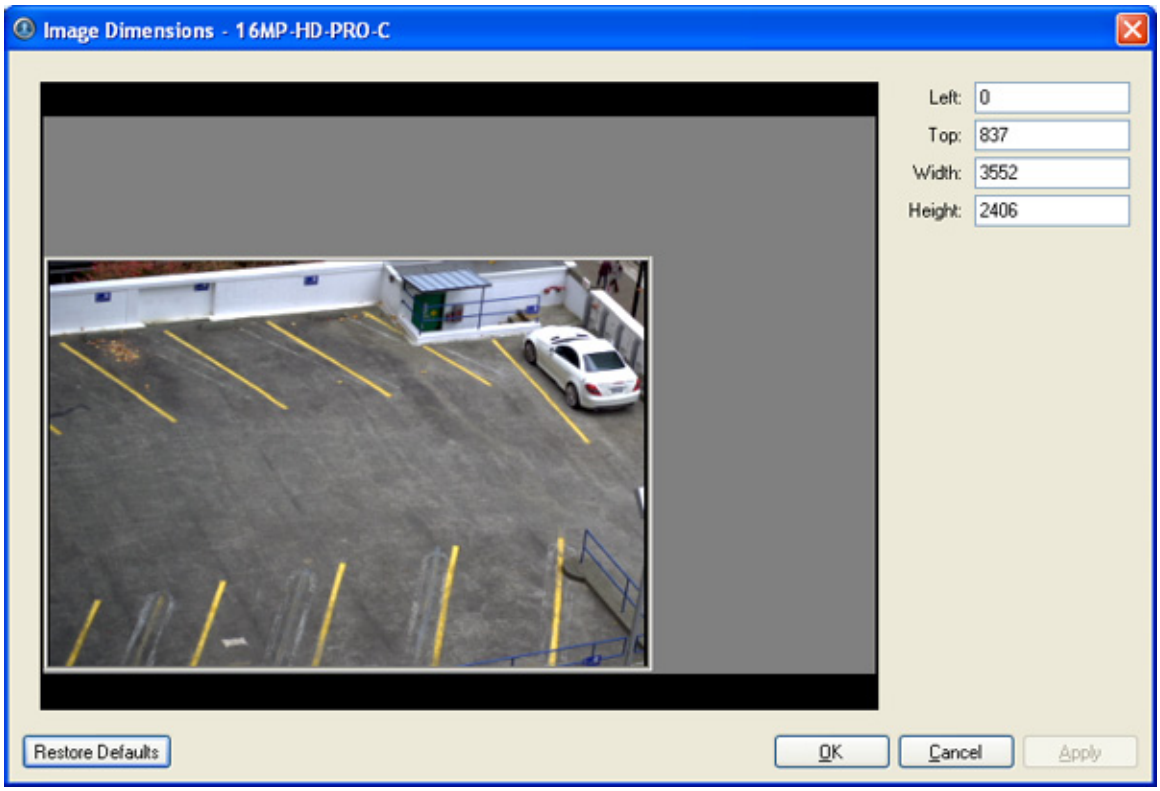


Figure A. Image Dimensions dialog box

4. Click **OK**.

Motion Detection

In the Motion Detection dialog box, you can define specific areas where motion is detected and configure the sensitivity and threshold for motion detection.

Selecting an Area to Detect Motion

In the Motion Detection dialog box, define the green motion detection area of a camera image. Motion detection is ignored in the areas not highlighted in green.

1. Right-click the camera in the System Explorer and select **Setup** to open the camera Setup dialog box.
   See Accessing the Camera Setup for more information.
2. Click **Motion Detection**.
3. In the Motion Detection dialog box, select the buttons above the image panel and use your mouse to define the green motion detection area. The motion detection area must be defined before motion is detected:
   - **Set Area:** select this button then draw green rectangles to define motion detection areas. If necessary, draw multiple rectangles to create your motion detection area.
   - **Clear Area:** select this button and draw rectangles to erase sections from the motion detection area.
   - **Draw:** select this button and manually draw motion detection area. This tool allows you to be very specific and highlight unusual shapes.
   - **Set All:** select this button to highlight the entire image for motion detection.
   - **Clear All:** select this button to clear the image of motion detection areas.

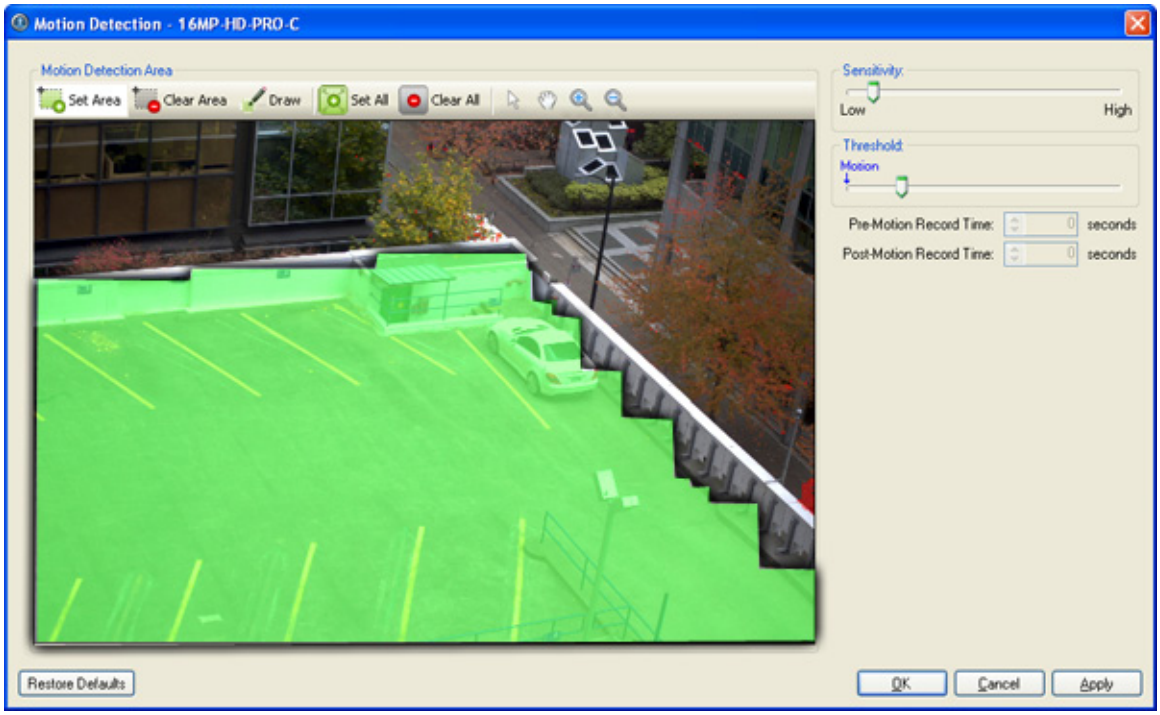


Figure A. Motion Detection dialog box

4. Click **OK**.

To define the sensitivity and threshold for the motion detection area, see Controlling Motion Sensitivity and Threshold.

Controlling Motion Sensitivity and Threshold

In the Motion Detection dialog box, you can control the camera's sensitivity threshold for motion. You can also define how much time should be recorded before and after the motion event.

1. Right-click the camera in the System Explorer and select **Setup** to open the camera Setup dialog box.
   See Accessing the Camera Setup for more information.
2. Click **Motion Detection**. The Motion Detection dialog box appears.
3. Move the **Sensitivity** slider to adjust how much each pixel must change before it is considered in motion.

   The higher the sensitivity, the smaller the amount of pixel change is required before a motion is detected.
4. Move the **Threshold** slider to adjust how many pixels must change before the image is considered to have motion.

   The higher the threshold, the higher the number of pixels must change before the image is considered to have motion.

Tip: The **Motion** indicator above the Threshold slider will move to indicate how much motion is occurring in the current scene.

5. In the **Pre-Motion Record Time** and **Post-Motion Record Time** boxes, specify how much time you want the camera to record before and after the motion event.
6. Click **OK**.

Privacy Zones

You can set privacy zones in the camera's field of view to block out regions of the camera image that you do not want to view or record.

Adding a Privacy Zone

1. Right-click the camera in the System Explorer and select **Setup** to open the camera Setup dialog box.
   See Accessing the Camera Setup for more information.
2. Click **Privacy Zones**.
3. In the Privacy Zones dialog box, click **Add** and a green box will appear on the image.

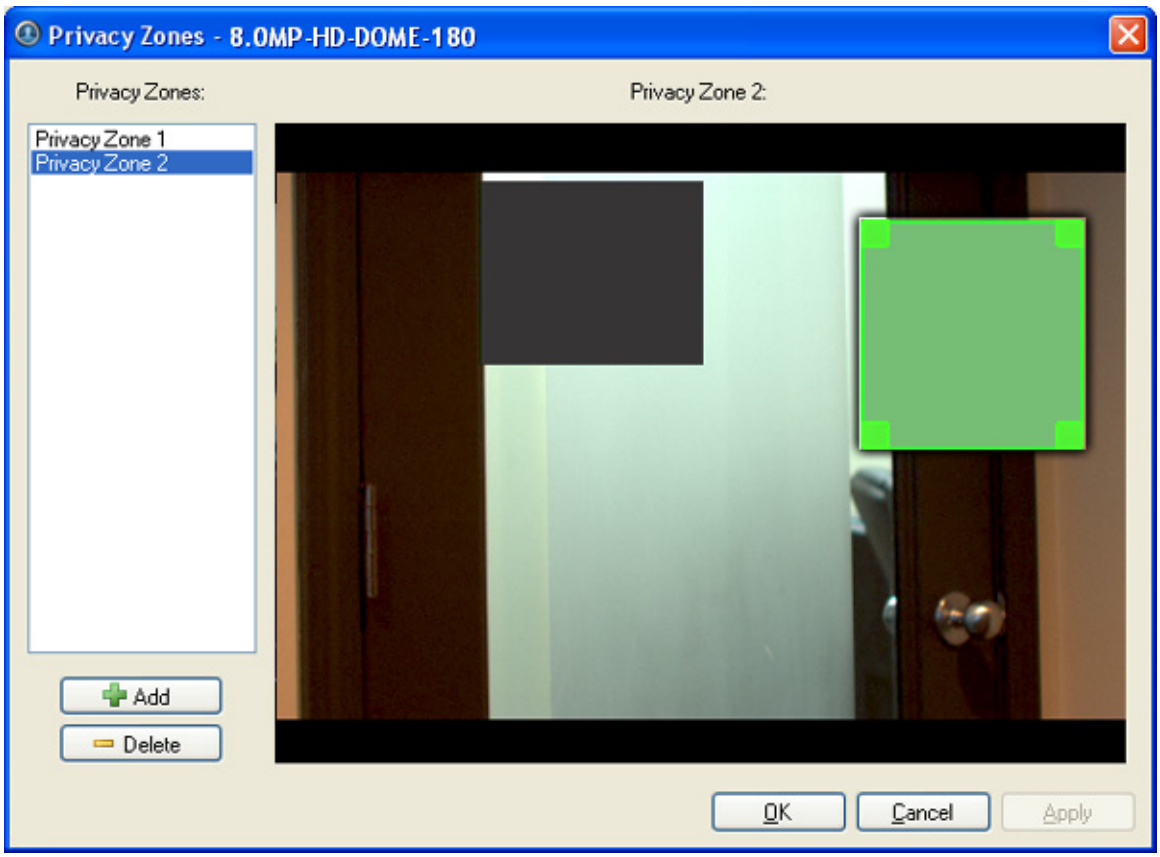


Figure A. Privacy Zones dialog box

4. Move and resize the green box until it covers the area you want to block out.
5. Click **OK**.

Editing and Deleting a Privacy Zone

1. Right-click the camera in the System Explorer and select **Setup** to open the camera Setup dialog box.
   See Accessing the Camera Setup for more information.
2. Click **Privacy Zones**.
3. In the Privacy Zones dialog box, select a privacy zone from Privacy Zone list and perform one of the following:
   - To edit the privacy zone, adjust the green box on the image.
   - To delete the privacy zone, click **Delete**.
4. Click **OK**.

Manual Recording

Manual recording allows you to control video recording outside a camera's recording schedule. Manual recording can only be activated when viewing live camera images. See Triggering Manual Recording for more information.

In the Manual Recording dialog box, you can define the maximum recording duration and the pre-trigger recording time for each camera.

Changing Manual Recording Settings

1. Right-click the camera in the System Explorer and select **Setup** to open the camera Setup dialog box.
   See Accessing the Camera Setup for more information.
2. Click **Manual Recording**. The Manual Recording dialog box appears.

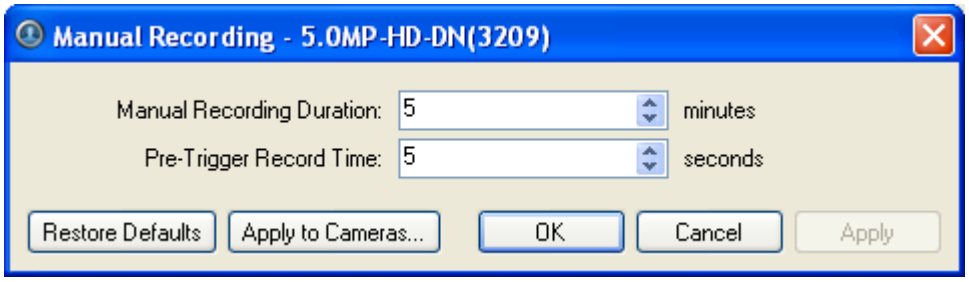


Figure A. Manual Recording dialog box

3. Specify the following:
    - **Manual Recording Duration:** enter the maximum duration of a manual recording if it is not manually stopped.
    - **Pre-Trigger Record Time:** enter the amount of time the camera's images are recorded before manual recording is activated.
4. Click **Apply to Cameras...** to apply the same settings to other cameras of the same model.
5. Click **OK**.

Digital Inputs and Outputs

In the Digital Inputs and Outputs dialog box, set up the external digital inputs and outputs that are connected to the camera.

The external devices can be used to create alarms or trigger recording events and specific actions. Use the rules engine in the server Setup to define the actions that occur in response to the digital inputs and outputs. See Rules for more information.

Setting Up Digital Inputs

1. Right-click the camera in the System Explorer and select **Setup** to open the camera Setup dialog box.
   See Accessing the Camera Setup for more information.
2. Click **Digital Inputs and Outputs**.
3. In the Digital Inputs area, select an input.

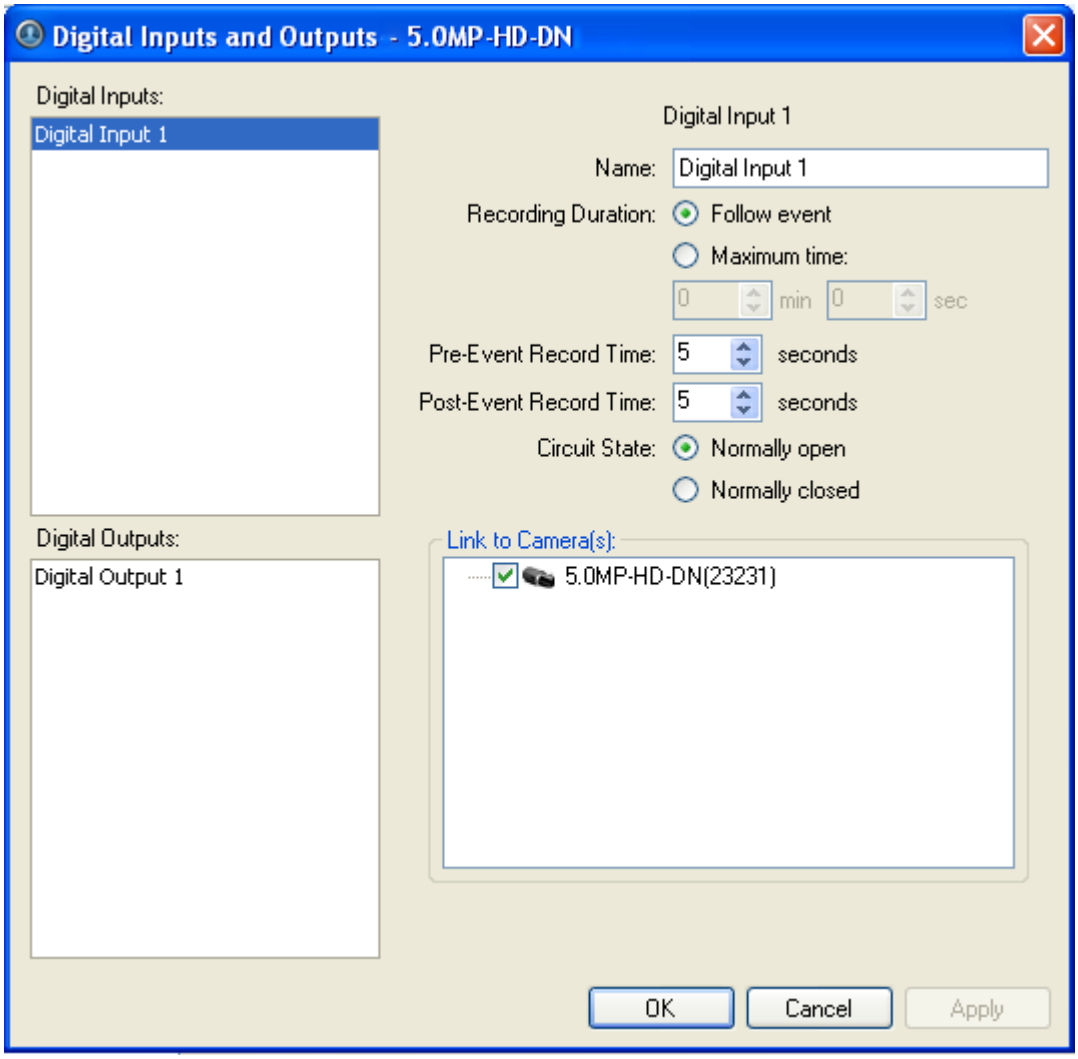


Figure A. Digital Inputs and Outputs dialog box: Digital Inputs Settings

4. Specify the following:
    - **Name:** enter a name to identify the digital input.
    - **Recording Duration:** select **Follow Event** to record the entire digital input event. Or, select **Maximum Time** to limit the recording time.
    - **Pre-Event Record Time:** enter the amount of time to record before the digital input is triggered.
    - **Post-Event Record Time:** enter the amount of time to continue recording after the digital input returns to its normal state.
    - **Circuit State:** select the digital input's default circuit state.
    - **Link to Camera(s):** select the cameras that need to be linked to this input for recording.

If the Recording Schedule is configured to record digital inputs, the cameras selected in the Link to Camera(s) area are used to record this digital input.

5. Click **OK**.

Setting Up Digital Outputs

Note: The dialog box may appear different depending on the camera. Some cameras do not offer the full set of configuration options.

1. Right-click the camera in the System Explorer and select **Setup** to open the camera Setup dialog box.
   See Accessing the Camera Setup for more information.
2. Click **Digital Inputs and Outputs**.
3. In the Digital Outputs area, select an output.

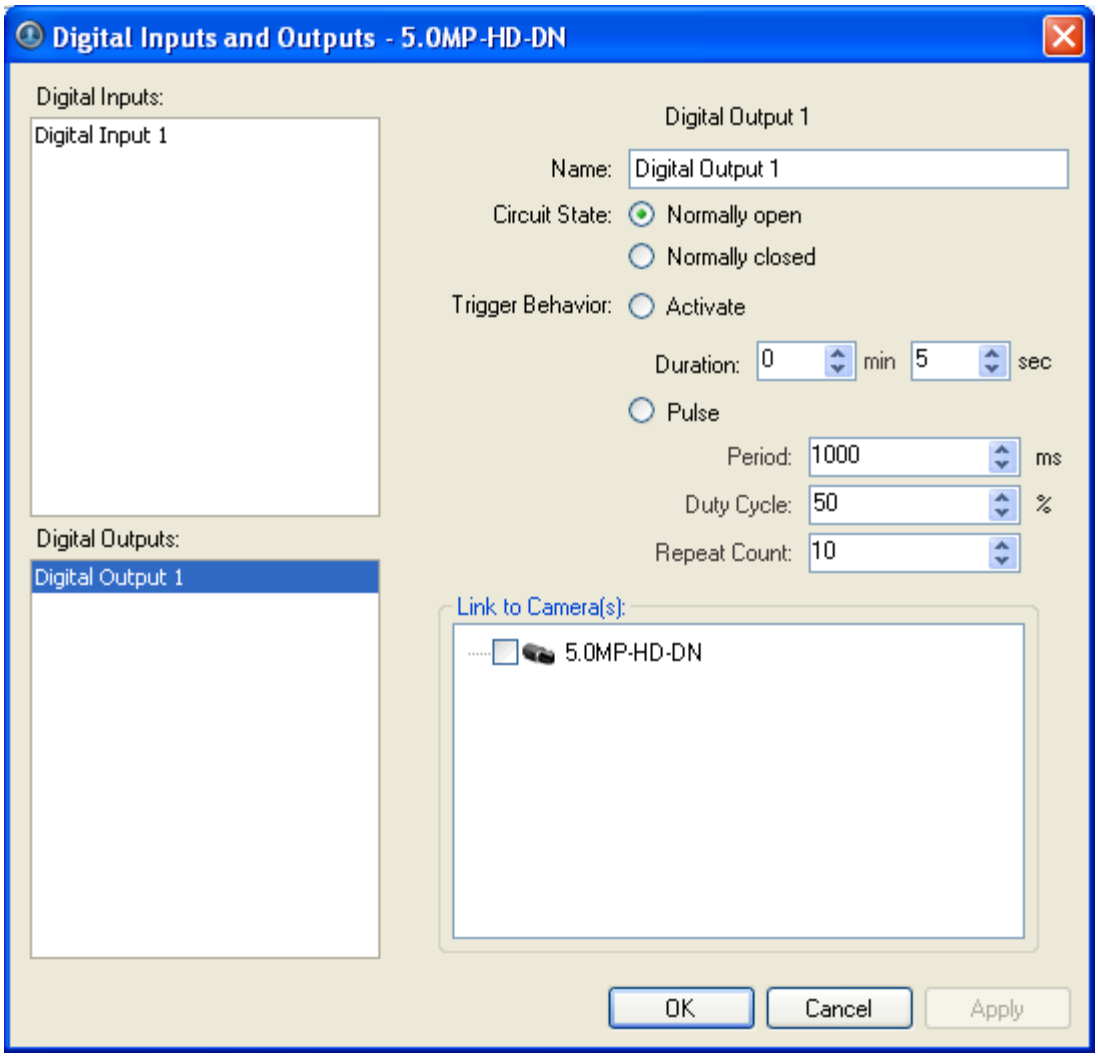


Figure A. Digital Inputs and Outputs dialog box: Digital Output Settings

4. Enter a name to identify the digital output.
5. Select one of the Circuit State options to define the digital output's default circuit state.
6. The Trigger Behavior options define what occurs when the output activated.
    - Select **Activate** to enable the digital output in continuous mode. The **Duration** fields allow you to specify how long the digital output should be active for.
    - Select **Pulse** to enable the digital output in pulse mode. Specify the **Period**, **Duty Cycle**, and **Repeat Count** for the pulse.
7. Select the cameras this digital output should be linked to.

    When you view the live video from the selected cameras, you can manually trigger this digital output. See Triggering Digital Output for more information.
8. Click **OK**.

Microphone

Note: Audio recording requires an Audio Channel License.

Use the Microphone dialog box to change the settings for the microphone input on a supported device. You can link the audio with any camera connected to the server.

Note: The dialog box may appear different depending on the camera. Some cameras do not offer the full set of configuration options.

Changing Microphone Settings

1. Right-click the camera in the System Explorer and select **Setup** to open the camera Setup dialog box.
   See Accessing the Camera Setup for more information.
2. Click **Microphone**. The Microphone dialog box appears.

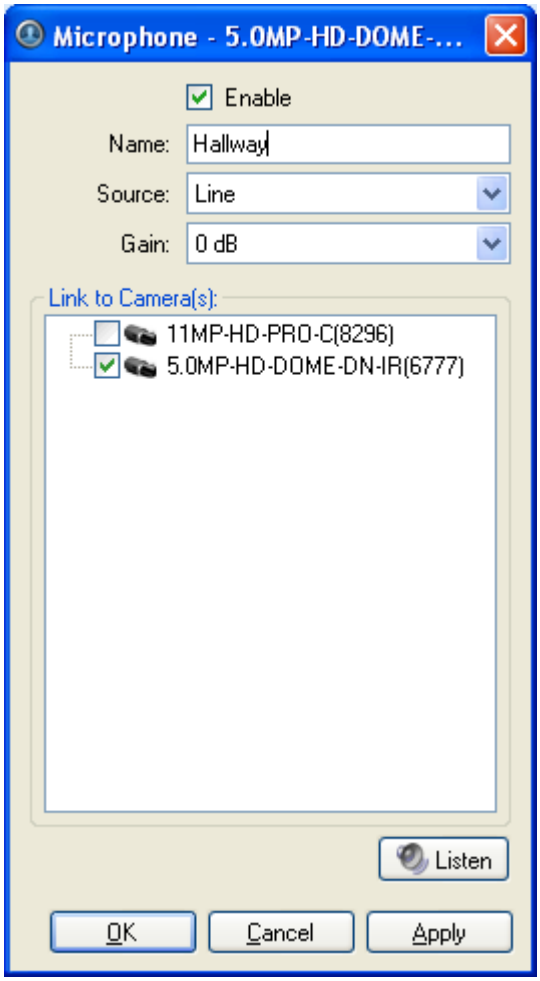


Figure A. Microphone dialog box

3. Complete the following fields:
    - **Enable:** select this check box to enable audio recording from this input.

      Note: An error message will appear if you do not have an Audio Channel License.
    - **Name:** enter a name for the audio input.
    - **Source:** select either line or microphone depending on the type of audio source.
    - **Gain:** select the amount of analog gain to be applied to the audio in the device.

      Values above **0 dB** will increase the volume of the audio source and negative values will decrease the volume.
4. Click **Listen** to test the settings and listen to the audio source.
5. In the Link to Camera(s) area, select the camera video that is linked with the audio.
6. Click **OK**.

Client Setup

You can modify the local client properties in the client Setup dialog box. The client Setup includes configuring the following settings:

Accessing the Client Setup

Perform one of the following steps to open the client Setup dialog box in the Avigilon Control Center Client software.

- Select **Tools > Setup...** and select the local client from the left pane.
- In the System Explorer, right-click the local client and select **Setup**.

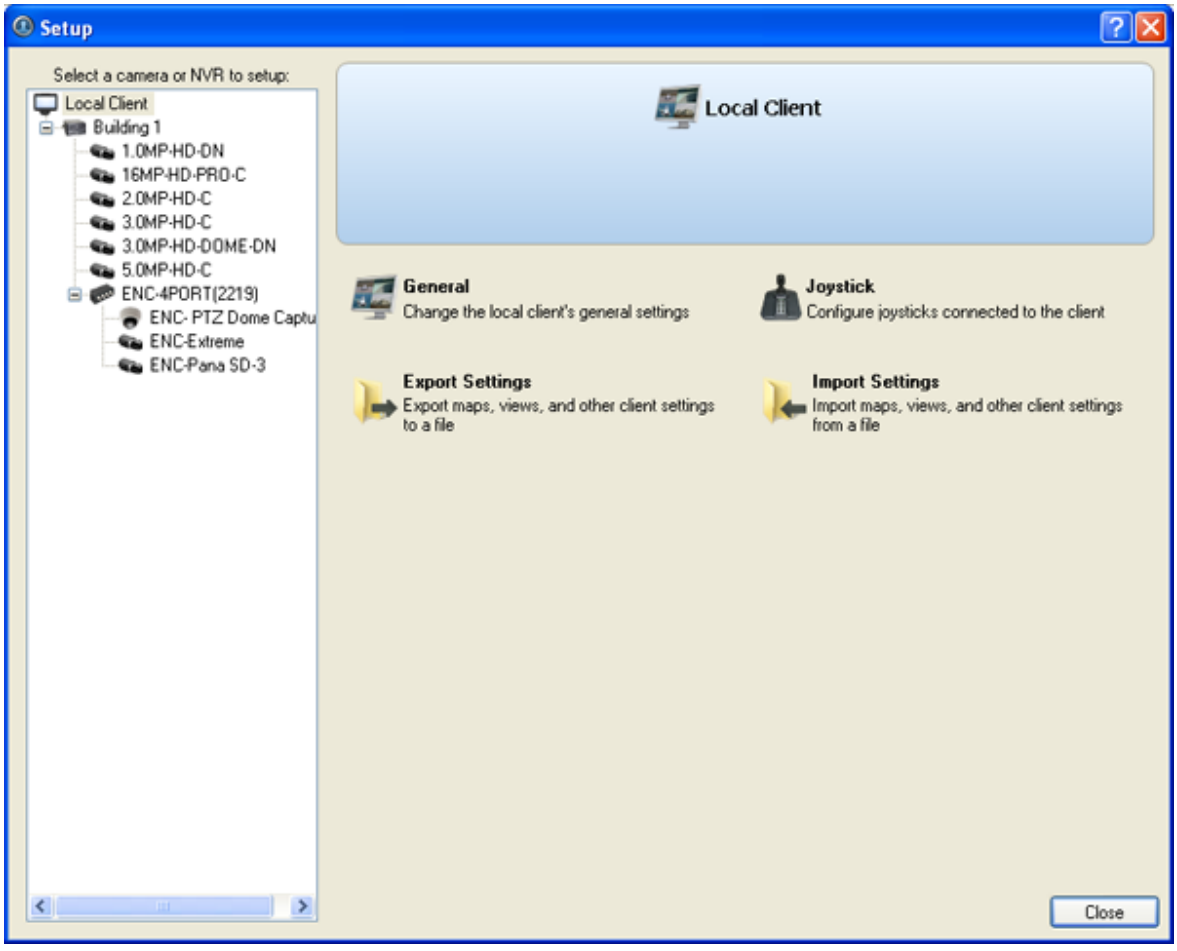


Figure A. Setup Local Client dialog box

General

Use the client General dialog box to change the local client's log in preferences and connection speed.

The client's connection speed can be changed to match the available incoming network bandwidth. This is useful when streaming video over the internet.

Changing General Client Settings

1. Right-click the local client in the System Explorer and select **Setup** to open the client Setup dialog box.
   For more information, see Accessing the Client Setup.
2. Click **General**.
3. In the General dialog box, complete the following fields as required:

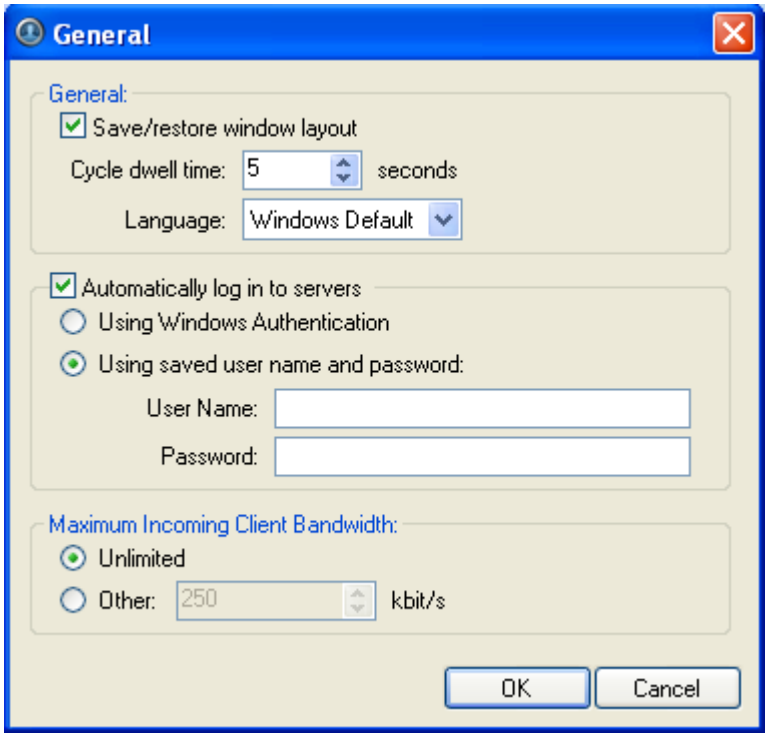


Figure A. General dialog box

- **Save/restore window layout:** select this check box if you want the application to remember your layout preferences.
- **Cycle dwell time:** enter the number of seconds the application waits before it cycles to a different View. See Cycling Through Views for more information.

- **Language:** select a language from the drop down list to change the application language. Select **Windows Default** for the application to automatically display the same language as the local client.
- **Automatically log in to servers:** select this check box to enable the application to automatically log you into all servers that are available on the network. Select the type of login you use: **Windows Authentication** — your Windows login; or **saved user name and password** — your Avigilon Control Center username and password.
- In the Maximum Incoming Client Bandwidth area, select **Unlimited**, or select **Other** and specify the maximum kilobits per second (kbit/s) you want to allow.

4. Click **OK**.

Joystick

The Avigilon Control Center Client software supports two types of joysticks: standard Microsoft DirectX USB Joysticks and the Avigilon Professional Joystick Keyboard.

Use the Joystick dialog box to configure joystick settings.

Configuring a Standard USB Joystick

Use the Joystick dialog box to configure the buttons used in your standard Microsoft DirectX USB joystick.

1. Connect the joystick.
2. Right-click the local client in the System Explorer and select **Setup** to open the client Setup dialog box.
   For more information, see Accessing the Client Setup.
3. Click **Joystick**.
4. If the joystick is not automatically detected, an error message will appear. Click **Scan for Joysticks...**.

   Note: The error message will not appear if the joystick was detected.

   When the joystick is detected, the Joystick dialog box appears.

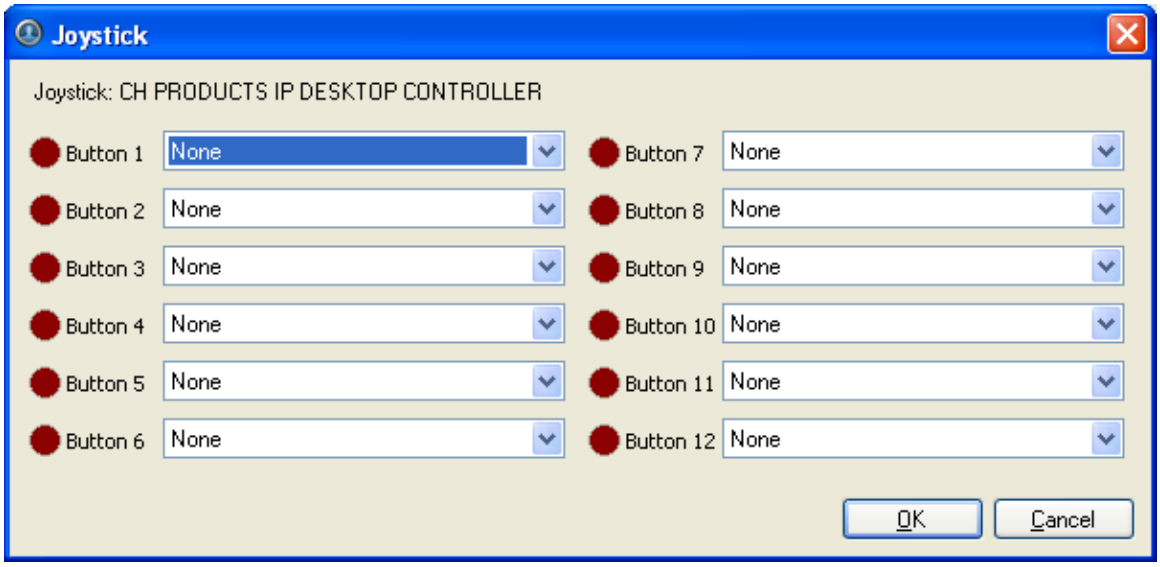


Figure A. Joystick dialog box

5. Set up an action for each button on the joystick:
    a. Press a button on the joystick. The button label is highlighted in the Joystick dialog box.
    b. Select an action for the button from the drop down list.
    c. Repeat this procedure for each button on the joystick.
6. Click **OK**.

Configuring an Avigilon Professional Joystick Keyboard

The Avigilon Professional Joystick Keyboard is a USB add-on that contains a joystick for controlling zoom and pan within image panels, a jog shuttle for controlling the Timeline, and a keypad programmed with the Client software keyboard commands.

By default, the keyboard is installed in right-hand mode. Use the Joystick dialog box to configure left-hand mode.

1. Connect the keyboard.
2. Right-click the local client in the System Explorer and select **Setup** to open the client Setup dialog box.
   For more information, see Accessing the Client Setup.
3. Click **Joystick**.
4. If the keyboard is not automatically detected, an error message will appear. Click **Scan for Joysticks...**.

Note: The error message will not appear if the keyboard was detected.

When the keyboard is detected, the Joystick dialog box appears.

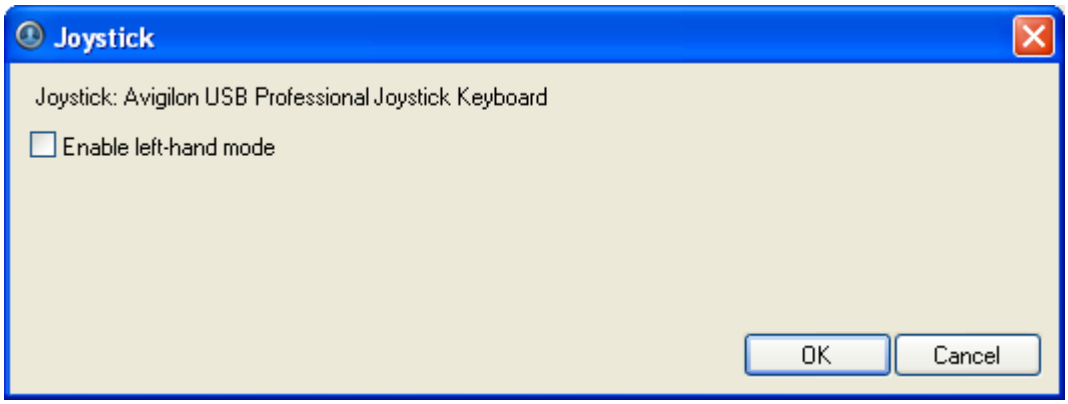


Figure A. Joystick dialog box

5. Select the **Enable left-hand mode** check box.
6. Click **OK**.

The keyboard is now configured for left-hand mode.

Rotate the keyboard until the joystick is on the left and the jog shuttle is on the right. Reinstall the keypad cover with the View button labels at the top.

Exporting Settings

You can export your personalized settings for the Client software so that the settings can be backed up or used on a different computer.

To export server settings like Recording Schedules, Users & Groups, Device, POS Source, and Device Connection settings, see the *Avigilon Control Center Server User Guide*.

Note: Some features are not displayed if the server does not have the required license, or if you do not have the user permissions to access the feature.

Exporting client settings

1. Right-click the local client in the System Explorer and select **Setup** to open the client Setup dialog box.
   For more information, see Accessing the Client Setup.
2. Click **Export Settings**.
3. Select the items you want to export.

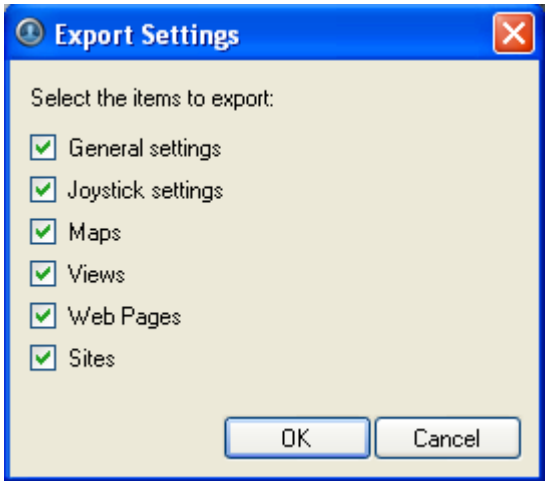


Figure A. Export Settings dialog box

The **General settings** include display quality, deinterlacing, manually added servers, image overlays, and client connection speed.

4. Click **OK**.
5. In the Save As dialog box, name and save the file.

   Exported client settings can only be saved in Avigilon Client Settings File (AVC) format.

Import Settings

Import and use settings that were previously exported from the local client, or from a different computer.

Importing client settings

1. Right-click the local client in the System Explorer and select **Setup** to open the client Setup dialog box.
   For more information, see Accessing the Client Setup.
2. Click **Import Settings**.
3. In the Select File to Import From dialog box, browse to the settings file you want to import, and click **Open**.
4. Select the specific settings you want to import.

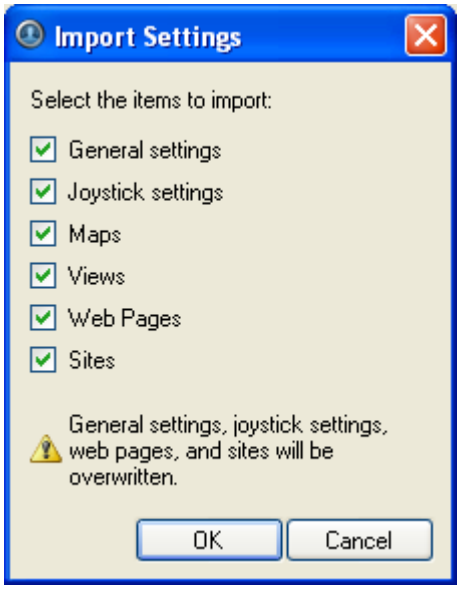


Figure A. Import Settings dialog box

5. Click **OK**.

Site View

What is Site View?

Site View is a way to customize the way cameras and servers are displayed in the System Explorer.

The System Explorer is the left pane of the application window, where all your servers and cameras are organized for easy access. The System Explorer is able to organize your surveillance system in two ways: Server View and Site View. Server View lists all the servers, cameras, and encoders that are available to you, and gives you quick access to your maps, web pages, and saved Views.

Site View allows you to customize the way cameras, servers, encoders, maps, saved Views and web pages are displayed in the System Explorer. You can organize the cameras by location, or only display maps of the surveillance site.

Accessing Site View

Site View allows you to customize the System Explorer display. The default Server View lists all the cameras on the network by the server they are connected to. This may not be logical for your needs, so you can create a Site View that reflects your surveillance requirements. For example, you can create a Site View that mimics the layout of each floor in your building, or group all the cameras that face the north end of your surveillance site.

To access the Site View, performing the following:

- In the System Explorer pane, select **Site View** from the views drop down list.

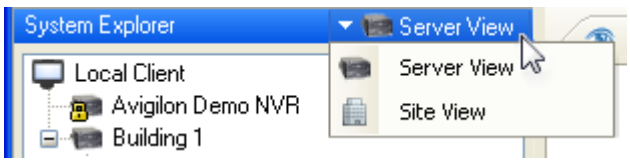


Figure A. System Explorer

If you have not yet created a Site View, you will be prompted to set up a new Site View. Click **Yes** to add a site, see Adding a Site for more information.

Adding a Site

The System Explorer Site View allows you to customize the way cameras, servers, encoders, personalized maps, saved Views and web pages are displayed. Add new sites to group items together.

1. Select **File > Edit Site View...** to open the Edit Site View dialog box.

   If you try to access the System Explorer Site View before a site has been added, you will be prompted to set up a new site. Click **Yes** to open the Edit Site View dialog box.

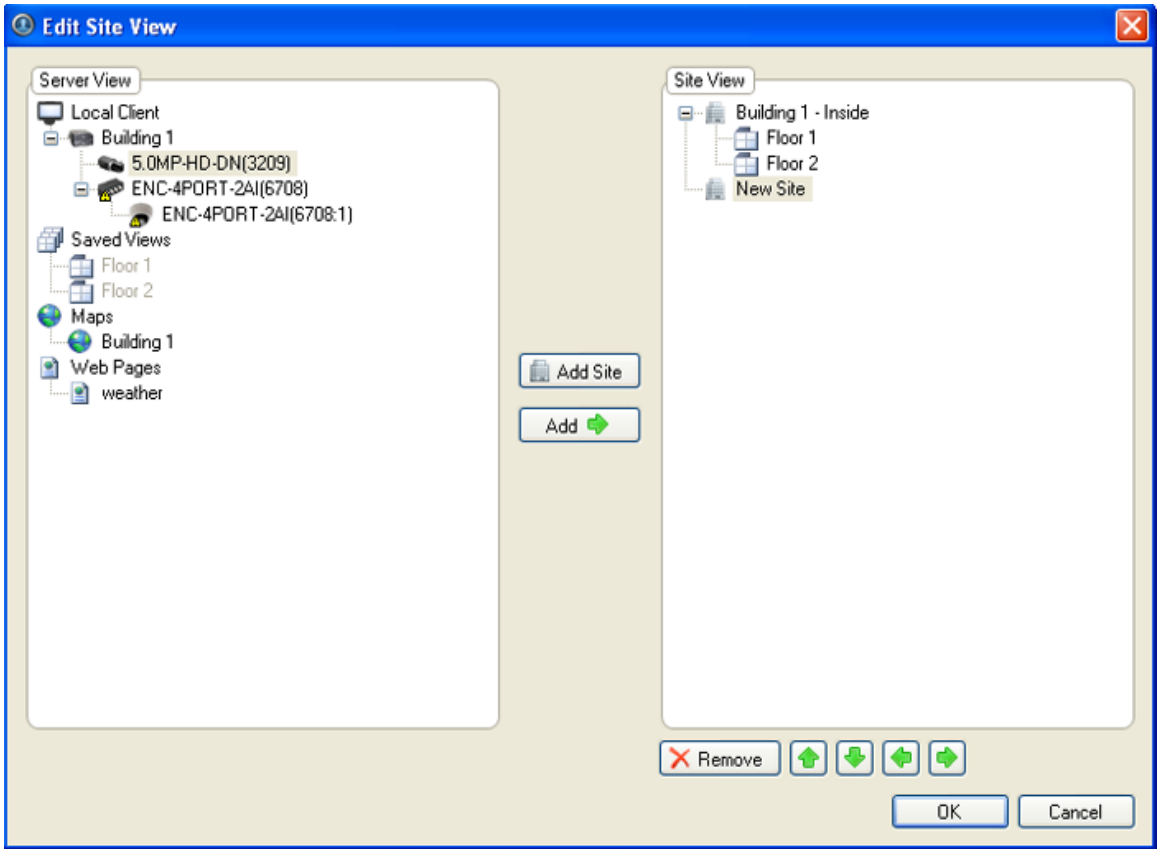


Figure A. Edit Site View dialog box

2. In the Site View pane, select and rename the New Site.
3. In the Server View pane, select any of the listed items and click **Add**.

   Note: Only the servers you are logged into are displayed.

4. Once the selected item has been added to the Site View pane, use the green arrows to position the item in your Site View.
5. Click **Add Site** to create a new site to group items under.
6. Click **Remove** to remove any item from the Site View.

7. When your Site View is complete, click **OK**.

Editing and Deleting a Site

Whenever your site requirements change, you can edit or delete the configured Site View.

1. Select **File > Edit Site View** to open the Edit Site View dialog box.
2. In the Edit Site View dialog box, perform one of the following:
    - To edit the Site View, make the required changes then click **OK**.
    - To delete the entire Site View, select each site and click **Remove**. When there are no sites listed in the Site View, click **OK**.

      Next time you attempt to open Site View in the System Explorer, you will be prompted to create a new Site View.

Views

What are Views?

A View is a tab composed of image panels that allow you to organize how video is monitored.

For example, you can choose to monitor video from multiple cameras simultaneously by using different layouts.

Adding and Removing a View

Views allow you to customize how you monitor video. You can add a new View to an existing window or open a new View in its own window to make use of multiple monitors. Views can also be removed as required.

Adding a New View to the Application Window

Perform one of the following to open a new View in the application window:

- Select **File > New View**.
- From the toolbar, click the  **New View** button.

Adding a View to a New Window

Perform one of the following to open a new View window.

- Select **File > New Window**.
- From the toolbar, click the  **New Window** button.

A new window appears. You can now position this window to make use of multiple monitors.

Closing a View from the Application Window

Perform one of the following to remove a View from the application window:

- Select **File > Close View**.
- On the View tab, click the red **Close View** button.

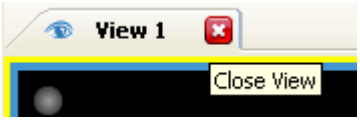


Figure A. Close View button

Closing a Window

- Select **File > Close Window**.

Selecting a Layout for a View

You can organize how video from multiple cameras are displayed by selecting a View layout.

- Select **View > Layouts > # Division**.
- On the toolbar, select one of the layout options.

Figure A. Layouts on the Toolbar

Making a View Full Screen

You can enlarge a View to maximize the use of the monitor.

Making a View Full Screen

- On the toolbar, click  **Full Screen**.

Ending Full Screen

- On the toolbar at the top left of the screen, click 

.

Tip: The toolbar is hidden when the application is idle. Move your mouse to display the toolbar.

Cycling Through Views

Once you have multiple Views setup, you can cycle through the Views by displaying each for a few seconds. This is useful when monitoring a large number of cameras.

1. Activate the Cycle Tab function by performing one of the following:
    - From the View menu, select **Cycle Views**.
    - On the toolbar, click  **Cycle Views**.

If required, the cycle dwell time can be changed, see Changing General Client Settings for more information.

Saving a View

Once you have set up a particular View, you can save the View for use again in the future. A saved View records the View layout, the cameras displayed in each image panel, and the image panel display settings.

Saving a View

1. Select **File > Save View**.
2. In the Save As dialog box, name the View and click **OK**.

Your saved view will appear in the System Explorer.

Figure A. Saved Views

Opening a saved View

Perform one of the following

- In the System Explorer, right-click the saved View and select **Open**.
- Drag the saved View from the System Explorer to the current View in the application or new window.

Renaming a saved View

1. In the System Explorer, right-click the saved View and select **Rename**.
2. In the Rename View dialog box, enter a new name and click **OK**.

Deleting a saved View

1. In the System Explorer, right-click the saved View and select **Delete**.
2. In the confirmation dialog box, click **Yes**.

Maps

A map is a graphical representation of your physical surveillance site, and an alternative view to the System Explorer. You can open a map in any image panel.

You can add cameras, encoders, servers, saved views, and other maps to your map to help you quickly navigate through your surveillance site.

To watch a video overview of the Maps feature, see *Module 4 - Working with Maps and Web Pages* in the Avigilon University - End User Stream.

Using a Map

You can view a map in any image panel, and open video or alarms from the map.

1. To open a map in a image pane, perform one of the following:
    - Drag the map from the System Explorer to an image panel.
    - In the System Explorer, right-click the map and select **Add to View**

Figure A. System Explorer: Maps List

2. When the map appears in an image panel, perform any of the following:

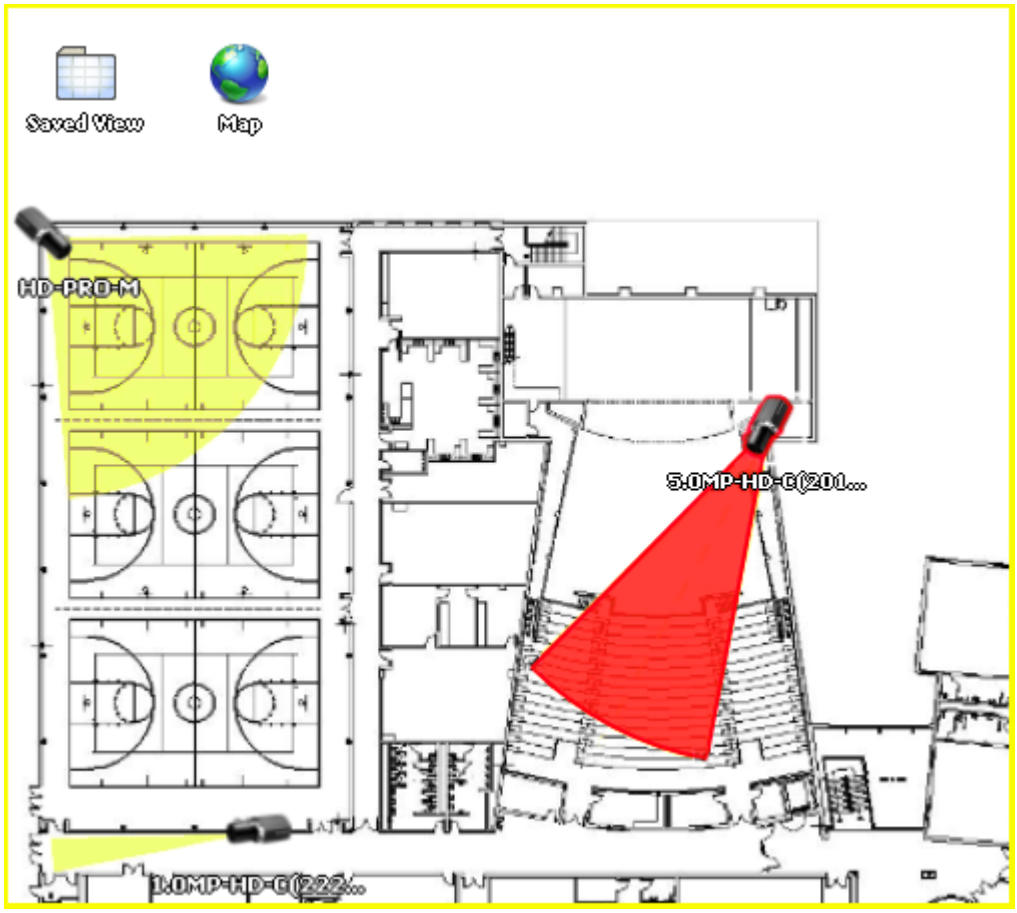


Figure B. Map display in an image panel.

To...	Do this...
Review an alarm	When a camera flashes in red, the alarm linked to the camera has been triggered. • Click the camera to monitor the live alarm video.
Display video from a camera on the map	• Drag a camera from the map to an image panel. • Click the camera on the map.
Open a linked map	• Click the map icon on the map. You can use the **Forward** and **Back** buttons to retrace your steps.
Open a linked View	• Click the Saved View placed on the map.

Adding a Map

You can create a map from any image in JPEG, BMP, PNG, or GIF format.

1. To start a new map, perform one of the following:
    - From the **File** menu, select **New Map**.
    - In the System Explorer, right-click the **Maps** icon, and select **New Map**.
2. In the Select Map Image dialog box, locate your map image and click **Open**.
3. In the **Map Editing** view, drag and place cameras from the System Explorer onto the map.

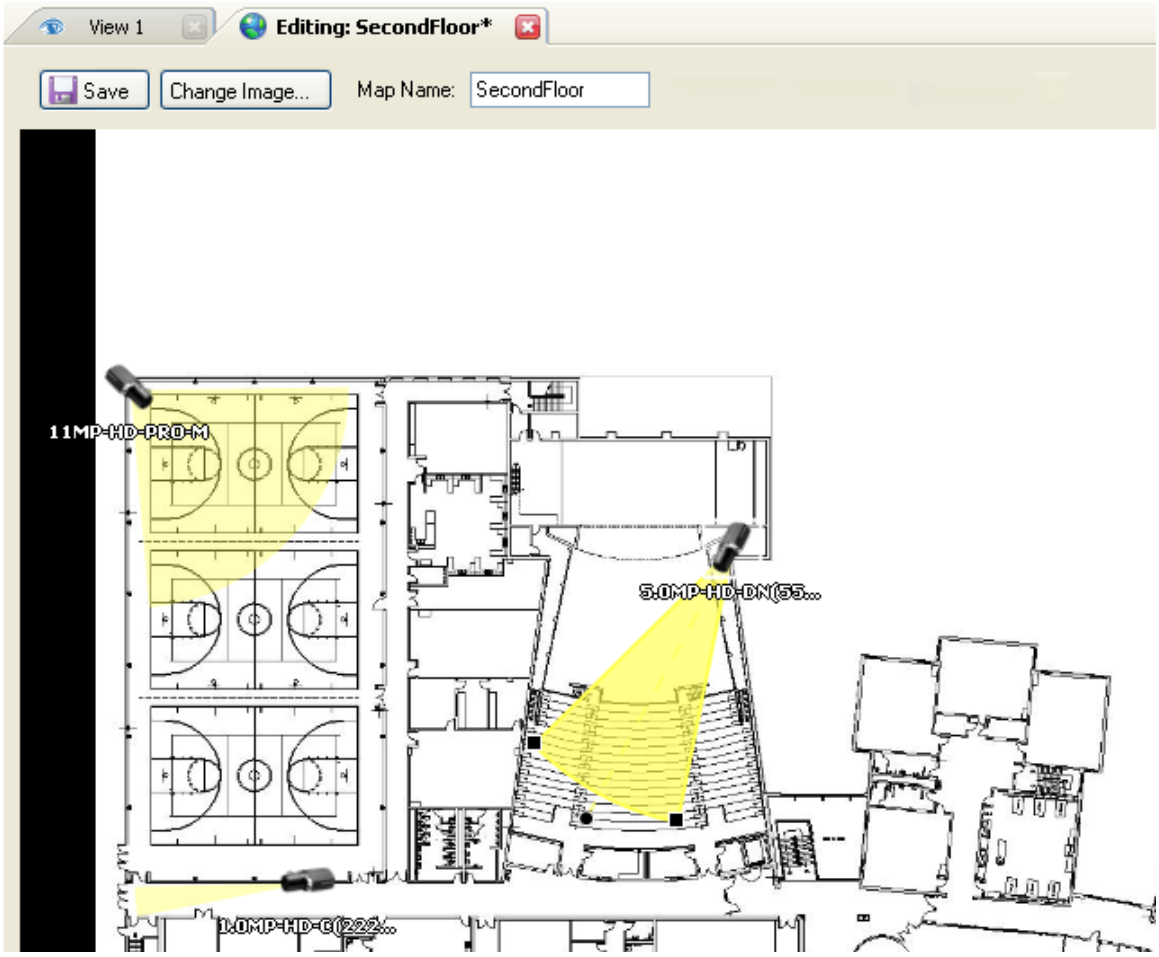


Figure A. Editing: Map tab

By default a camera is displayed as an icon with a yellow triangle to represent its field of view.

4. Drag encoders, servers, saved views and other maps from the System Explorer onto the map image, as required.

5. In the **Map Icon Properties** box, you can change the way icons are displayed on the map. Select any icon on the map and perform the following:

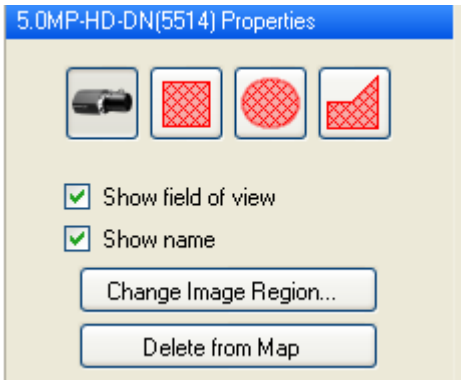


Figure B. Camera icon properties

4.

a. To replace an icon with a clickable shape region, select one of the shape buttons. You can choose a rectangle, ellipse, or polygon region to replace the icon.

b. Select the **Show name** check box to display the object's name on the map.

c. Click **Delete from Map** to remove the icon or clickable shape region from the map.

d. (Cameras only) Select the **Show field of view** check box to display the camera's yellow field of view.

To adjust the field of view, drag the corners of the yellow triangle to expand the field of view or drag the black circle icon at the end of the triangle to rotate the field of view.

e. (Cameras only) Click **Change Image Region...** to change the video region associated with the camera on the map.

In the Change Image Region dialog box, drag the corners of the green overlay to change the view, then click **OK**.

5. In the **Map Name** field, enter a name for the map.

6. Click **Save**.

Editing and Deleting a Map

Whenever a map no longer meets your current requirements, you can update the map or delete the old map.

Editing a Map

1. In the System Explorer, right-click a map and select **Edit**.

Figure A. System Explorer: Maps list

2. Make the necessary changes to the map and click **Save**.

Deleting a Map

1. In the System Explorer, right-click the map and select **Delete**.
2. When the confirmation dialog box appears, click **Yes**.

Web Pages

You can view online content while monitoring videos in a View, by adding web pages to the Avigilon Control Center.

To watch a video overview of the web pages feature, see *Module 4 - Working with Maps and Web Pages* in the Avigilon University - End User Stream.

Using a Web Page

To open a web page, perform one of the following

- Drag the web page from the System Explorer to an image panel.
- In the System Explorer, right-click the web page and select **Add to View**.

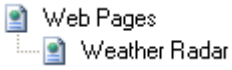


Figure A. Saved web pages

The web page is displayed in one of the image panels. Use the web browser buttons to navigate through the internet.

Figure B. Web image panel buttons.

Adding a Web Page

You can add web pages to the Avigilon Control Center Client software to enable quick access to web pages that are part of your surveillance system.

1. To open the Add Web Page dialog box, perform one of the following:

- From the File menu, select **New Web Page**.
- In the System Explorer, right-click the Web Pages icon, and select **New Web Page**.

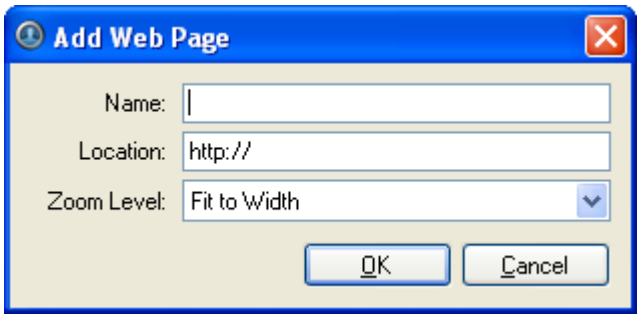


Figure A. Add Web Page dialog box

2. Enter a name for the web page.
3. Enter the web page URL in the **Location** field.
4. Select a **Zoom Level** for viewing the web page inside an image panel.
5. Click **OK**.

Editing and Deleting a Web Page

Whenever a web page becomes out of date, you can choose to update the web page address or delete the web page.

Editing a Web Page

1. In the System Explorer, right-click a web page and select **Edit**.

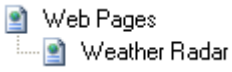


Figure A. Saved web pages

2. Make the required changes to the web page and click **OK**.

Deleting a Web Page

1. In the System Explorer, right-click the web page and select **Delete**.
2. When the confirmation dialog box appears, click **Yes**.

Video

The Avigilon Control Center Client software allows you to view multiple live and recorded video streams in a View, while giving you control of PTZ cameras, digital zoom, audio, manual recording, digital outputs, and other playback settings.

To watch a video of the application's video features, see *Module 1 - Introduction to Avigilon Control Center Client and Viewing Live Video* and *Module 2 - Identifying, Bookmarking, Searching and Exporting Video* in the Avigilon University - End User Stream.

Note: Some features are not displayed if the server does not have the required license, or if you do not have the user permissions to access the feature.

Viewing Live Video

While viewing live video, you can perform any of the following procedures.

Adding and Removing Cameras in a View

To view a camera's video, display the camera in a View. The video can be removed from the View when it is no longer needed.

Adding a Camera to a View

Perform one of the following:

- Drag the camera from the System Explorer pane to an empty image panel in a View.
- In the System Explorer, right-click the camera and select **Add to View**.

  The camera is added to the next empty image panel in the View layout.

Tip: You can drag the same camera to multiple image panels to view the images at different zoom levels or with different video adjustment properties.

Removing a Camera From a View

Perform one of the following:

- Right-click the image panel, and select **Close**.
- Inside the image panel, click  **Close**.

Displaying Live Video

Once a camera video has been added to an image panel, you can choose to view the live video stream. You can set the entire View to display live video, or only set specific image panels to display live video.

Live video is indicated by a blue border around the image panel.

- To display live video in a View, perform one of the following:
  - Select **View > Live**.
  - On the toolbar, select 

.
- To switch an individual image panel to view live video, right-click the image panel and select **Live**.

Zooming and Panning a Video

The zoom and pan tools allow you to focus on specific regions in a camera video.

Using the Zoom Tools

You can rotate the scroll wheel on your mouse to zoom in and out of a video image. Or you can use the Zoom tools in the application:

1. Select a Zoom tool:
   - From the **Tools** menu, select **Zoom In Tool** or **Zoom Out Tool**.
   - On the toolbar, click  **Zoom In Tool** or  **Zoom Out Tool**.
2. Click the image panel until you reach the desired zoom depth.

Using the Pan Tools

You can right-click and drag inside an image panel to pan the video image, or you can perform the following:

1. Select the Pan tool:
    - From the Tools menu, select **Pan Tool**.
    - On the toolbar, click the **Pan Tool**.
2. Drag the video image in any direction inside the image panel.

Controlling PTZ Cameras

Pan, Tilt, Zoom (PTZ) controls allow you to control cameras with PTZ functionality. You can control a PTZ camera by using the onscreen controls or by using the tools in the PTZ Controls pane.

1. To display the PTZ Controls pane, perform one of the following:
    - From the **Tools** menu, select **PTZ Controls**.
    - On the toolbar, click **PTZ Controls**.

    The PTZ Controls pane is displayed on the left, below the System Explorer.

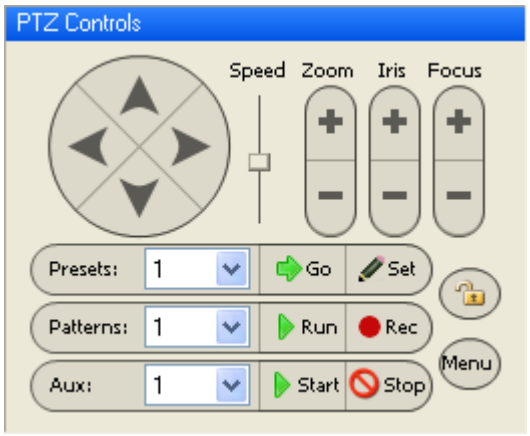


Figure A. PTZ Controls

2. Display the video from a PTZ camera in the current View.
3. To pan or tilt, perform one of the following:
    - Drag the mouse pointer in the direction that you want to move the camera. The further the mouse is from the center of the image panel, the faster the camera will move.

- Click the **Pan/Tilt** arrow buttons in the PTZ Controls pane. The speed for all pan/tilt movements can be adjusted using the **Speed** slider.

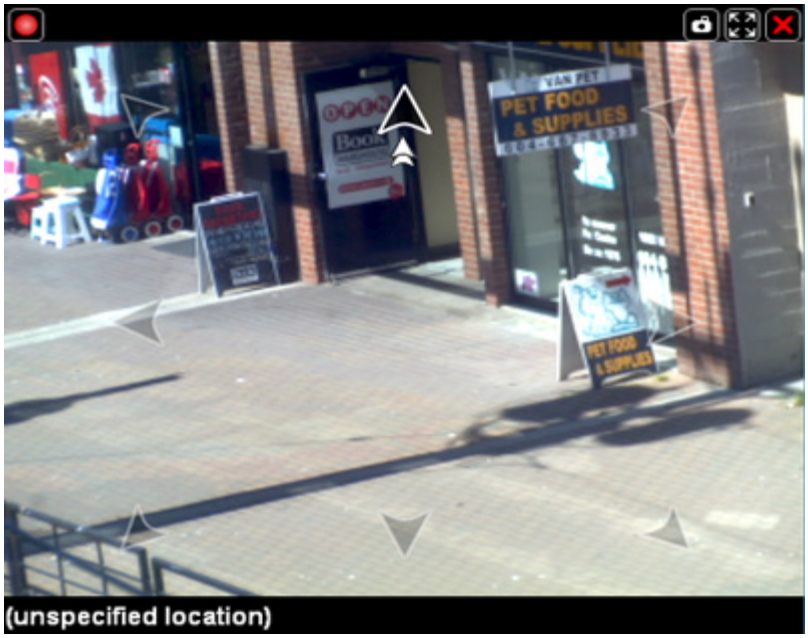


Figure B. PTZ On-Screen Controls

4. Use the other PTZ controls to perform any of the following:

Action	Control	Procedure
To zoom		Perform one of the following: • Click on the zoom controls in the PTZ Controls area. • Click the image panel and use the mouse scroll wheel to zoom in and out.
To control the **Iris** or **Focus**		Click the **+** and **-** buttons.
To program a PTZ preset		1. Use the PTZ buttons to move the camera field-of-view to the desired position. 2. In the PTZ Controls pane, select a preset number and click **Set**.

To activate a PTZ preset		Select a preset number and click **Go**.
To program a PTZ pattern		1. In the PTZ Controls pane, select a pattern number and click **Rec**. 2. Use the PTZ controls to initiate a series of camera movements. 3. In the PTZ Controls pane, click **Stop**.
To activate a PTZ pattern		In the PTZ Controls pane, select a pattern number and click **Run**. The pattern will repeat until the pattern is stopped or another pattern is set.
To activate an auxiliary command		1. Select an command number and click **Start** to initiate the auxiliary output. 2. Click **Stop** to turn off the auxiliary output.
To display the PTZ camera onscreen menu		1. Click the **Menu** button. 2. In the PTZ Controls pane, use the pan/tilt controls to navigate the menu. Use the **Pan/Tilt** buttons to navigate the menu. Use the **Zoom** buttons to modify your selection choices. Use the **Focus** buttons to confirm or cancel your selections.
To lock the PTZ controls		Click the **Lock** button. No other user will be able to use the PTZ controls for the selected camera until you unlock the

		controls or log out.

Listening to Audio in a View

If there is a microphone linked to a camera, the Audio bar is displayed in the image panel when you view the camera's video.

Note: This feature is only available if there is a microphone and a Audio Channel License installed.

To control the audio settings, perform any of the following:

- In the lower-right corner of the image panel, click the **Speaker** icon to mute or activate the audio.
- Move the slider to change the volume level.

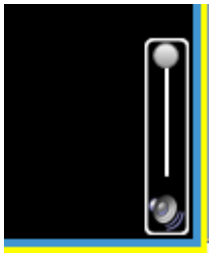
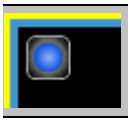
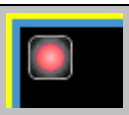
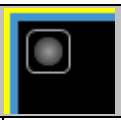


Figure A. Audio bar

Triggering Manual Recording

When viewing live video, you can click the **Manual Recording** icon to force the camera to record the current video stream regardless of the camera's recording schedule.

The **Recorder Indicator** overlay must be enabled for manual recording to function. See Overlaying Information on the Image Panel for more information.

		
If the icon is blue, it is in Continuous Recording mode.	If the icon is red, an event has caused the camera to begin recording.	If the icon is grey, the camera is not recording.

Starting Manual Recording

- In the top-left corner of the image panel, click the record indicator to start manual recording.

Figure A. Manual Recording indicator

The record indicator is highlighted in blue to indicate that the camera is recording. Manual recording continues until it is stopped, or until the maximum recording duration is reached. The maximum duration is configured in the Manual Recording dialog box, see Manual Recording Settings for more information.

Stopping Manual Recording

- In the top-left corner of the image panel, click the record indicator to stop manual recording.

Figure B. Manual Recording indicator

Triggering Digital Output

While you view live video in an image panel, you can manually trigger any digital output that is linked to the camera.

The digital output is configured in the Digital Inputs and Outputs dialog box, see Setting Up Digital Outputs for more information.

1. Open the camera's live video in an image panel.
2. In the image panel, click **Trigger Digital Output**.
3. If you have more than one digital output linked to the camera, you will be prompted to select the digital output you want to trigger.

Viewing Recorded Video

While viewing recorded video, you can perform any of the following procedures:

Adding and Removing Cameras in a View

To view a camera's video, display the camera in a View. The video can be removed from the View when it is no longer needed.

Adding a Camera to a View

Perform one of the following:

- Drag the camera from the System Explorer pane to an empty image panel in a View.
- In the System Explorer, right-click the camera and select **Add to View**.

  The camera is added to the next empty image panel in the View layout.

Tip: You can drag the same camera to multiple image panels to view the images at different zoom levels or with different video adjustment properties.

Removing a Camera From a View

Perform one of the following:

- Right-click the image panel, and select **Close**.
- Inside the image panel, click  **Close**.

Displaying Recorded Video

Once a camera video has been added to an image panel, you can choose to view the camera's recorded video. You can set the entire View to display recorded video, or only set specific image panels to display recorded video.

Recorded video is indicated by a green border around the image panel.

- To display recorded video in a View, perform one of the following:
  - Select **View > Recorded**.
  - On the toolbar, select 

.
- To switch an individual image panel to view recorded video, right-click the image panel and select **Recorded**.

Zooming and Panning a Video

The zoom and pan tools allow you to focus on specific regions in a camera video.

Using the Zoom Tools

You can rotate the scroll wheel on your mouse to zoom in and out of a video image. Or you can use the Zoom tools in the application:

1. Select a Zoom tool:
    - From the **Tools** menu, select **Zoom In Tool** or **Zoom Out Tool**.
    - On the toolbar, click  **Zoom In Tool** or  **Zoom Out Tool**.
2. Click the image panel until you reach the desired zoom depth.

Using the Pan Tools

You can right-click and drag inside an image panel to pan the video image, or you can perform the following:

1. Select the Pan tool:
    - From the Tools menu, select **Pan Tool**.
    - On the toolbar, click the  **Pan Tool**.
2. Drag the video image in any direction inside the image panel.

Listening to Audio in a View

If there is a microphone linked to a camera, the Audio bar is displayed in the image panel when you view the camera's video.

Note: This feature is only available if there is a microphone and a Audio Channel License installed.

To control the audio settings, perform any of the following:

- In the lower-right corner of the image panel, click the **Speaker** icon to mute or activate the audio.
- Move the slider to change the volume level.

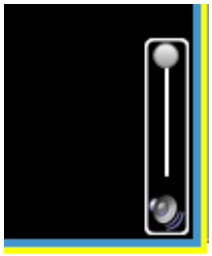


Figure A. Audio bar

Playing Back Recorded Video

The Timeline displays the time period when video were recorded and provides several controls for playing back the recordings.

The colored bars on the Timeline display a camera's recording history:

- A red bar indicates the camera recorded an event (for example, an alarm or motion event).
- A blue bar indicates the camera recorded video, but not in response to any event.
- White areas indicate that the camera did not record any video.
- An orange bar indicates a bookmark in the camera's recording history.

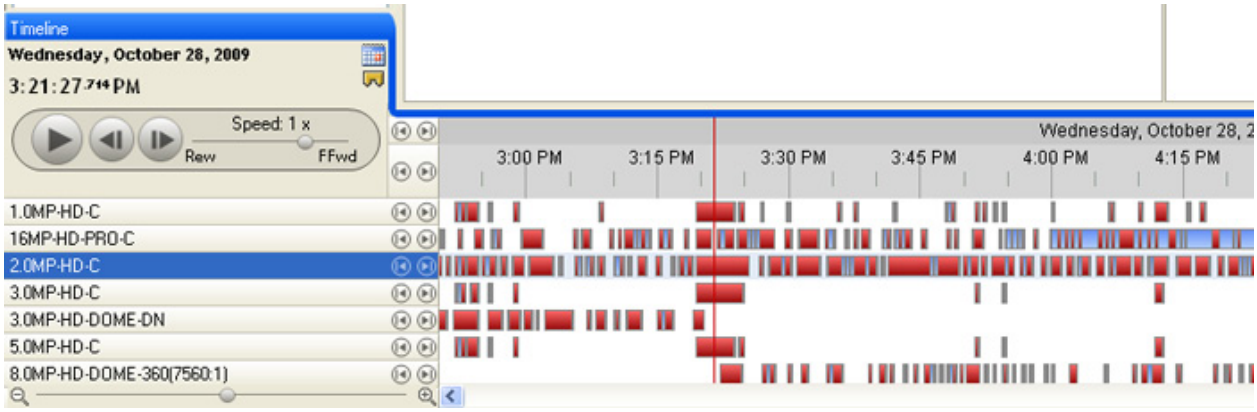
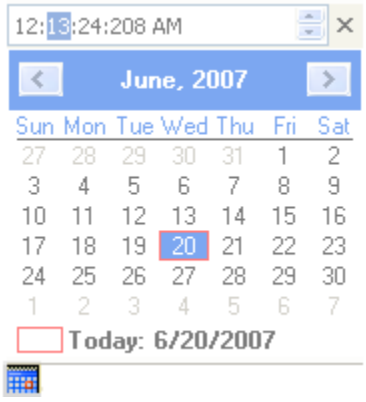
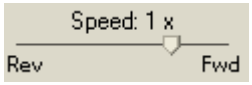
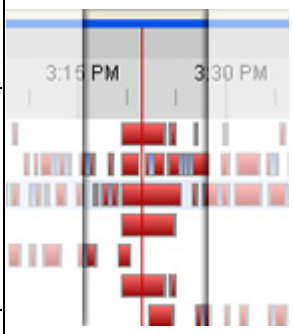


Figure A. Playback tools on the Timeline

Perform any of the following actions to control the playback of recorded video files:

Action	Tool	Procedure
To select a playback time		Perform one of the following: • Click the calendar and select a date and time. • On the Timeline, click on an area with recorded data indicated by a colored bar.
To add a		Click **Add Bookmark** to add a bookmark on the

bookmark		Timeline. See Bookmarking Recorded Video for more information.
To start playback		Click **Play**.
To stop playback		Click **Pause**.
To move forward a frame		Click **Step Forward**.
To move back a frame		Click **Step Backward**.
To control the playback direction and speed		Click and drag the slider to the right to move the video forward, or to the left to move the video in reverse. The further the slider is away from the center the faster the playback speed.
To jump forward or back on the Timeline		On the Timeline, click one of the **Go Forward** or **Go Back** buttons to move to different points on the Timeline.
To expand the Timeline to a specific moment in time		Perform one of the following: • Move the slider to zoom in or zoom out on the Timeline. • You can also use the mouse scroll wheel to zoom in or zoom out on the Timeline.
To center the Timeline on the time marker		Right-click the Timeline, and select **Center on Marker.**
To move through the Timeline quickly with the time marker		Drag the time marker through the Timeline.
To pan the Timeline		Perform one of the following:

		• Move the Timeline horizontal scroll bar at the bottom of the application window. • Right-click and drag the Timeline.

Bookmarking Recorded Video

You can add bookmarks to help identify segments of recorded video. Bookmarked video can be protected against scheduled data cleanup so the video is never deleted.

Adding a bookmark

1. To open the Edit Bookmark dialog box, perform one of the following:
   - On the Timeline, click **Add Bookmark**.
   - Drag the time marker to the beginning of the time you want to bookmark, then right-click and select **Add Bookmark**.

   The Edit Bookmark dialog box appears, and the bookmark time range is highlighted on the Timeline

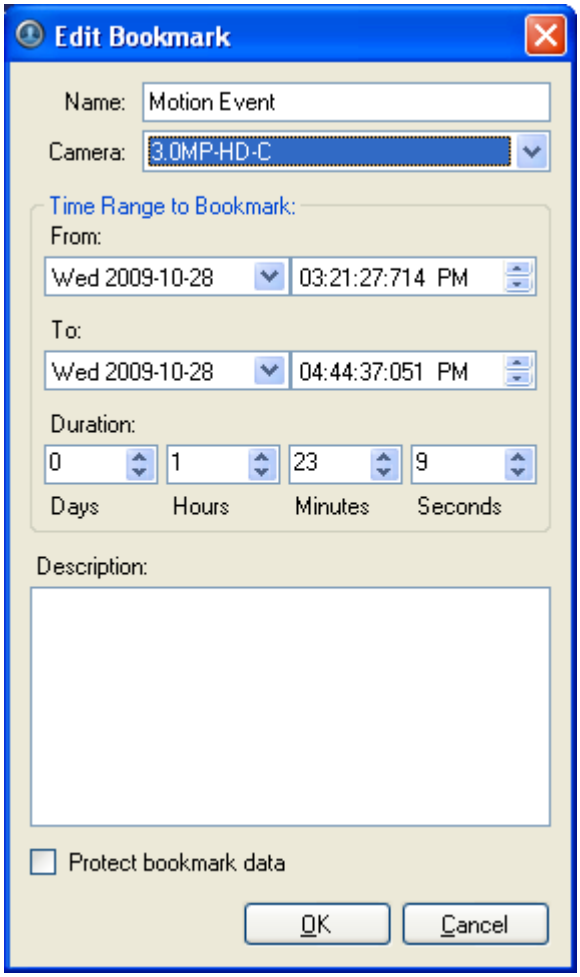


Figure A. Add Bookmark dialog box

2. In the **Name** field, enter a name for the bookmark.
3. In the **Camera** drop down list, select the camera the bookmark is attached to.
4. In the Time Range to Bookmark area, enter the time period you want to bookmark.

   You can also move the black time range markers on the Timeline to adjust the time range.
5. In the **Description** field, enter any required information about the bookmark.
6. To protect the bookmark data from deletion select the **Protect bookmark data** check box.

   Note: Protected bookmarks are never deleted. Be aware that bookmarked video occupy space on the server and become the oldest stored video.
7. Click **OK**.

Editing, deleting or exporting a bookmark

1. Click the bookmark on the Timeline then perform one of the following:

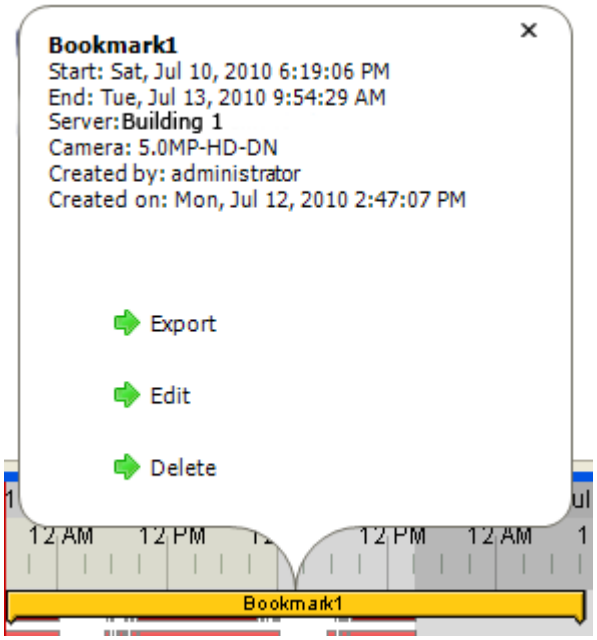


Figure B. Bookmark properties

To	Do this...
Edit a bookmark	Click **Edit** then make the necessary changes to the Edit Bookmark dialog box and click **OK**. Refer to the Adding a Bookmark procedure for details about the Edit Bookmark dialog box.
Delete a bookmark	Click **Delete**. When the confirmation dialog box appears, click **Yes**.
Export a bookmark	Click **Export** then complete the Export tab. See Exporting Recorded Video and Images for more information.

Adjusting Video Display in Image Panels

You can adjust the image panel display settings to enhance the video display on your monitor.

Maximizing an Image Panel

You can enlarge an image panel to help magnify the video displayed.

Maximizing an Image Panel

Perform one of the following:

- Right-click an image panel and select **Maximize**.
- Inside the image panel, click  **Maximize**.
- Double-click the image panel.

Restoring an Image Panel

Perform one of the following:

- Right-click the maximized image panel, and select **Restore Down**.
- Inside the image panel, click  **Restore Down**.
- Double-click the image panel.

Displaying Video Overlays

When you monitor video in a View, you can select the type of information that is displayed over the video in each image panel.

- Select **View > Image Overlays**, then select one or more of the following:

Option	Description
Camera Name	Displays the name given to the camera.
Camera Location	Displays the location given to the camera.
Timestamp	Displays the exposure timestamp of the video. The timestamp only appears when viewing recorded video.
Record Indicator	Displays the recording status of a camera. The recording status is indicated by the round **Record Indicator** icon on the top left corner of the image panel. The Record Indicator only appears when viewing live video. The color of the icon indicates the camera's recording status. ▪ Red: recording because an event occurred ▪ Blue: recording ▪ Grey: not recording Select the **Record Indicator** icon at any time to begin manual recording.
PTZ Controls	Displays the controls for controlling PTZ cameras on the video image.

Motion Activity	Highlights detected motion events in red.
License Plate	Displays license plate numbers as they are detected. **Note:** This feature is only available if the License Plate Recognition feature is installed.

Changing the Display Quality

If you do not have sufficient network bandwidth or processing power, you may not be able to view video at the full image rate and full quality. You can bias the image panels to display video in high quality/low frame rate or low quality/high frame rate.

The Change Display Quality settings only affect the image panel display and does not affect the actual video quality or image rate transmitted between the camera and the server. To modify the camera's display settings, see Compression and Image Rate settings.

1. Open the Change Display Quality dialog box:
   - Select **Tools > Change Display Quality...**.
   - In the toolbar, click  **Change Display Quality**.
2. In the Change Display Quality dialog box, select one of the following:

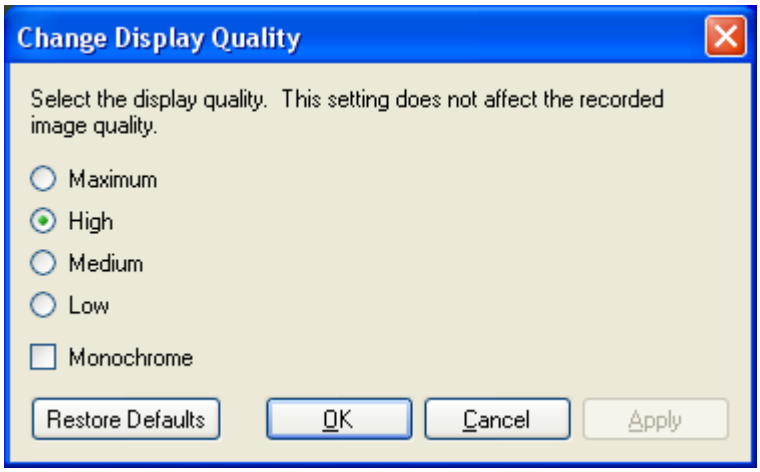


Figure A. Change Display Quality dialog box

   - **Maximum:** displays the full video quality and results in lowest displayed image rate.
   - **High:** displays 1/4 of the full video resolution.
   - **Medium:** displays 1/16 of the full video resolution.

- **Low:** displays 1/64 of the full video resolution and results in the highest displayed image rate.

3. Select the **Monochrome** check box to display the video in black and white.
4. Click **OK**.

Changing the Image Panel Display Settings

You can change the image panel display settings to bring out video details that are hard to see with the image panel's default settings.

Note: These settings only affect the image panel display and do not affect the camera's actual configuration.

1. Right-click an image panel and select **Display Adjustments...**.

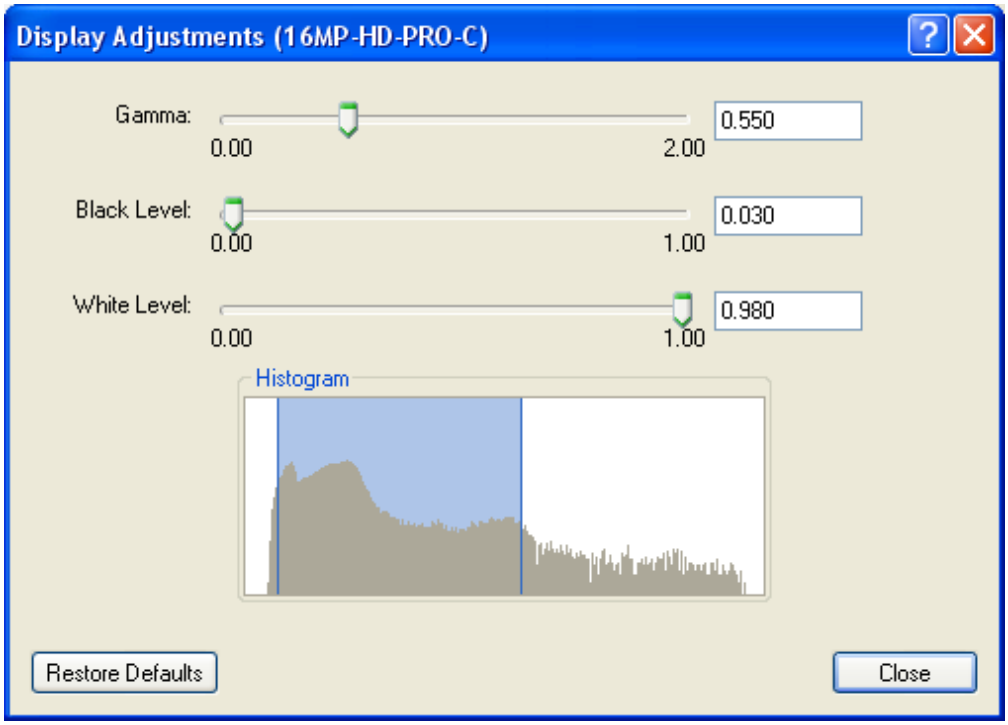


Figure A. Display Adjustments dialog box

2. Move the sliders to adjust the **Gamma**, **Black Level** and **White Level**.

   The image panel displays a preview of your adjustments.

3. Click **Restore Defaults** to clear your changes.
4. Click **Close**.

Viewing Analog Video in Deinterlaced Mode

If there are visible interlacing artifacts in the analog camera video, you can enable the deinterlacing filter to help improve the video image.

- To enable the deinterlacing filter, select **View > Display Deinterlaced Images**.

Alarms

The Alarms tab allows you to monitor and acknowledge alarms through the Avigilon Control Center Client software. Alarms are created in the server Setup, see Alarms for more information.

To watch a video overview of the Alarm Monitoring feature, see *Module 5 - Alarm Monitoring* in the Avigilon University - End User Stream.

Accessing the Alarms Tab

Perform one of the following steps to open the Alarms tab:

- From the **Tools** menu, select **Alarms...**.
- On the toolbar, click 

.

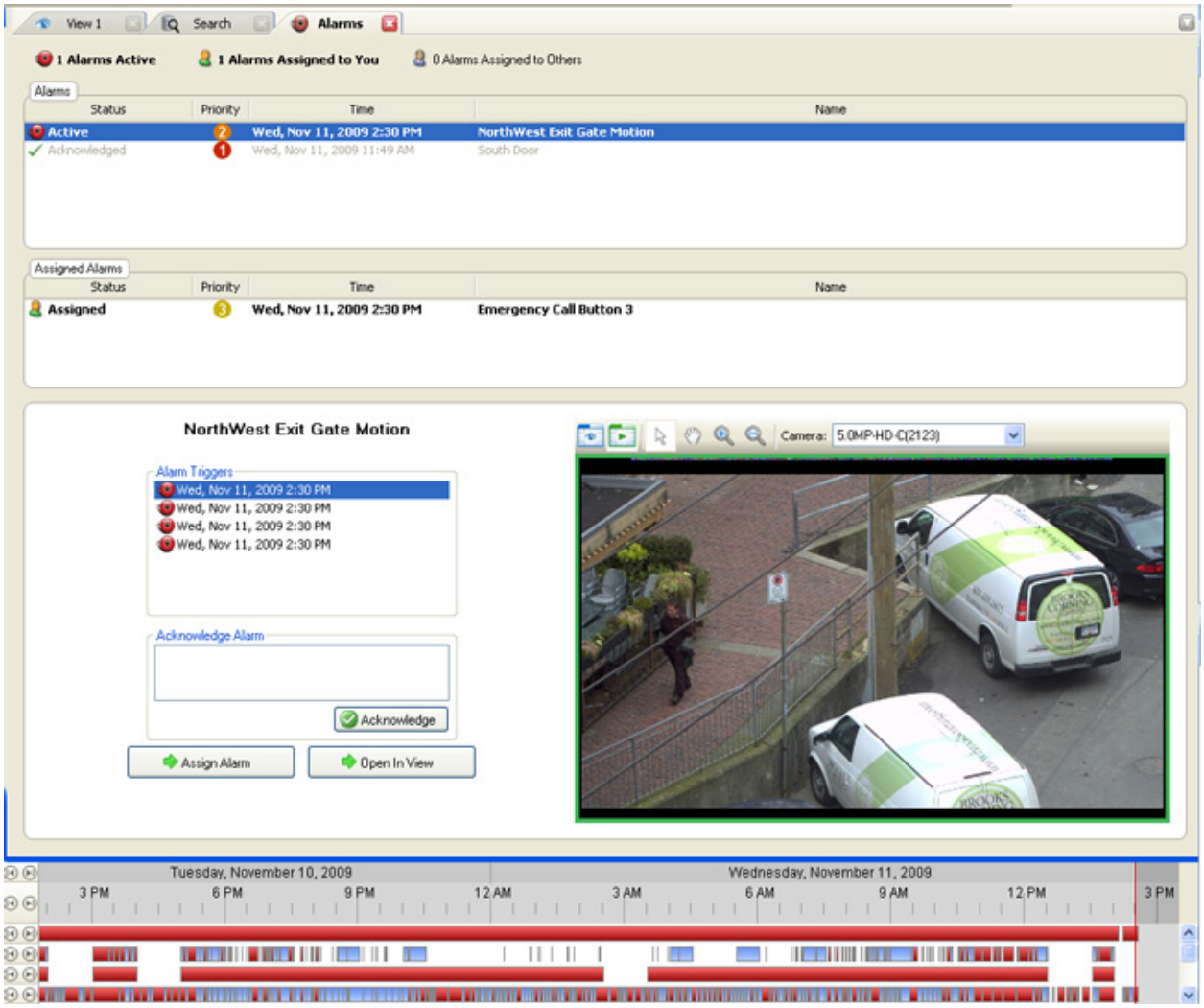


Figure A. Alarms tab

The Alarms tab is divided into the following areas:

- In the Alarms list is a list of alarms that are active, acknowledged, or assigned to another user. The alarms are sorted by status, priority then time.
- In the Assigned Alarms list is a list of alarms assigned to you. This list is not displayed when there are no alarms assigned to you.
- The Alarm Details area displays the alarm triggers and video when an alarm is selected from the Alarms list.
- The Timeline is used to play back the recorded alarm video.

Reviewing Alarms

In the Alarms tab, you can review alarm video and manage alarms. Active alarms can be assigned to yourself, and acknowledged alarms can be exported or purged as required.

Viewing Alarm Video

You can review active and acknowledged alarm video in detail through the alarm image panel, or opening the alarm video in a new View.

1. Select an alarm from the Alarms list. The alarm details are displayed.
2. In the Alarm Triggers list, select an alarm trigger to display the video for that alarm instance.
3. Use the alarm image panel controls to review the video in more detail.

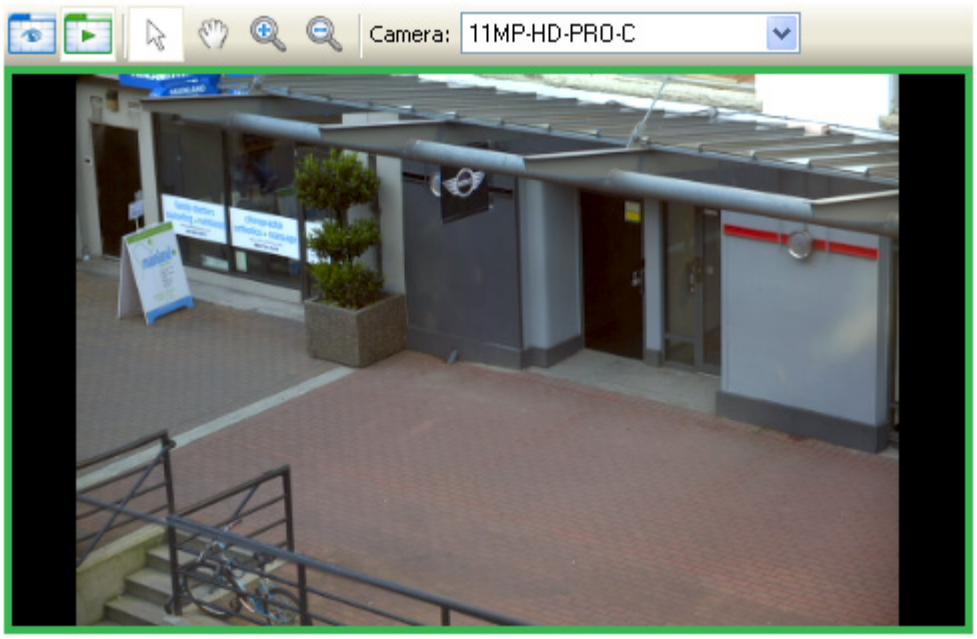


Figure A. Alarm image panel

   - In the **Camera** drop down list, select a camera that is linked to the alarm to review the video.
   - Use the **Zoom** and **Pan** tools to view specific parts of the video image in more detail. See Zooming and Panning in a Video for more information.
   - Use the **Live** and **Recorded** buttons to alternate from the recorded alarm video and the camera's live stream. See Viewing Live and Recorded Video for more information.

4. Click **Open In View** to open the alarm video in a new View.

5. Use the Timeline to control the video play back. See Playing Back Recorded Video for more information.

Assigning an Alarm

You can assign an alarm to yourself to avoid a duplication of effort in reviewing the alarm. Assigned alarms are hidden from other users until the alarm has been acknowledged.

Although you can only assign alarms to yourself, you can also unassign the alarm at any time.

1. Select an active alarm from the Alarms list.
2. When the alarm details are displayed, click **Assign Alarm**.

   The alarm is added to your Assigned Alarms list.
3. To unassign an alarm, select the alarm from the Assigned Alarms list and click **Unassign Alarm**.

Acknowledging an Alarm

Acknowledging an alarm indicates an alarm has been reviewed and is no longer active. You can acknowledge any alarm that is active or assigned to you.

1. After reviewing the alarm, enter notes describing the nature of the alarm in the Acknowledge Alarm text box.
2. Click **Acknowledge**.
3. If there is digital output linked to the alarm, a dialog box may appear to request permission to activate the digital output. Activate the digital output as required.

The Alarm is given an Acknowledged status in the Alarms list.

Searching Alarms

You can search through an alarm's history to review previous instances of the alarm.

1. Select an acknowledged alarm from the Alarms list.
2. In the alarm details area, click **Search Alarm**. See Performing an Alarm Search for more information.

Exporting Alarms

You can export alarm video for review on other computers.

1. Select an acknowledged alarm from the Alarms list.
2. In the alarm details area, click **Export Alarm**. See Exporting Recorded Video and Images for more information.

Purging an Alarm

Purging an alarm removes the alarm from the Alarms list until the alarm is activated again. Although the alarm is no longer listed in the Alarms list, the alarm information remains in the system and can still be searched.

1. Select an acknowledged alarm from the Alarms list.
2. In the alarm details area, click **Purge Alarm**.

Arming Image Panels

Arming an image panel reserves the image panel specifically for displaying video linked to alarms or rules. Armed image panels allow you to review and acknowledge alarms while monitoring video in a View. Any image panel can be armed or disarmed as required.

If there are no armed image panels, alarm video will appear in the next empty image panel in the current View, or in a new View if all current image panels are in use.

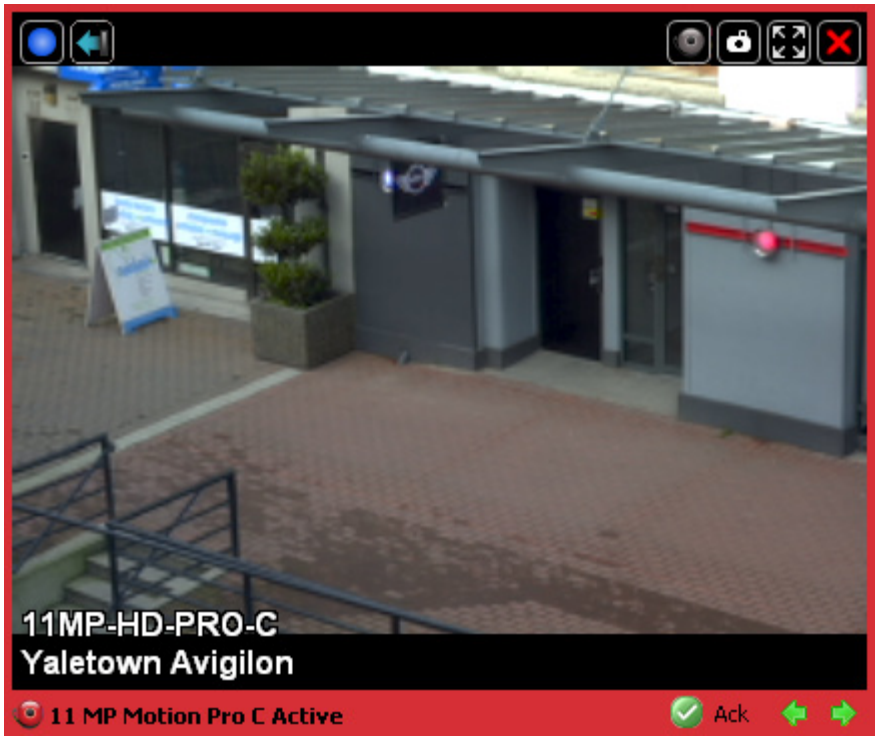


Figure A. Armed image panel

To arm or disarm an image panel, perform the following:

- In an image panel, click the **Arm Panel** button. The image panel is given a red border to show that it is armed.
- To acknowledge an alarm in the armed image panel, click the **Acknowledge** button.
- If the alarm is linked to multiple cameras, you can use the green arrows to move between the video linked to the alarm.
- To disarm an image panel, click the **Disarm Panel** button.

If multiple alarms are triggered at the same time, the linked video are queued within the armed image panel. The alarms are displayed by order of alarm priority then time. Once an alarm is acknowledged or assigned to a user, the alarm video is removed from the armed image panel.

Note: If you choose to close the video in the armed image panel, the alarm continues to be active until the alarm is acknowledged.

Video triggered by a rule are queued in the armed image panel after alarms, with the most recent video displayed first. Rules video are unlabeled and do not require acknowledgement.

License Plates

License Plate Recognition is a licensed feature that allows you to monitor the vehicle license plates that are detected by the Avigilon Control Center.

You can activate the license plate overlay to monitor license plates as they are detected. Or you can use the License Plate Watch List feature to notify you when specific license plates are detected.

To setup License Plate Recognition, see License Plate Recognition for more information.

License Plate Overlay

While you are monitoring video in an image panel, you can also monitor the license plates that come into the camera's License Plate Recognition field.

When the license plate overlay is enabled, license plate numbers are displayed in the bottom right corner of the image panel as license plates are detected by the camera.

To enable the License Plate overlay:

- Select **View > Image Overlays > License Plate**.

For more information about other overlays, see Displaying Video Overlays.

License Plate Recognition Watch List

The Watch List tracks the license plates you've configured the Avigilon Control Center System to recognize, and displays the detected matches in the License Plate Matches dialog box.

To configure the Watch List, see Configuring the Watch List for more information.

Note: The Watch List is only available if the License Plate Recognition feature is installed.

Reviewing the License Plate Matches

1. Open the License Plate Matches dialog box.

   The License Plate Matches dialog box automatically appears whenever license plates from the Watch List are detected. To review matches at a separate time, select **LPR > License Plate Matches...**

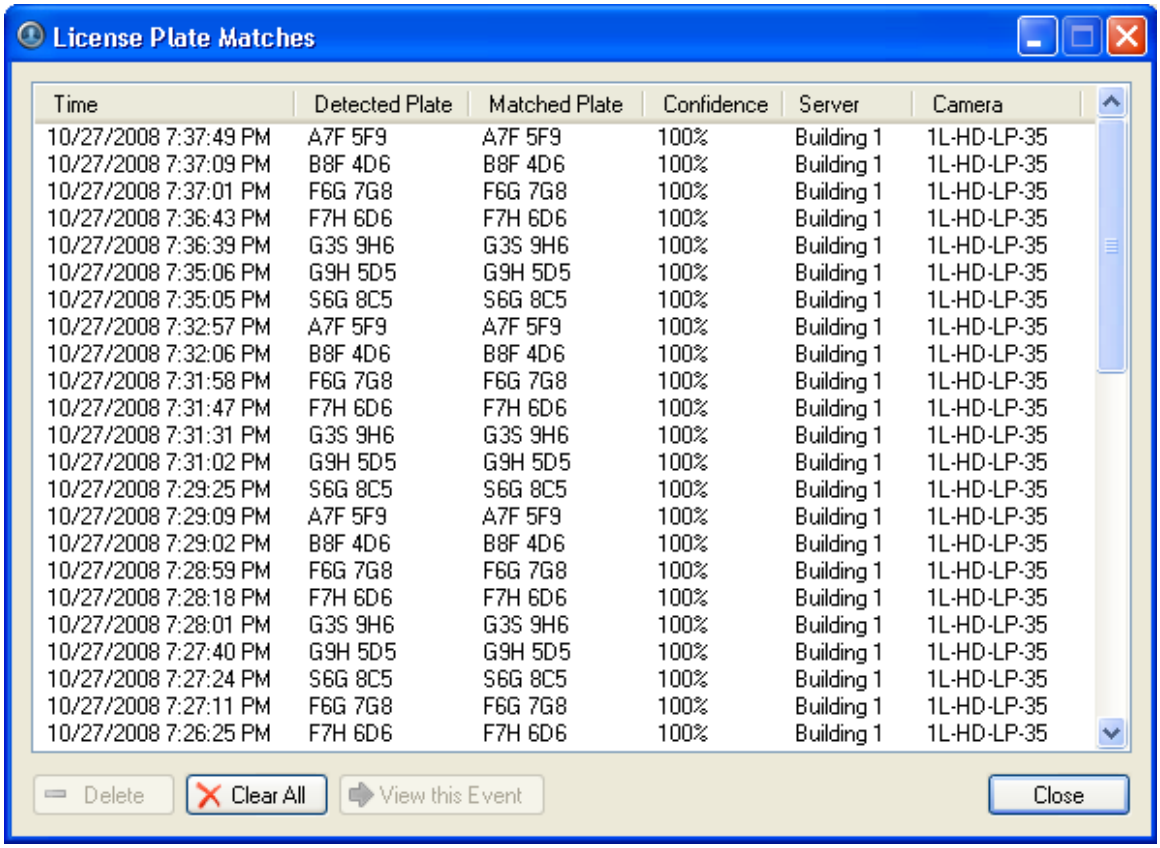


Figure A. License Plate Matches dialog box.

2. Select one of the license plate matches and perform one of the following:

   - Click **View this Event** or double-click the selected license plate to open a snapshot of the detected license plate in a new View.
   - Click **Delete** to delete the license plate from the list.
   - Click **Clear All** to delete the current match list. The list will repopulate as new license plates are detected.

3. Click **Close**.

Search

You can search for recorded video by alarms, license plates, events, thumbnails or POS transactions.

To watch a video overview of the Search features, see *Module 2 - Identifying, Bookmarking, Searching and Exporting Video* in the Avigilon University - End User Stream.

Note: Some features are not displayed if the server does not have the required license, or if you do not have the user permissions to access the feature.

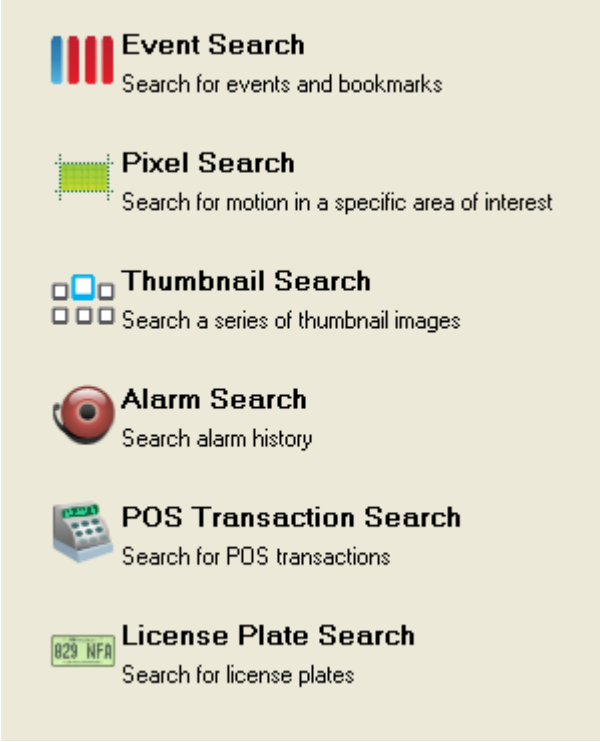


Figure A. Search options

Performing an Event Search

The Event Search allows you to search for a specific motion or digital input event by time range for the selected cameras.

1. Click 

to open the Search tab.
2. In the Search tab, select **Event Search**.

   The Search:Event tab is displayed.

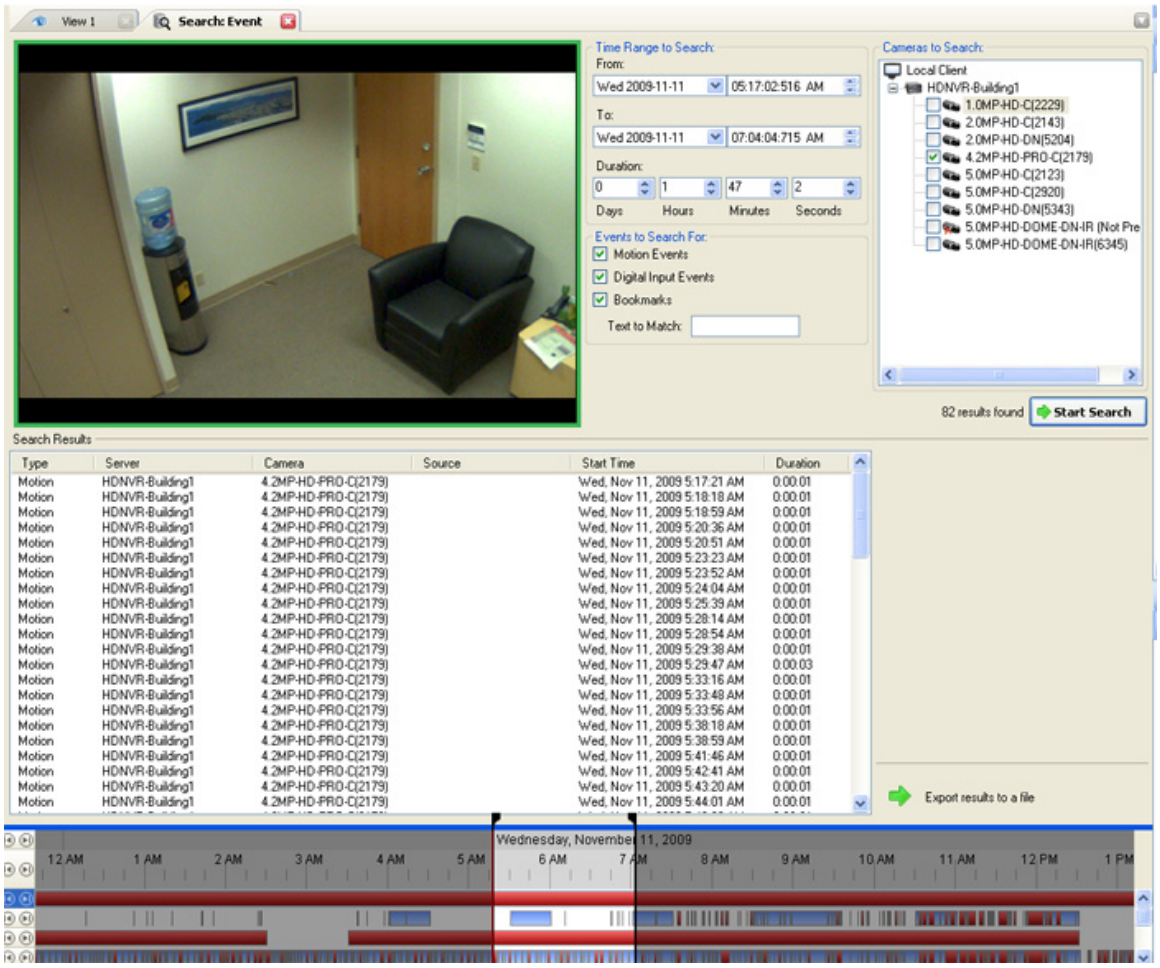


Figure A. Search: Event tab

3. In the Camera to Search area, select all the cameras you want to include in the search.
4. In the Time Range to Search area, set the date and time range of your search. The time range is highlighted on the Timeline by the black time range markers. You can also drag the time range markers to modify the time range.

5. In the Events to Search For area, select the types of events or bookmarks to include in the search.
6. In the Text to Match area, enter text to search for in the titles and descriptions of bookmarks.
7. Click **Start Search**.

Viewing Event Search Results

1. In the Search Results area, select a search result. The event timeline is highlighted and the related video is displayed in the search image panel.
2. Use the Timeline controls to review the event. See Playing Back Recorded Video for more information.
3. If you want to further refine your search, click **Perform a pixel search on this event** to perform a pixel search on the selected result. See Performing a Pixel Search for more information.
4. Click **Export this event** to export the selected event video. See Exporting Recorded Video and Images for more information about the available export settings.
5. To export all listed results, click **Export results to a file** and save the file.

Performing a Pixel Search

The Pixel Search allows you to search for motion events in specific areas of the camera's field of view.

1. Click 

to open the Search tab.
2. In the Search tab, select **Pixel Search**.

   The Search:Pixel tab displays.

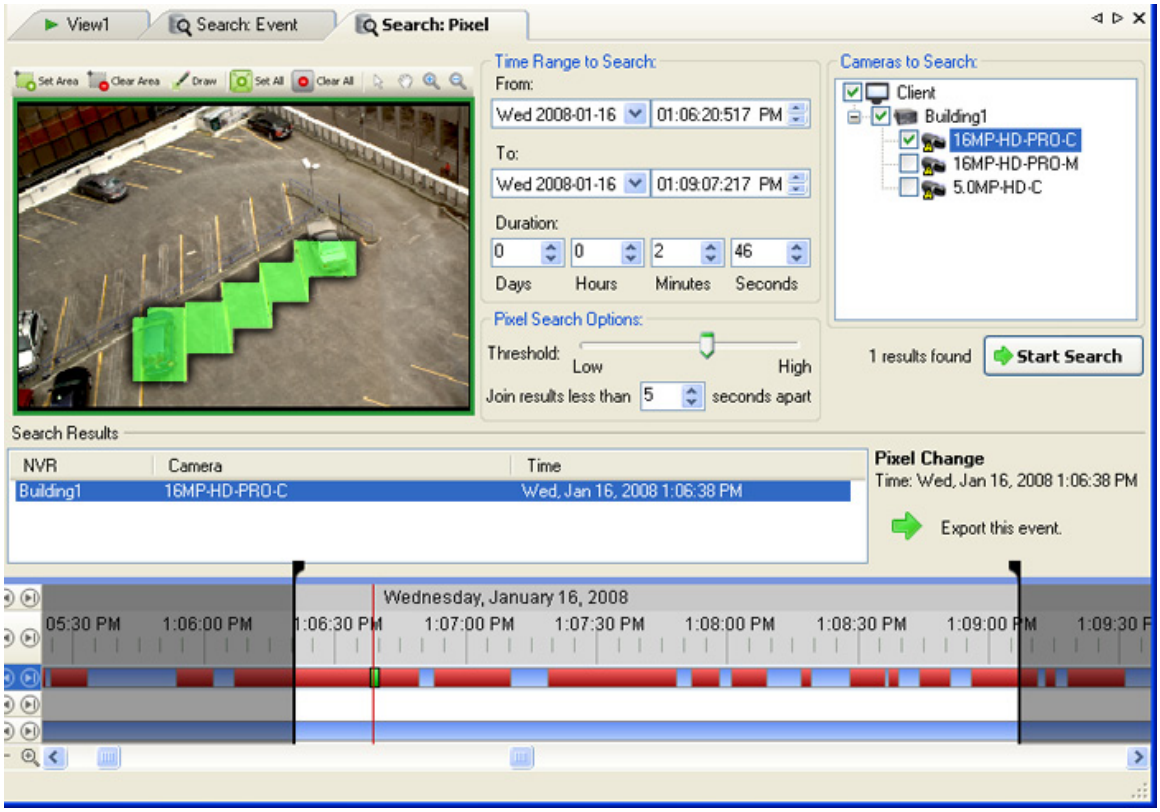


Figure A. Search:Pixel tab

By default, the entire video image is highlighted in green.

3. In the Camera to Search area, select a camera.
4. In the Time Range to Search area, set the date and time range of your search. The time range is highlighted on the Timeline by the black time range markers. You can also drag the time range markers to modify the time range.
5. Define the pixel search region by using the motion detection selection tools above the image panel. The pixel search will be performed in all areas highlighted in green.
6. In the Pixel Search Options area, drag the **Threshold** slider to select the amount of motion required to return a search result.

   The higher the threshold, the greater number of pixels must change before a result is returned.
7. Enter a number in the **Join results less than** field to define the minimum number of seconds between motion events before they are considered separate search results.
8. Click **Start Search**.

Viewing Pixel Search Results

1. In the Search Results area, select a search result. The event timeline is highlighted and the related video is displayed in the search image panel.
2. Use the Timeline controls to review the event. See Playing Back Recorded Video for more information.
3. Click **Export this event** to export the selected event video. See Exporting Recorded Video and Images for more information about the available export settings.
4. To export all listed results, click **Export results to a file** and save the file.

Performing a Thumbnail Search

The Thumbnail Search allows you to search through a specific period of time by viewing a series of thumbnail images.

1. Click 

to open the Search tab.
2. In the Search tab, select **Thumbnail Search**.

   The Search:Thumbnails tab displays.

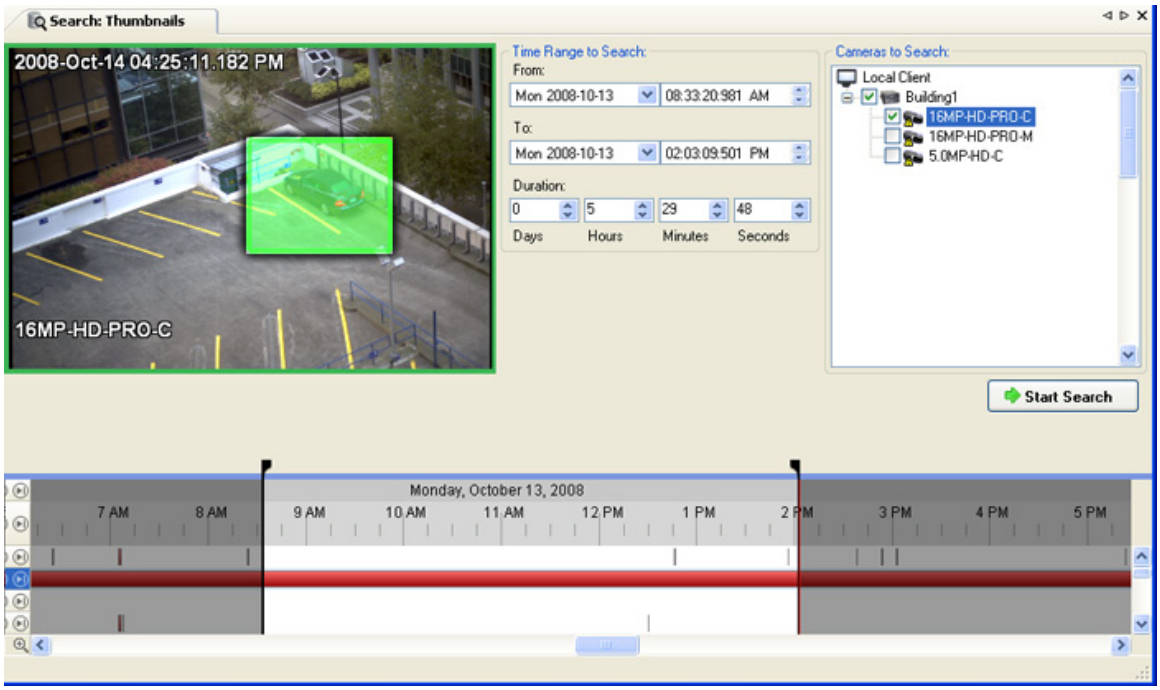


Figure A. Search:Thumbnails tab

3. In the Camera to Search area, select a camera.
4. In the Time Range to Search area, set the date and time range of your search. The time range is highlighted on the Timeline by the black time range markers. You can also drag the time range markers to modify the time range.
5. In the image panel, define the search region by moving the edges of the green overlay. Use this feature if you only want to see thumbnails for a region of the video image instead of the whole field of view.

   The thumbnail search will only be performed on the area highlighted in green.
6. Click **Start Search**.

Viewing Thumbnail Search Results

The search results display thumbnails at equal intervals on the Timeline.

1. To change the size of the search result thumbnails, select **Large Thumbnails**, **Medium Thumbnails**, or **Small Thumbnails** from the drop-down menu above the search results and click **Search Again**.

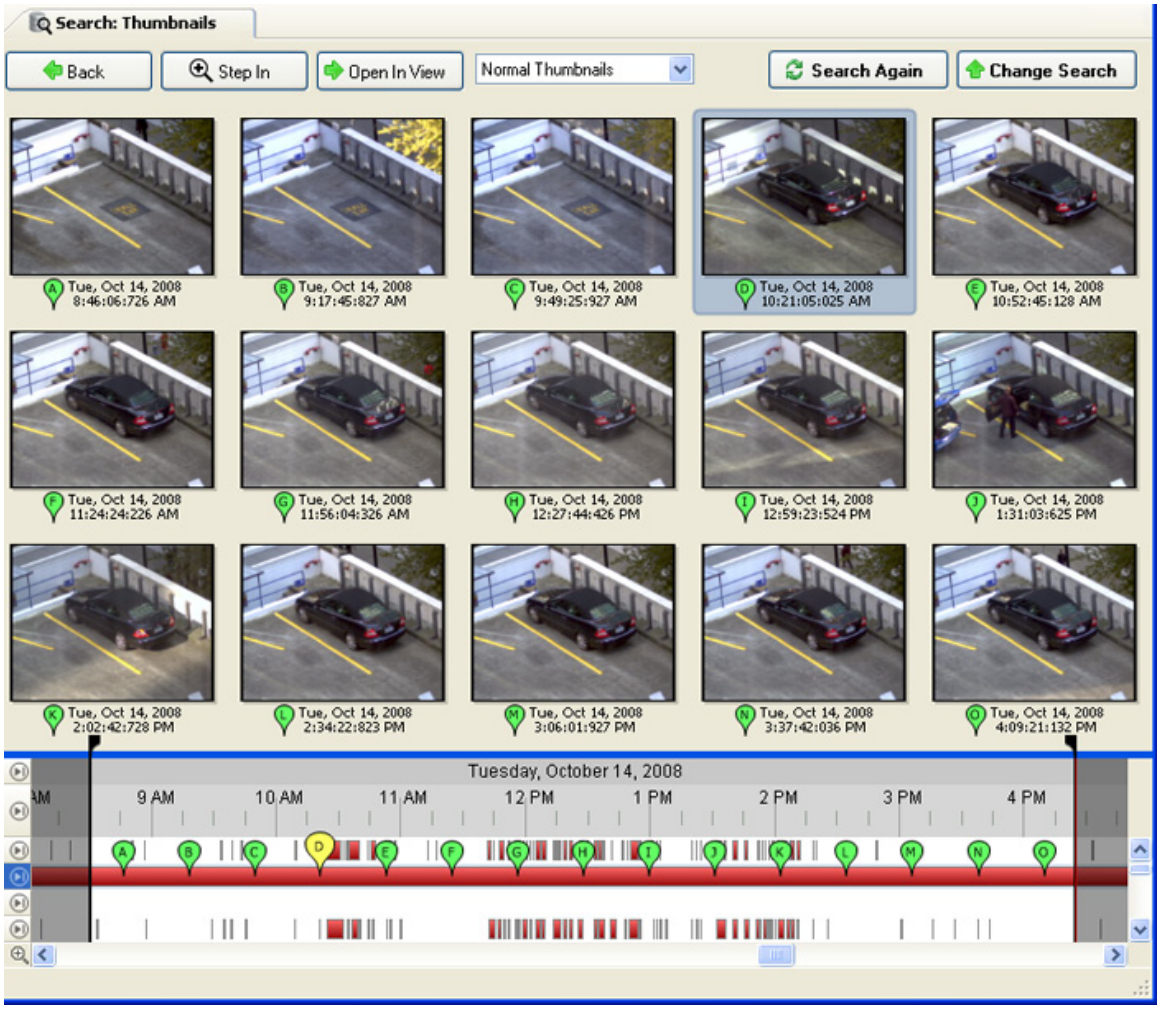


Figure B. Search:Thumbnail results tab

2. Select a thumbnail to highlight the image on the Timeline.
3. Click **Step In**, or double-click the thumbnail to perform another search around the thumbnail.

   Click **Back** to return to the previous results page.
4. Click **Open In View** to open the recorded video in a new View.

Performing an Alarm Search

Alarm search allows you to search for alarm events by time range for the selected alarms.

1. Click 

to open the Search tab.

2. In the Search tab, select **Alarm Search**.

   The Search:Alarms tab is displayed.

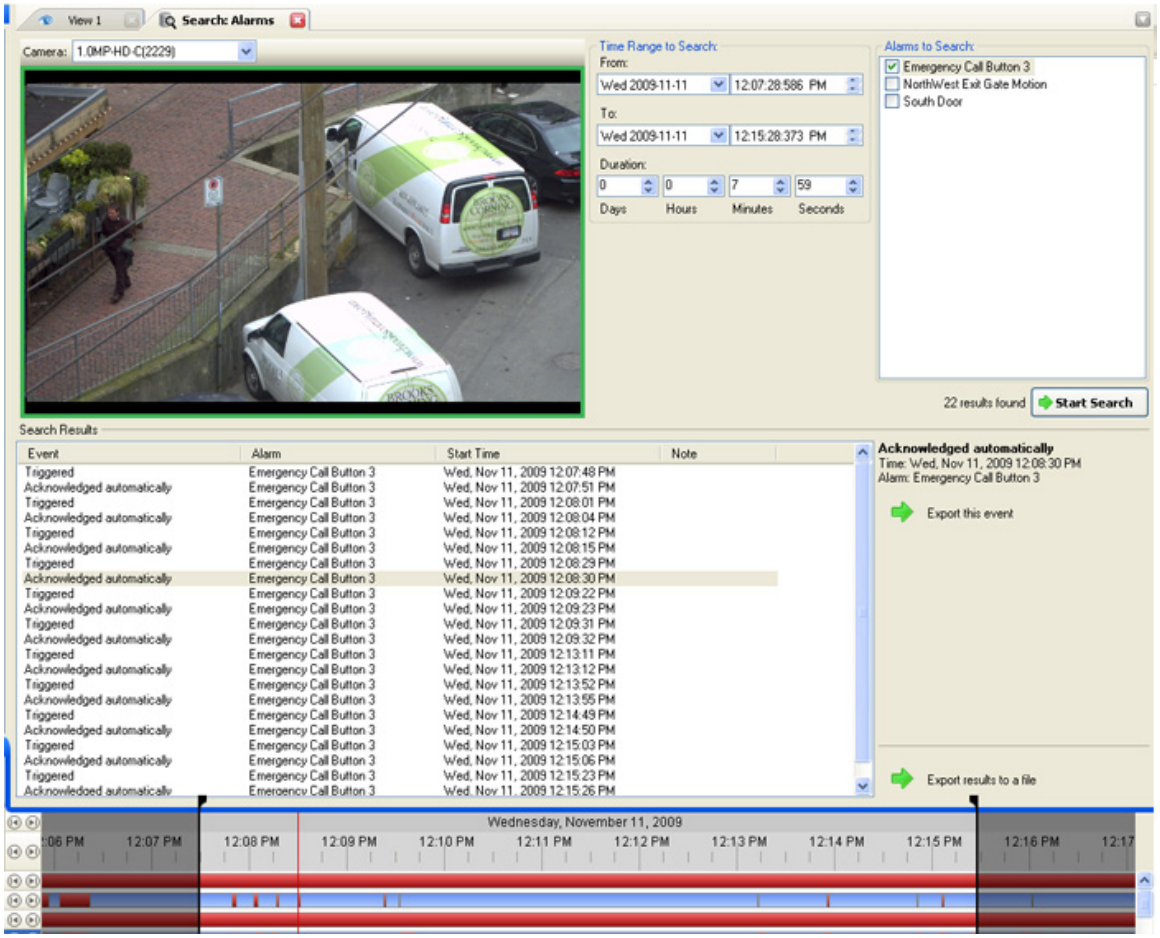


Figure A. Search:Alarms tab

3. In the Alarm to Search list, select all the alarms you would like to include in the alarm search.
4. In the Time Range to Search area, set the date and time range of your search. The time range is highlighted on the Timeline by the black time range markers. You can also drag the time range markers to modify the time range.
5. Click **Start Search**.

Viewing Alarm Search Results

1. In the Search Results area, select a search result. The event timeline is highlighted and the related video is displayed in the search image panel.
2. Use the Timeline controls to review the event. See Playing Back Recorded Video for more information.

3. If the event is linked to multiple cameras, select a camera from the **Camera** drop down list to change the video displayed in the image panel.

4. Click **Export this event** to export the selected event video. See Exporting Recorded Video and Images for more information about the available export settings.

5. To export all listed results, click **Export results to a file** and save the file.

Performing a POS Transaction Search

The POS Transaction Search allows you to search for POS transactions by transaction data source, content in the raw transaction data, and time range.

1. Click 

to open the Search tab.

2. In the Search tab, select **POS Transactions Search**.

   The Search: POS Transactions tab is displayed.

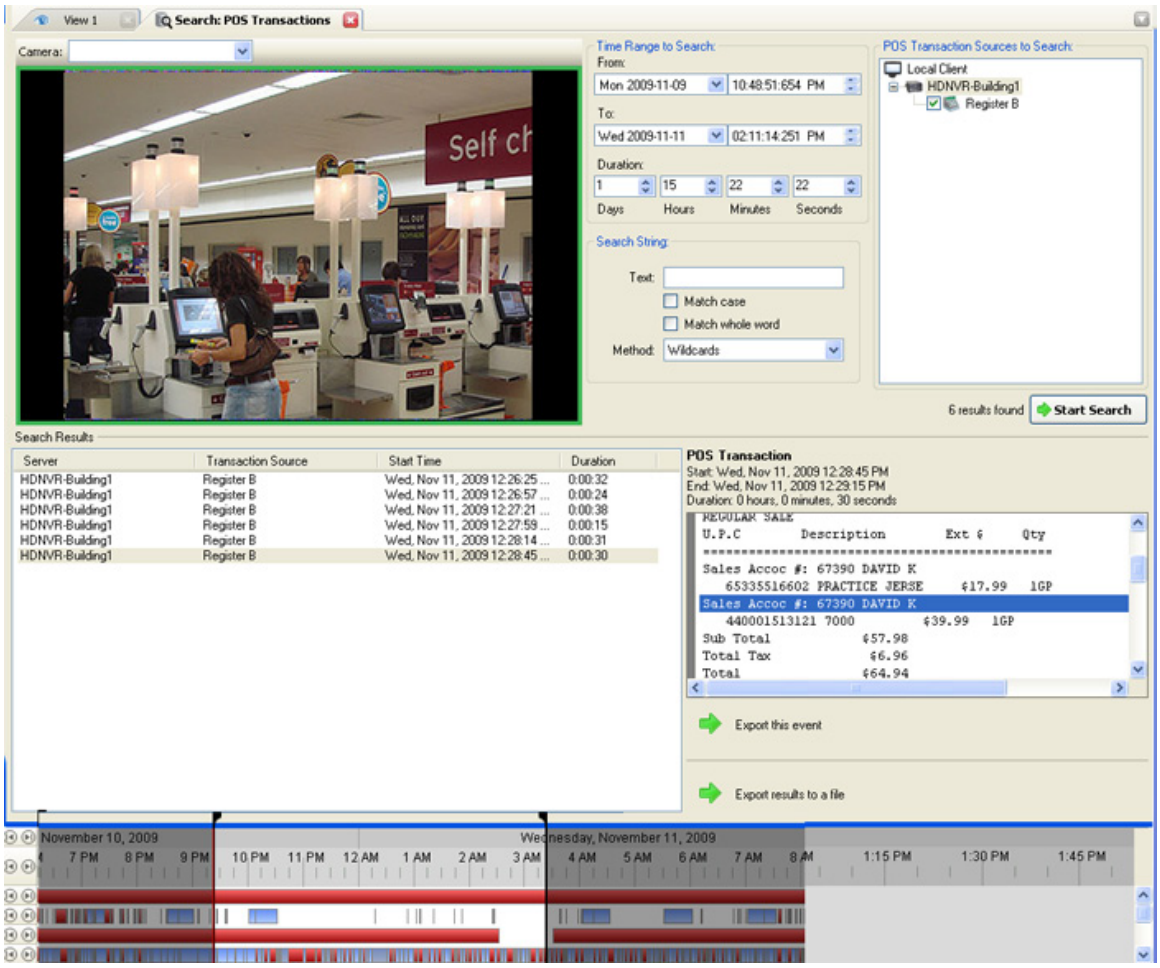


Figure A. Search:POS Transactions tab

3. In the POS Transaction Sources to Search area, select all the POS transaction sources you would like to include in the search.
4. In the Time Range to Search area, set the date and time range of your search. The time range is highlighted on the Timeline by the black time range markers. You can also drag the time range markers to modify the time range.
5. In the Search Text area, enter any text you want to search for, then select **Match case** and/or **Match whole word**, and choose a search method.

   Leave the **Text** field blank to find all transactions.
6. Click **Start Search**.

Viewing POS Transaction Search Results

1. In the Search Results area, select a search result. The event timeline is highlighted and the related video is displayed in the search image panel.
2. Use the Timeline controls to review the event. See Playing Back Recorded Video for more information.
3. If the event is linked to multiple cameras, select a camera from the **Camera** drop down list to change the video displayed in the image panel.
4. Click **Export this event** to export the selected event video. See Exporting Recorded Video and Images for more information about the available export settings.
5. To export all listed results, click **Export results to a file** and save the file.

Performing a License Plate Search

The License Plate Search allows you to search for specific license plates detected by the selected cameras. You can search for license plates not listed in the Watch List.

Note: The License Plate Search is only available if the License Plate Recognition feature is installed.

1. Click 

to open the Search tab.
2. In the Search tab, select **License Plate Search**.

   The Search: License Plates tab is displayed.

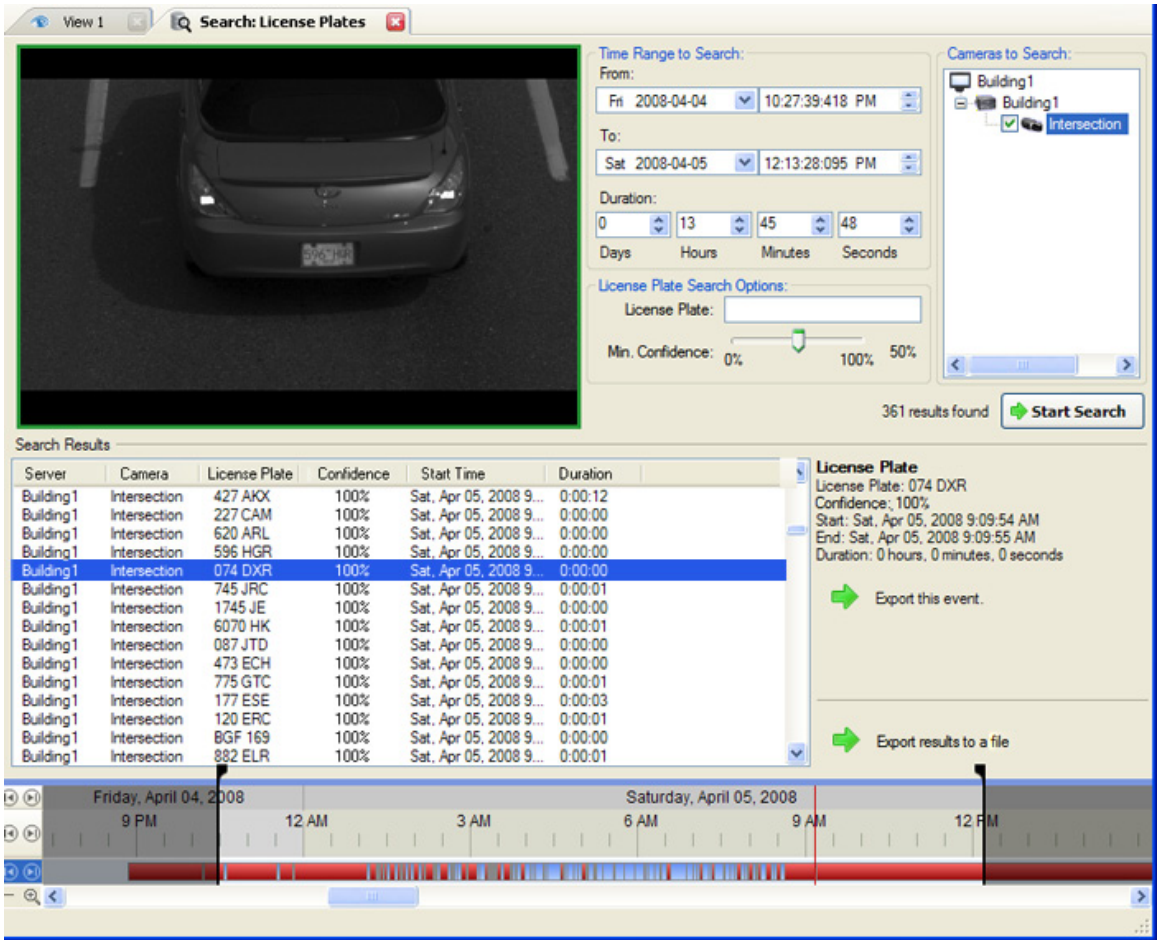


Figure A. Search: License Plates tab

3. In the Camera to Search area, select all the cameras you want to include in the search.
4. In the Time Range to Search area, set the date and time range of your search. The time range is highlighted on the Timeline by the black time range markers. You can also drag the time range markers to modify the time range.
5. In the License Plate Search Options area, enter the license plate number and minimum confidence for a match.
6. Click **Start Search**.

Viewing LPR Search Results

1. In the Search Results area, select a search result. The event timeline is highlighted and the related video is displayed in the search image panel.
2. Use the Timeline controls to review the event. See Playing Back Recorded Video for more information.

3. If the event is linked to multiple cameras, select a camera from the **Camera** drop down list to change the video displayed in the image panel.
4. Click **Export this event** to export the selected event video. See Exporting Recorded Video and Images for more information about the available export settings.
5. To export all listed results, click **Export results to a file** and save the file.

Export

You can export video and still images. You can specify a number of options to ensure the exported files are appropriate for your needs.

To watch a video overview of the Export features, see *Module 2 - Identifying, Bookmarking, Searching and Exporting Video* in the Avigilon University - End User Stream.

Note: Some features are not displayed if the server does not have the required license, or if you do not have the user permissions to access the feature.

Saving a Snapshot of an Image

A Snapshot allows you to export a single frame in a video. You can specify the file format and various options, like overlays and resolution.

1. Open the snapshot Export tab:

   - In the image panel, click the  **Save Snapshot** icon.
   - Right-click the image panel and select **Save Snapshot**.

   The snapshot Export tab is displayed.

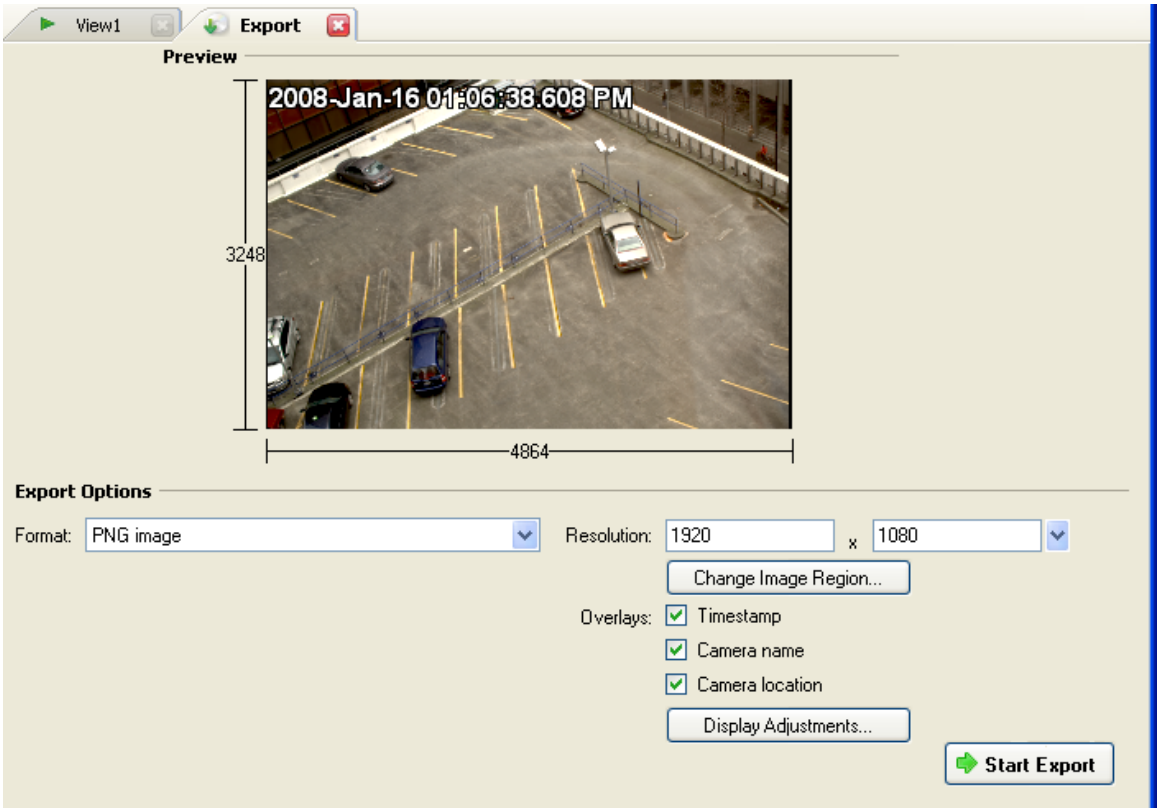


Figure A. Export tab for Snapshot export

2. In the Export Options area, select the image export format from the **Format** drop down list: **PNG**, **JPEG**, **TIFF**, **PDF**, **Print**, or **Native** format.

3. For the selected export image format, define your preferences:

Format	Image options
Native **Note:** The Native format requires the Avigilon Control Center Player to view.	This is the recommended export format because the exported image maintains original compression and can be authenticated against tampering in the Avigilon Control Center Player. ▪ Select the **Export the Control Center Player Installer** check box if you want a copy of the Avigilon Control Center Player to be distributed with your native image file.
PNG	1. In the **Resolution** field, select a resolution for the video image. You can manually enter the resolution or click the drop down arrow to select a standard resolution. **Note:** The **Resolution** field automatically maintains the image aspect ratio. 2. Click **Change Image Region...** to change the region of the video image that is exported.

	In the Change Image Region dialog box, modify the size and position of the green overlay, then click **OK**. The Preview image panel will show the modified image region. 3. Select the required image overlays: **Timestamp**, **Camera name**, and **Camera location**. 4. Click **Display Adjustments** to adjust the Gamma, Black Level and/or White Level.
JPEG	1. In the **Compression** field, select a compression level. 2. Set the image **Resolution**. 3. Click **Change Image Region** to only export a specific region of the image. 4. Select the required image overlays. 5. Click **Display Adjustments** to modify the image quality.
TIFF	1. Set the image **Resolution**. 2. Click **Change Image Region** to only export a specific region of the image. 3. Select the required image overlays. 4. Click **Display Adjustments** to modify the image quality.
Print	1. Click **Change Image Region** to only export a specific region of the image. 2. Click **Printer Settings...** to change the selected printer and paper size. 3. Select the required image overlays. 4. Click **Add Export Notes...** to add notes about the exported image. The notes are printed below the exported image. 5. Click **Display Adjustments** to modify the image quality.
PDF	1. Click **Change Image Region** to only export a specific region of the image. 2. Select the required image overlays.

	3. Click **Add Export Notes...** to add notes about the exported image. 4. Click **Display Adjustments** to modify the image quality.

4. Click **Start Export**.
5. In the Save As dialog box, name the export file and click **Save**.

   The Preview area displays the video stream you are exporting.
6. When the export is complete, click **OK**.

Exporting Live Images

The Live Export tab exports live video as a series of still images. You can specify the file format, and set related options like overlays and resolution.

1. Select **File > Live Export...**.

   The Live Export tab is displayed.

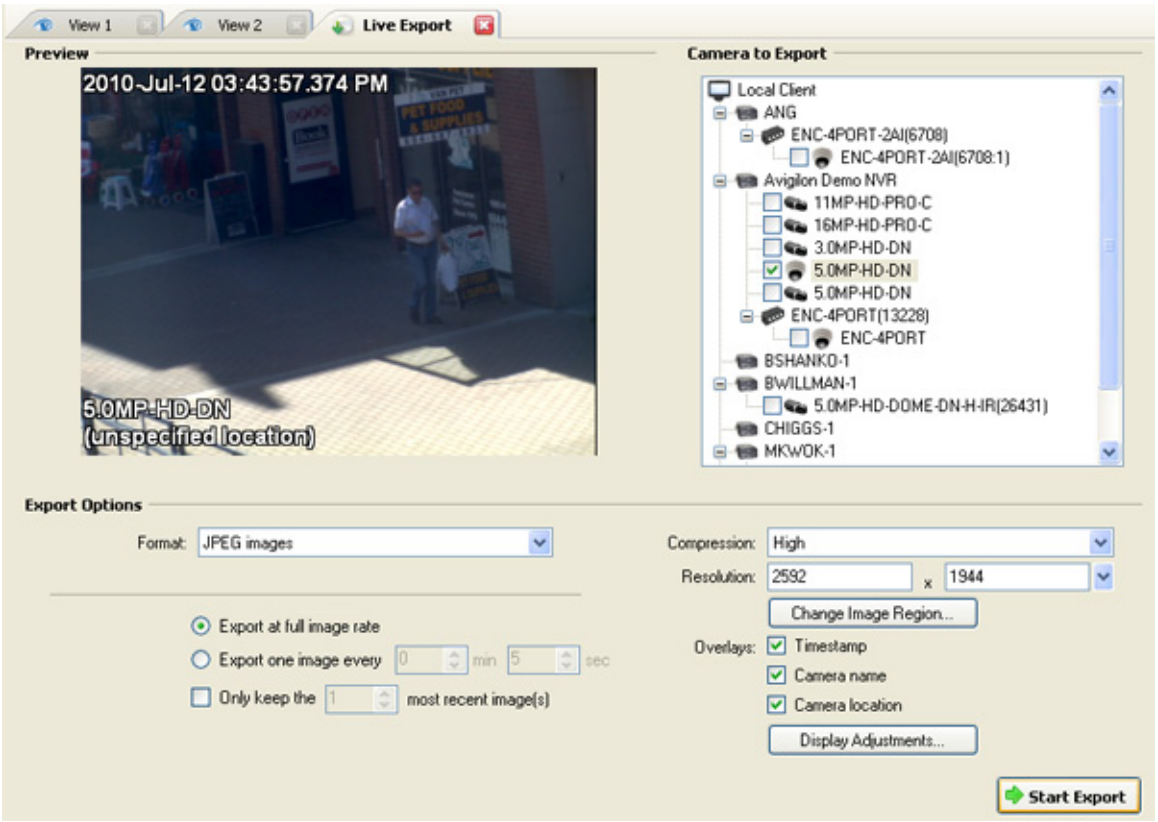


Figure A. Live Export tab

2. In the Camera to Export list, select the camera video you want to export.
3. In the Export Options area, select one of the following export formats in the **Formats** drop down list: **PNG**, **JPEG**, or **TIFF**.
4. Set the export image rate:

Option	Description
Export at full image rate	Select this option to export the live stream at the full image rate.
Export one image every __ min __sec	Select this option to control the time interval between each exported image. For example, if you enter *5* min. *0* sec., only one image will be exported every 5 minutes.
Only keep the __ most recent image(s)	Select this check box to limit the number of images stored. Be aware that if you do not limit the number of images stored, the export will continue until your hard drive is full.

5. (JPEG images only)

   In the **Compression** field, select a compression level.
6. In the **Resolution** field, select a resolution for the video image. You can manually enter the resolution or click the drop down arrow to select a standard resolution.

   Note: The **Resolution** field automatically maintains the image aspect ratio.
7. Click **Change Image Region...** to change the region of the video image that is exported.

   In the Change Image Region dialog box, modify the size and position of the green overlay, then click **OK**. The Preview image panel will show the modified image region.
8. Select the required image overlays: **Timestamp**, **Camera name**, and **Camera location**.
9. Click **Display Adjustments** to adjust the Gamma, Black Level and/or White Level.
10. Click **Start Export**.
11. In the Save As dialog box, name the export file and click **Save**.

    The Preview area displays the video stream you are exporting.

    Note: The live export will continue until stopped.
12. Click **Stop Export** to stop the export.

Exporting Recorded Video and Images

You can export recorded video and still images that are stored on the server.

Note: Only recorded video can be exported in video format.

Accessing the Export Tab

The Export tab can be accessed in any of the following ways:

- Select **File > Export**.
- On the toolbar, click 

.
- When searching for a specific video image, select a search result and click **Export this event**.
- When viewing bookmarked video, right-click a bookmark on the Timeline and select **Export**.

Exporting Native Video

When you export video files, you can choose to export the video in the Native (AVE) format.

The AVE format is the recommended format for exporting video because you can export video from multiple cameras in a single file, and the video maintains its original compression. AVE video can be played in the Avigilon Control Center Player, where the video can be authenticated against tampering and be re-exported to other formats.

1. Click 

to open the Export tab. For more information, see Accessing the Export Tab.

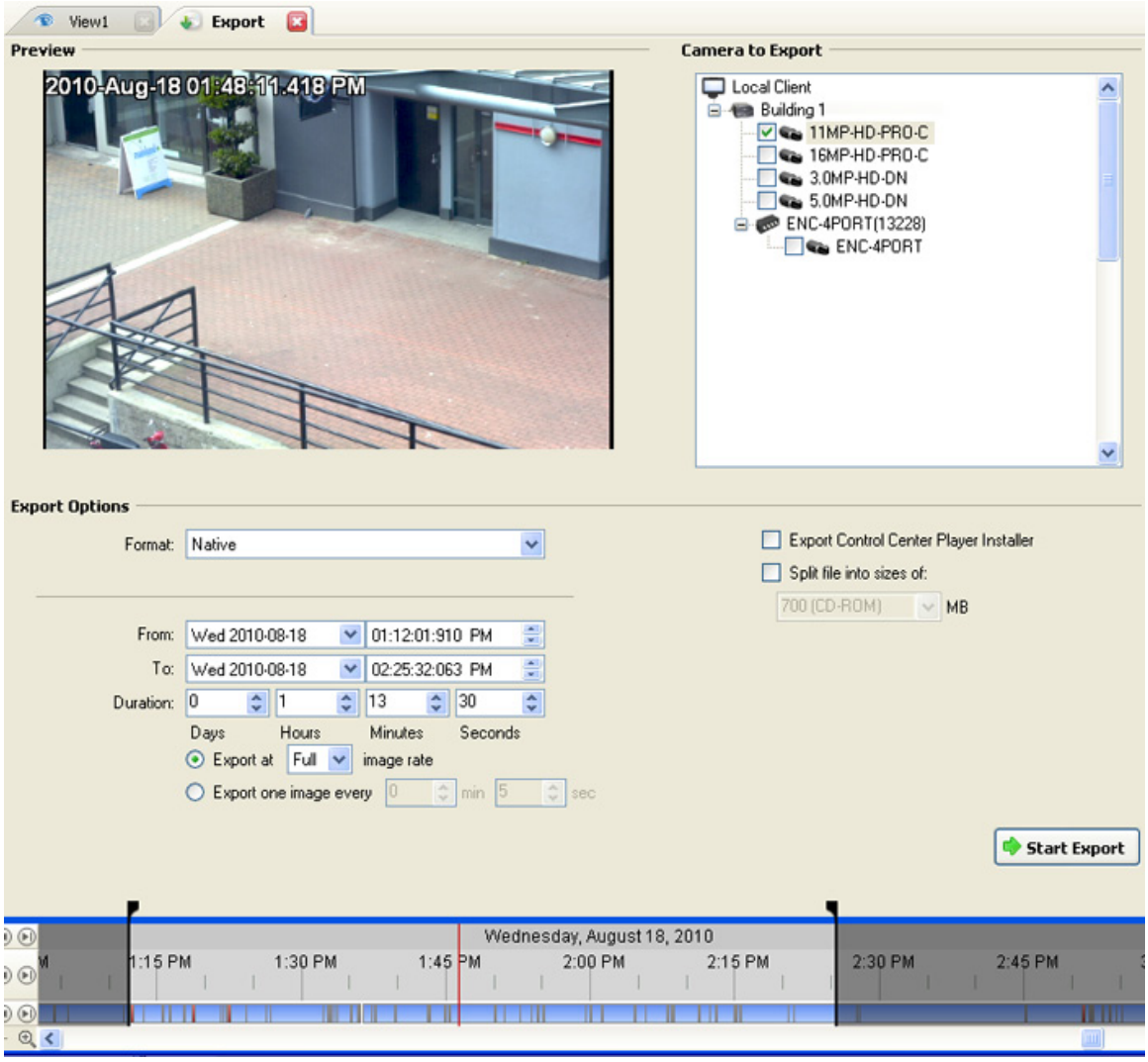


Figure A. Export tab for recorded video export

2. In the **Format** drop down list, select **Native**.
3. In the Camera to Export list, select all the camera video you want to export.
4. Enter the time range in the **From**, **To**, **Duration** fields. The time range is highlighted on the Timeline by black time range markers. You can also drag the time range markers to modify the time range.
5. Set the export image rate:

Option	Description
Export at __ image rate	Select this option to control how many images per second are exported. For example, the video is streaming at 30 images per second. If you select **1/2**, only 15 images for that second will be exported.

Export one image every __ min __sec	Select this option to control the time interval between each exported video image. For example, if you enter *5* min. *0* sec., only one image will be exported every 5 minutes.

6. Select the **Export the Control Center Player Installer** if you want a copy of the Avigilon Control Center Player to distribute with the AVE video file.
7. Select the **Split file into sizes of:** check box to split the exported file into smaller files so the exported files can be stored on optical media, like a CD or DVD.
8. Click **Start Export**.
9. In the Save As dialog box, name the export file and click **Save**.

   The Preview area displays the video stream you are exporting.
10. When the export is complete, click **OK**.

Exporting AVI Video

When you export video files, you can choose to export the video in Audio Video Interleave (AVI) format.

1. Click 

to open the Export tab. For more information, see Accessing the Export Tab.

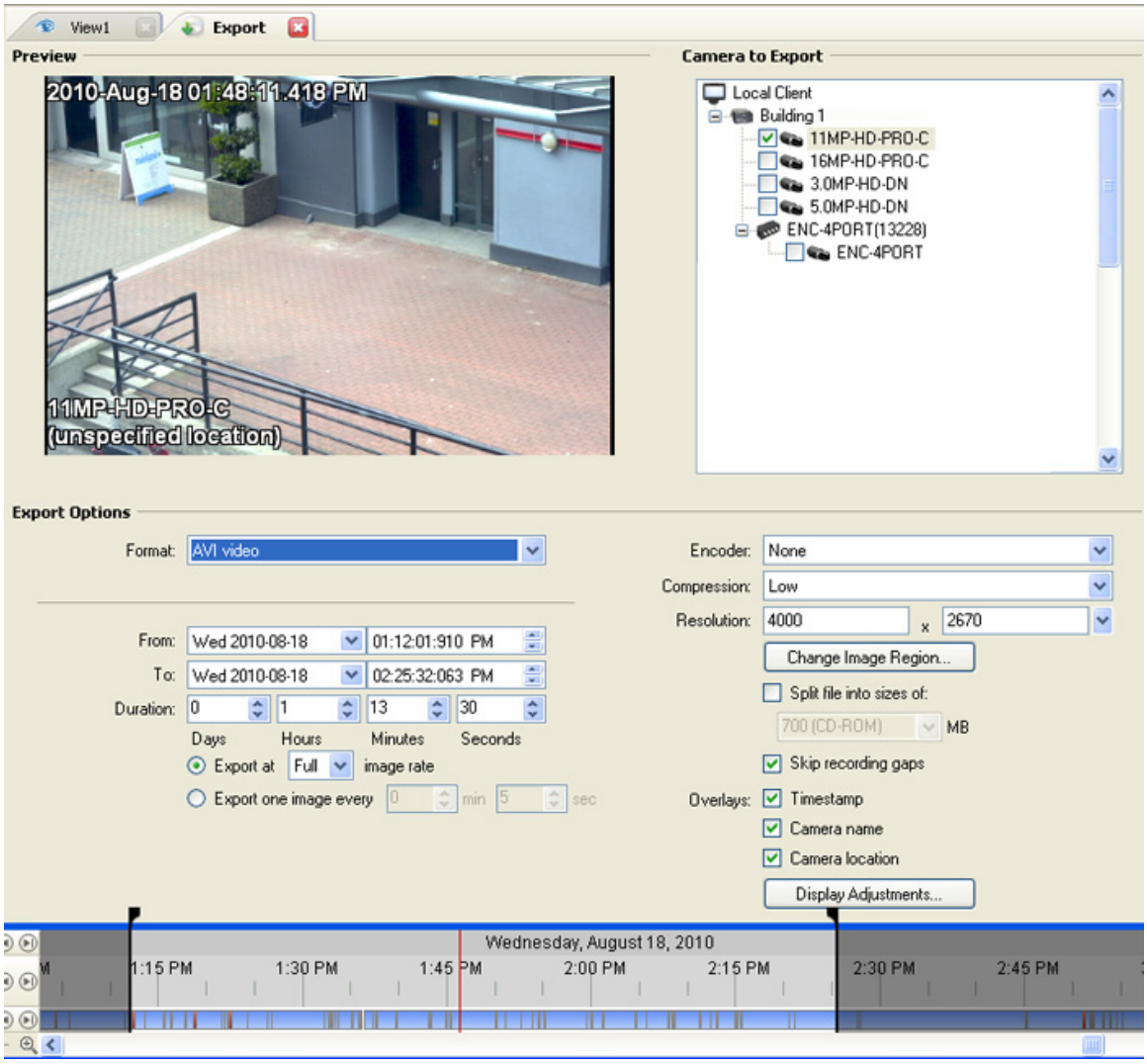


Figure A. Export tab for recorded video export

2. In the **Format** drop down list, select **AVI video**.
3. In the Camera to Export list, select all the camera video you want to export.
4. Enter the time range in the **From**, **To**, **Duration** fields. The time range is highlighted on the Timeline by black time range markers. You can also drag the time range markers to modify the time range.
5. Set the export image rate:

Option	Description
Export at __ image rate	Select this option to control how many images per second are exported. For example, the video is streaming at 30 images per second. If you select **1/2**, only 15 images for that second will be exported.

Export one image every __ min __sec	Select this option to control the time interval between each exported video image. For example, if you enter *5* min. *0* sec., only one image will be exported every 5 minutes.

6. In the **Encoder** field, select the compression used. The **VC-1 (Windows Media Video)** compression is included by default because it is tailored for high-resolution AVI encoding.
7. In the **Compression** field, select a compression level.
8. In the **Resolution** field, select a resolution for the video image. You can manually enter the resolution or click the drop down arrow to select a standard resolution.

   Note: The **Resolution** field automatically maintains the image aspect ratio.

   For high resolution video (11MP or 16MP) the greatest resolution option will be less than the camera's actual resolution because most media players cannot play high resolution AVI files.
9. Select the **Split file into sizes of:** check box to split the exported file into smaller files so the exported files can be stored on optical media, like a CD or DVD.
10. Click **Change Image Region...** to change the region of the video image that is exported.

    In the Change Image Region dialog box, modify the size and position of the green overlay, then click **OK**. The Preview image panel will show the modified image region.
11. Select the **Skips recording gaps** check box to avoid pauses in the video caused by gaps in the recorded video file.
12. Select the required image overlays: **Timestamp**, **Camera name**, and **Camera location**.
13. Click **Display Adjustments** to adjust the Gamma, Black Level and/or White Level.
14. Click **Start Export**.
15. In the Save As dialog box, name the export file and click **Save**.

    The Preview area displays the video stream you are exporting.
16. When the export is complete, click **OK**.

Exporting PNG, JPEG or TIFF Images

When you export recorded video, you can choose to export the video as still images in PNG, JPEG, or TIFF format.

1. Click 

to open the Export tab. For more information, see Accessing the Export Tab.

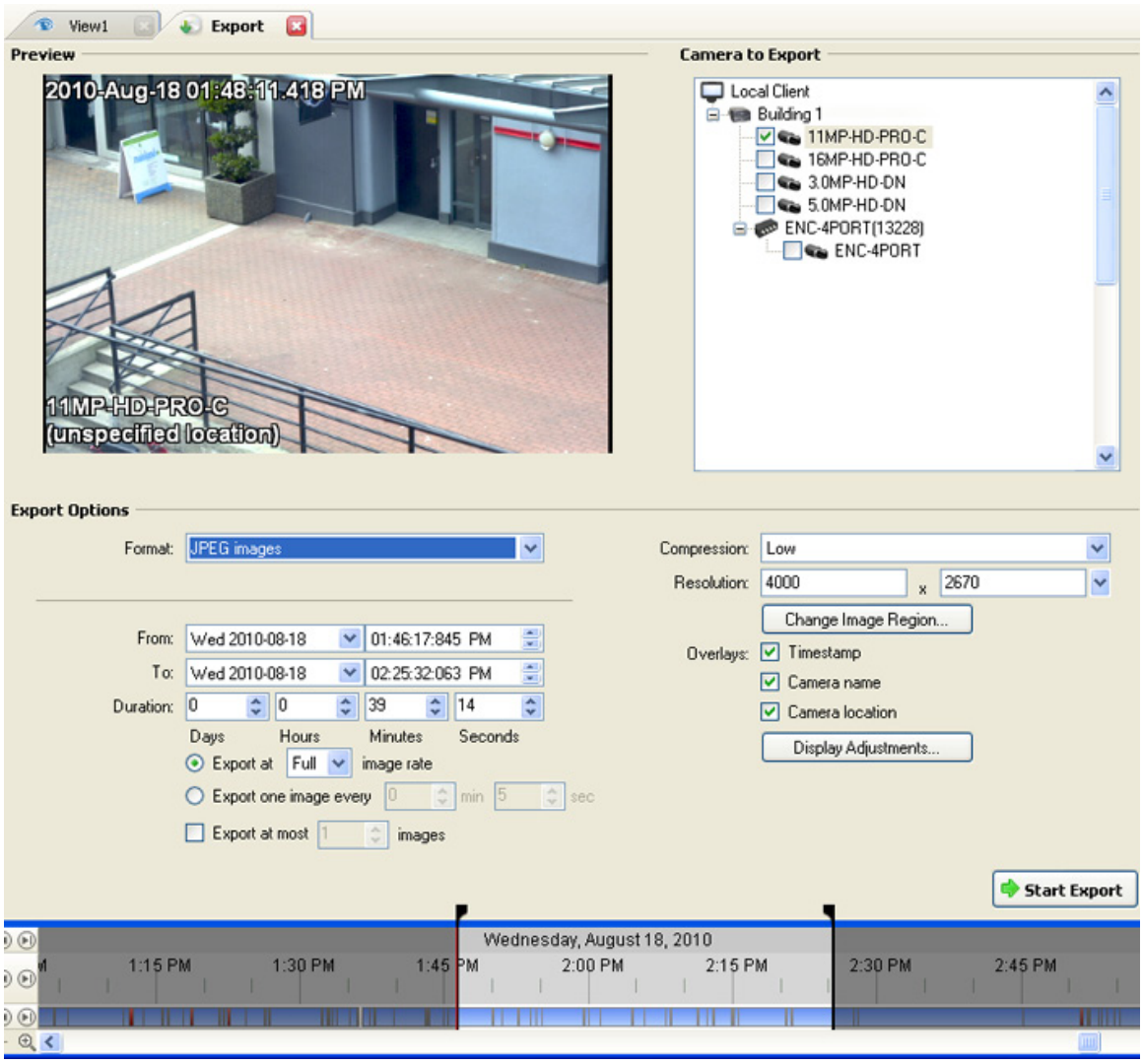


Figure A. Export tab for still image export

2. In the **Format** drop down list, select one of the following export formats: **PNG Images**, **JPEG Images**, or **TIFF Images**.
3. In the Camera to Export list, select all the camera video you want to export.
4. Enter the time range in the **From**, **To**, **Duration** fields. The time range is highlighted on the Timeline by black time range markers. You can also drag the time range markers to modify the time range.
5. Set the export image rate:

Option	Description
Export at __ image rate	Select this option to control how many images per second are exported. For example, the video is streaming at 30 images per second. If you select **1/2**, only 15

	images for that second will be exported.
Export one image every __ min __sec	Select this option to control the time interval between each exported video image. For example, if you enter *5* min. *0* sec., only one image will be exported every 5 minutes.

6. Select the **Export at most __ images** check box to limit the number of images that is exported. Enter the number of images you want exported.

   If this option is selected, the export will stop either when the number of specified images has been exported or when the specified time range has been reached.

7. (JPEG only)

   In the **Compression** field, select a compression level.

8. In the **Resolution** field, select a resolution for the video image. You can manually enter the resolution or click the drop down arrow to select a standard resolution.

   Note: The **Resolution** field automatically maintains the image aspect ratio.

9. Click **Change Image Region...** to change the region of the video image that is exported.

   In the Change Image Region dialog box, modify the size and position of the green overlay, then click **OK**. The Preview image panel will show the modified image region.

10. Select the required image overlays: **Timestamp**, **Camera name**, and **Camera location**.

11. Click **Display Adjustments** to adjust the Gamma, Black Level and/or White Level.

12. Click **Start Export**.

13. In the Save As dialog box, name the export file and click **Save**.

    The Preview area displays the video stream you are exporting.

14. When the export is complete, click **OK**.

Exporting PDF and Print Images

When you export recorded video, you can choose to export the video as still images for printing or in PDF format.

1. Click 

to open the Export tab. For more information, see Accessing the Export Tab.

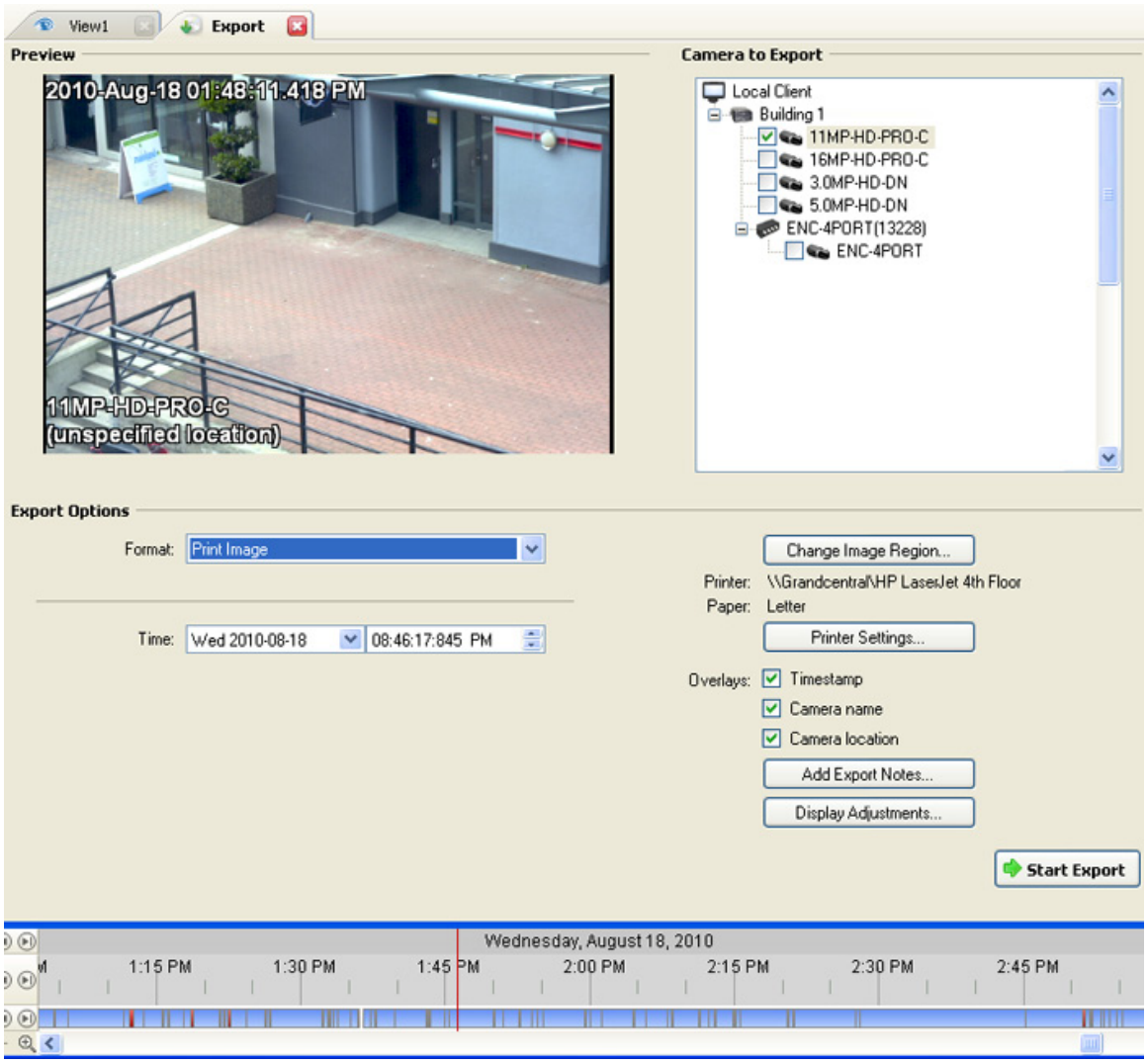


Figure A. Export tab for still image export

2. In the **Format** drop down list, select one of the following export formats: **Print Image** or **PDF File**.
3. In the Camera to Export list, select all the camera video you want to export.
4. In the **Time** field, enter the exact date and time of the video image you want to export.
5. Click **Change Image Region...** to change the region of the video image that is exported.

   In the Change Image Region dialog box, modify the size and position of the green overlay, then click **OK**. The Preview image panel will show the modified image region.
6. (Print Image only) Click **Print Settings** to change the printer and paper size that the image is printed on.
7. Select the required image overlays: **Timestamp**, **Camera name**, and **Camera location**.
8. Click **Add Export Notes** to add notes about the exported image. The notes are added below the image.

9. Click **Display Adjustments** to adjust the Gamma, Black Level and/or White Level.
10. Click **Start Export**.
11. In the Save As dialog box, name the export file and click **Save**.

    The Preview area displays the video stream you are exporting.
12. When the export is complete, click **OK**.

Exporting WAV Audio

If a video contains audio, the audio is exported with the video. If required, you can choose to only export the audio file.

Note: Audio recording requires an Audio Channel License. Without an audio license, no audio would have been recorded with the video.

1. Click 

to open the Export tab. For more information, see Accessing the Export Tab.

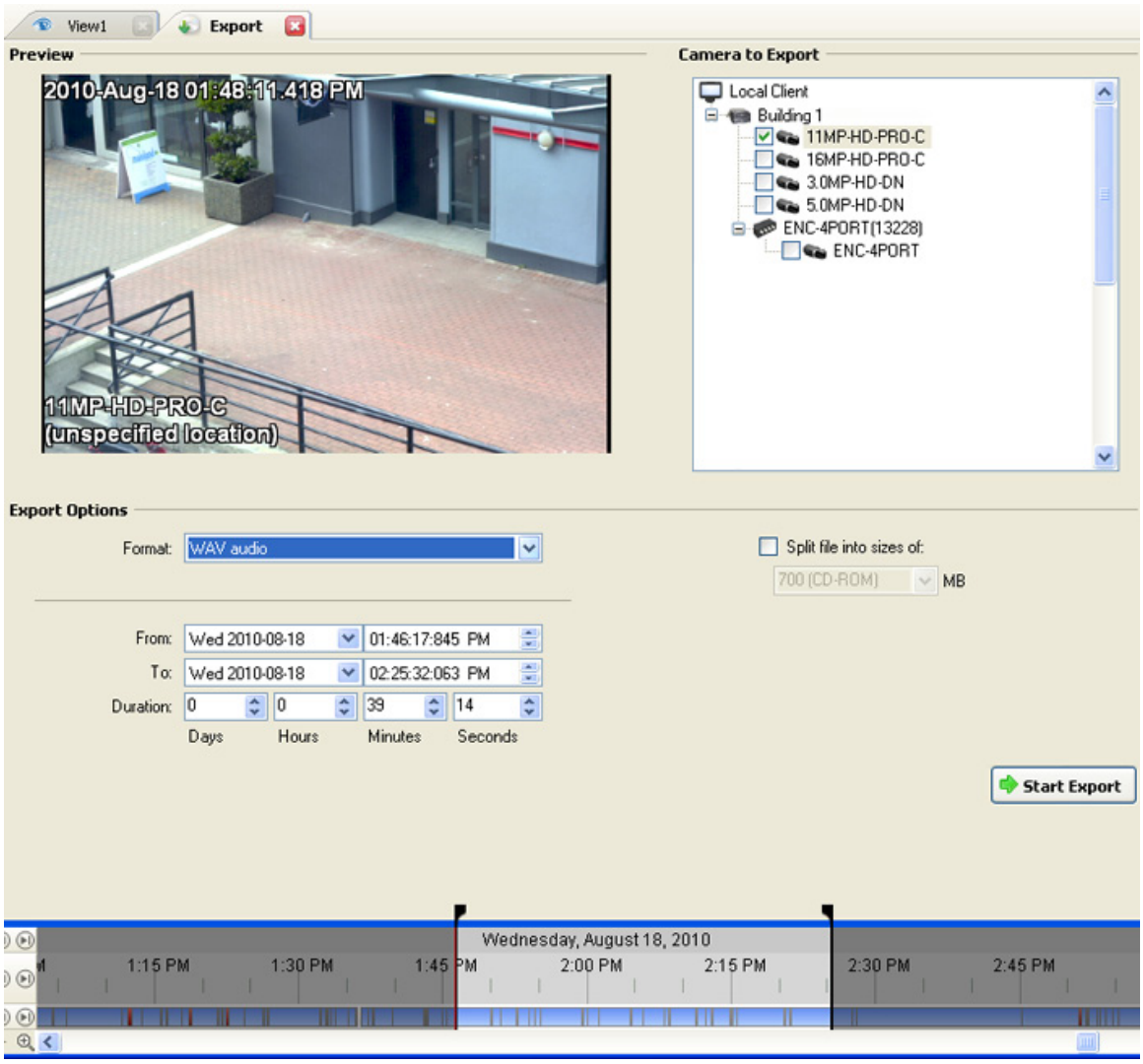


Figure A. Export tab for audio export

2. In the **Format** drop down list, select **WAV**.
3. In the Camera to Export list, select all the camera video you want to export.
4. Enter the time range in the **From**, **To**, **Duration** fields. The time range is highlighted on the Timeline by black time range markers. You can also drag the time range markers to modify the time range.
5. Click **Start Export**.
6. In the Save As dialog box, name the export file and click **Save**.

   The Preview area displays the video linked with the audio you are exporting.
7. When the export is complete, click **OK**.

Backup

Video can be automatically backed up on a schedule that is defined in the server Scheduled Backup settings. However, you can manually backup video as needed from the Backup tab.

For information on configuring the Scheduled Backup settings, see Changing Scheduled Backup Settings.

Note: Some features are not displayed if the server does not have the required license, or if you do not have the user permissions to access the feature.

Backing Up Recorded Video On Demand

The backup files are stored in a backup folder set by the Avigilon Control Center Admin Tool. See the *Avigilon Control Center Server User Guide* for information about changing the backup folder.

1. Select **File > Backup...**

   The Backup tab is displayed.

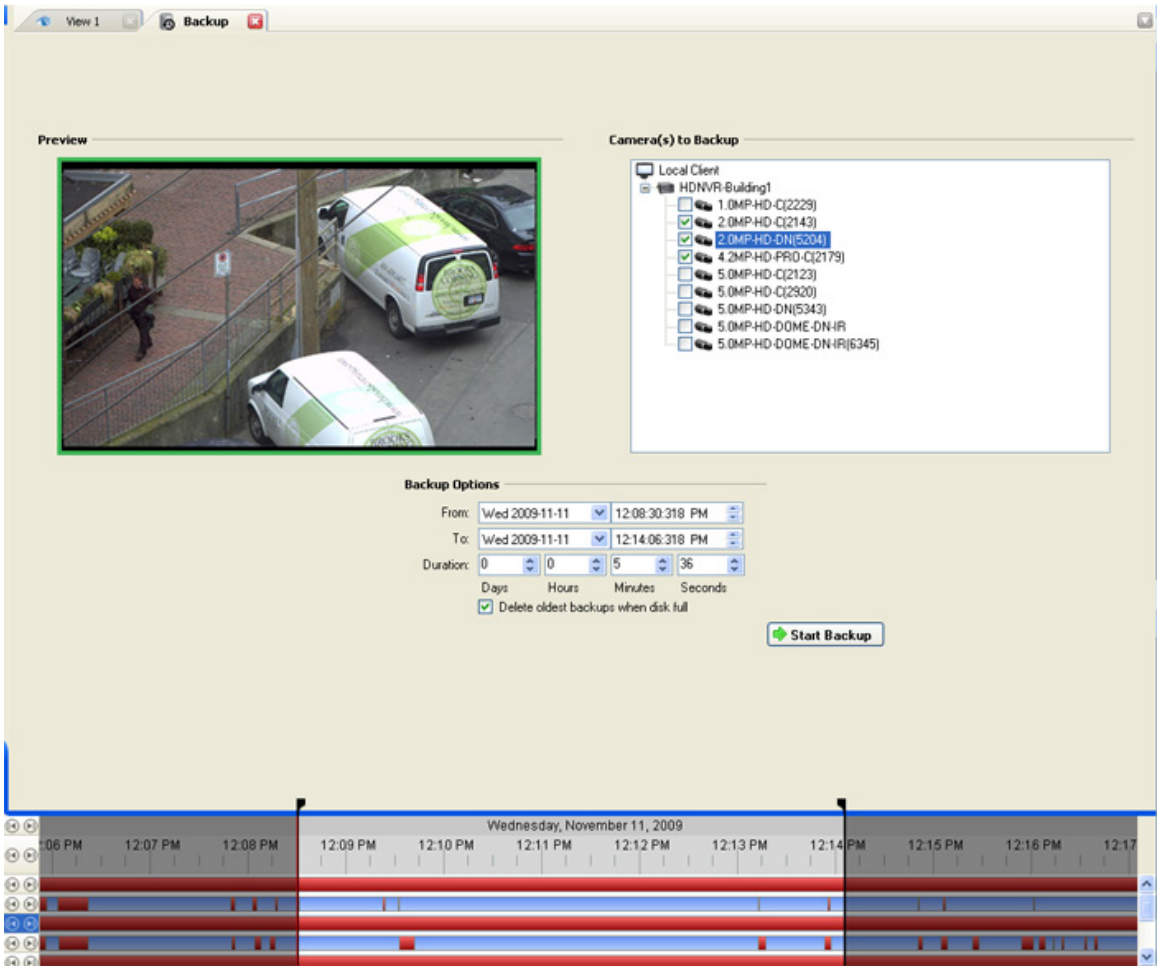


Figure A. Backup tab

2. In the Camera(s) to Backup area, select all the cameras you want to backup
3. In the Backup Options area, set the time range you want to backup. The time range is highlighted on the Timeline by the black time range markers. You can also drag the time range markers to modify the time range.
4. Ensure the **Delete oldest backups when disk full** check box is selected.
5. Click **Start Backup**.

   Video is always backed up in the Avigilon Backup (AVK) format. You can review the backed up video in the Avigilon Control Center Player.

Appendix

Accessing the Web Client

You can access your Avigilon High Definition Surveillance System through the Web Client. The Web Client is a simplified version of the Client software. It allows you to monitor your surveillance system, search for video events and export recorded video outside the Client software. Be aware that you cannot modify any system settings through the Web Client.

You can access the Web Client through the Internet Explorer web browser.

Note: The Web Client is only compatible with Internet Explorer.

To access the Web Client, you need the Avigilon server's IP address and port number. This information is available in the Avigilon Control Center Admin Tool installed on the server. See the *Avigilon Control Center Server User Guide* for more information.

1. To access the Web Client, open Internet Explorer and enter the following address: http://<*server ip address*>:<*port number*>/ (For example, http://192.168.2.62:50083/)

   If you have not accessed the Web Client before, you may be prompted to install the required software before the Web Client will open.

2. When the login screen appears, enter your username and password for the server.

The Web Client is opened in your browser, and you can access the video and cameras connected to the server.

Note: You can only access one server at a time through the Web Client.

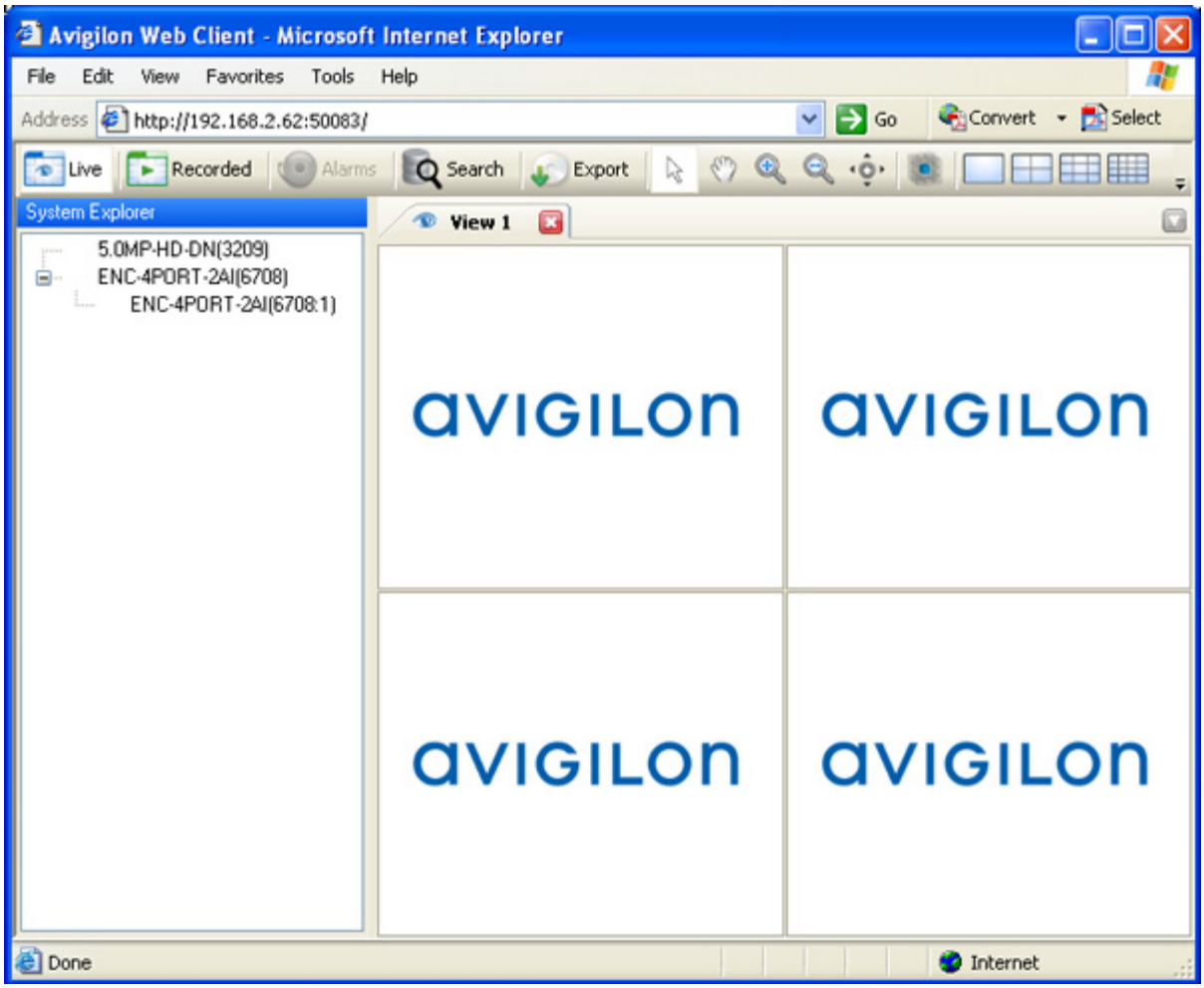


Figure A. Avigilon Control Center Web Client

Reporting Bugs

If an error occurs in the Avigilon Control Center System, you can contact Avigilon Support at support@avigilon.com or +1.888.281.5182.

To help diagnose your problem, the Avigilon Support team may ask you to provide a System Bug Report. The System Bug Report is a zip file generated by the Avigilon Control Center Client software that contains the system log and error reports for each of the servers you have access to.

1. Select **Help > System Bug Report...**.
2. When the Download System Bug Report dialog box appears, click **Download**.
3. In the Save As dialog box, name the file and click **Save**.
4. Once the System Bug Report has downloaded successfully, click **Close**.

Keyboard Commands

Use any of the keyboard commands below to help you navigate the Avigilon Control Center Client software.

The Key Combination column show the commands used on a standard keyboard, while the Keypad Combination column show the commands used on an Avigilon USB Professional Joystick Keyboard.

Image Panel & Camera Commands

Command	Key Combination	Keypad Combination (Image Panel buttons)
Select image panel Image panel # are displayed after pressing the first key.	* + <*image panel #*> + Enter	 + <*image panel #*> + ENTER
Select camera Cameras are selected using their *logical ID*.	/ + <*Logical ID*> + Enter	 + <*Logical ID*> + ENTER
Select the next panel	Tab	
Select the previous panel	Shift + Tab	
Clear panel selection	* + 0 + Enter	
Remove camera from selected panel	Backspace	
Expand/Collapse selected panel	Ctrl + E	
Add bookmark for selected camera **Note:** For recorded	Ctrl + B	

video only.		
Start/Stop manual recording for selected camera	Ctrl + R	
Start/Stop audio for selected camera	Ctrl + A	
Snapshot image of selected camera video	F4	
Enable digital output		
Acknowledge the alarm currently displayed in an armed image panel		

View Commands

Command	Key Combination	Keypad Combination (View buttons)
Select the next view	Ctrl + Tab	
Select the previous view	Ctrl + Shift + Tab	
Jump to view	Ctrl + 1 to 9	
Start/Stop cycle views	Ctrl + Y	
Create new view	Ctrl + T	
Close current view	Ctrl + W	

Create new window	Ctrl + N	
Switch current view to live view mode	Ctrl + L	
Switch current view to recorded view mode	Ctrl + P	
Remove all cameras from current view	Ctrl + Backspace	
Enable/Disable full screen mode for current view	F11	
Open saved View The saved View number is displayed in the System Explorer after pressing the first button.		OPEN 3 + <Saved View #> + ENTER

Playback Commands

Command	Key Combination	Keypad Combination (Timeline buttons)
Play/Pause	Spacebar	
Increase playback speed	Page Up	
Decrease playback speed	Page Down	
Step to next frame	Shift + →	

Step to previous frame	Shift + ←	
Go to next event	Alt + →	
Go to previous event	Alt + ←	
Go forward one second	Ctrl + →	
Go forward five seconds	Ctrl + Shift + →	
Go back one second	Ctrl + ←	
Go back five seconds	Ctrl + Shift + ←	
Zoom in on the Timeline	Ctrl + Alt + +	
Zoom out on the Timeline	Ctrl + Alt + -	
Scroll forward on the Timeline	Ctrl + Alt + →	
Scroll backward on the Timeline	Ctrl + Alt + ←	
Go to start of the Timeline	Ctrl + Alt + Home	
Go to end of the Timeline	Ctrl + Alt + End	

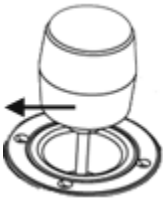
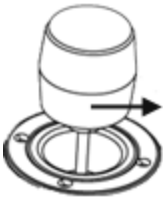
Center the Timeline on marker	Ctrl + C	

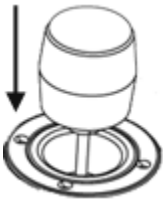
Layout Commands

Command	Key Combination	Keypad Combination (View buttons)
Change to 1 Division layout	Alt + 1	LAYOUT 4 + PREV 1
Change to 4 Division layout	Alt + 2	LAYOUT 4 + NEXT 2
Change to 9 Division layout	Alt + 3	LAYOUT 4 + OPEN 3
Change to 16 Division layout	Alt + 4	LAYOUT 4 + LAYOUT 4
Change to 25 Division layout	Alt + 5	LAYOUT 4 + 5
Change to 36 Division layout	Alt + 6	LAYOUT 4 + CLOSE 6
Change to 6 Division (1 + 5) layout	Alt + 7	LAYOUT 4 + 7
Change to 8 Division (1 + 7) layout	Alt + 8	LAYOUT 4 + 8
Change to 13 Division (1 + 12) layout	Alt + 9	LAYOUT 4 + 9
Change to 10 Division (2 + 8) layout	Alt + 0	LAYOUT 4 + 0
Change to next layout	Alt +]	

Change to previous layout	Alt + [	

PTZ Commands (Digital and Mechanical)

Command	Key Combination	Keypad Combination (PTZ buttons)
Toggle PTZ controls	Ctrl + D	
Zoom in	+	
Zoom out	-	
Pan left	←	
Pan right	→	

Tilt up	↑	
Tilt down	↓	
Increase PTZ speed	Shift + ↑	The further the joystick is from center, the faster the speed.
Decrease PTZ speed	Shift + ↓	The closer the joystick is to center, the slower the speed.
Open iris	Home	
Close iris	End	
Focus near	Insert	
Focus far	Delete	
PTZ menu left	←	
PTZ menu right	→	
PTZ menu up	↑	

PTZ menu down		
Activate preset		PRESET + <*Preset #*> + ENTER
Run pattern		PATTERN + <*Pattern #*> + ENTER
Start auxiliary		 + <*Aux #*> + ENTER
Stop auxiliary		 + <*Aux #*> + ENTER

Index

This Page Left Intentionally Blank

Avigilon™ Control Center Standard Web Client User Guide

Version 5.4.2

Avigilon Corporation
http://www.avigilon.com

Revised: 2014-12-09

PDF-WEBCLIENT5-S-E-Rev1

Table of Contents

What is the Avigilon Control Center Web Client?

The Avigilon Control Center Web Client is a simplified, web-based version of the Avigilon Control Center Client software. The Web Client allows you to access any camera that is connected to a Control Center Server.

Through the Web Client you can monitor live and recorded video, and search or export events in the camera's recording history.

The Web Client can be accessed from any Internet Explorer browser (version 6+) that is connected to your local network.

For More Information

Visit Avigilon at **http://www.avigilon.com/** for additional product documentation.

The Avigilon Training Center

The Avigilon Training Center provides free online training videos that demonstrate how to set up and use the Avigilon Surveillance System. Register online at the Avigilon Partner Portal site to begin: **http://avigilon.force.com/login**

Support

For additional support information, visit **http://avigilon.com/support-and-downloads/**. The Avigilon Partner Portal also provides self-directed support resources - register and login at **http://avigilon.force.com/login**.

Regular Avigilon Technical Support is available Monday to Friday from 12:00 a.m. to 6:00 p.m. Pacific Standard Time (PST):

- North America: +1.888.281.5182 option 1
- International: +800.4567.8988 or +1.604.629.5182 option 1

Emergency Technical Support is available 24/7:

- North America: +1.888.281.5182 option 1 then dial 9
- International: +800.4567.8988 or +1.604.629.5182 option 1 then dial 9

E-mails can be sent to: **support@avigilon.com**.

Upgrades

Software and firmware upgrades will be made available for download as they become available. Check **http://avigilon.com/support-and-downloads/** for available upgrades.

Feedback

We value your feedback. Please send any comments on our products and services to **feedback@avigilon.com**

Accessing the Control Center Web Client

NOTE: You cannot modify any system settings through the Control Center Web Client.

To access the Web Client, you need the IP address and port number of the server in your Site. The IP address is listed in the server's Setup tab in the Avigilon Control Center Client. The port number can be found in the Admin Tool under **Settings** > **Network**.

For more information, see the *Avigilon Control Center Client User Guide*.

1. To access the Web Client, open Internet Explorer (version 6+) and enter the address of your Web Client in the following format:

   http://*<server ip address>*:*<port number>*/

   (For example, http://192.168.2.62:38880/)

   If you have not accessed the Web Client before, you may be prompted to install the required plug-in software before the Web Client will open.

2. When the login screen appears, enter your username and password for the Site.

The Web Client will open in your browser, and you can access the video and cameras that are connected to the server.

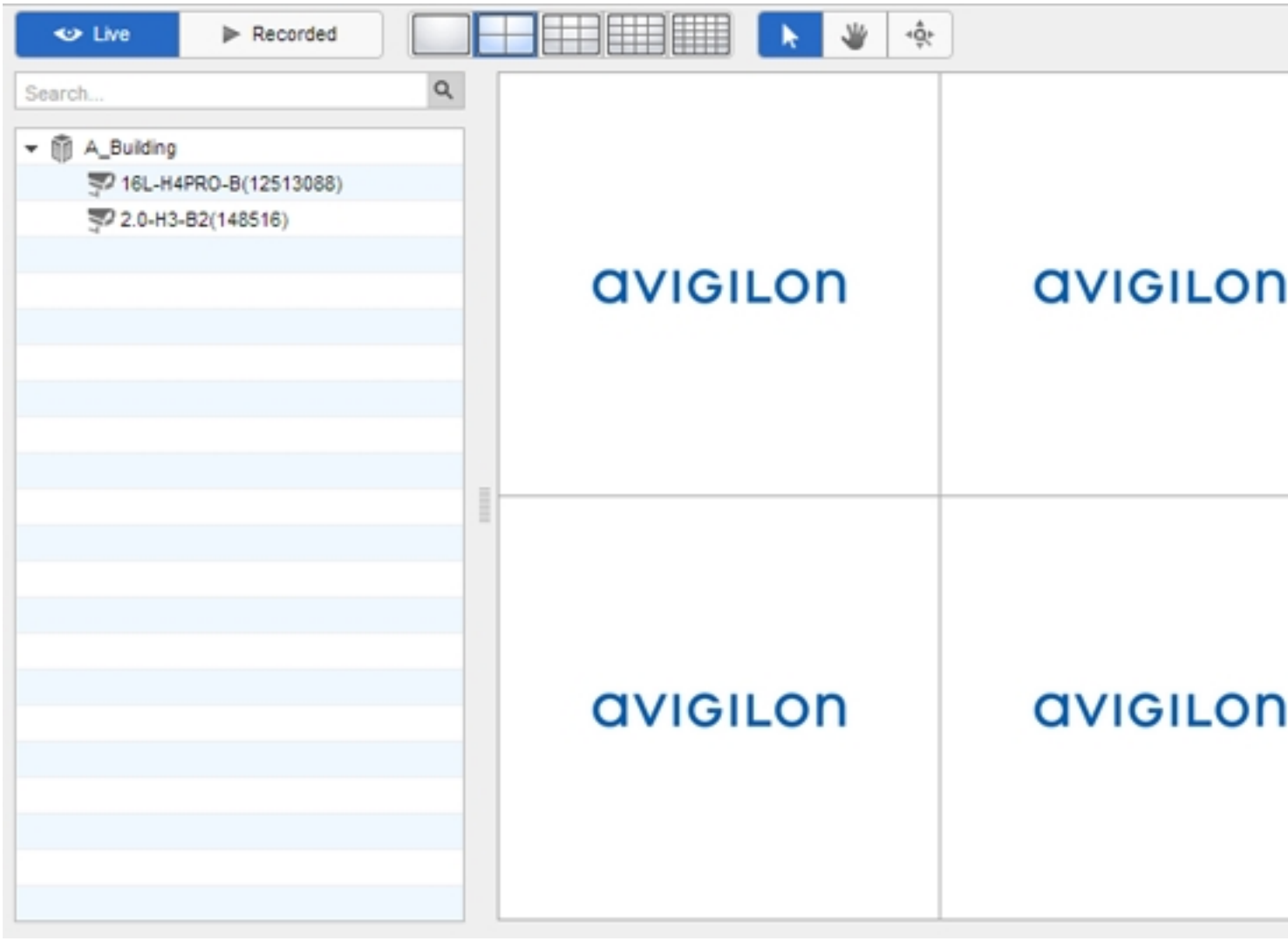


Figure 1: The Avigilon Control Center Web Client

What are Views?

A View tab is where you watch camera video. Inside the View tab is a set of image panels that allows you to organize how video is displayed.

You can arrange image panels into different layouts to take advantage of different camera angles and save View layouts that you like.

For more information on controlling live and recorded video, see **Monitoring Video**.

Adding and Removing a View

View tabs allow you to customize how you monitor video. You can open a new View in the browser to see more video. Views can also be removed as required.

To...	Do this...
Open a new View tab	Click  >  .
Close a View tab	On the View tab, click  .

View Layouts

You can organize how video is displayed through View layouts. You can choose to display video in 1 - 64 image panels. You can also customize the shape of image panels to accommodate cameras that are installed vertically to capture long hallways.

There are 10 pre-configured layouts that you can edit to fit your needs.

Selecting a Layout for a View

You can organize how video is displayed by selecting a View layout. The figure below shows the default View layouts.

- On the toolbar, select  , then select one of the following layout options.

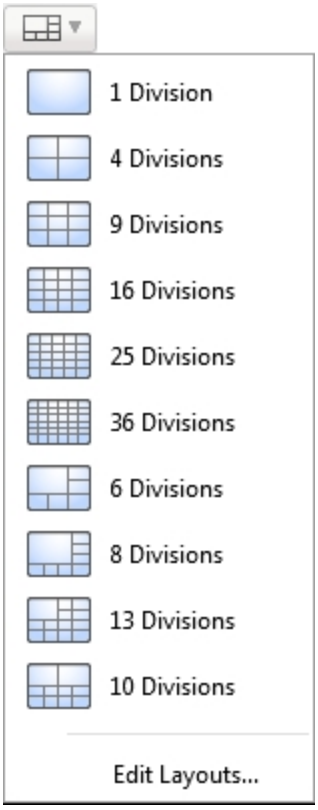


Figure 2: Layouts in the toolbar

Editing a View Layout

If the default View layouts do not fit your surveillance requirements, you can customize a View layout.

1. On the toolbar, select  > **Edit Layouts...**.

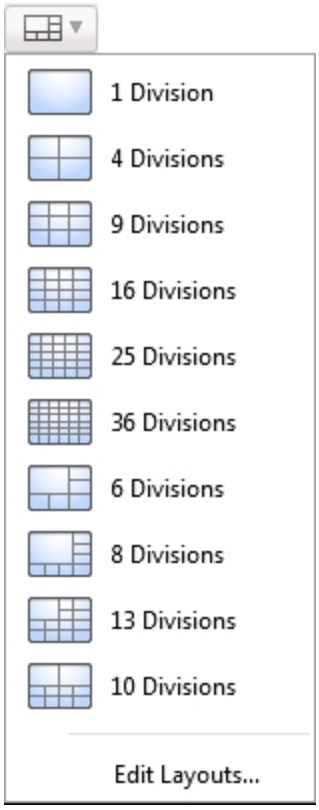


Figure 3: Layouts in the toolbar

2. In the Edit Layouts dialog box, select the layout you want to change.
3. Enter the number of **Columns:** and **Rows:** you want in your layout.

4. In the layout diagram, do any of the following to further customize the layout.

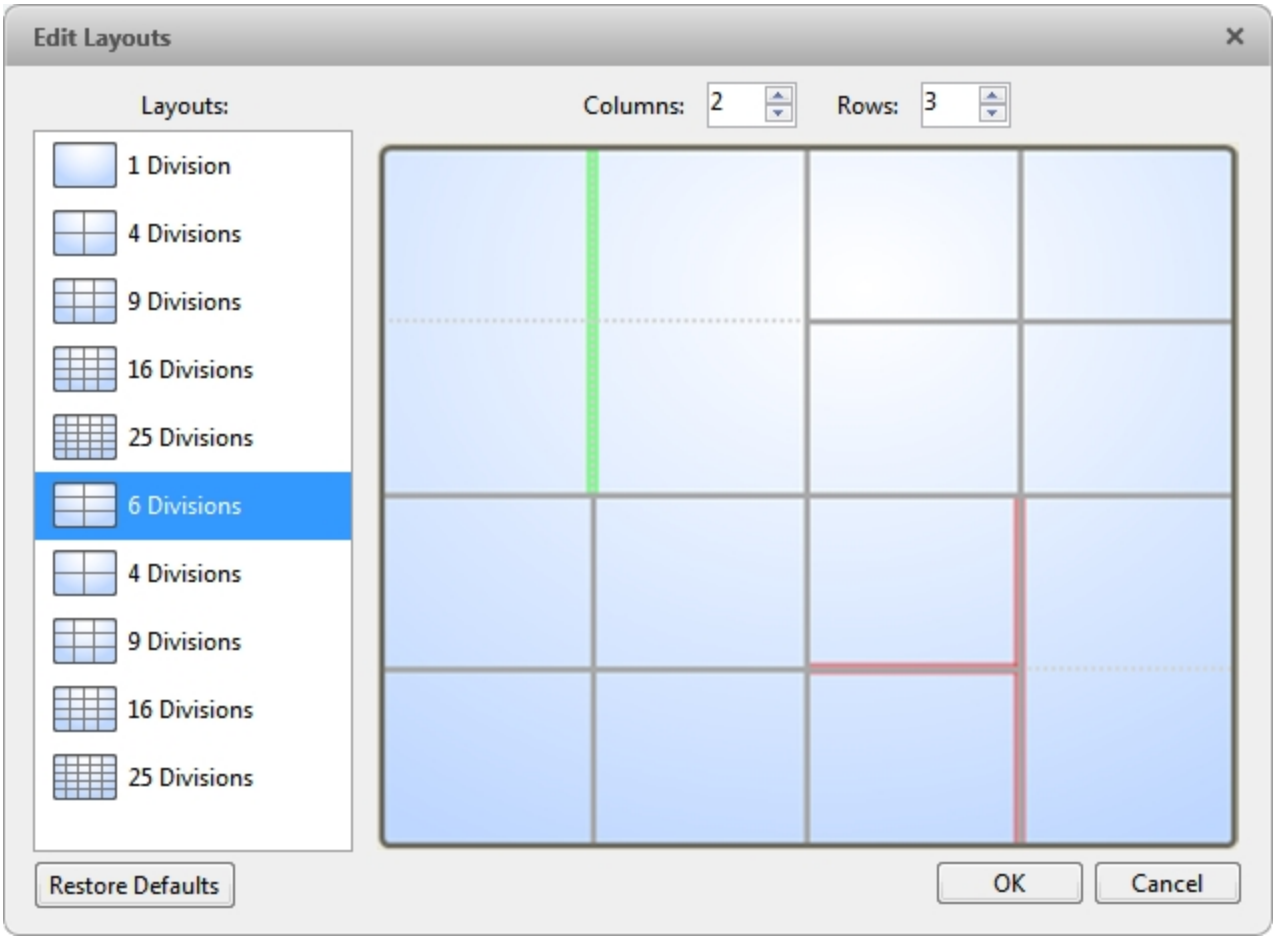


Figure 4: The Edit Layouts dialog box

- To create a larger image panel, select a gray line to delete the border between two image panels. When a line is highlighted in red, the line can be deleted.
- To restore an image panel, select a dotted line to divide a larger image panel into two. When a dotted line is highlighted in green, the line can be restored.
- To restore all default View layouts, click **Restore Defaults**. All custom layouts in the Layouts: list will be replaced.

NOTE: You can only add or subtract lines to create a rectangular shape.

5. Click **OK** to save your changes. The previous View layout has been replaced with your customized layout.

Tip: The keyboard commands used to access View layouts are linked to the layout's position in the Layouts: list. For example, if your custom layout is placed at the top of the Layouts: list (layout 1), you can press Alt + 1 to use that layout.

Making a View Full Screen

You can maximize a View to fill an entire monitor screen.

- On the toolbar, click  .

Ending Full Screen Mode

- While the View is in full screen mode, click  .

Cycling Through Views

If you have multiple Views open, you can cycle through the View tabs by displaying each one for a few seconds. This is useful when monitoring a large number of cameras.

- To activate the Cycle Views feature, click  .

Saved Views

Once you have set up a View you like, you can save the View to share with other users in the Site. A saved View remembers the current View layout, the cameras displayed in each image panel, and the image panel display settings.

NOTE: You can only add and view cameras that are connected to the server that you are accessing through the Web Client.

Saving a View

1. In the toolbar, click  .
2. In the dialog box which appears, complete the following:

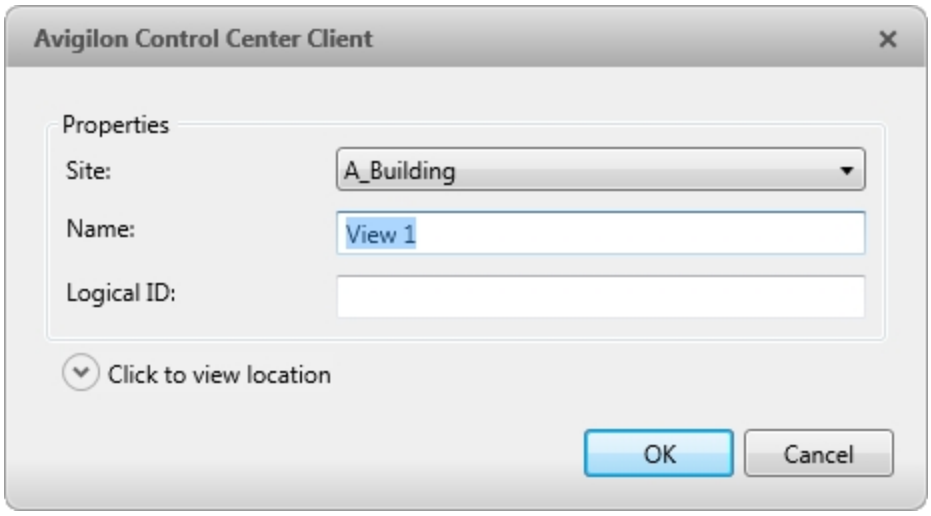


Figure 5: Edit View dialog box

a. Select the Site that the View should be added to.

b. Give the saved View a name.

c. Assign a **Logical ID:** to the View. The logical ID is a unique number that is used to open the saved View through keyboard commands.

d. Click  to choose where the saved View appears in the System Explorer.

- If your Site includes virtual sub-sites, select a location for the saved View. The list on the right updates to show what is stored in that directory.
- In the Site directory, drag the saved View up and down to set where it is displayed.

e. Click **OK**.

Your saved View is added to the System Explorer under the selected Site. You can now manage the saved View as a part of your Site.

Opening a Saved View

Do one of the following

- In the System Explorer, double-click the saved View.
- In the System Explorer, right-click the saved View and select **Open**.
- Drag the saved View from the System Explorer to the current View in the application or new window.

Editing a Saved View

1. Open a saved View.
2. Make any required changes to the View tab.
3. Click  .

Renaming a Saved View

1. In the System Explorer, right-click the saved View and select **Edit...**.
2. In the Edit View dialog box, enter a new name or logical ID and click **OK**.

Deleting a Saved View

1. In the System Explorer, right-click the saved View and select **Delete**.
2. In the confirmation dialog box, click **Yes**.

Monitoring Video

Inside a View tab, you can monitor and control video from multiple cameras. Once you open a camera in a View tab, you can control the camera's live and recorded video stream. You also have access to the camera's PTZ controls, connected audio devices, digital outputs, and other playback settings.

To organize how video is displayed in the View tab, see **What are Views?**.

NOTE: Some features are not displayed if the server does not have the required license, or if you do not have the required user permissions.

Adding and Removing Cameras in a View

To monitor video, add a camera to a View. Camera video can be removed from a View at any time.

Adding a Camera to a View

Do one of the following:

- Drag the camera from the System Explorer to an empty image panel in the View tab.
- Double-click a camera in the System Explorer.
- In the System Explorer, right-click the camera and select **Add To View**.

  The camera is added to the next empty image panel in the View layout.

Tip: You can drag the same camera to multiple image panels to watch the video at different zoom levels.

Removing a Camera from a View

Do one of the following:

- Right-click the image panel and select **Close**.
- Inside the image panel, click  .

Viewing Live and Recorded Video

NOTE: Some features are not displayed if the server does not have the required license, or if you do not have the required user permissions.

When you monitor video, you can choose to watch live and recorded video in the same View, or only one type of video per View.

Once you've added cameras to the View, perform the following:

- To switch all of the image panels in the View between live and recorded video, click either  **Live** or  **Recorded** on the toolbar.

- To switch individual image panels between live and recorded video, right-click the image panel and select either **Live** or **Recorded**.

Image panels displaying recorded video have a **green** border.

Zooming and Panning in a Video

Use the zoom and pan tools to focus on specific areas in the live or recorded video stream.

Using the Zoom Tools

There are two ways to digitally zoom in and zoom out of a video image:

- Move your mouse over the video image, then rotate your mouse wheel forward and backward.
- On the toolbar, select  or  , then click the image panel until you reach the desired zoom depth.

Using the Pan Tools

There are two ways to pan through the video image:

- Right-click and drag inside an image panel
- On the toolbar, select  , then click and drag the video image in any direction inside the image panel.

Maximizing and Restoring an Image Panel

You can maximize an image panel to enlarge the video display.

Maximizing an Image Panel

Do one of the following:

- Right-click an image panel and select **Maximize**.
- Inside the image panel, click  .
- Double-click the image panel.

Restoring an Image Panel

In a maximized image panel, do one of the following:

- Right-click the maximized image panel and select **Restore Down**.
- Inside the image panel, click  .
- Double-click the image panel.

Making Image Panel Display Adjustments

You can change the image panel display settings to bring out video details that are hard to see with the image panel's default settings.

1. Right-click an image panel and select **Display Adjustments...**.

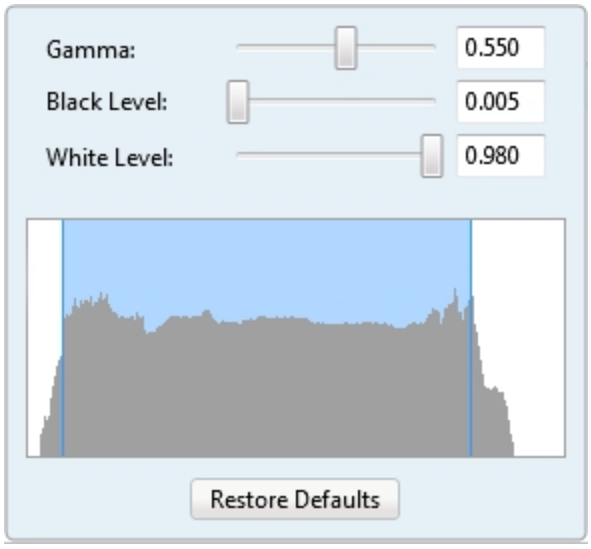


Figure 6: The Display Adjustments... panel

   The Display Adjustments... settings are displayed in a floating pane immediately beside the image panel.

2. Move the sliders to adjust the **Gamma:**, **Black Level:** and **White Level:**.

   The image panel displays a preview of your changes.

3. Click **Restore Defaults** to clear your changes.

Listening to Audio in a View

If there is an audio input device linked to a camera, the button is displayed in the image panel when you watch the camera's video. To listen to the streaming audio, make sure there are speakers connected to your computer. By default the audio is muted.

The camera's microphone must be enabled before you can listen to any audio. The button is not displayed if the microphone is disabled.

To control audio playback, do any of the following:

- In the lower-right corner of the image panel, click to mute or activate the audio.
- Move the slider to change the volume.

Controlling Live Video

In this section are features that are only available while monitoring live video.

Broadcasting Audio in a View

If there are speakers linked to a camera, the button is displayed in the image panel when you watch the camera's video. The button allows you to broadcast your verbal response to what is occurring in the video, like a Public Address (P.A.) system.

The camera's speakers must be enabled before you can broadcast any audio. The button is not displayed if the speakers are disabled.

- To broadcast audio, hold and speak into your microphone. The red bar moves to show the microphone's audio input levels. If the level is low, speak louder or adjust the microphone volume in the Windows Control Panel.
- Release the button to stop the broadcast.

Using Instant Replay

To review an event that just occurred, you can immediately access recently recorded video through the instant replay feature.

- Right-click the image panel and select one of the instant replay options:
  - **Replay - 30 Seconds**
  - **Replay - 60 Seconds**
  - **Replay - 90 Seconds**

The image panel immediately plays back the camera's most recently recorded video.

PTZ Cameras

PTZ cameras can be controlled through the image panel on-screen controls or by using the tools in the PTZ Controls pane.

Some tools and features may not be displayed if they are not supported by your camera.

Controlling PTZ Cameras

Pan, Tilt, Zoom (PTZ) controls allow you to control cameras with PTZ features. You can control a PTZ camera by using the on-screen controls or by using the tools in the PTZ Controls pane.

NOTE: For video analytics devices, classified object detection only works when the camera is in its Home position.

1. In the toolbar, click . PTZ controls are now enabled in image panels that are displaying PTZ video.
2. In the image panel, click .

   The PTZ Controls are displayed in a floating pane immediately beside the image panel.

   NOTE: The controls may appear differently depending on the camera. Some options are disabled or hidden if they are not supported by the camera.

Figure 7: The PTZ Controls

3. To pan or tilt, do one of the following:
   - In the image panel, drag your mouse from the center to move the camera in that direction. The farther the cursor is from the center of the image panel, the faster the camera will move.
   - If the camera supports Click to Center, click anywhere on the image panel to center the camera to that point.

Figure 8: PTZ On-screen controls

4. Use the other PTZ controls to perform any of the following:

To...	Do this...
Zoom	• Click  to zoom in. • Click  to zoom out. • Click the image panel and use the mouse scroll wheel to zoom in and out. • If the camera supports Drag to Zoom, click and drag to create a green box to define the area you want to zoom in and see. • Right-click the image panel and select **Zoom Out Full**.
Control the iris	• Click  to close the iris. • Click  to open the iris.
Control the focus	• Click  to focus near the camera. • Click  to focus far from the camera.
Program a PTZ preset	1. Move the camera's field of view into position. 2. In the **Presets** drop down list, select a number then click  . 3. In the dialog box, enter a name for the preset. 4. Select the **Set as home preset** check box if you want this to be the camera's Home preset. 5. Click **OK**.
Activate a PTZ preset	Select a preset then click  .
Return to the Home preset position	If the PTZ camera supports a Home preset position, click  to return the camera to its Home position.
Program a PTZ pattern	1. In the PTZ Controls pane, select a pattern number and click  . 2. Use the PTZ controls to move the camera and create the pattern. 3. Click  to stop recording the pattern.
Activate a PTZ pattern	In the PTZ Controls pane, select a pattern number and click  . The pattern will repeat until the pattern is stopped or another pattern is run.
Program a PTZ tour	For more information, see **Programming PTZ Tours**.
Activate a PTZ tour	In the PTZ Controls pane, select a tour number and click  .

To...	Do this...
	The tour will repeat until stopped or until other PTZ controls are used.
Activate an auxiliary command	1. Select an aux command number and click  . 2. Click  to turn off the auxiliary output.
Display the PTZ camera on-screen menu	1. Click  . 2. To move through the menu options, click any of the following: • Click  to move down the options. • Click  to move up the options. • Click  to confirm your selection. • Click  to cancel your selection.
Lock the PTZ controls	Click  . Other users will be unable to use the PTZ controls for this camera until you unlock the controls or log out.

Programming PTZ Tours

If the PTZ camera supports guard tours, the tours can be programmed through the PTZ controls pane. Tours allow the PTZ camera to automatically move between a series of preset positions, and can be set to pause at each preset for a specific amount of time for video monitoring.

NOTE: For video analytics devices, classified object detection only works when the camera is in its Home position.

1. Create all the PTZ presets you need for this tour.
2. In the PTZ Controls pane, select a tour number then click  . The Edit PTZ Tour dialog box is displayed.

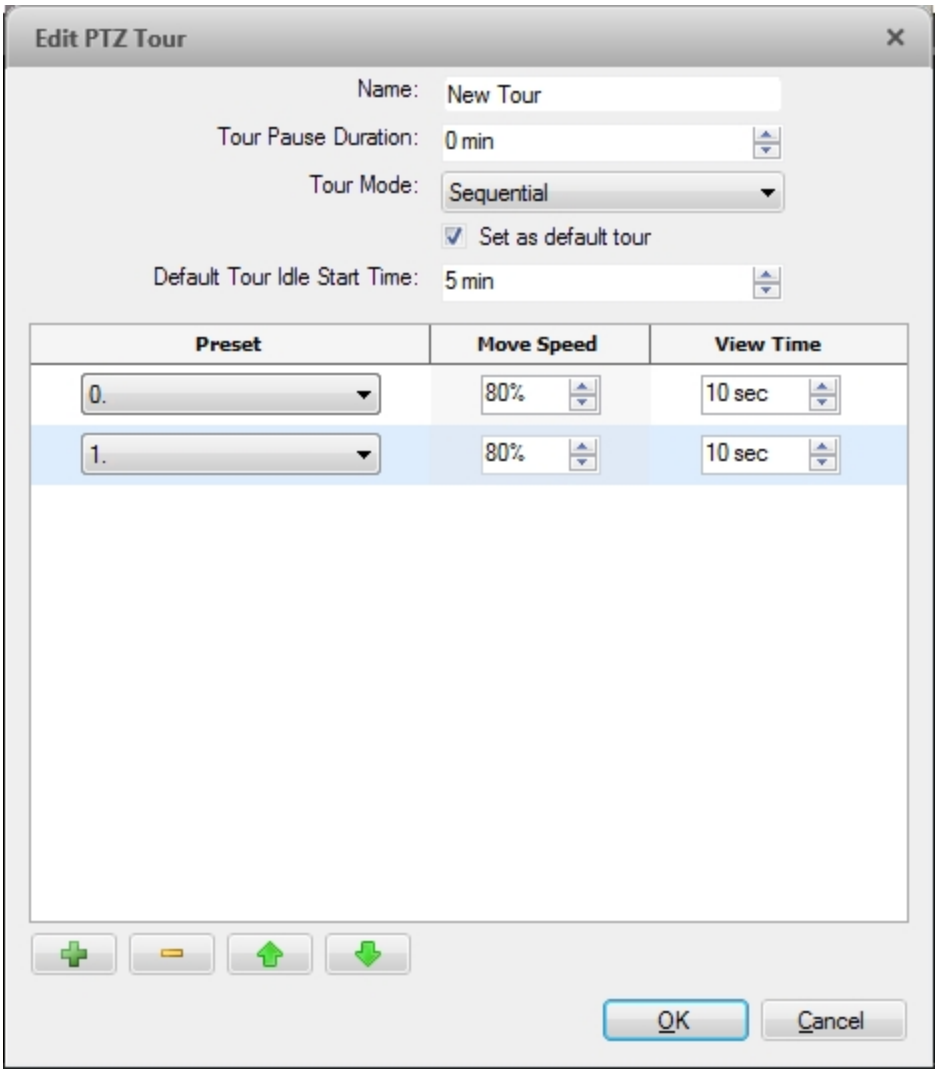


Figure 9: The Edit PTZ Tour dialog box

3. In the Edit PTZ Tour dialog box, give the tour a name.
4. In the **Tour Pause Duration:** field, enter the amount of time before a tour repeats. Tours repeat until manually stopped, or until other PTZ controls are used.
5. In the **Tour Mode:** drop down list, select one of the following:
    - **Sequential:** the PTZ camera will go to each preset in the set order.
    - **Random:** the PTZ camera will go to each preset in random order.
6. Select the **Set as default tour** check box if you want this tour to run automatically.
    - The **Default Tour Idle Start Time:** field is now enabled. Enter the amount of time the PTZ camera must be idle before this tour automatically starts.
7. To add a preset to the list, click .
    a. In the **Preset** column, select a preset from the drop down list.
    b. In the **Move Speed** column, enter how fast you want the PTZ camera to move to this preset. The

higher the %, the faster the camera moves.

c. In the **View Time** column, enter the amount of time you want the PTZ camera to stay at this preset position. The view time is 10 seconds by default.

d. Repeat step 7 until all the presets for this tour have been added.

8. To remove a preset, select the preset then click .
9. To re-order a preset, select the preset then click or . The preset order only affects tours that use Sequential mode.
10. Click **OK** to save the tour.

Triggering Manual Recording

Cameras are set to follow a recording schedule. If an event occurs outside the camera's recording schedule, you can click the record indicator icon to force the camera to record the event.

Camera Recording States

		
Recording	Recording triggered by an event	Not recording

Starting and Stopping Manual Recording

In an image panel that is displaying video, do either of the following:

- In the top-left corner of the image panel, click  to start manual recording.

  The recording indicator is highlighted in blue to show that the camera is recording. Manual recording continues until it is stopped or until the maximum manual recording time is reached.

- Click  to manually stop video recording.

Triggering Digital Outputs

While you monitor live video in an image panel, you can manually trigger any digital output that is connected to the camera.

To trigger a digital output:

1. Open the camera's live video in an image panel.
2. In the image panel, click  .
3. If there is more than one digital output linked to the camera, you will be prompted to select the digital output you want to trigger.

Monitoring Live POS Transactions

If a camera is linked to a point of sale (POS) transaction source, you can monitor live POS transactions while you monitor video from the linked camera.

1. Open the camera's video in an image panel.
2. In the image panel, click .

   NOTE: If the camera is not linked to a POS transaction source, the icon is not displayed.

   If there is more than one POS transaction source linked to the camera, you will be prompted to select one. The POS transactions are displayed in the next image panel.

   Each transaction is separated by date and time, and the most recent transaction is highlighted in blue.
3. To display cameras that are linked to the POS transaction source, click in the POS transaction image panel.

   If multiple cameras are connected to the POS transaction source, you will be prompted to select one.

Controlling Recorded Video

In this section are features that are only available while monitoring recorded video.

Playing Back Recorded Video

The Timeline displays when video was recorded and lets you control video playback.

The colored bars on the Timeline show the camera's recording history:

- A red bar shows the camera has recorded a motion event.
- A blue bar shows the camera has recorded video.
- White areas show periods of time during which the camera has not recorded any video.
- An yellow bar is a bookmark in the camera's recording history.

For more information about bookmarks, see **Bookmarking Recorded Video**.

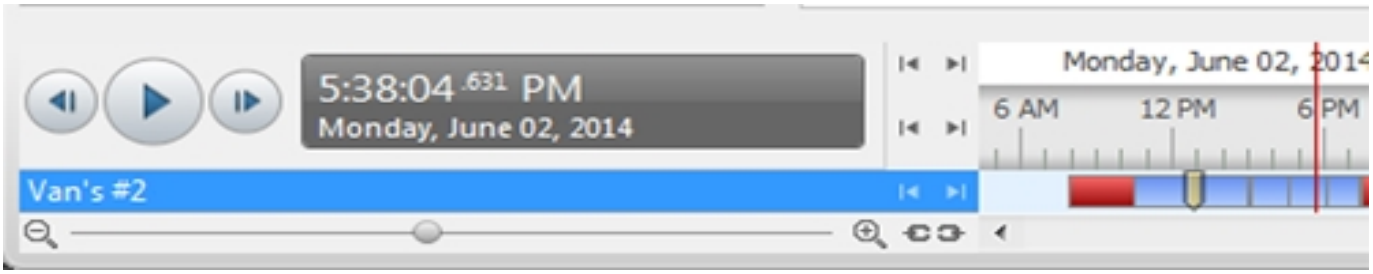
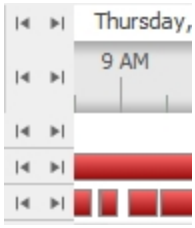
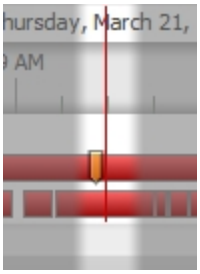


Figure 10: Playback controls on the Timeline

To...	Do this...
Select a playback time	• Click the dark gray date display and select a specific date and time. • Click a point on the Timeline.
Start playback	Click . • Click to fast forward. Tap the arrow again to increase the playback speed.

To...	Do this...	
	• Click to rewind. Tap the arrow again to increase the playback speed. You can play the video up to eight times the original speed.	
Stop playback	Click . • Click to step forward one frame. • Click to step backward one frame.	
Jump forward or backward on the Timeline		On the Timeline, click or to move to set points on the Timeline.
Zoom in or out of the Timeline		• Move the slider on the bottom left to zoom in or out on the Timeline. • Place your mouse over the Timeline and use the scroll wheel to zoom in or out on the Timeline. You can zoom in to a quarter of a second, and zoom out to see years if recorded video exists.
Center the Timeline on the time marker		Right-click the Timeline, and select **Center on Marker.**
Pan the Timeline		• Click and drag the time marker through the Timeline. • Move the horizontal scroll bar under the Timeline. • Right-click and drag the Timeline.

Bookmarking Recorded Video

You can add bookmarks to recorded video to help you find and review an event later. Bookmarked video can be protected against scheduled data cleanup so that the video is never deleted.

Adding a Bookmark

Tip: You can add a bookmark any time the Timeline is displayed.

1. Drag the time marker to where you want to start the bookmark, then right-click the Timeline and select **Add Bookmark**.

   The Edit Bookmark dialog box appears, and the bookmark time range is highlighted on the Timeline.

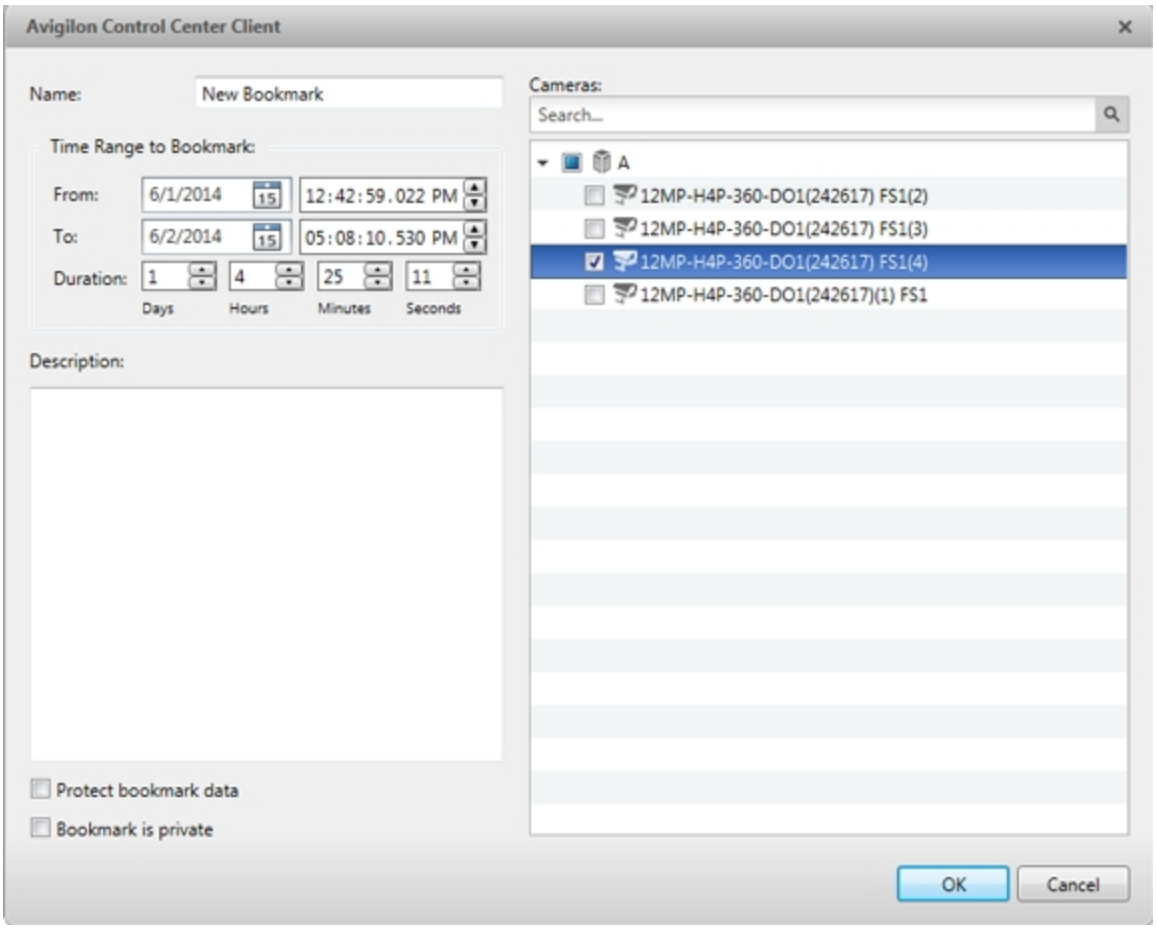


Figure 11: Edit Bookmark dialog box

2. Enter a **Name:** for the bookmark.
3. In the **Cameras:** pane, select all the cameras that need to be attached to this bookmark.

   NOTE: You can only bookmark multiple cameras from the same Site.
4. In the **Time Range to Bookmark:** area, enter the full duration of the bookmark.

   You can also move the black time range markers on the Timeline to adjust the time range.
5. In the **Description:** field, enter extra any information you want to include with the bookmark.
6. To protect the bookmark video from being deleted, select the **Protect bookmark data** check box.

   NOTE: Protected bookmarks are never deleted. Be aware that bookmarked videos take up space and can become the oldest video on the server.
7. To make the bookmark private, select the **Bookmark is private** check box. Private bookmarks are only visible to the user who marked the bookmark as private, and the system administrator. No one else will have access to the bookmark.
8. Click **OK**.

Exporting, Editing, or Deleting a Bookmark

1. Click the bookmark on the Timeline, then do one of the following:

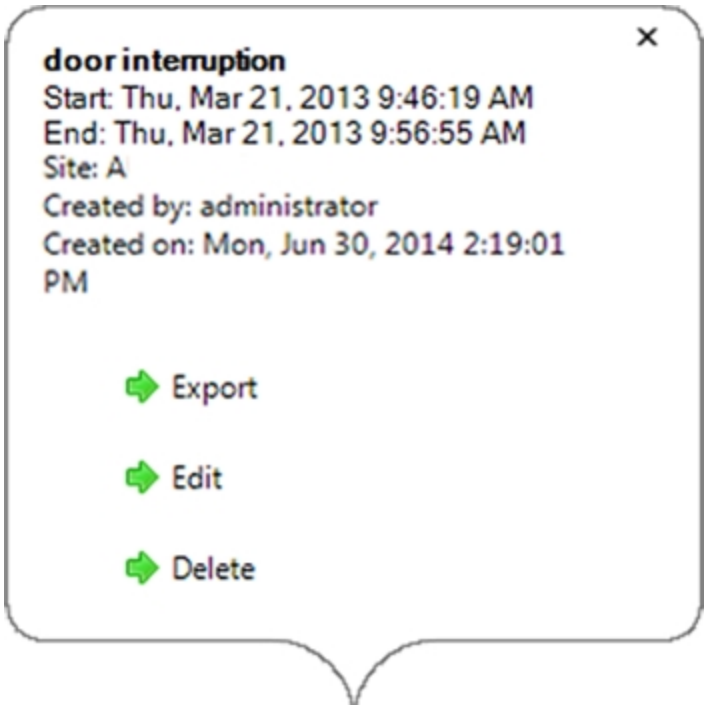


Figure 12: Pop-up Bookmark properties

To	Do this...
Export a bookmark	Click **Export**, then complete the Export tab.
Edit a bookmark	Click **Edit**, then make your changes.
Delete a bookmark	Click **Delete**. When the confirmation dialog box appears, click **Yes**.

When editing a bookmark, refer to **Adding a Bookmark** for details about the editable options.

When exporting a bookmark, refer to **Export** for information about the export options.

Reviewing Recorded POS Transactions

While you watch recorded video, you can review POS transactions that occur at the same time.

1. Select a camera that is linked to the POS transaction source and display the camera's recorded video
2. In the image panel, click .

   If there is more than one POS transaction source linked to the camera, you will be prompted to select one. The POS transactions are displayed in the next image panel.

   - Each transaction is separated by date and time.
   - When you select a transaction, the video jumps to that event on the Timeline.
   - Scroll up or down to see other recorded POS transactions.

3. To display cameras that are linked to the POS transaction source, click  in the POS transaction image panel.

   If multiple cameras are connected to the POS transaction source, you will be prompted to select one.

4. Use the Timeline to review the video in more detail.

For more information about Timelines, see **Playing Back Recorded Video**.

If you want to find a specific POS transaction, see **Performing a POS Transaction Search**.

Working with Maps

A map is a graphical reference of your surveillance site. You can create a map out of any image of your location, then add cameras, encoders, saved Views, and other maps to the image to help you quickly navigate through your surveillance site.

Adding a Map

You can create a map from any image in JPEG, BMP, PNG, or GIF format. The image is used as the map background and cameras are added on top to show where they are located in your surveillance Site.

NOTE: You can only add and view cameras that are connected to the server that you are accessing through the Web Client.

1. In the System Explorer, right-click a Site or Site folder and select **New Map...**.
2. In the Map Properties dialog box, click **Change Image...** and locate your map image.

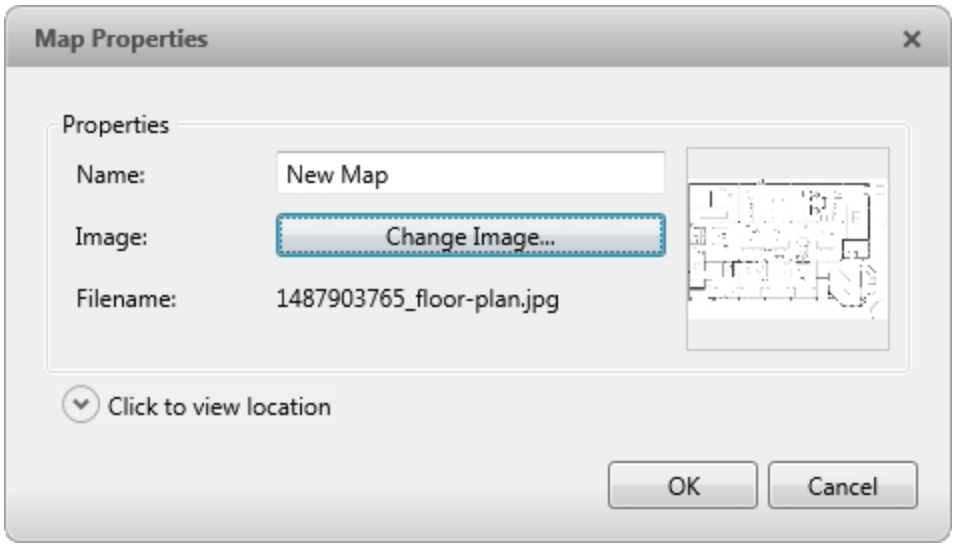


Figure 13: The Map Properties dialog box

3. In the **Name:** field, enter a name for the map.
4. Click to choose where the map appears in the System Explorer. By default, the map is added to the Site that you initially selected.
    - If your Site includes virtual sub-sites, select a location for the map. The list on the right updates to show what is stored in that directory.
    - In the Site directory, drag the map up and down to set where it is displayed.
5. Click **OK**.

    In the following Editing: Map tab, you can click **Edit Properties...** to open the Map Properties dialog box again.

6. Drag and place cameras from the System Explorer onto the map.

Figure 14: The Editing: Map tab

By default a camera is displayed as an icon with a yellow triangle to represent its field of view.

- Drag the black points at the end of the yellow field of view to re-size and position the camera angle.

7. Drag encoders, saved Views, and other maps that you need from the System Explorer onto the map.
8. In the **Map Icon Properties** options, you can change the way icons are displayed on the map. Select any icon on the map then do the following:

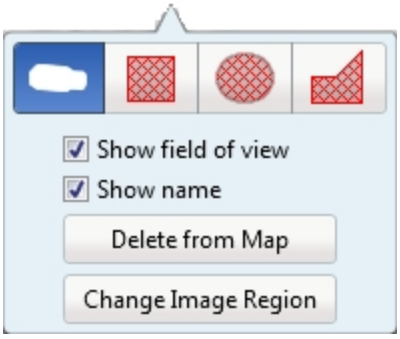


Figure 15: Map Icon Properties options

a. To replace an icon with a clickable shape region, select one of the shape buttons. You can replace the icon with a rectangle, ellipse, or polygon region.

b. Select the **Show name** check box to display the object's name on the map.

c. Click **Delete from Map** to remove the object from the map.

d. (Cameras only) Select the **Show field of view** check box to display the camera's yellow field of view. This option is only available when the camera icon is used.

   Drag the corners of the yellow triangle to expand the field of view. Drag the black circle at the end of the triangle to rotate the field of view.

9. Click  to save your new map.

Using a Map

You can open a map in any image panel, then open video or alarms from the map.

1. To open a map in an image panel, do one of the following:
   - Double-click in the System Explorer.
   - Drag from the System Explorer to an image panel.
   - In the System Explorer, right-click and select **Add To View**
2. When the map appears in an image panel, do any of the following:

Figure 16: Map in an image panel.

To...	Do this...
Display video from a camera on the map	• Drag a camera from the map to a different image panel, or • Click the camera on the map.

To...	Do this...
Open a linked map	• Click the map icon on the map. You can use the **Forward** and **Back** buttons to move between maps.
Open a linked View	• Click the saved View on the map.

Editing and Deleting a Map

You can update a map or delete an old map anytime.

1. In the System Explorer, right-click  then select one of the following:
    - To edit the map, select **Edit...**. Refer to **Adding a Map** for details about the editable options.
    - To delete the map, select **Delete**. When the confirmation dialog box appears, click **Yes**.

Working with Web Pages

You can quickly review online content while monitoring videos by adding web pages to the System Explorer.

Adding a Web Page

You can add web pages to a Site for quick access to internet content that is related to your surveillance system.

1. In the System Explorer, right-click a Site or Site folder and select **New Web Page...**.

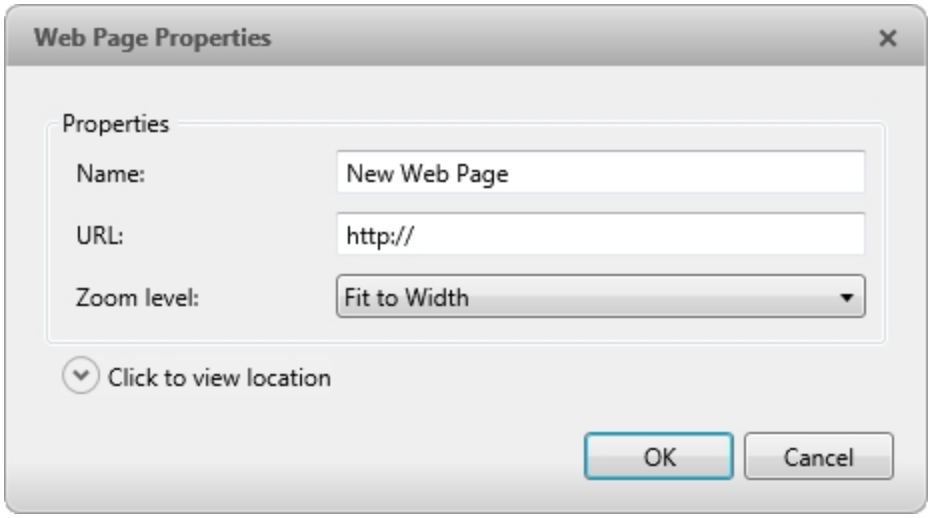


Figure 17: The Web Page Properties dialog box

2. Enter a **Name:** for the web page.
3. Enter the web page URL in the **URL:** field.
4. Select a **Zoom level:** for viewing the web page inside an image panel.
5. Click to choose where the web page appears in the System Explorer. By default, the web page is added to the Site you initially selected.
    - If your Site includes virtual sub-sites, select a location for the web page. The list on the right updates to show what is stored in that directory.
    - In the Site directory, drag the web page up and down to set where it is displayed.
6. Click **OK**.

Using a Web Page

To open a web page, do one of the following:

- Double-click in the System Explorer.
- Drag from the System Explorer to an image panel.

- In the System Explorer, right-click and select **Add To View**.

The web page is displayed in one of the image panels. Use the web browser buttons to navigate through the internet.

Figure 18: Web Page controls.

Editing and Deleting a Web Page

Whenever a web page address becomes out of date, you can choose to update the web page or delete the web page from the Site.

1. In the System Explorer, right-click then select one of the following:
    - To edit the web page, select **Edit...**. Refer to **Adding a Web Page** for information about the editable options.
    - To delete the web page, select **Delete**. When the confirmation dialog box appears, click **Yes**.

Search

You can quickly search for recorded video that is linked to an event or search through a camera's recording history.

NOTE: Some features are not displayed if the server does not have the required license, or if you do not have the required user permissions.

Performing a Bookmark Search

The Bookmark Search allows you to search for a specific bookmark.

1. In the New Task menu, click 

   The Search: Bookmark tab is displayed. All available bookmarks are listed on the left.

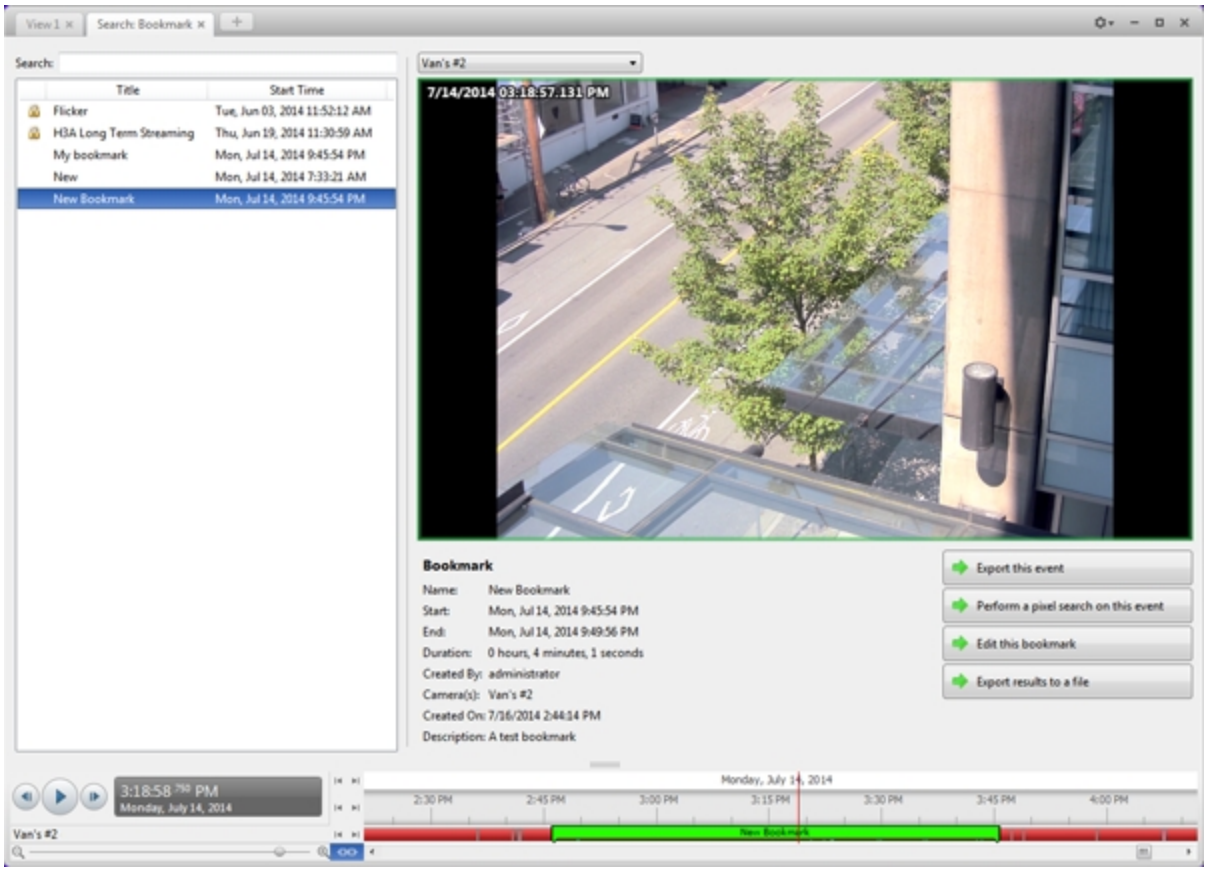


Figure 19: The Search: Bookmark tab

2. In the **Search:** field, enter any text that may appear in the bookmark's title, description, linked camera name, or the name of the user who created the bookmark.

   The search is automatically performed on all the listed bookmarks until only the matches are displayed.

Viewing Bookmark Search Results

1. In the Bookmark list, select a bookmark. The bookmark is highlighted on the Timeline and the video is displayed in the image panel. Details about the bookmark are displayed under the image panel.
2. Use the Timeline controls to review the event.

   For more information, see **Playing Back Recorded Video**.
3. If the search result is linked to multiple cameras, select a camera from the drop down list above the image panel to change the video that is displayed.
4. Click **Export this event** to export the selected bookmark.
5. If you want to further refine your search, click **Perform a pixel search on this event**. You can now search for pixel changes in the selected bookmarked video.

   For more information, see **Performing a Pixel Search**.
6. Click **Edit this bookmark** to edit the bookmark.

   For more information, see **Bookmarking Recorded Video**.

Performing an Event Search

The Event Search allows you to search for specific motion events and digital input events.

1. In the New Task menu, click 

   The Search: Event tab is displayed.

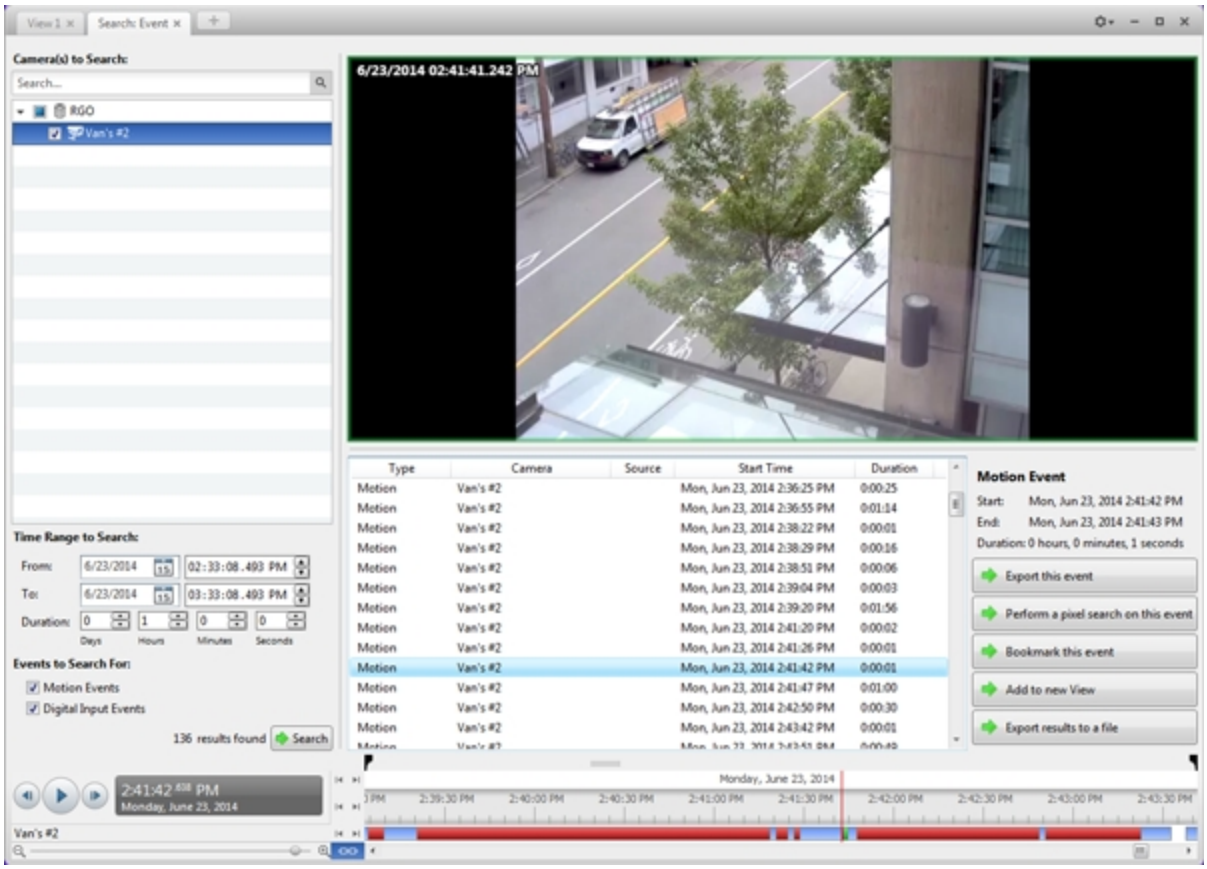


Figure 20: The Search: Event tab

2. In the **Camera(s) to Search:** area, select all the cameras you want to include in the search.
3. In the **Time Range to Search:** area, set the date and time range of your search. The time range is highlighted on the Timeline by the black time range markers. You can also drag the time range markers to modify the time range.
4. In the **Events to Search For:** area, select the types of events to include in the search.
5. Click **Search**.

Viewing Event Search Results

1. In the **Search Results** area, select a search result. The event is highlighted on the Timeline and the video is displayed in the image panel. Details about the search result are displayed to the right.
2. Use the Timeline controls to review the event.

   For more information, see **Playing Back Recorded Video**.
3. Click **Export this event** to export the selected event video.

   For more information, see **Export**.
4. If you want to further refine your search, click **Perform a pixel search on this event**. You can now search for pixel changes in the selected search result.

   For more information, see **Performing a Pixel Search**.

5. Click **Bookmark this event** to bookmark the selected search result.

   For more information, see **Bookmarking Recorded Video**.

6. To export all listed search results, click **Export results to a file** and save the file. The search results can be saved as either a CSV or Text file.

Performing a Pixel Search

The Pixel Search allows you to search for tiny pixel changes in specific areas in the camera's field of view.

1. In the New Task menu, click 

   The Search: Pixel tab is displayed.

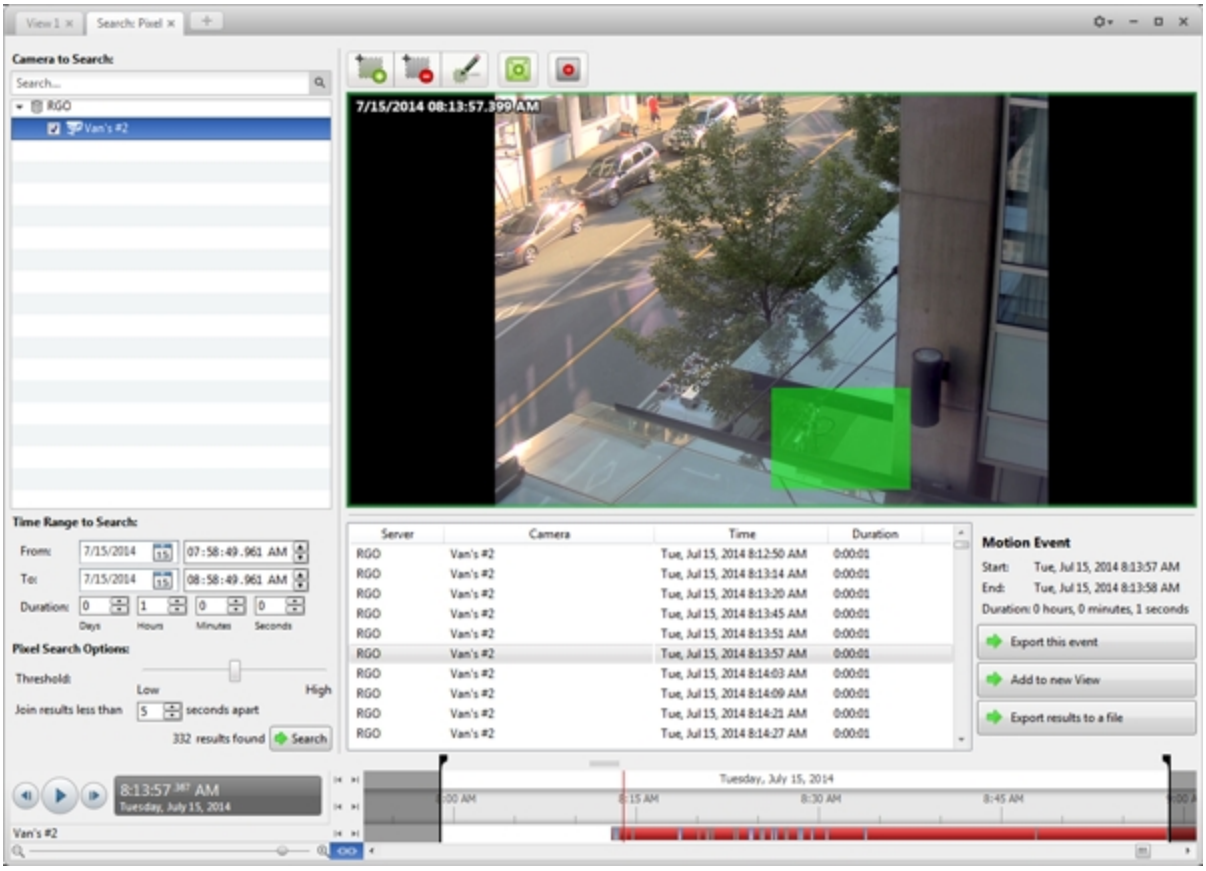


Figure 21: The Search: Pixel tab

   By default, the entire search image panel is highlighted in green.

2. In the **Camera to Search:** area, select a camera.

3. In the **Time Range to Search:** area, set the date and time range of your search. The time range is highlighted on the Timeline by the black time range markers. You can also drag the time range markers to modify the time range.

4. Define the pixel search area by using the motion detection tools above the image panel.

   Tip: If you are looking for something very specific, limit the green area to a dot to find what you're looking for more quickly.

5. In the Pixel Search Options: area, drag the **Threshold:** slider to select the amount of motion required to return a search result.

   A high threshold requires more pixels to change before results are found.

6. Enter a number in the **Join results less than** field to set the minimum number of seconds between separate search results. You can enter any number between 1-100 seconds.

7. Click **Search**.

Viewing Pixel Search Results

1. In the **Search Results** area, select a search result. The event is highlighted on the Timeline and the video is displayed in the image panel. Details about the search result are displayed to the right.

2. Use the Timeline controls to review the event.

   For more information, see **Playing Back Recorded Video**.

3. Click **Export this event** to export the selected event video.

   For more information, see **Export**.

4. To export all listed search results, click **Export results to a file** and save the file. The search results can be saved as either a CSV or Text file.

Performing a POS Transaction Search

The POS Transaction Search allows you to search for specific transactions.

1. In the New Task menu, click  .

   The Search: POS Transactions tab is displayed.

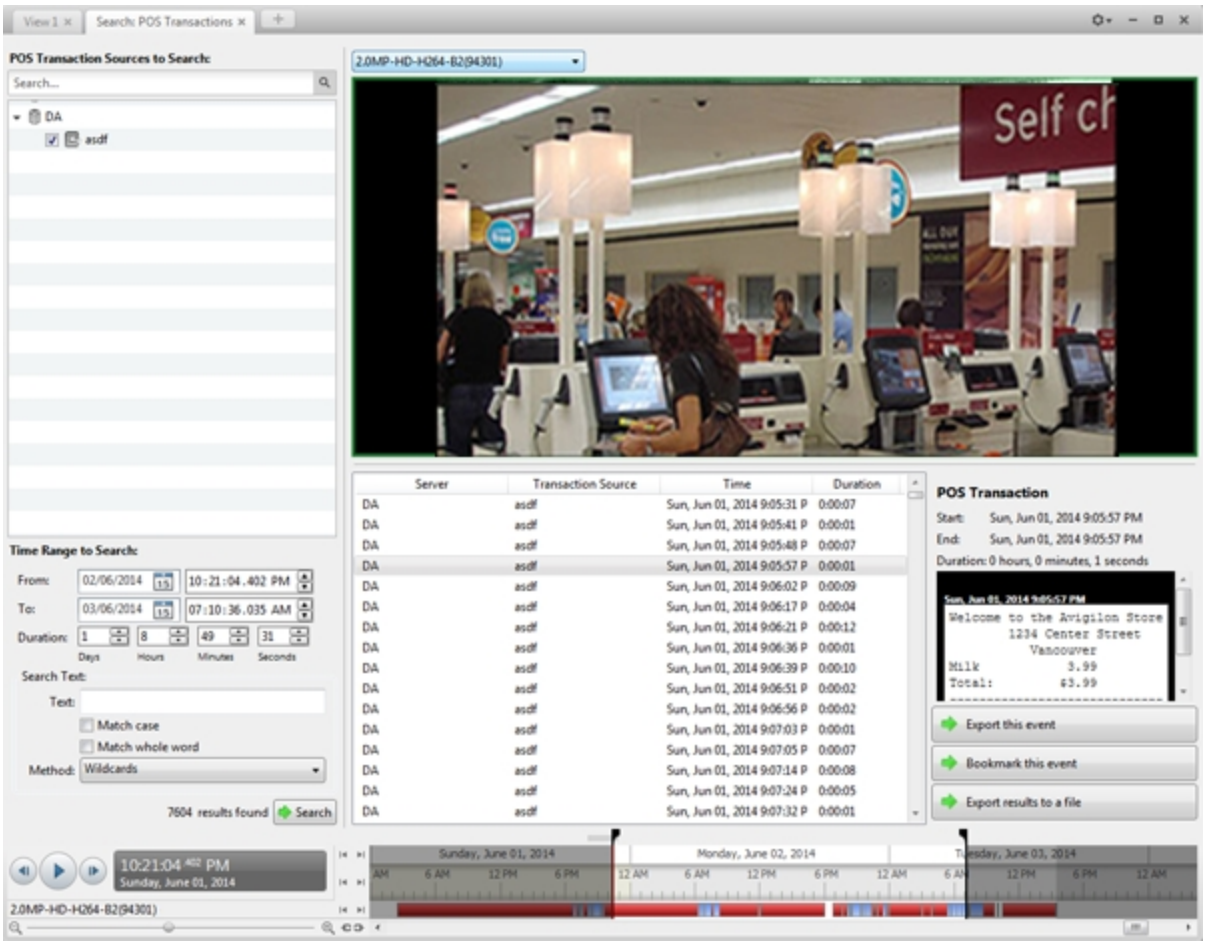


Figure 22: The Search: POS Transactions tab

2. In the **POS Transaction Sources to Search:** area, select all the POS transaction sources you would like to include in the search.
3. In the **Time Range to Search:** area, set the date and time range of your search. The time range is highlighted on the Timeline by the black time range markers. You can also drag the time range markers to modify the time range.
4. In the **Search Text:** area, enter any text that will help you filter the search results. For example, you can enter product names or transaction values.

   Use the **Wildcards** and **Regular expressions** search methods to find a range of results. Leave the **Text:** field blank to find all transactions.
5. Click **Search**.

Viewing POS Transaction Search Results

1. In the **Search Results** area, select a search result. The event is highlighted on the Timeline and the video is displayed in the image panel. Details about the search result are displayed to the right.
2. Use the Timeline controls to review the event.

   For more information, see **Playing Back Recorded Video**.

3. If the search result is linked to multiple cameras, select a camera from the drop down list above the image panel to change the video that is displayed.
4. Click **Export this event** to export the selected event video.

   For more information, see **Export**.
5. To export all listed search results, click **Export results to a file** and save the file. The search results can be saved as either a CSV or Text file.

Performing a Thumbnail Search

The Thumbnail Search is a visual search that displays search results as a series of thumbnail images.

1. In the New Task menu, click  .

   The Search: Thumbnails tab is displayed.

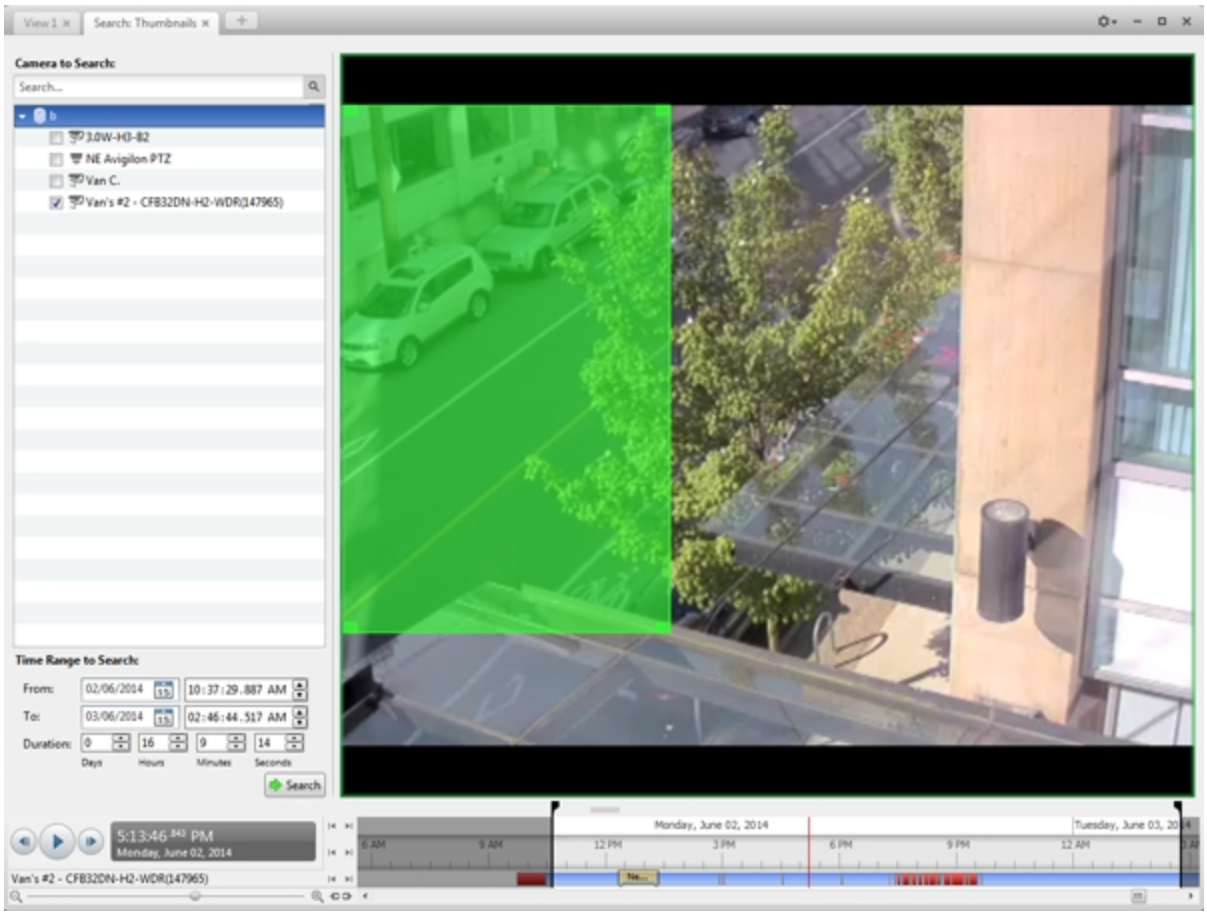


Figure 23: The Search: Thumbnails tab

2. In the **Camera to Search:** area, select a camera.
3. In the **Time Range to Search:** area, set the date and time range of your search. The time range is

highlighted on the Timeline by the black time range markers. You can also drag the time range markers to modify the time range.

4. In the image panel, move or drag the edges of the green overlay to focus the search on one area in the video image. Only the area highlighted in green will be searched.
5. Click **Search**.

Viewing Thumbnail Search Results

The search results display thumbnails at equal intervals on the Timeline.

1. To change the size of the search result thumbnails, select **Large Thumbnails**, **Medium Thumbnails**, or **Small Thumbnails** from the menu above the search results.

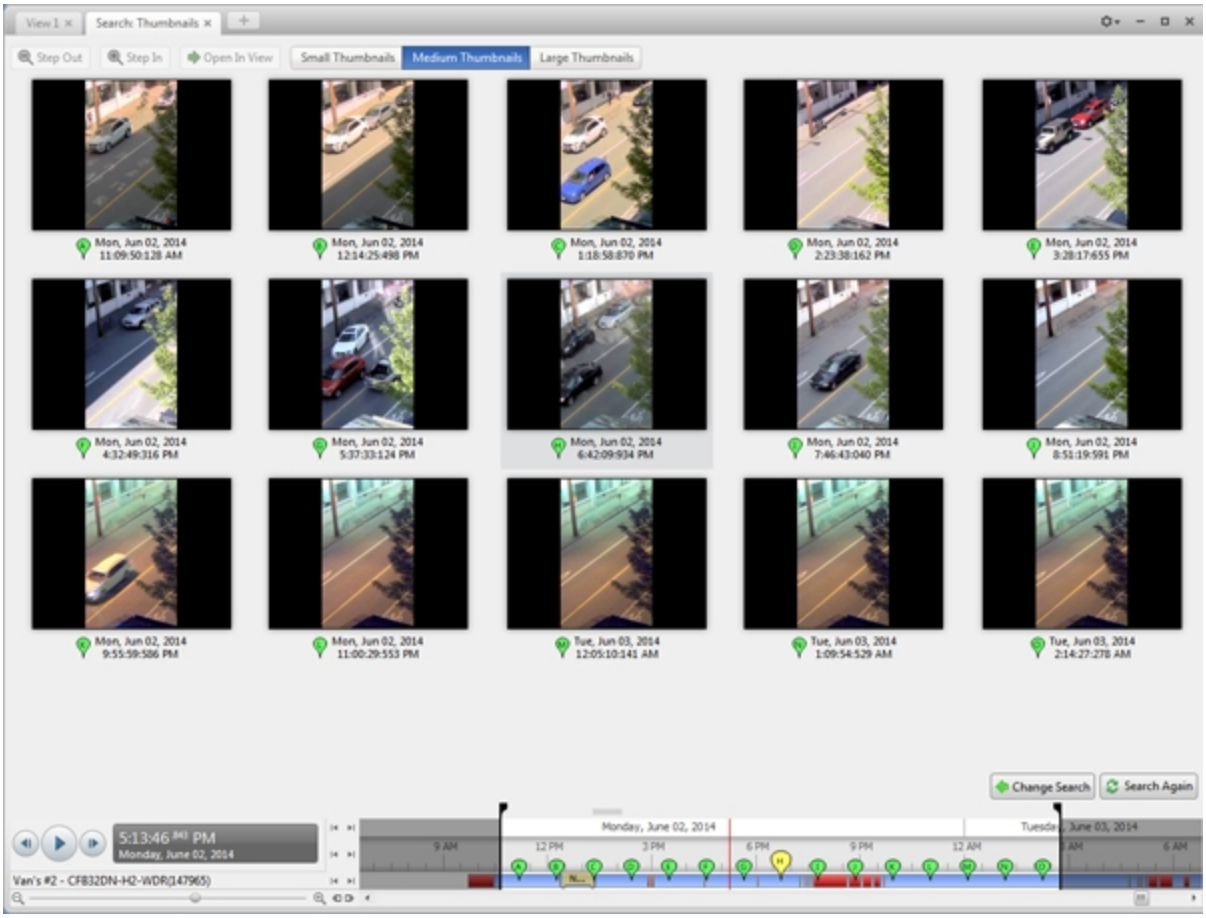


Figure 24: The Search: Thumbnails results tab

2. Select a thumbnail to highlight the video on the Timeline.
3. Click **Step In**, or double-click the thumbnail to perform another search around the thumbnail.

   Click **Step Out** to return to the previous results page.
4. Click **Open In View** (after selecting a thumbnail) to open the recorded video in a new View.
5. Click **Change Search** to change the search criteria.

Export

You can export video in multiple video and image formats. The Export tab can be accessed from bookmark options, the New Task menu, and any Search tab.

You can also export snapshots of an image panel as you monitor video.

It is recommended that you export video of individual events and back up video for your archives. For more information, see **Backup**.

Exporting Native Video

The Native (AVE) format is the recommended format for exporting video. You can export video from multiple cameras in a single file, and the video maintains its original compression. AVE video is played in the Avigilon™ Control Center Player, where the video can be authenticated against tampering and re-exported to other formats.

If there is audio linked to the video, the audio is automatically included in the export.

If you are exporting a large amount of video for your records, back up the video instead. For more information, see **Backing Up Recorded Video On Demand**.

1. In the New Task menu, click  . The Export tab opens.

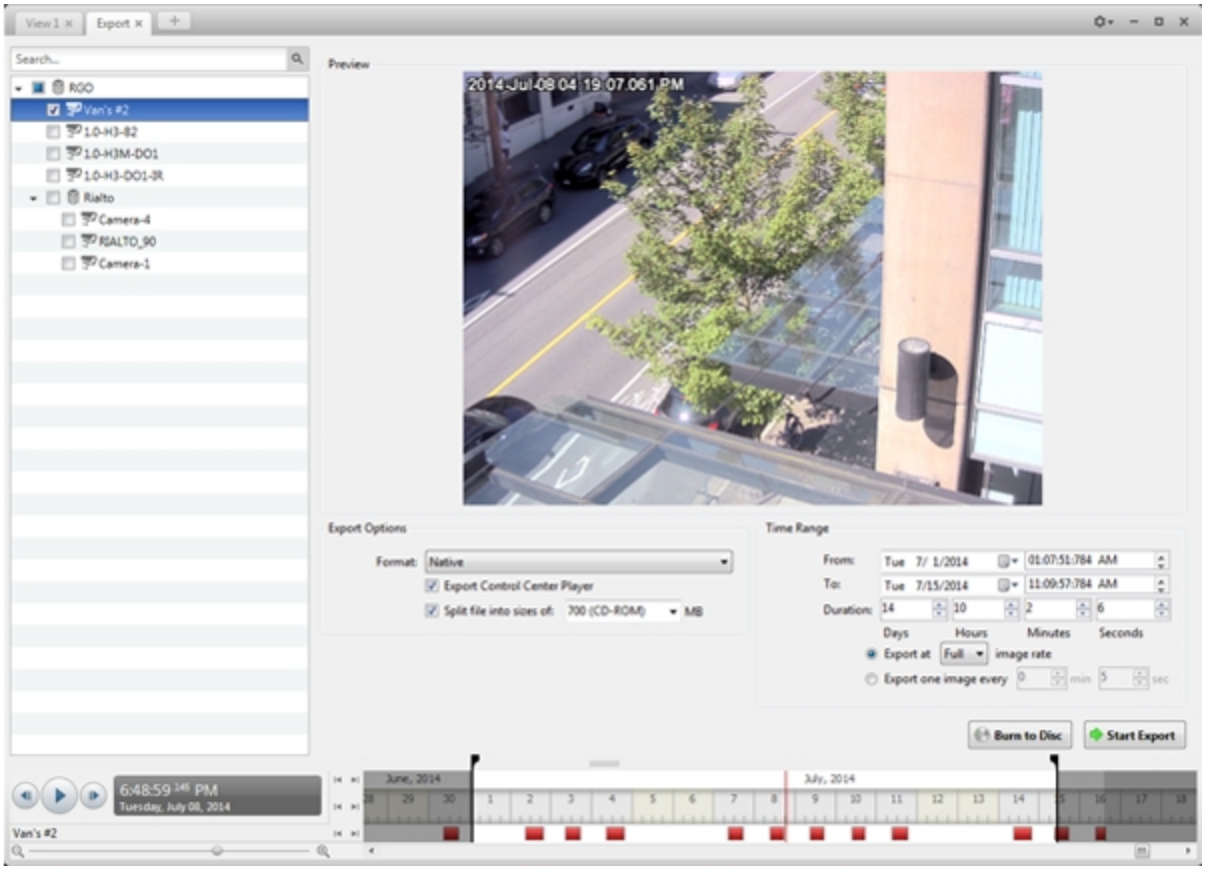


Figure 25: The Export tab for AVE export

2. In the **Format:** drop down list, select **Native**.
3. In the System Explorer, select the camera video you want to export.
4. To automatically divide the export into separate files, select the **Split file into sizes of:** check box, then select one of the options from the drop down list, or manually enter the size of each file in MB.

   This option allows you to export smaller files for storing in a flash drive or on optical media.

   This setting is automatically disabled if you choose to burn the export to disc because the system auto-detects the disc size.
5. Enter the **Time Range** you want to export. The **Time Range** is highlighted on the Timeline by black time range markers. You can also drag the time range markers to modify the time range.
6. Set the export image rate:

Option	Description
Export at _ image rate	Select this option to control how many images per second are exported. For example, the video is streaming at 30 images per second. If you select **1/2**, only 15

Option	Description
	images for that second will be exported.
Export one image every _ min _sec	Select this option to control the time between each exported video image. For example, if you enter *5* min. *0* sec., only one image will be exported for every 5 minutes of video.

7. Click one of the following:
   - **Start Export**: to save the file locally.
     - In the Save As dialog box, name the export file and click **Save**.
   - **Burn to Disc**: to burn the file directly to disc media.

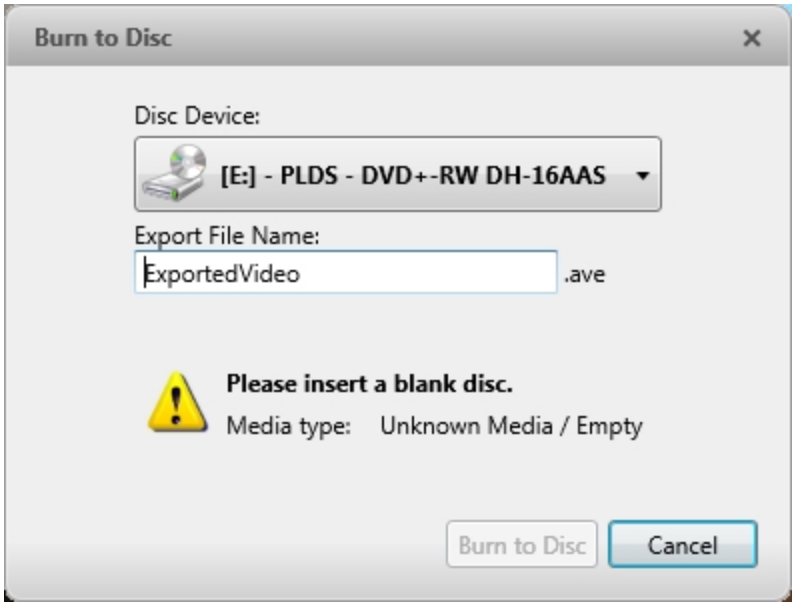


Figure 26: The Burn to Disc Dialog Box

   a. When the dialog box appears, insert a disc and select the media burning drive.
   b. Name the export file. The file name is automatically given a numbered suffix to help identify which file you are playing if the export spans multiple discs.
   c. Click **Burn to Disc** to start the export. If this button is disabled, the disc may be corrupt or full.
   d. Monitor the export progress to see if extra discs are required. When a disc is full, the export automatically pauses and you are asked to insert a new disc. After you insert a new disc, click **Resume Export**.

The number of discs required to export a video varies widely depending on the type of camera and disc used. Video is stored on the server with minimal compression to maximize the function of Avigilon's

HDSM™ technology, so the size of an export can be quite large due to the camera's high megapixel resolution and frame rate.

Generally, if you export a 2 minute video from a 2MP H.264 HD camera into AVE format, you will export a 93 MB file. To reduce the number of discs required, you can lower the frame rate or use a disc type with a larger capacity. Be aware that reducing the frame rate too much may cause the exported video to be jerky or missing data.

8. When the export is complete, click **OK**.

Exporting AVI Video

Video exported in Audio Video Interleave (AVI) format can be played in most media players. Be aware that you can only export one video at a time in this format.

1. In the New Task menu, click  . The Export tab opens.

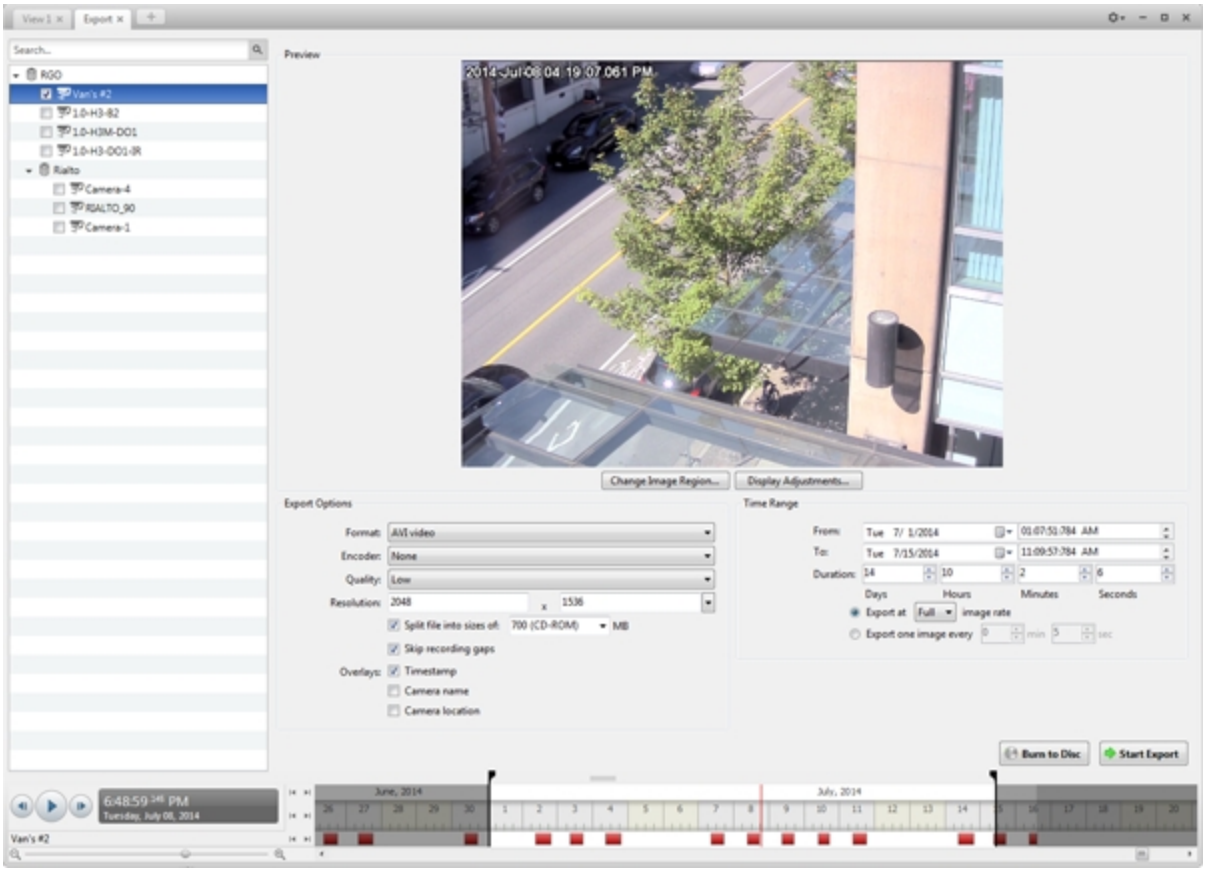


Figure 27: Export tab for AVI export

2. In the **Format:** drop down list, select **AVI video**.
3. In the System Explorer, select the camera video you want to export.
4. In the **Encoder:** field, select the compression used. The VC-1 (Windows Media Video) compression is

included by default because it is tailored for high-resolution AVI encoding.

If you are planning to burn the export to disc, it is important to select a compression method to help reduce the export size and maintain video quality.

5. In the **Quality:** drop down list, select the exported image quality level.
6. In the **Resolution:** field, select a resolution for the video image. You can manually enter the resolution or click the drop down arrow to select a standard resolution.

   NOTE: The Resolution: field automatically maintains the image aspect ratio.
7. To automatically divide the export into separate files, select the **Split file into sizes of:** check box, then select one of the options from the drop down list, or manually enter the size of each file in MB.

   This option allows you to export smaller files for storing in a flash drive or on optical media.

   This setting is automatically disabled if you choose to burn the export to disc because the system auto-detects the disc size.
8. Select the **Skip recording gaps** check box to avoid pauses in the video caused by gaps in the recording.
9. Select the image overlays you want: **Timestamp**, **Camera name**, and **Camera location**.

   Select the **Video Analytics Activity** overlay to include video analytics bounding boxes with the video. These boxes cannot be hidden or removed from the exported video.
10. Enter the **Time Range** you want to export. The **Time Range** is highlighted on the Timeline by black time range markers. You can also drag the time range markers to modify the time range.
11. Set the export image rate:

Option	Description
Export at _ image rate	Select this option to control how many images per second are exported. For example, the video is streaming at 30 images per second. If you select **1/2**, only 15 images for that second will be exported.
Export one image every _ min _sec	Select this option to control the time between each exported video image. For example, if you enter *5* min. *0* sec., only one image will be exported for every 5 minutes of video.

12. Click **Change Image Region...** to only export part of the video image. In the **Change Image Region...** dialog box, move and resize the green overlay to select the region you want to export, then click **OK**. Only areas highlighted in green will be exported.
13. Click **Display Adjustments...** to adjust the **Gamma:**, **Black Level:** and/or **White Level:**.
14. Click one of the following:

- **Start Export**: to save the file locally.
    - In the Save As dialog box, name the export file and click **Save**.
- **Burn to Disc**: to burn the file directly to disc media.

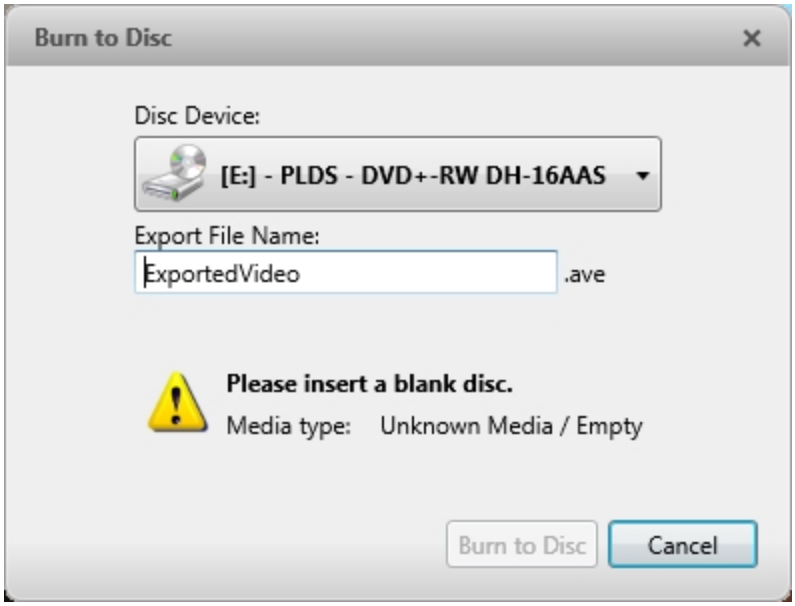


Figure 28: The Burn to Disc Dialog Box

a. When the dialog box appears, insert a disc and select the media burning drive.

b. Name the export file. The file name is automatically given a numbered suffix to help identify which file you are playing if the export spans multiple discs.

c. Click **Burn to Disc** to start the export. If this button is disabled, the disc may be corrupt or full.

d. Monitor the export progress to see if extra discs are required. When a disc is full, the export automatically pauses and you are asked to insert a new disc. After you insert a new disc, click **Resume Export**.

The number of discs required to export a video varies widely depending on the type of camera and disc used. Video is stored on the server with minimal compression to maximize the function of Avigilon's HDSM technology, so the size of an export can be quite large due to the camera's high megapixel resolution and frame rate.

Generally, if you export a 2 minute video from a 2MP H.264 HD camera into uncompressed AVI format, you will export a 2.7 GB file. If you select an **Encoder:** format and compress the video, you can export a 224 MB video at high quality. It is recommended that you always select an Encoder: format for AVI export to help significantly reduce the file size.

To further reduce the file size you can select a lower quality setting, lower the export frame rate, reduce the video resolution, or focus the export on a specific image region. Be aware that reducing each of the available settings too much may cause the export to be blurry or missing frames.

If it is important to have a high quality and full frame rate export, it is recommended that you use the AVE export format instead. AVE export intelligently compresses the video to create a smaller export file while

maintaining video data so that you can search, re-export video, and authenticate the video against tampering through the Avigilon Control Center Player software.

15. When the export is complete, click **OK**.

Exporting a Print Image

You can export a frame of video directly to your printer or as a PDF, and include notes related to the image.

To print a photo of the video you are currently watching, take a snapshot. For more information, see **Exporting a Snapshot of an Image**.

1. In the New Task menu, click  . The Export tab opens.

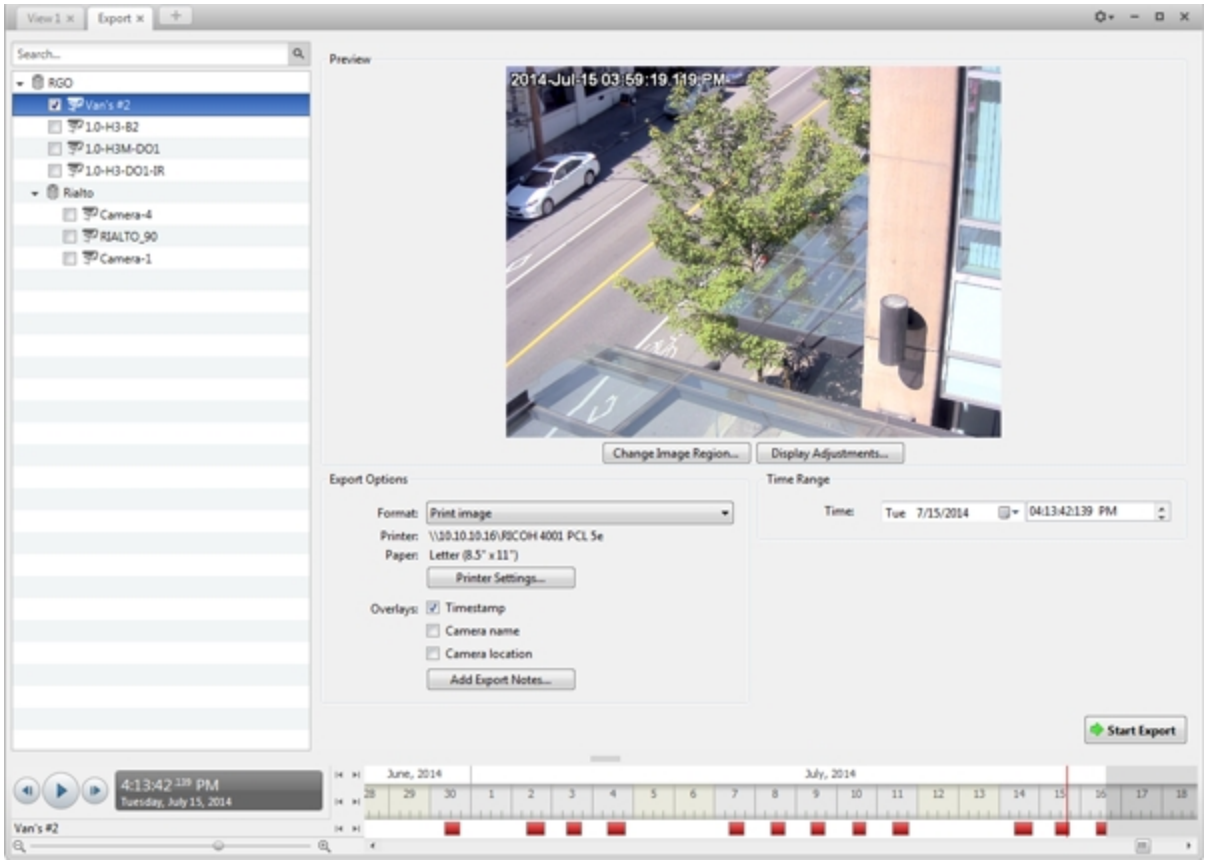


Figure 29: Export tab for print image export

2. In the **Format:** drop down list, select **Print image** or **PDF file**.
3. In the System Explorer, select the camera video you want to export.
4. (Print Image Only) Click **Printer Settings...** to change the printer and paper size that the image is printed on.
5. Select the image overlays you want: **Timestamp**, **Camera name**, and **Camera location**.

6. Click **Add Export Notes...** to add notes about the exported image. The notes are added below the image.

7. In the **Time Range** box, enter the exact date and time of the video image you want to export.
8. Click **Change Image Region...** to only export part of the video image. In the **Change Image Region...** dialog box, move and resize the green overlay to select the region you want to export, then click **OK**. Only areas highlighted in green will be exported.
9. Click **Display Adjustments...** to adjust the **Gamma:**, **Black Level:** and/or **White Level:**.
10. Click **Start Export**.
    - If you are exporting a Print image, the image is sent to the printer.
    - If you are exporting a PDF file, save the image.

    The Preview area displays the video you are exporting.
11. When the export is complete, click **OK**.

Exporting a Snapshot of an Image

You can export a snapshot of any image panel with video. When you export a snapshot, you are exporting what the image panel is currently displaying.

1. To export a snapshot, do one of the following:
    - In the image panel, click  .
    - Right-click the image panel and select **Save Snapshot**.

    The snapshot Export tab is opened, and the image you want to export is displayed.

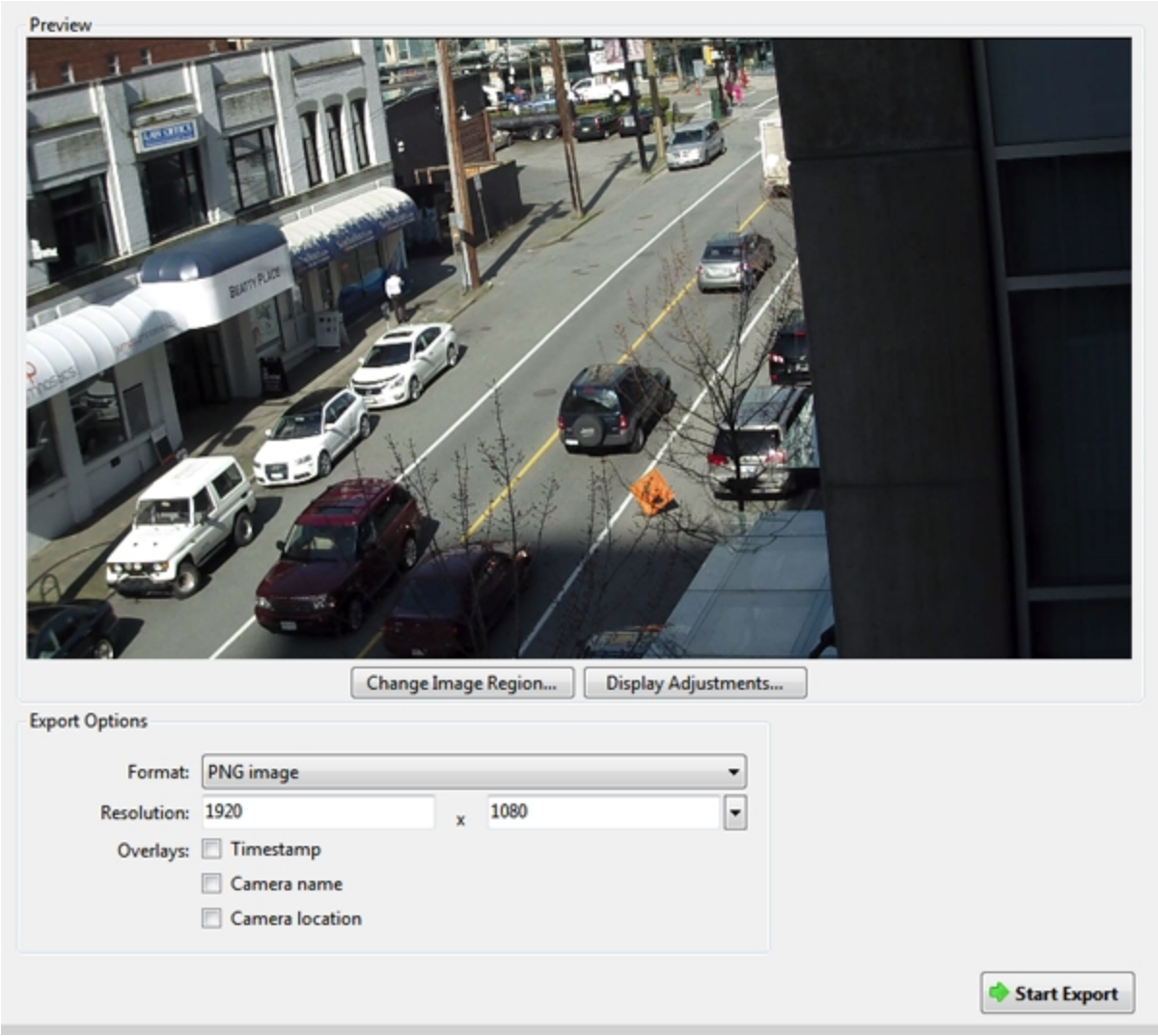


Figure 30: The Export tab for snapshot export

2. In the **Format:** drop down list, select an export format.
3. For the selected export format, define your preferences:

Format	Export options
Native **NOTE:** The Native format requires the Avigilon Control Center Player to view.	This is the recommended export format because the exported image maintains its original compression and can be authenticated against tampering in the Avigilon Control Center Player.
PNG image	1. In the **Resolution:** field, select a resolution for the video image. You can manually enter the resolution or click the drop down arrow to select a standard resolution. **NOTE:** The Resolution: field automatically maintains the image aspect ratio. 2. Select the image overlays you want: **Timestamp**, **Camera name**, and **Camera location**.

Format	Export options
	3. Click **Change Image Region...** to only export part of the video image. In the **Change Image Region** dialog box, move and resize the green overlay, then click **OK**. Only areas highlighted in green are exported. 4. Click **Display Adjustments...** to adjust the **Gamma:**, **Black Level:**, and/or **White Level:**.
JPEG image	1. In the **Quality:** drop down list, select the exported image quality level. 2. Set the image **Resolution:**. 3. Select the image overlays you want. 4. Click **Change Image Region...** to only export a part of the video image. 5. Click **Display Adjustments...** to modify the image quality.
TIFF image	1. Set the image **Resolution:**. 2. Select the image overlays you want. 3. Click **Change Image Region...** to only export a part of the video image. 4. Click **Display Adjustments...** to modify the image quality.
Print image	1. Click **Printer Settings...** to change the selected printer and paper size. 2. Select the image overlays you want. 3. Click **Add Export Notes...** to add notes about the exported image. The notes are printed below the image. 4. Click **Change Image Region...** to only export a part of the video image. 5. Click **Display Adjustments...** to modify the image quality.
PDF file	1. Select the image overlays you want. 2. Click **Add Export Notes...** to add notes about the exported image. 3. Click **Change Image Region...** to only export a part of the video image. 4. Click **Display Adjustments...** to modify the image quality.

4. Click **Start Export**.
5. In the Save As dialog box, name the export file and click **Save**. If you are printing the snapshot, the image is sent to your printer instead.

   The Preview area displays the snapshot you are exporting.
6. When the export is complete, click **OK**.

Exporting Still Images

Video can be exported as a series of still PNG images, JPEG images, or TIFF images. When you export a series of still images, you are exporting each frame of video as an independent file.

If you only want one photo of the video you are watching, take a snapshot. For more information, see **Exporting a Snapshot of an Image**.

1. In the New Task menu, click  . The Export tab opens.

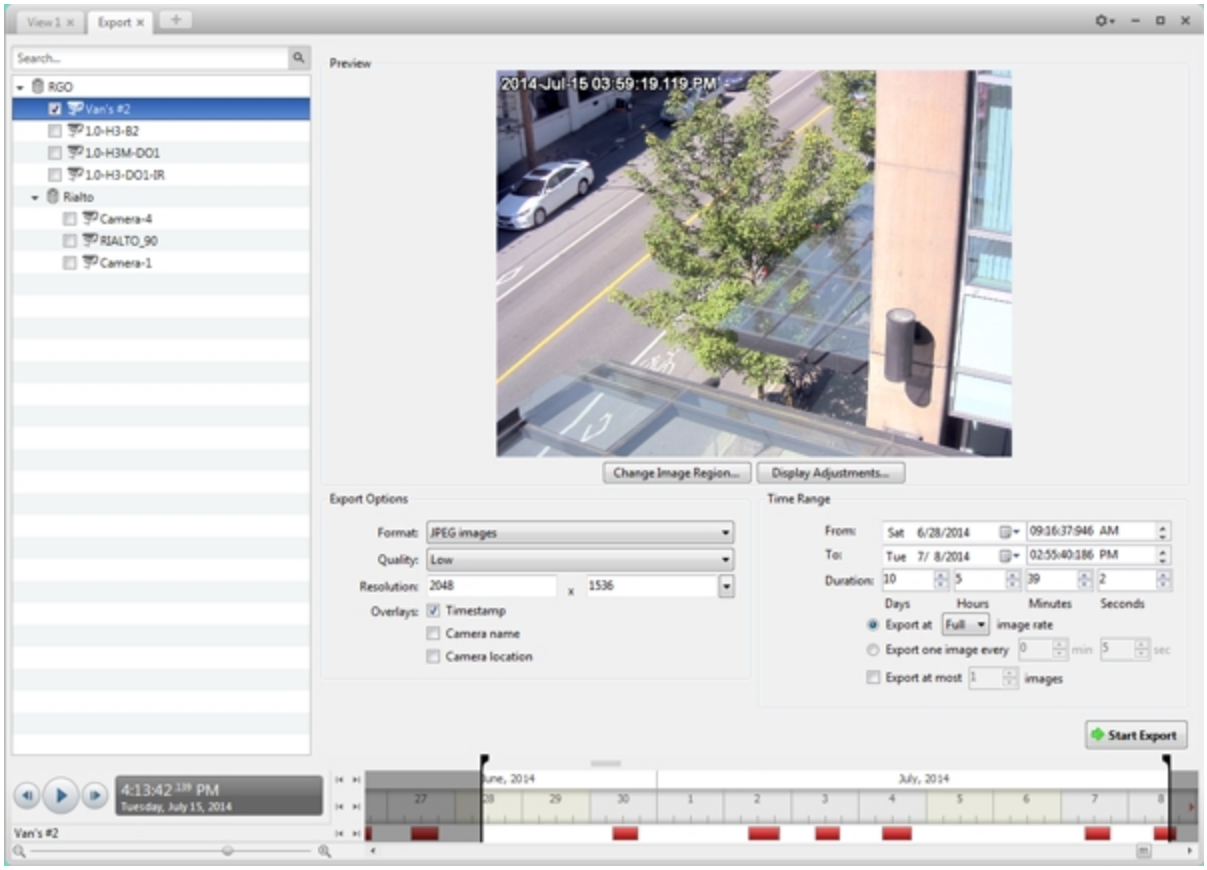


Figure 31: Export tab for still image export

2. In the **Format:** drop down list, select **PNG images**, **JPEG images**, or **TIFF images**.
3. In the System Explorer, select the camera video you want to export.
4. (JPEG only) In the **Quality:** drop down list, select the exported image quality level.
5. In the **Resolution:** field, select a resolution for the video image. You can manually enter the resolution or click the drop down arrow to select a standard resolution.

   NOTE: The Resolution: field automatically maintains the image aspect ratio.
6. Select the image overlays you want: **Timestamp**, **Camera name**, and **Camera location**.
7. Enter the **Time Range** you want to export. The **Time Range** is highlighted on the Timeline by black time range markers. You can also drag the time range markers to modify the time range.

8. Set the export image rate:

Option	Description
Export at _ image rate	Select this option to control how many images per second are exported. For example, the video is streaming at 30 images per second. If you select **1/2**, only 15 images for that second will be exported.
Export one image every _ min _sec	Select this option to control the time between each exported video image. For example, if you enter *5* min. *0* sec., only one image will be exported for every 5 minutes of video.

9. To limit the number of images that are exported, select the **Export at most _ images** check box and enter a number.
10. Click **Change Image Region...** to only export part of the video image. In the **Change Image Region...** dialog box, move and resize the green overlay to select the region you want to export, then click **OK**. Only areas highlighted in green will be exported.
11. Click **Display Adjustments...** to adjust the **Gamma:**, **Black Level:** and/or **White Level:**.
12. Click **Start Export**.
13. In the Save As dialog box, name the export file and click **Save**.

    The Preview area displays the video you are exporting.
14. When the export is complete, click **OK**.

Exporting WAV Audio

If you want to export audio with video, simply export the video in Native or AVI format. Any audio that is linked to the video is automatically included in the export file.

This procedure exports the audio alone.

1. In the New Task menu, click  . The Export tab opens.

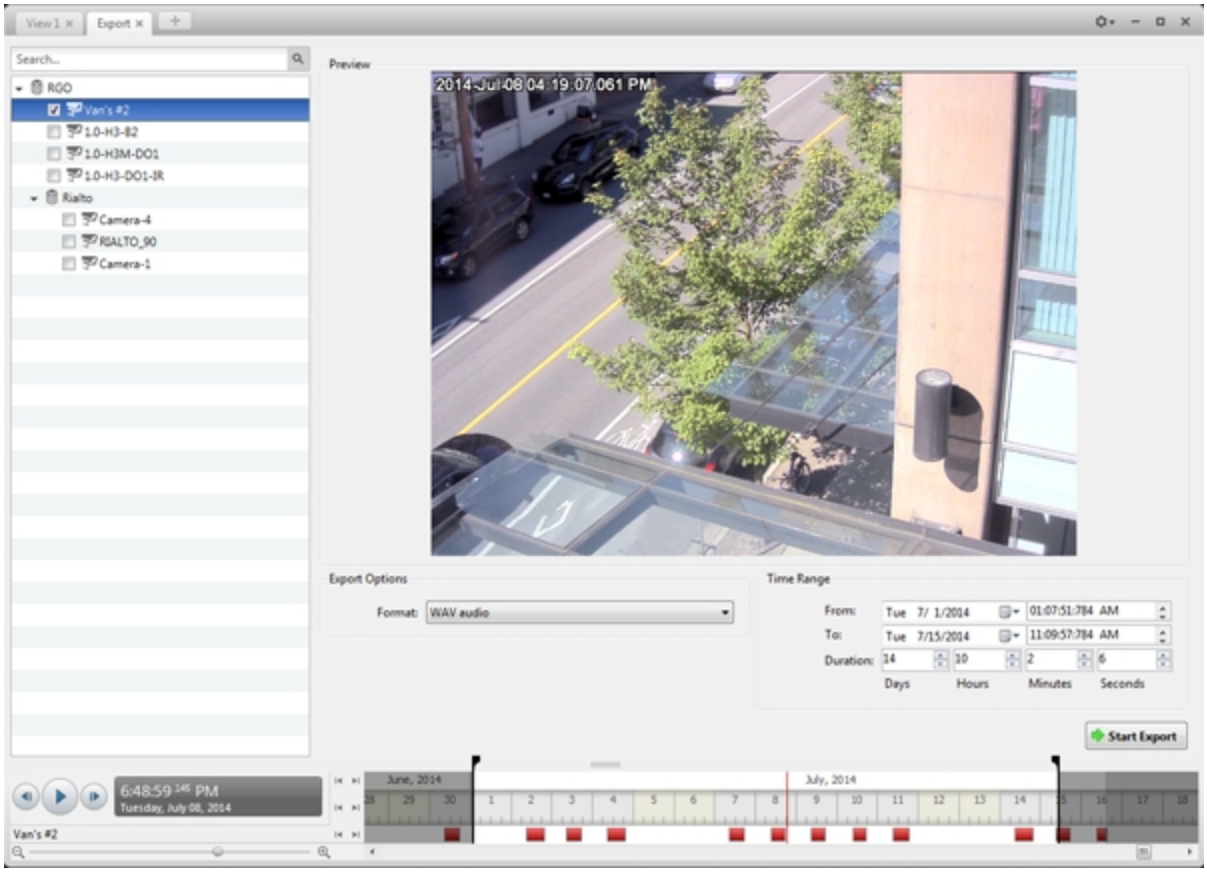


Figure 32: Export tab for audio export

2. In the **Format:** drop down list, select **WAV audio**.
3. In the System Explorer, select the camera that the audio is linked to.
4. Enter the **Time Range** you want to export. The **Time Range** is highlighted on the Timeline by black time range markers. You can also drag the time range markers to modify the time range.
5. Click **Start Export**.
6. In the Save As dialog box, name the export file and click **Save**.

   The Preview area displays the video linked to the audio you are exporting.
7. When the export is complete, click **OK**.

Backup

If you need to export a large amount of camera video, it is faster to back up the content into Avigilon Backup (AVK) format. AVK files can be opened in the Avigilon™ Control Center Player and re-exported as needed.

It is recommended that you export video of individual events and back up video for your archives. For more information, see **Export**.

Be aware that you can only back up video if the option is enabled in the Avigilon Control Center Admin Tool. For more information, see *The Avigilon Control Center Server User Guide*.

Backing Up Recorded Video On Demand

If you want a copy of the recorded video in your system, use the backup feature. Video is always backed up in Avigilon Backup (AVK) format. You can review the backed up video in the Avigilon Control Center Player.

The backup files are stored in a backup folder set by the Avigilon™ Control Center Admin Tool. For information about changing the backup folder, see *The Avigilon Control Center Server User Guide*.

1. In the application window, click  >  .

   The Backup tab is displayed.

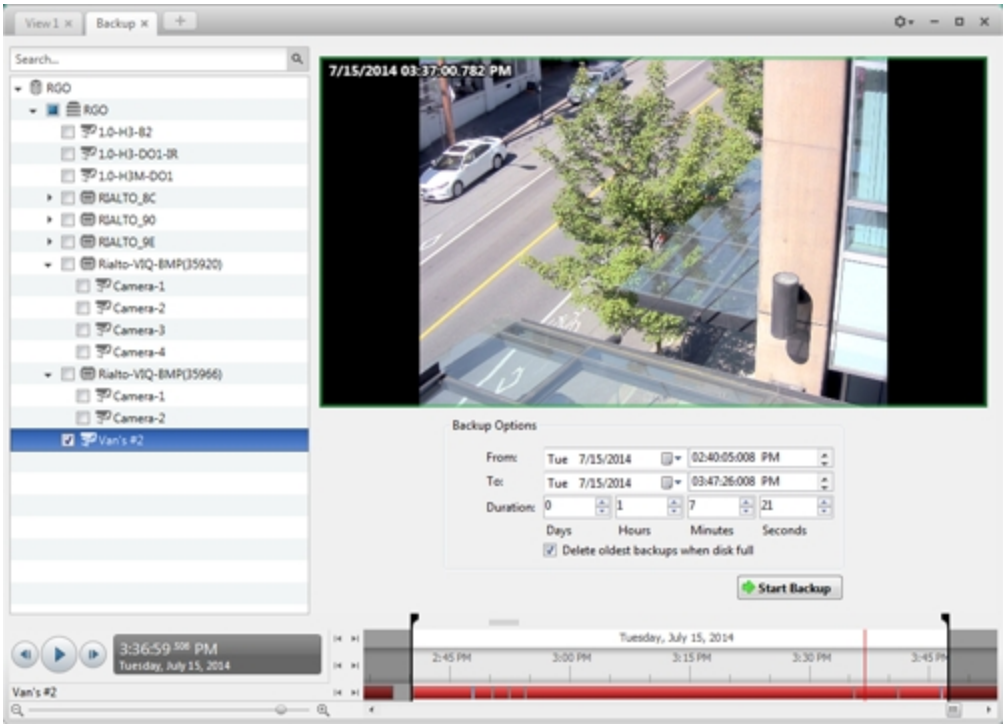


Figure 33: The Backup tab

2. In the System Explorer, select all the cameras you want to back up.

3. In the **Backup Options** area, set the time range you want to back up. The time range is highlighted on the Timeline by the black time range markers. You can also drag the time range markers to change the time range.
4. Select the **Delete oldest backups when disk full** check box to allow the application to automatically overwrite old backup files when the backup folder is full.
5. Click **Start Backup**.
6. When the backup is complete, click **OK**.

This Page Left Intentionally Blank

Avigilon™ Control Center Enterprise Web Client User Guide

Version 5.4.2

Avigilon Corporation
http://www.avigilon.com

Revised: 2014-12-09

PDF-WEBCLIENT5-E-E-Rev1

Table of Contents

What is the Avigilon Control Center Web Client?

The Avigilon Control Center Web Client is a simplified, web-based version of the Avigilon Control Center Client software. The Web Client allows you to access any camera that is connected to a Control Center Server.

Through the Web Client you can monitor live and recorded video, and search or export events in the camera's recording history.

The Web Client can be accessed from any Internet Explorer browser (version 6+) that is connected to your local network.

For More Information

Visit Avigilon at **http://www.avigilon.com/** for additional product documentation.

The Avigilon Training Center

The Avigilon Training Center provides free online training videos that demonstrate how to set up and use the Avigilon Surveillance System. Register online at the Avigilon Partner Portal site to begin: **http://avigilon.force.com/login**

Support

For additional support information, visit **http://avigilon.com/support-and-downloads/**. The Avigilon Partner Portal also provides self-directed support resources - register and login at **http://avigilon.force.com/login**.

Regular Avigilon Technical Support is available Monday to Friday from 12:00 a.m. to 6:00 p.m. Pacific Standard Time (PST):

- North America: +1.888.281.5182 option 1
- International: +800.4567.8988 or +1.604.629.5182 option 1

Emergency Technical Support is available 24/7:

- North America: +1.888.281.5182 option 1 then dial 9
- International: +800.4567.8988 or +1.604.629.5182 option 1 then dial 9

E-mails can be sent to: **support@avigilon.com**.

Upgrades

Software and firmware upgrades will be made available for download as they become available. Check **http://avigilon.com/support-and-downloads/** for available upgrades.

Feedback

We value your feedback. Please send any comments on our products and services to **feedback@avigilon.com**

Accessing the Control Center Web Client

NOTE: You cannot modify any system settings through the Control Center Web Client.

To access the Web Client, you need the IP address and port number of the server in your Site. The IP address is listed in the server's Setup tab in the Avigilon Control Center Client. The port number can be found in the Admin Tool under **Settings > Network**.

If you are running a multi-server Site, you only need to access one of the servers in your Site to have access to all the available cameras.

For more information, see the *Avigilon Control Center Client User Guide*.

1. To access the Web Client, open Internet Explorer (version 6+) and enter the address of your Web Client in the following format:

   http://<*server ip address*>:<*port number*>/

   (For example, http://192.168.2.62:38880/)

   If you have not accessed the Web Client before, you may be prompted to install the required plug-in software before the Web Client will open.

2. When the login screen appears, enter your username and password for the Site.

The Web Client will open in your browser, and you can access the video and cameras that are connected to the server.

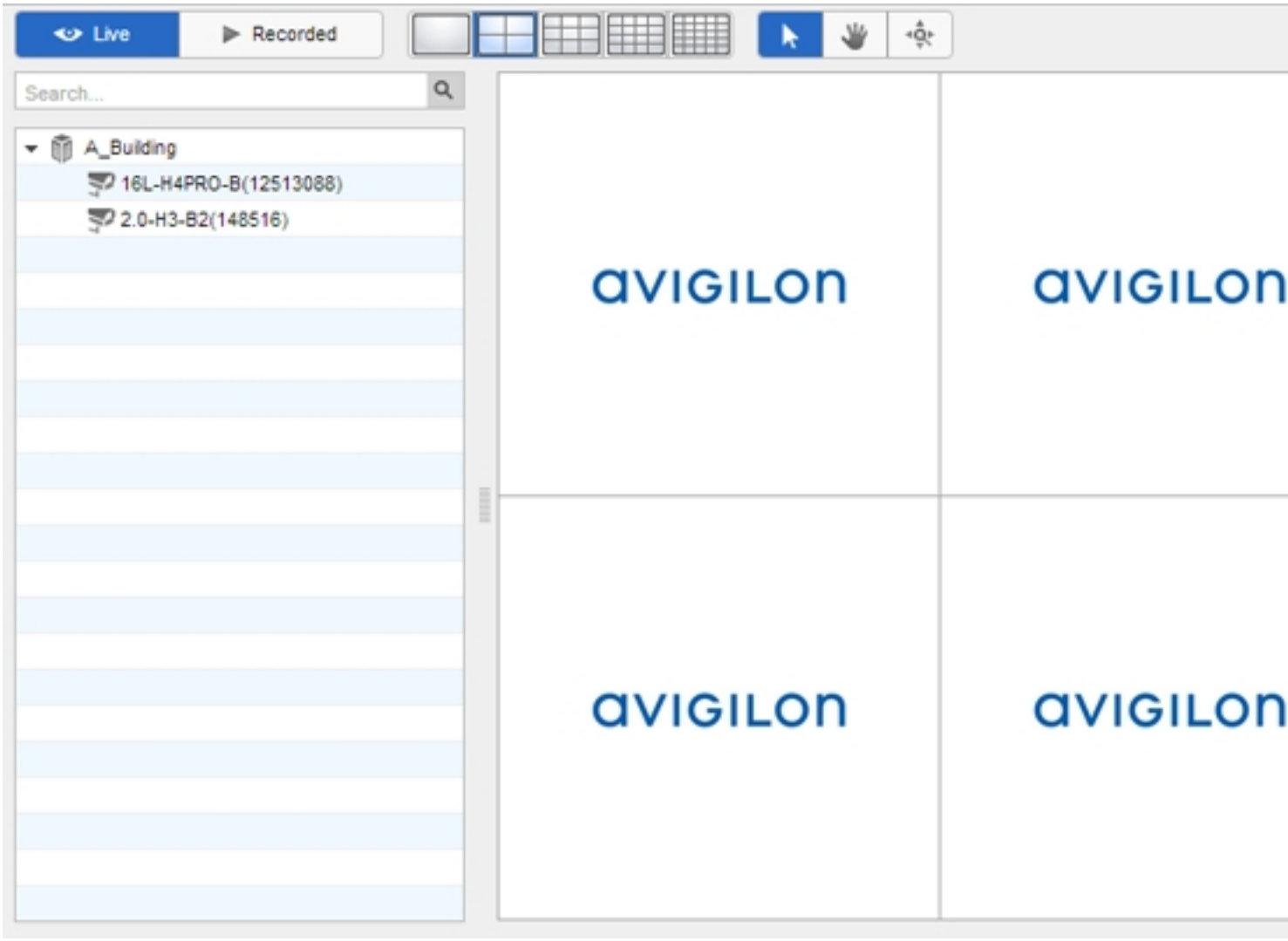


Figure 1: The Avigilon Control Center Web Client

What are Views?

A View tab is where you watch camera video. Inside the View tab is a set of image panels that allows you to organize how video is displayed.

You can arrange image panels into different layouts to take advantage of different camera angles and save View layouts that you like.

You can share Views with other users during investigations, and organize how video is displayed across multiple monitors.

For more information on controlling live and recorded video, see **Monitoring Video**.

Adding and Removing a View

View tabs allow you to customize how you monitor video. You can open a new View in the browser to see more video. Views can also be removed as required.

If you want to make use of a large number of monitors, like a video wall, see **Virtual Matrix**.

To...	Do this...
Open a new View tab	Click + >  .
Close a View tab	On the View tab, click  .

View Layouts

You can organize how video is displayed through View layouts. You can choose to display video in 1 - 64 image panels. You can also customize the shape of image panels to accommodate cameras that are installed vertically to capture long hallways.

There are 10 pre-configured layouts that you can edit to fit your needs.

Selecting a Layout for a View

You can organize how video is displayed by selecting a View layout. The figure below shows the default View layouts.

- On the toolbar, select  , then select one of the following layout options.

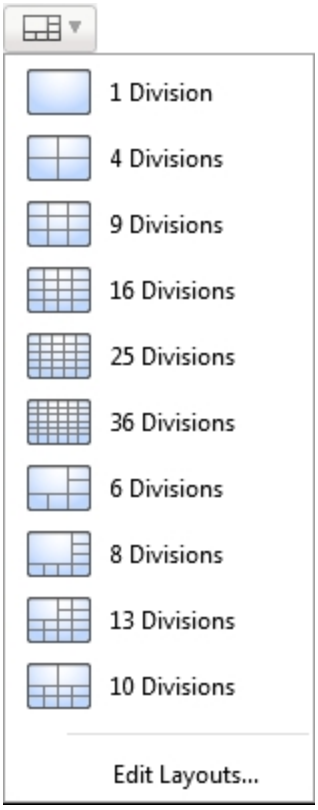


Figure 2: Layouts in the toolbar

Editing a View Layout

If the default View layouts do not fit your surveillance requirements, you can customize a View layout.

1. On the toolbar, select  > **Edit Layouts...**.

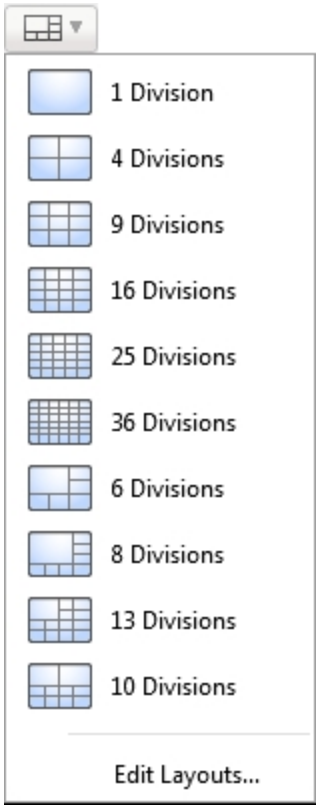


Figure 3: Layouts in the toolbar

2. In the Edit Layouts dialog box, select the layout you want to change.
3. Enter the number of **Columns:** and **Rows:** you want in your layout.

4. In the layout diagram, do any of the following to further customize the layout.

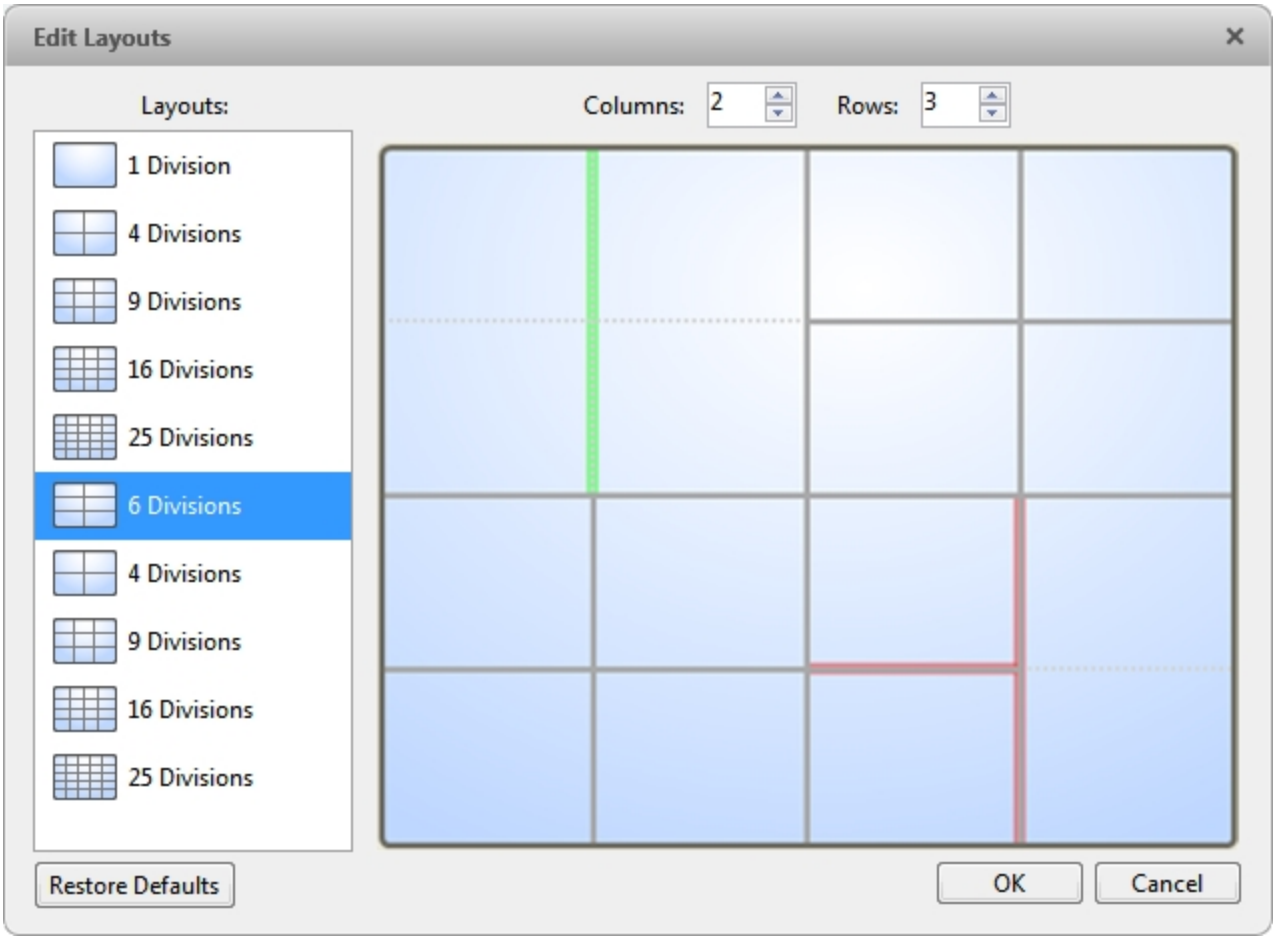


Figure 4: The Edit Layouts dialog box

- To create a larger image panel, select a gray line to delete the border between two image panels. When a line is highlighted in red, the line can be deleted.
- To restore an image panel, select a dotted line to divide a larger image panel into two. When a dotted line is highlighted in green, the line can be restored.
- To restore all default View layouts, click **Restore Defaults**. All custom layouts in the Layouts: list will be replaced.

NOTE: You can only add or subtract lines to create a rectangular shape.

5. Click **OK** to save your changes. The previous View layout has been replaced with your customized layout.

Tip: The keyboard commands used to access View layouts are linked to the layout's position in the Layouts: list. For example, if your custom layout is placed at the top of the Layouts: list (layout 1), you can press Alt + 1 to use that layout.

Making a View Full Screen

You can maximize a View to fill an entire monitor screen.

- On the toolbar, click  .

Ending Full Screen Mode

- While the View is in full screen mode, click  .

Cycling Through Views

If you have multiple Views open, you can cycle through the View tabs by displaying each one for a few seconds. This is useful when monitoring a large number of cameras.

- To activate the Cycle Views feature, click  .

Saved Views

Once you have set up a View you like, you can save the View to share with other users in the Site. A saved View remembers the current View layout, the cameras displayed in each image panel, and the image panel display settings.

NOTE: You can only add and view cameras that are connected to the server that you are accessing through the Web Client.

Saving a View

1. In the toolbar, click  .
2. In the dialog box which appears, complete the following:

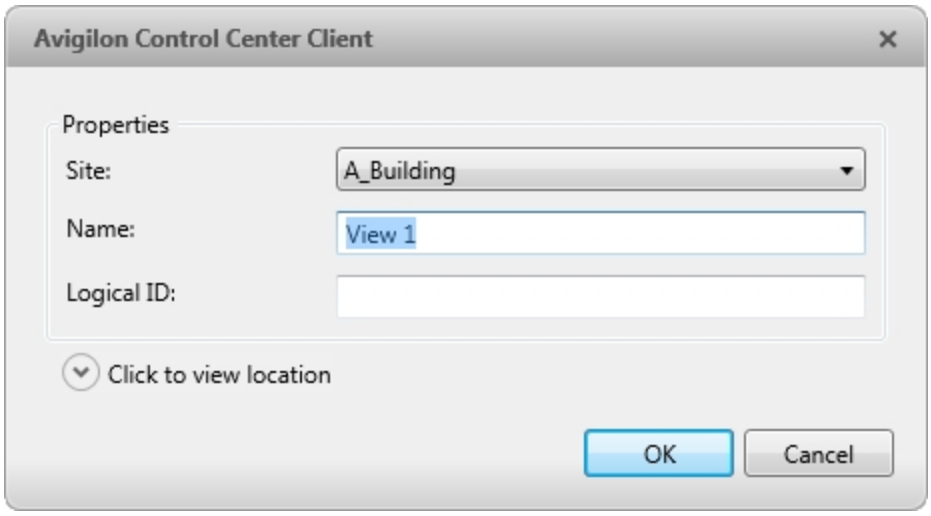


Figure 5: Edit View dialog box

a. Select the Site that the View should be added to.

b. Give the saved View a name.

c. Assign a **Logical ID:** to the View. The logical ID is a unique number that is used to open the saved View through keyboard commands.

d. Click  to choose where the saved View appears in the System Explorer.

- If your Site includes virtual sub-sites, select a location for the saved View. The list on the right updates to show what is stored in that directory.
- In the Site directory, drag the saved View up and down to set where it is displayed.

e. Click **OK**.

Your saved View is added to the System Explorer under the selected Site. You can now manage the saved View as a part of your Site.

Opening a Saved View

Do one of the following

- In the System Explorer, double-click the saved View.
- In the System Explorer, right-click the saved View and select **Open**.
- Drag the saved View from the System Explorer to the current View in the application or new window.

Editing a Saved View

1. Open a saved View.
2. Make any required changes to the View tab.
3. Click  .

Renaming a Saved View

1. In the System Explorer, right-click the saved View and select **Edit...**.
2. In the Edit View dialog box, enter a new name or logical ID and click **OK**.

Deleting a Saved View

1. In the System Explorer, right-click the saved View and select **Delete**.
2. In the confirmation dialog box, click **Yes**.

Collaborating

If you want to show another user an incident or need help investigating an event, you can share your current View with another user. You will both be able to control the View and show each other your findings.

Sharing a View

1. In the toolbar, click  .
2. In the following dialog box, select the user you want to collaborate with, then click **OK**.

   The users are listed by username and computer name. The computer name is used to help you identify a specific user if the username is shared by several people. Only users who are currently logged in to the Site are displayed.

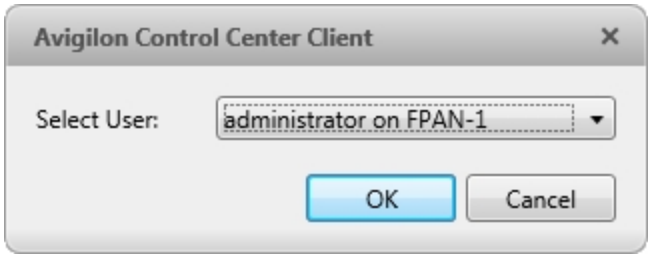


Figure 6: The Select User: dialog box

   a. The user you select will see a pop-up message with your invitation to collaborate and may choose to accept or decline.

   b. You will receive a pop-up message with the user's response to your invitation.

      If they say *Yes*, the View you are looking at is automatically opened as a new tab in your collaborator's window.

3. Repeat this procedure to collaborate with multiple users.

While you are collaborating, any changes made to the current View by a collaborator are shared with the other collaborators. Anything that you can do in a standard View can be done in a shared View.

Leaving a Shared View

- To leave a shared View, just close the View tab. The remaining users stay in collaboration mode.

Virtual Matrix

The optional Virtual Matrix feature allows you to control the View displayed on multiple monitors, or a video wall, from any instance of the application. To use this feature, the Virtual Matrix software must be installed on the system that all the displays are connected to.

Be aware that you will only be able to see and add cameras that are connected to this server.

A copy of the Virtual Matrix software can be downloaded from the Avigilon website.

For more information about the Virtual Matrix software, see *The Avigilon Control Center Virtual Matrix User Guide*.

Once the Virtual Matrix has been installed and loaded, the monitors connected to the system are automatically added to a Site. All monitors linked by the Virtual Matrix software are displayed in the System Explorer as followed by the monitor name.

Adding and Removing Virtual Matrix Monitors

You can only add or remove Virtual Matrix monitors through the Virtual Matrix software.

For more information, see the *Avigilon Control Center Virtual Matrix User Guide*.

Controlling Virtual Matrix Monitors

In the System Explorer, each represents a View that is displayed on a connected Virtual Matrix monitor.

To control what is displayed on each Virtual Matrix monitor, you need to open the monitor:

- In the System Explorer, right-click and select **Open**.
- Double-click or drag from the System Explorer to the current View.

The Virtual Matrix monitor is opened in a new tab and can be controlled like any View -- you can change the View layout, control video display, and use any active PTZ controls. The changes you make should automatically appear on the Virtual Matrix monitor.

When you are done, you can close the Virtual Matrix monitor tab. The monitor will continue to display the View you have configured until you make new changes or the Virtual Matrix is shut down.

Monitoring Video

Inside a View tab, you can monitor and control video from multiple cameras. Once you open a camera in a View tab, you can control the camera's live and recorded video stream. You also have access to the camera's PTZ controls, connected audio devices, digital outputs, and other playback settings.

To organize how video is displayed in the View tab, see **What are Views?**.

NOTE: Some features are not displayed if the server does not have the required license, or if you do not have the required user permissions.

Adding and Removing Cameras in a View

To monitor video, add a camera to a View. Camera video can be removed from a View at any time.

Adding a Camera to a View

Do one of the following:

- Drag the camera from the System Explorer to an empty image panel in the View tab.
- Double-click a camera in the System Explorer.
- In the System Explorer, right-click the camera and select **Add To View**.

  The camera is added to the next empty image panel in the View layout.

Tip: You can drag the same camera to multiple image panels to watch the video at different zoom levels.

Removing a Camera from a View

Do one of the following:

- Right-click the image panel and select **Close**.
- Inside the image panel, click  .

Viewing Live and Recorded Video

NOTE: Some features are not displayed if the server does not have the required license, or if you do not have the required user permissions.

When you monitor video, you can choose to watch live and recorded video in the same View, or only one type of video per View.

Once you've added cameras to the View, perform the following:

- To switch all of the image panels in the View between live and recorded video, click either  **Live** or  **Recorded** on the toolbar.

- To switch individual image panels between live and recorded video, right-click the image panel and select either **Live** or **Recorded**.

Image panels displaying recorded video have a **green** border.

Zooming and Panning in a Video

Use the zoom and pan tools to focus on specific areas in the live or recorded video stream.

Using the Zoom Tools

There are two ways to digitally zoom in and zoom out of a video image:

- Move your mouse over the video image, then rotate your mouse wheel forward and backward.
- On the toolbar, select  or  , then click the image panel until you reach the desired zoom depth.

Using the Pan Tools

There are two ways to pan through the video image:

- Right-click and drag inside an image panel
- On the toolbar, select  , then click and drag the video image in any direction inside the image panel.

Maximizing and Restoring an Image Panel

You can maximize an image panel to enlarge the video display.

Maximizing an Image Panel

Do one of the following:

- Right-click an image panel and select **Maximize**.
- Inside the image panel, click  .
- Double-click the image panel.

Restoring an Image Panel

In a maximized image panel, do one of the following:

- Right-click the maximized image panel and select **Restore Down**.
- Inside the image panel, click  .
- Double-click the image panel.

Making Image Panel Display Adjustments

You can change the image panel display settings to bring out video details that are hard to see with the image panel's default settings.

1. Right-click an image panel and select **Display Adjustments...**.

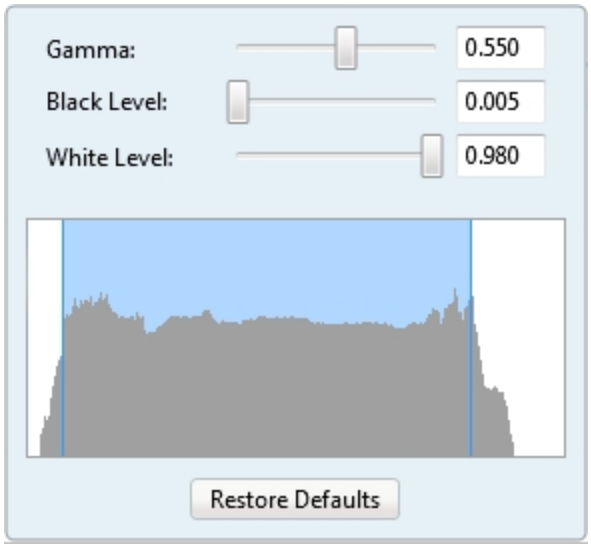


Figure 7: The Display Adjustments... panel

   The Display Adjustments... settings are displayed in a floating pane immediately beside the image panel.

2. Move the sliders to adjust the **Gamma:**, **Black Level:** and **White Level:**.

   The image panel displays a preview of your changes.

3. Click **Restore Defaults** to clear your changes.

Listening to Audio in a View

If there is an audio input device linked to a camera, the button is displayed in the image panel when you watch the camera's video. To listen to the streaming audio, make sure there are speakers connected to your computer. By default the audio is muted.

The camera's microphone must be enabled before you can listen to any audio. The button is not displayed if the microphone is disabled.

To control audio playback, do any of the following:

- In the lower-right corner of the image panel, click to mute or activate the audio.
- Move the slider to change the volume.

Controlling Live Video

Broadcasting Audio in a View

If there are speakers linked to a camera, the button is displayed in the image panel when you watch the camera's video. The button allows you to broadcast your verbal response to what is occurring in the video, like a Public Address (P.A.) system.

The camera's speakers must be enabled before you can broadcast any audio. The button is not displayed if the speakers are disabled.

- To broadcast audio, hold and speak into your microphone. The red bar moves to show the microphone's audio input levels. If the level is low, speak louder or adjust the microphone volume in the Windows Control Panel.
- Release the button to stop the broadcast.

Using Instant Replay

To review an event that just occurred, you can immediately access recently recorded video through the instant replay feature.

- Right-click the image panel and select one of the instant replay options:
  - **Replay - 30 Seconds**
  - **Replay - 60 Seconds**
  - **Replay - 90 Seconds**

The image panel immediately plays back the camera's most recently recorded video.

PTZ Cameras

PTZ cameras can be controlled through the image panel on-screen controls or by using the tools in the PTZ Controls pane.

Some tools and features may not be displayed if they are not supported by your camera.

Controlling PTZ Cameras

Pan, Tilt, Zoom (PTZ) controls allow you to control cameras with PTZ features. You can control a PTZ camera by using the on-screen controls or by using the tools in the PTZ Controls pane.

NOTE: For video analytics devices, classified object detection only works when the camera is in its Home position.

1. In the toolbar, click . PTZ controls are now enabled in image panels that are displaying PTZ video.
2. In the image panel, click .

   The PTZ Controls are displayed in a floating pane immediately beside the image panel.

NOTE: The controls may appear differently depending on the camera. Some options are disabled or hidden if they are not supported by the camera.

Figure 8: The PTZ Controls

3. To pan or tilt, do one of the following:
   - In the image panel, drag your mouse from the center to move the camera in that direction. The farther the cursor is from the center of the image panel, the faster the camera will move.
   - If the camera supports Click to Center, click anywhere on the image panel to center the camera to that point.

Figure 9: PTZ On-screen controls

4. Use the other PTZ controls to perform any of the following:

To...	Do this...
Zoom	• Click to zoom in.

To...	Do this...
	• Click  to zoom out. • Click the image panel and use the mouse scroll wheel to zoom in and out. • If the camera supports Drag to Zoom, click and drag to create a green box to define the area you want to zoom in and see. • Right-click the image panel and select **Zoom Out Full**.
Control the iris	• Click  to close the iris. • Click  to open the iris.
Control the focus	• Click  to focus near the camera. • Click  to focus far from the camera.
Program a PTZ preset	1. Move the camera's field of view into position. 2. In the **Presets** drop down list, select a number then click  . 3. In the dialog box, enter a name for the preset. 4. Select the **Set as home preset** check box if you want this to be the camera's Home preset. 5. Click **OK**.
Activate a PTZ preset	Select a preset then click  .
Return to the Home preset position	If the PTZ camera supports a Home preset position, click  to return the camera to its Home position.
Program a PTZ pattern	1. In the PTZ Controls pane, select a pattern number and click  . 2. Use the PTZ controls to move the camera and create the pattern. 3. Click  to stop recording the pattern.
Activate a PTZ pattern	In the PTZ Controls pane, select a pattern number and click  . The pattern will repeat until the pattern is stopped or another pattern is run.
Program a PTZ tour	For more information, see **Programming PTZ Tours**.
Activate a PTZ tour	In the PTZ Controls pane, select a tour number and click  . The tour will repeat until stopped or until other PTZ controls are used.
Activate an auxiliary command	1. Select an aux command number and click  .

To...	Do this...
	2. Click  to turn off the auxiliary output.
Display the PTZ camera on-screen menu	1. Click  . 2. To move through the menu options, click any of the following: • Click  to move down the options. • Click  to move up the options. • Click  to confirm your selection. • Click  to cancel your selection.
Lock the PTZ controls	Click  . Other users will be unable to use the PTZ controls for this camera until you unlock the controls or log out.

Programming PTZ Tours

If the PTZ camera supports guard tours, the tours can be programmed through the PTZ controls pane. Tours allow the PTZ camera to automatically move between a series of preset positions, and can be set to pause at each preset for a specific amount of time for video monitoring.

NOTE: For video analytics devices, classified object detection only works when the camera is in its Home position.

1. Create all the PTZ presets you need for this tour.
2. In the PTZ Controls pane, select a tour number then click  . The Edit PTZ Tour dialog box is displayed.

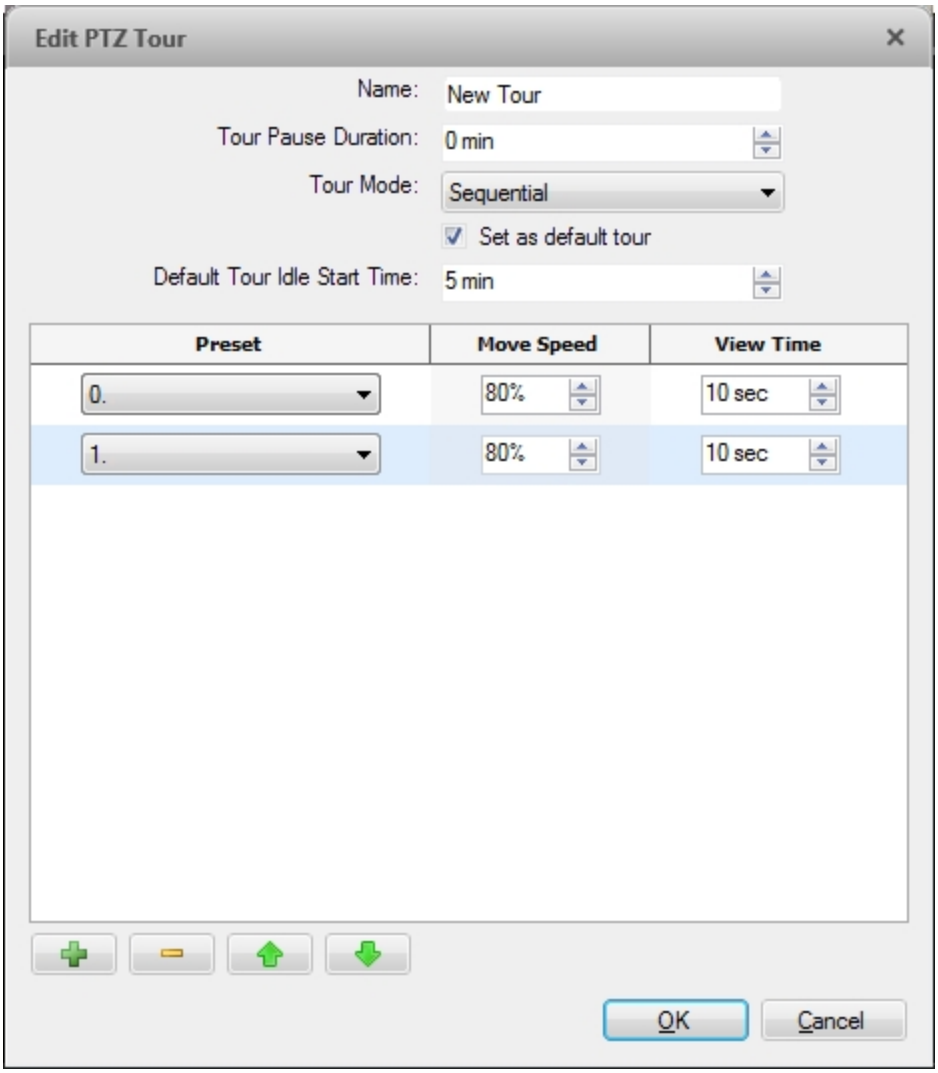


Figure 10: The Edit PTZ Tour dialog box

3. In the Edit PTZ Tour dialog box, give the tour a name.
4. In the **Tour Pause Duration:** field, enter the amount of time before a tour repeats. Tours repeat until manually stopped, or until other PTZ controls are used.
5. In the **Tour Mode:** drop down list, select one of the following:
    - **Sequential:** the PTZ camera will go to each preset in the set order.
    - **Random:** the PTZ camera will go to each preset in random order.
6. Select the **Set as default tour** check box if you want this tour to run automatically.
    - The **Default Tour Idle Start Time:** field is now enabled. Enter the amount of time the PTZ camera must be idle before this tour automatically starts.
7. To add a preset to the list, click .
    a. In the **Preset** column, select a preset from the drop down list.
    b. In the **Move Speed** column, enter how fast you want the PTZ camera to move to this preset. The

higher the %, the faster the camera moves.

c. In the **View Time** column, enter the amount of time you want the PTZ camera to stay at this preset position. The view time is 10 seconds by default.

d. Repeat step 7 until all the presets for this tour have been added.

8. To remove a preset, select the preset then click .
9. To re-order a preset, select the preset then click or . The preset order only affects tours that use Sequential mode.
10. Click **OK** to save the tour.

Triggering Manual Recording

Cameras are set to follow a recording schedule. If an event occurs outside the camera's recording schedule, you can click the record indicator icon to force the camera to record the event.

Camera Recording States

		
Recording	Recording triggered by an event	Not recording

Starting and Stopping Manual Recording

In an image panel that is displaying video, do either of the following:

- In the top-left corner of the image panel, click  to start manual recording.

  The recording indicator is highlighted in blue to show that the camera is recording. Manual recording continues until it is stopped or until the maximum manual recording time is reached.

- Click  to manually stop video recording.

Triggering Digital Outputs

While you monitor live video in an image panel, you can manually trigger any digital output that is connected to the camera.

To trigger a digital output:

1. Open the camera's live video in an image panel.
2. In the image panel, click  .
3. If there is more than one digital output linked to the camera, you will be prompted to select the digital output you want to trigger.

Monitoring Live POS Transactions

If a camera is linked to a point of sale (POS) transaction source, you can monitor live POS transactions while you monitor video from the linked camera.

1. Open the camera's video in an image panel.
2. In the image panel, click .

   NOTE: If the camera is not linked to a POS transaction source, the icon is not displayed.

   If there is more than one POS transaction source linked to the camera, you will be prompted to select one. The POS transactions are displayed in the next image panel.

   Each transaction is separated by date and time, and the most recent transaction is highlighted in blue.
3. To display cameras that are linked to the POS transaction source, click in the POS transaction image panel.

   If multiple cameras are connected to the POS transaction source, you will be prompted to select one.

Controlling Recorded Video

In this section are features that are only available while monitoring recorded video.

Playing Back Recorded Video

The Timeline displays when video was recorded and lets you control video playback.

The colored bars on the Timeline show the camera's recording history:

- A red bar shows the camera has recorded a motion event.
- A blue bar shows the camera has recorded video.
- White areas show periods of time during which the camera has not recorded any video.
- An yellow bar is a bookmark in the camera's recording history.

For more information about bookmarks, see **Bookmarking Recorded Video**.

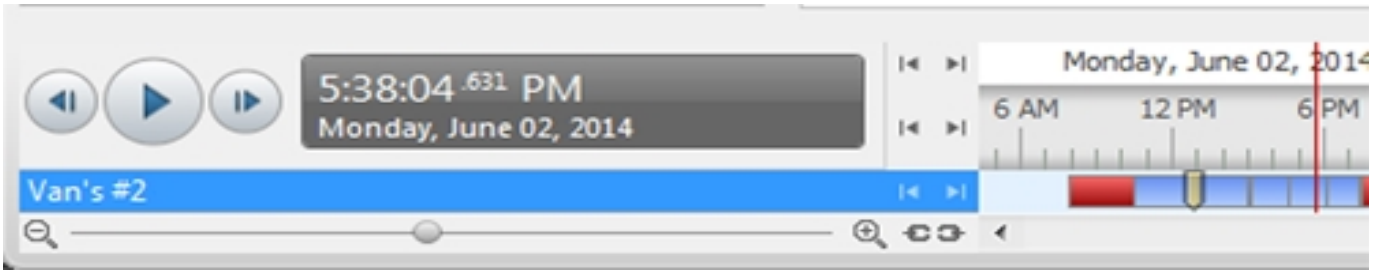
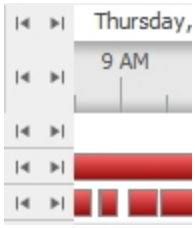
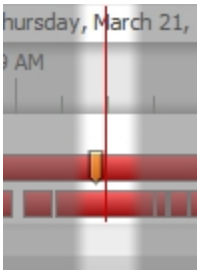


Figure 11: Playback controls on the Timeline

To...	Do this...
Select a playback time	• Click the dark gray date display and select a specific date and time. • Click a point on the Timeline.
Start playback	Click . • Click to fast forward. Tap the arrow again to increase the playback speed.

To...	Do this...
	• Click to rewind. Tap the arrow again to increase the playback speed. You can play the video up to eight times the original speed.
Stop playback	Click . • Click to step forward one frame. • Click to step backward one frame.
Jump forward or backward on the Timeline	 On the Timeline, click or to move to set points on the Timeline.
Zoom in or out of the Timeline	 • Move the slider on the bottom left to zoom in or out on the Timeline. • Place your mouse over the Timeline and use the scroll wheel to zoom in or out on the Timeline. You can zoom in to a quarter of a second, and zoom out to see years if recorded video exists.
Center the Timeline on the time marker	 Right-click the Timeline, and select **Center on Marker.**
Pan the Timeline	• Click and drag the time marker through the Timeline. • Move the horizontal scroll bar under the Timeline. • Right-click and drag the Timeline.

Bookmarking Recorded Video

You can add bookmarks to recorded video to help you find and review an event later. Bookmarked video can be protected against scheduled data cleanup so that the video is never deleted.

Adding a Bookmark

Tip: You can add a bookmark any time the Timeline is displayed.

1. Drag the time marker to where you want to start the bookmark, then right-click the Timeline and select **Add Bookmark**.

   The Edit Bookmark dialog box appears, and the bookmark time range is highlighted on the Timeline.

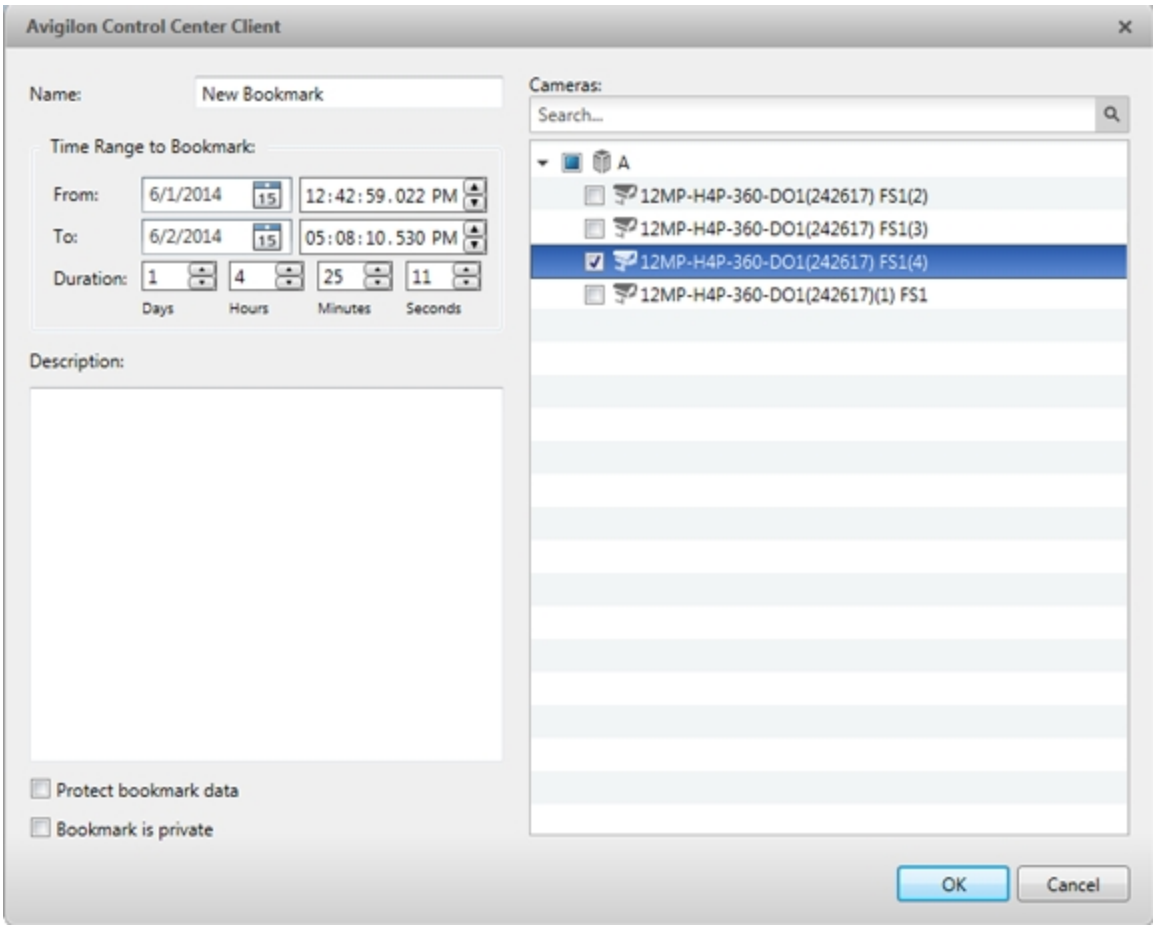


Figure 12: Edit Bookmark dialog box

2. Enter a **Name:** for the bookmark.
3. In the **Cameras:** pane, select all the cameras that need to be attached to this bookmark.

   NOTE: You can only bookmark multiple cameras from the same Site.
4. In the **Time Range to Bookmark:** area, enter the full duration of the bookmark.

   You can also move the black time range markers on the Timeline to adjust the time range.
5. In the **Description:** field, enter extra any information you want to include with the bookmark.
6. To protect the bookmark video from being deleted, select the **Protect bookmark data** check box.

   NOTE: Protected bookmarks are never deleted. Be aware that bookmarked videos take up space and can become the oldest video on the server.
7. To make the bookmark private, select the **Bookmark is private** check box. Private bookmarks are only visible to the user who marked the bookmark as private, and the system administrator. No one else will have access to the bookmark.
8. Click **OK**.

Exporting, Editing, or Deleting a Bookmark

1. Click the bookmark on the Timeline, then do one of the following:

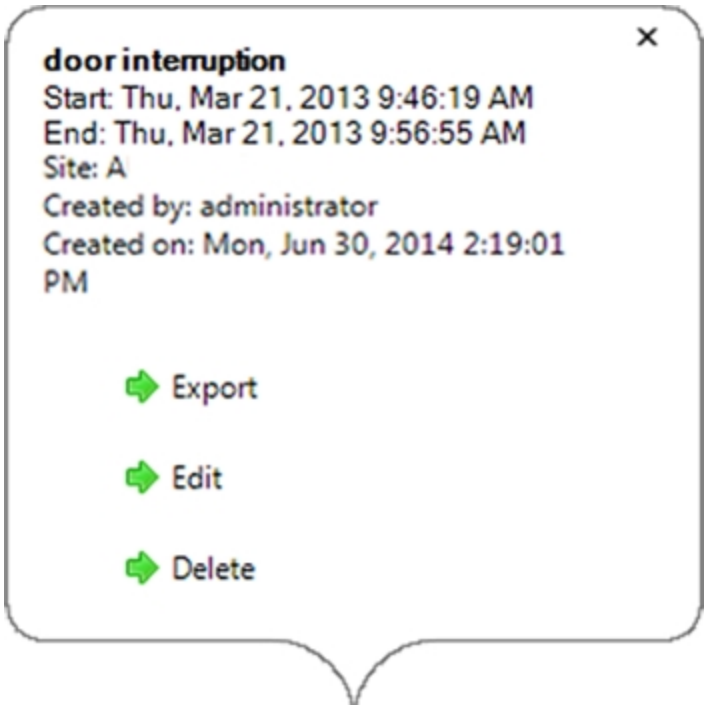


Figure 13: Pop-up Bookmark properties

To	Do this...
Export a bookmark	Click **Export**, then complete the Export tab.
Edit a bookmark	Click **Edit**, then make your changes.
Delete a bookmark	Click **Delete**. When the confirmation dialog box appears, click **Yes**.

When editing a bookmark, refer to **Adding a Bookmark** for details about the editable options.

When exporting a bookmark, refer to **Export** for information about the export options.

Reviewing License Plate Matches

If your system is configured to track specific license plates through the Watch List, you will be notified by a pop-up dialog box when matches are detected.

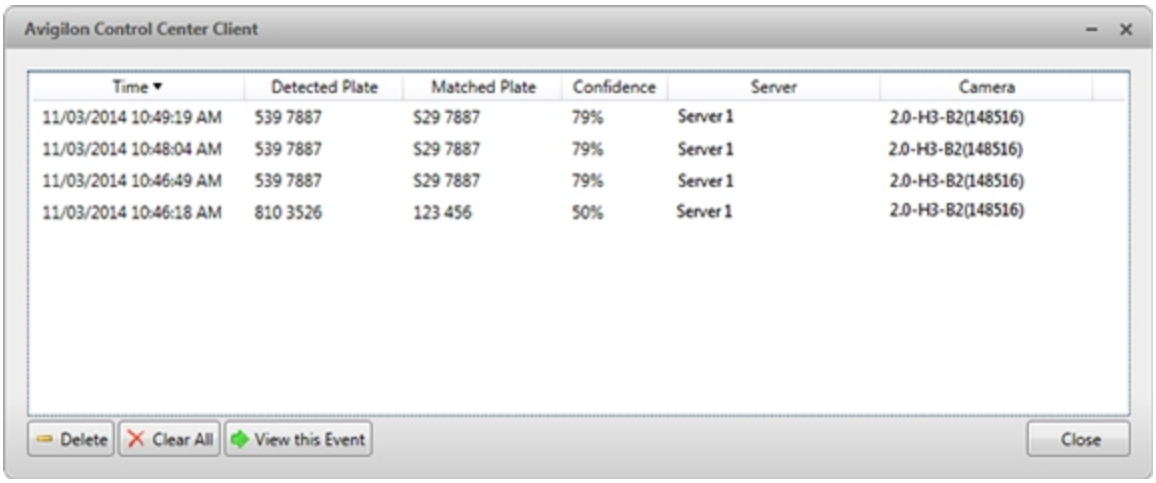


Figure 14: The License Plate Matches dialog box.

Select one of the license plate matches and do any of the following:

- Click **View this Event** or double-click the selected license plate to open a snapshot of the detected license plate in a new View.
- Click **Delete** to delete the license plate from the list.
- Click **Clear All** to empty the current match list. The list will be repopulated as new license plates are detected.

Reviewing Recorded POS Transactions

While you watch recorded video, you can review POS transactions that occur at the same time.

1. Select a camera that is linked to the POS transaction source and display the camera's recorded video
2. In the image panel, click .

   If there is more than one POS transaction source linked to the camera, you will be prompted to select one. The POS transactions are displayed in the next image panel.

   - Each transaction is separated by date and time.
   - When you select a transaction, the video jumps to that event on the Timeline.
   - Scroll up or down to see other recorded POS transactions.
3. To display cameras that are linked to the POS transaction source, click in the POS transaction image panel.

   If multiple cameras are connected to the POS transaction source, you will be prompted to select one.
4. Use the Timeline to review the video in more detail.

For more information about Timelines, see **Playing Back Recorded Video**.

If you want to find a specific POS transaction, see **Performing a POS Transaction Search**.

Working with Maps

A map is a graphical reference of your surveillance site. You can create a map out of any image of your location, then add cameras, encoders, saved Views, and other maps to the image to help you quickly navigate through your surveillance site.

Adding a Map

You can create a map from any image in JPEG, BMP, PNG, or GIF format. The image is used as the map background and cameras are added on top to show where they are located in your surveillance Site.

NOTE: You can only add and view cameras that are connected to the server that you are accessing through the Web Client.

1. In the System Explorer, right-click a Site or Site folder and select **New Map...**.
2. In the Map Properties dialog box, click **Change Image...** and locate your map image.

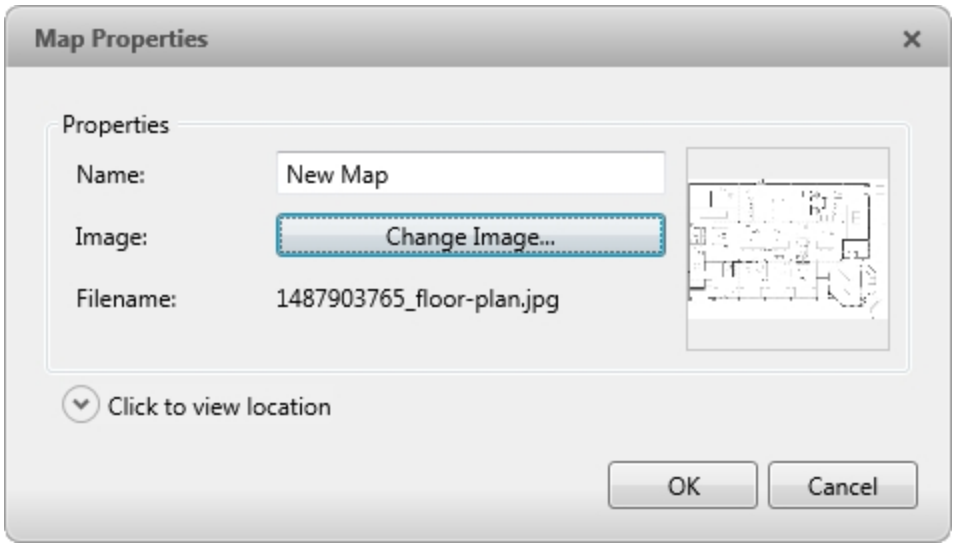


Figure 15: The Map Properties dialog box

3. In the **Name:** field, enter a name for the map.
4. Click to choose where the map appears in the System Explorer. By default, the map is added to the Site that you initially selected.
    - If your Site includes virtual sub-sites, select a location for the map. The list on the right updates to show what is stored in that directory.
    - In the Site directory, drag the map up and down to set where it is displayed.
5. Click **OK**.

    In the following Editing: Map tab, you can click **Edit Properties...** to open the Map Properties dialog box again.

6. Drag and place cameras from the System Explorer onto the map.

Figure 16: The Editing: Map tab

By default a camera is displayed as an icon with a yellow triangle to represent its field of view.

- Drag the black points at the end of the yellow field of view to re-size and position the camera angle.

7. Drag encoders, saved Views, Virtual Matrix monitors, and other maps that you need from the System Explorer onto the map.
8. In the **Map Icon Properties** options, you can change the way icons are displayed on the map. Select any icon on the map then do the following:

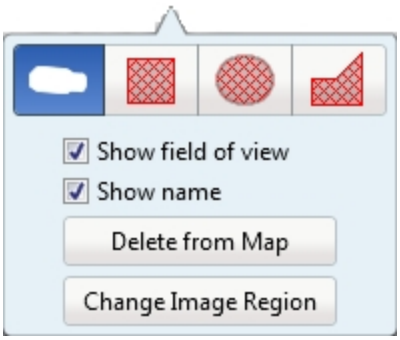


Figure 17: Map Icon Properties options

a. To replace an icon with a clickable shape region, select one of the shape buttons. You can replace the icon with a rectangle, ellipse, or polygon region.

b. Select the **Show name** check box to display the object's name on the map.

c. Click **Delete from Map** to remove the object from the map.

d. (Cameras only) Select the **Show field of view** check box to display the camera's yellow field of view. This option is only available when the camera icon is used.

   Drag the corners of the yellow triangle to expand the field of view. Drag the black circle at the end of the triangle to rotate the field of view.

9. Click  to save your new map.

Using a Map

You can open a map in any image panel, then open video or alarms from the map.

1. To open a map in an image panel, do one of the following:
   - Double-click in the System Explorer.
   - Drag from the System Explorer to an image panel.
   - In the System Explorer, right-click and select **Add To View**
2. When the map appears in an image panel, do any of the following:

Figure 18: Map in an image panel.

To...	Do this...
Review an alarm	When a camera flashes in red, an alarm linked to the camera has been triggered.

To...	Do this...
	• Click the camera to monitor the live alarm video.
Display video from a camera on the map	• Drag a camera from the map to a different image panel, or • Click the camera on the map.
Open a linked map	• Click the map icon on the map. You can use the **Forward** and **Back** buttons to move between maps.
Open a linked View	• Click the saved View on the map.

Editing and Deleting a Map

You can update a map or delete an old map anytime.

1. In the System Explorer, right-click  then select one of the following:
    - To edit the map, select **Edit...**. Refer to **Adding a Map** for details about the editable options.
    - To delete the map, select **Delete**. When the confirmation dialog box appears, click **Yes**.

Working with Web Pages

You can quickly review online content while monitoring videos by adding web pages to the System Explorer.

Adding a Web Page

You can add web pages to a Site for quick access to internet content that is related to your surveillance system.

1. In the System Explorer, right-click a Site or Site folder and select **New Web Page...**.

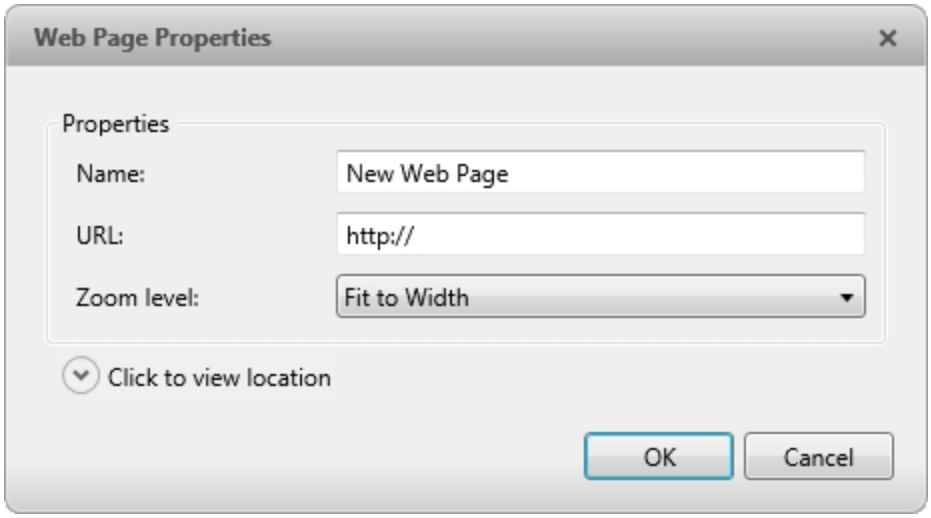


Figure 19: The Web Page Properties dialog box

2. Enter a **Name:** for the web page.
3. Enter the web page URL in the **URL:** field.
4. Select a **Zoom level:** for viewing the web page inside an image panel.
5. Click to choose where the web page appears in the System Explorer. By default, the web page is added to the Site you initially selected.
    - If your Site includes virtual sub-sites, select a location for the web page. The list on the right updates to show what is stored in that directory.
    - In the Site directory, drag the web page up and down to set where it is displayed.
6. Click **OK**.

Using a Web Page

To open a web page, do one of the following:

- Double-click in the System Explorer.
- Drag from the System Explorer to an image panel.

- In the System Explorer, right-click and select **Add To View**.

The web page is displayed in one of the image panels. Use the web browser buttons to navigate through the internet.

Figure 20: Web Page controls.

Editing and Deleting a Web Page

Whenever a web page address becomes out of date, you can choose to update the web page or delete the web page from the Site.

1. In the System Explorer, right-click then select one of the following:
    - To edit the web page, select **Edit...**. Refer to **Adding a Web Page** for information about the editable options.
    - To delete the web page, select **Delete**. When the confirmation dialog box appears, click **Yes**.

Monitoring Alarms

The Alarms tab allows you to monitor and acknowledge alarms. You can quickly review video of the event, bookmark the recorded incident, and export alarm video for further investigation.

Accessing the Alarms Tab

At the top of the application window, click  >  .

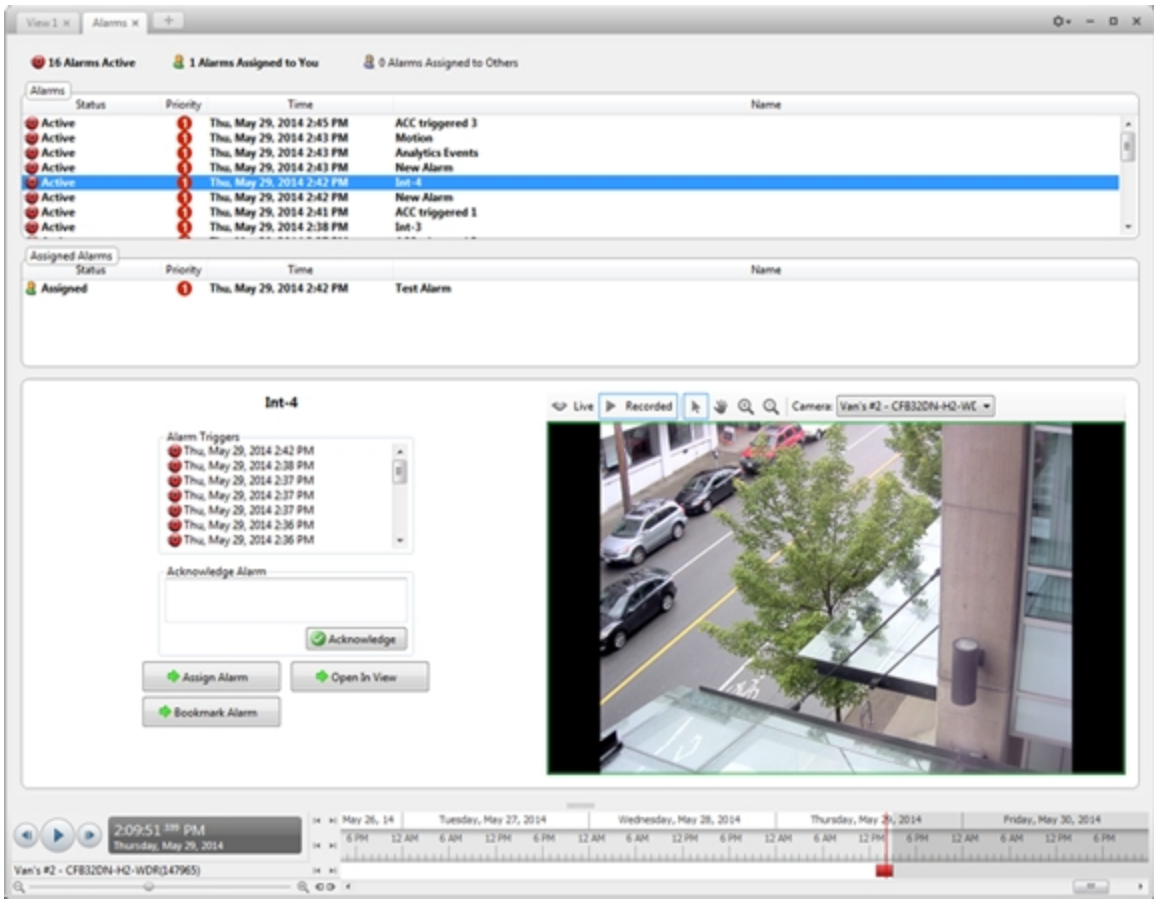


Figure 21: The Alarms tab

The Alarms tab is divided into the following areas:

- In the Alarms list are the alarms that are currently active, acknowledged, or assigned to another user. The alarms are sorted by Status, Priority, then Time.
- In the Assigned Alarms list are the alarms that are assigned to you. If there are no alarms assigned to you, the Assigned Alarms list is not displayed.
- In the bottom half of the screen is the Alarm Details area, where the triggers and video linked to the

selected alarm are displayed.

- The Timeline is used to play back recorded alarm video.

Reviewing Alarms

In the Alarms tab, you can review alarm video and manage alarms. Active alarms can be assigned to yourself, and acknowledged alarms can be exported or purged as required.

Reviewing Alarm Video

You can review active and acknowledged alarm video in detail through the alarm image panel, or by opening the alarm video in a new View.

1. Select an alarm from the **Alarms** list. The alarm details are displayed.
2. In the Alarm Triggers list, select an alarm trigger to display the video for that instance of the alarm.
3. Use the alarm image panel controls to review the video in more detail.

Figure 22: Alarm Image Panel

   - In the **Camera:** drop down list, select a camera that is linked to the alarm to review the video.
   - Use the **Zoom In Tool**, **Zoom Out Tool** and **Pan Tool** to review the video image in more detail.
   - Use the **Live** and **Recorded** buttons to alternate between the recorded alarm video and the camera's live stream.

4. Click **Open In View** to open the alarm video in a new View.
5. Use the Timeline to control video playback.

For information about the Timeline controls, see **Playing Back Recorded Video**

Acknowledging an Alarm

Acknowledging an alarm shows that an alarm has been reviewed and is no longer active. You can acknowledge any alarm that is active or assigned to you.

1. After reviewing the alarm, enter notes describing the nature of the alarm in the **Acknowledge Alarm** text box.
2. Click **Acknowledge**.
3. If there is a digital output linked to the alarm, a dialog box may appear to ask for permission to activate the digital output. Activate the digital output as required.

The Alarm is given an Acknowledged status in the Alarms list.

Assigning an Alarm

You can assign an alarm to yourself to let others know that the alarm is being reviewed.

Although you can only assign alarms to yourself, you can unassign the alarm at any time.

1. Select an **Active** alarm from the Alarms list.
2. When the alarm details are displayed, click **Assign Alarm**.

   The alarm is added to your Assigned Alarms list.
3. To unassign an alarm, select the alarm from the Assigned Alarms list and click **Unassign Alarm**.

Bookmarking an Alarm

You can bookmark active and acknowledged alarm video.

1. Select an alarm from the Alarms list, then click **Bookmark Alarm**.
2. When the Edit Bookmark dialog box appears, define the details of your bookmark.

   The Edit Bookmark dialog box automatically selects all the cameras that are linked to the alarm, and sets the time range to span the first and last alarm trigger. After you make any required changes, click **OK**.

For more information about the bookmark options, see **Bookmarking Recorded Video**.

Purging an Alarm

Purging an alarm removes the alarm from the Alarms list until the alarm is activated again. Although purged alarms are no longer listed in the Alarms list, you can still search through the alarm's history.

1. Select an **Acknowledged** alarm from the Alarms list.
2. In the Alarm Details area, click **Purge Alarm**.

Searching Alarms

You can search through an alarm's history to review other instances of the alarm.

1. Select an **Acknowledged** alarm from the Alarms list.
2. In the Alarm Details area, click **Search Alarm**.

For information about the alarm search options, see **Performing an Alarm Search**.

Exporting Alarms

You can export alarm video for review on other computers.

1. Select an **Acknowledged** alarm from the Alarms list.
2. In the Alarm Details area, click **Export Alarm**.

For information about the export options, see **Export**.

Arming Image Panels

Arming an image panel reserves the image panel specifically for displaying video linked to alarms or rules. Armed image panels allow you to review and acknowledge alarms while monitoring video in a View. Any image panel can be armed or disarmed as required.

If there are no armed image panels, alarm video will appear in the next empty image panel in the current View, or in a new View if all current image panels are in use.

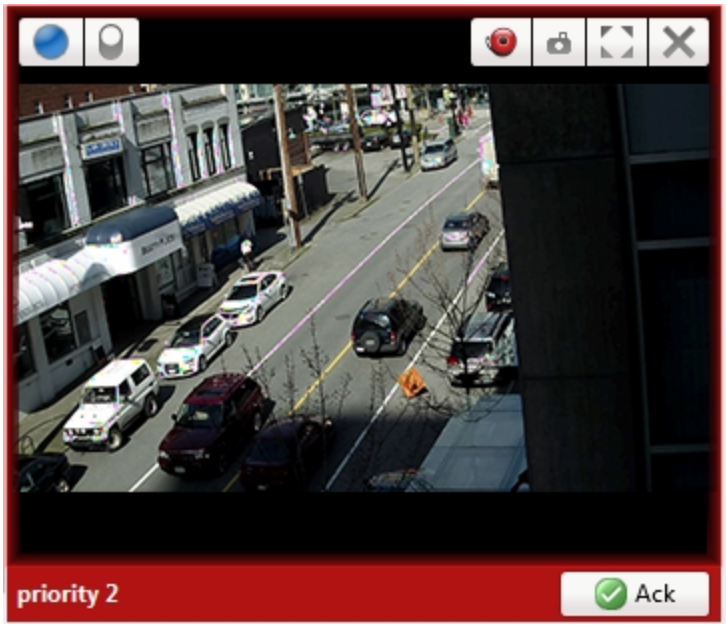


Figure 23: Armed image panel

Tip: You can still use the features that are common to all image panels in an armed panel, like taking snapshots or maximizing the image panel.

To...	Do this...
Arm an image panel	In an image panel, click . The image panel is given a **red** border and an alarm label to show that it is armed.
Acknowledge an alarm	Click .
Move between linked alarm video	If the alarm is linked to multiple cameras, use the green arrows to move between the linked cameras.
Disarm an image panel	In an armed image panel, click .

If multiple alarms are triggered at the same time, the linked videos are queued inside the armed image panel. The alarm videos are displayed by order of alarm priority, then time. Once an alarm is acknowledged or assigned to a user, the alarm video is removed from the armed image panel.

NOTE: If you choose to close a video in the armed image panel, the video is removed but the alarm continues to be active.

Videos triggered by a rule are queued in the armed image panel after alarms, with the most recent video displayed first. Rule videos are not labeled and do not need to be acknowledged.

Search

You can quickly search for recorded video that is linked to an event or search through a camera's recording history.

NOTE: Some features are not displayed if the server does not have the required license, or if you do not have the required user permissions.

Performing an Alarm Search

1. In the New Task menu, under Search, click  .

   The Search: Alarms tab is displayed.

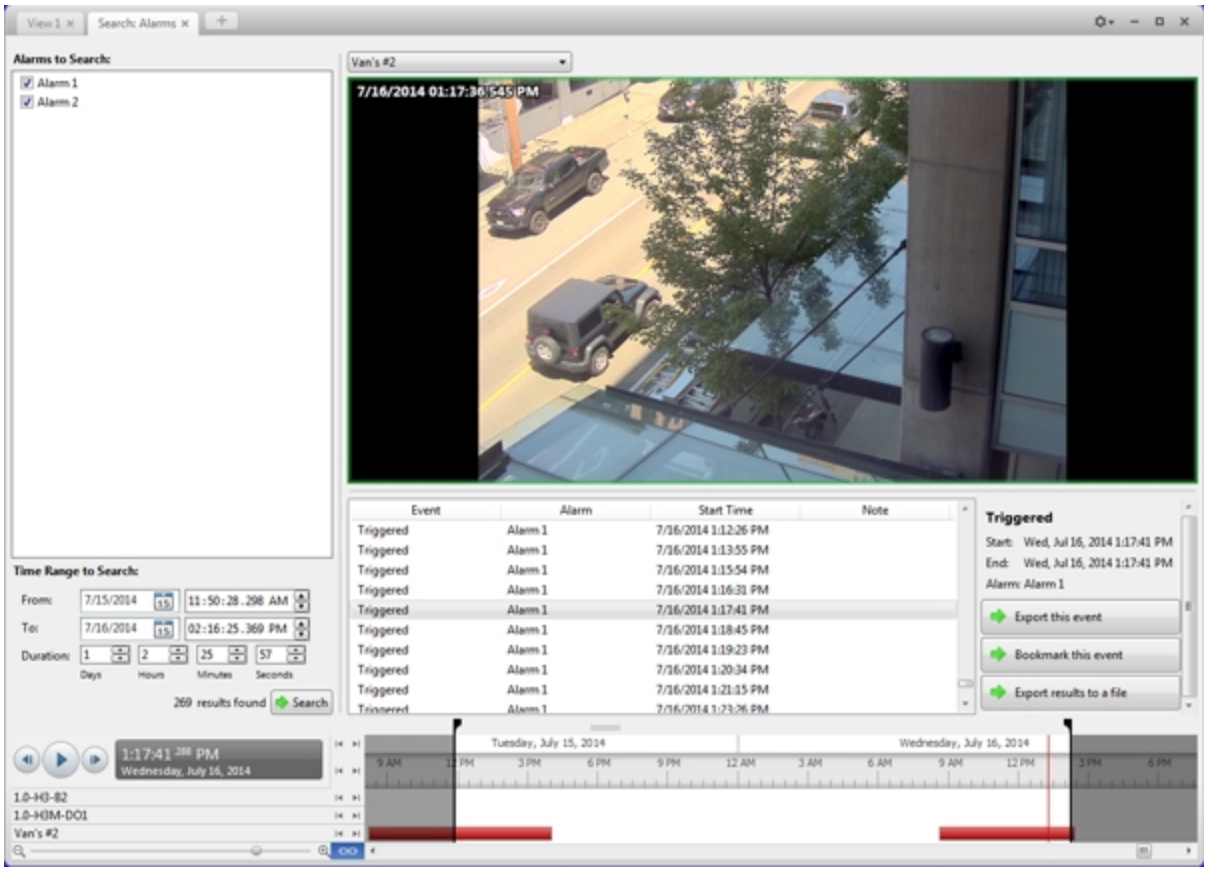


Figure 24: The Search: Alarms tab

2. In the **Alarms to Search:** list, select all the alarms you would like to include in the alarm search.
3. In the **Time Range to Search:** area, set the date and time range of your search. The time range is highlighted on the Timeline by the black time range markers. You can also drag the time range markers to modify the time range.
4. Click **Search**.

Viewing Alarm Search Results

1. In the **Search Results** area, select a search result. The event is highlighted on the Timeline and the video is displayed in the image panel. Details about the search result are displayed to the right.
2. Use the Timeline controls to review the event.

   For more information, see **Playing Back Recorded Video**.
3. If the search result is linked to multiple cameras, select a camera from the drop down list above the image panel to change the video that is displayed.
4. Click **Export this event** to export the selected event video.

   For more information, see **Export**.
5. To export all listed search results, click **Export results to a file** and save the file. The search results can be saved as either a CSV or Text file.

Performing a Bookmark Search

The Bookmark Search allows you to search for a specific bookmark.

1. In the New Task menu, click 

   The Search: Bookmark tab is displayed. All available bookmarks are listed on the left.

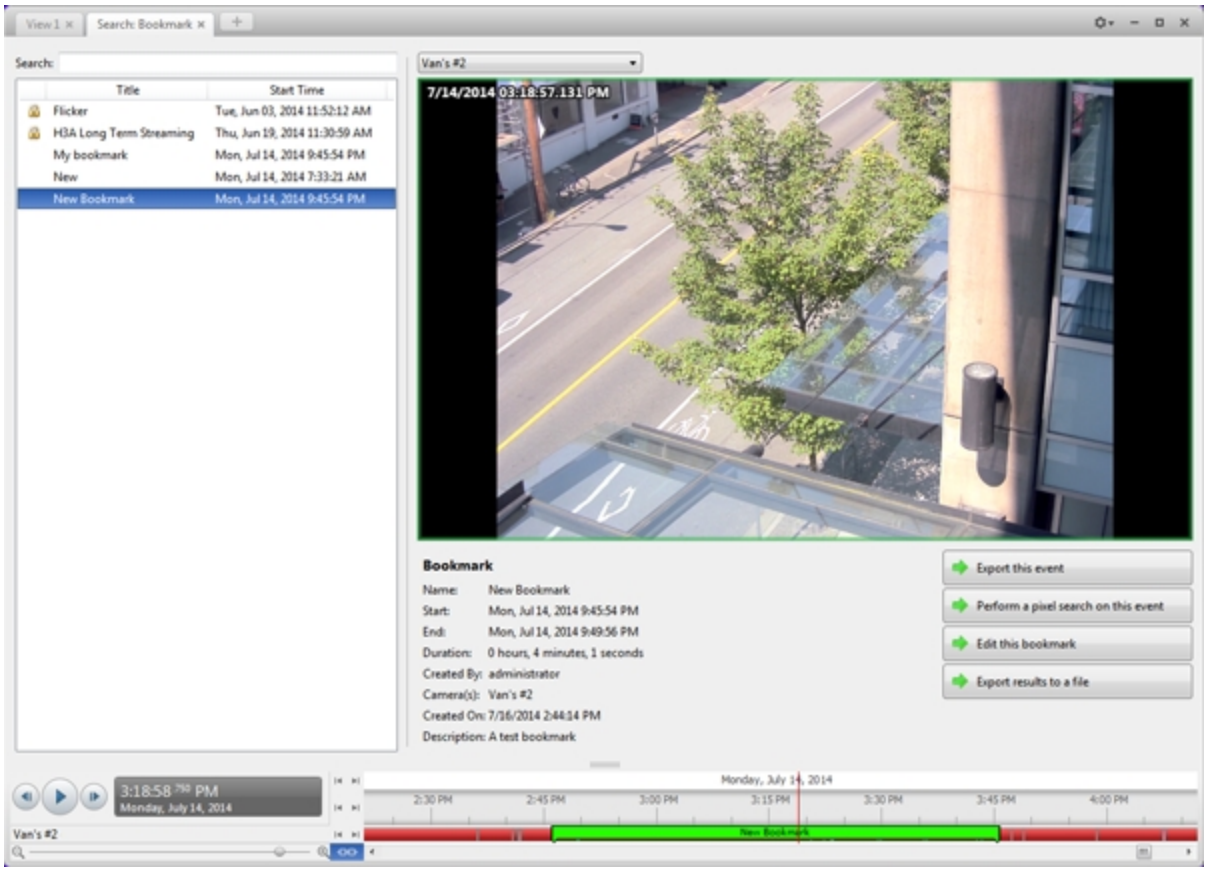


Figure 25: The Search: Bookmark tab

2. In the **Search:** field, enter any text that may appear in the bookmark's title, description, linked camera name, or the name of the user who created the bookmark.

   The search is automatically performed on all the listed bookmarks until only the matches are displayed.

Viewing Bookmark Search Results

1. In the Bookmark list, select a bookmark. The bookmark is highlighted on the Timeline and the video is displayed in the image panel. Details about the bookmark are displayed under the image panel.
2. Use the Timeline controls to review the event.

   For more information, see **Playing Back Recorded Video**.
3. If the search result is linked to multiple cameras, select a camera from the drop down list above the image panel to change the video that is displayed.
4. Click **Export this event** to export the selected bookmark.
5. If you want to further refine your search, click **Perform a pixel search on this event**. You can now search for pixel changes in the selected bookmarked video.

   For more information, see **Performing a Pixel Search**.
6. Click **Edit this bookmark** to edit the bookmark.

   For more information, see **Bookmarking Recorded Video**.

Performing an Event Search

The Event Search allows you to search for specific motion events and digital input events.

1. In the New Task menu, click 

   The Search: Event tab is displayed.

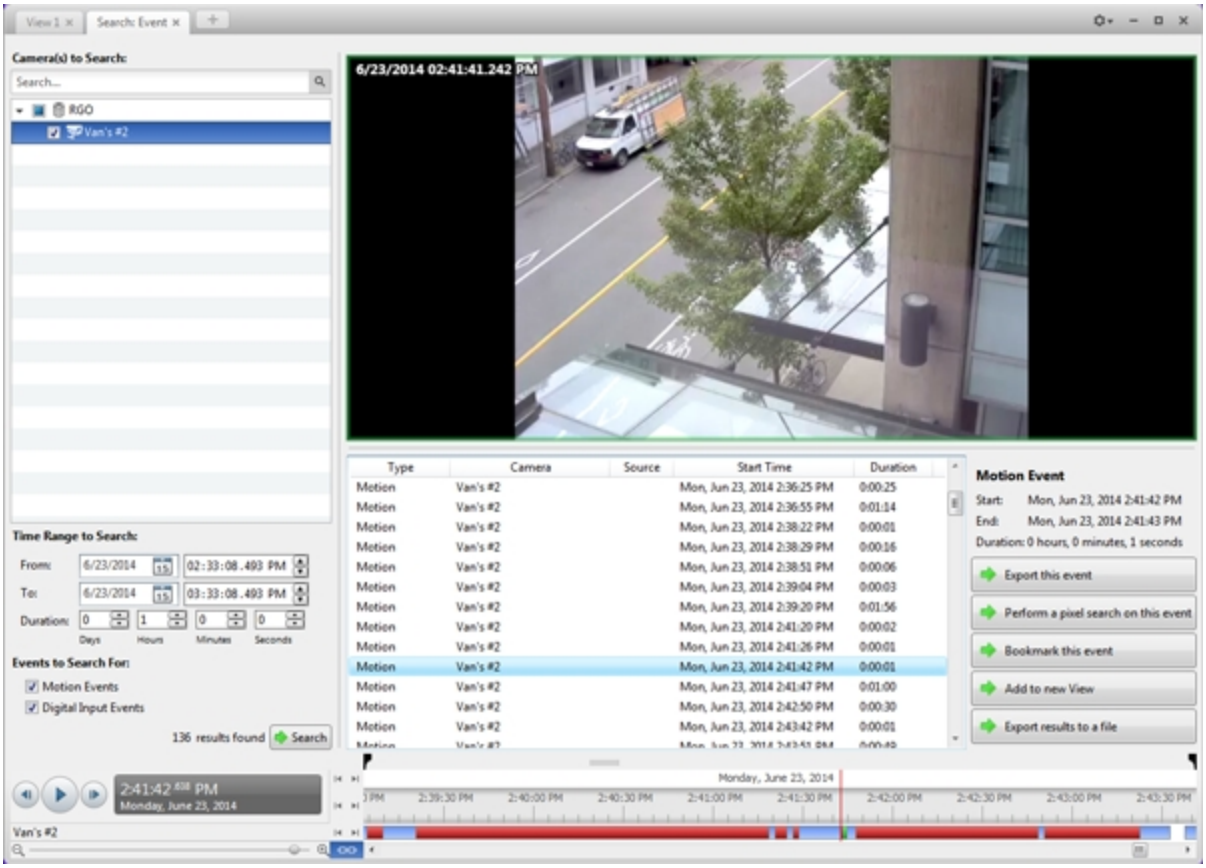


Figure 26: The Search: Event tab

2. In the **Camera(s) to Search:** area, select all the cameras you want to include in the search.
3. In the **Time Range to Search:** area, set the date and time range of your search. The time range is highlighted on the Timeline by the black time range markers. You can also drag the time range markers to modify the time range.
4. In the **Events to Search For:** area, select the types of events to include in the search.
5. Click **Search**.

Viewing Event Search Results

1. In the **Search Results** area, select a search result. The event is highlighted on the Timeline and the video is displayed in the image panel. Details about the search result are displayed to the right.
2. Use the Timeline controls to review the event.

For more information, see **Playing Back Recorded Video**.

3. Click **Export this event** to export the selected event video.

   For more information, see **Export**.

4. If you want to further refine your search, click **Perform a pixel search on this event**. You can now search for pixel changes in the selected search result.

   For more information, see **Performing a Pixel Search**.

5. Click **Bookmark this event** to bookmark the selected search result.

   For more information, see **Bookmarking Recorded Video**.

6. To export all listed search results, click **Export results to a file** and save the file. The search results can be saved as either a CSV or Text file.

Performing a License Plate Search

1. In the New Task menu, under Search, click 

   The Search: License Plates tab is displayed.

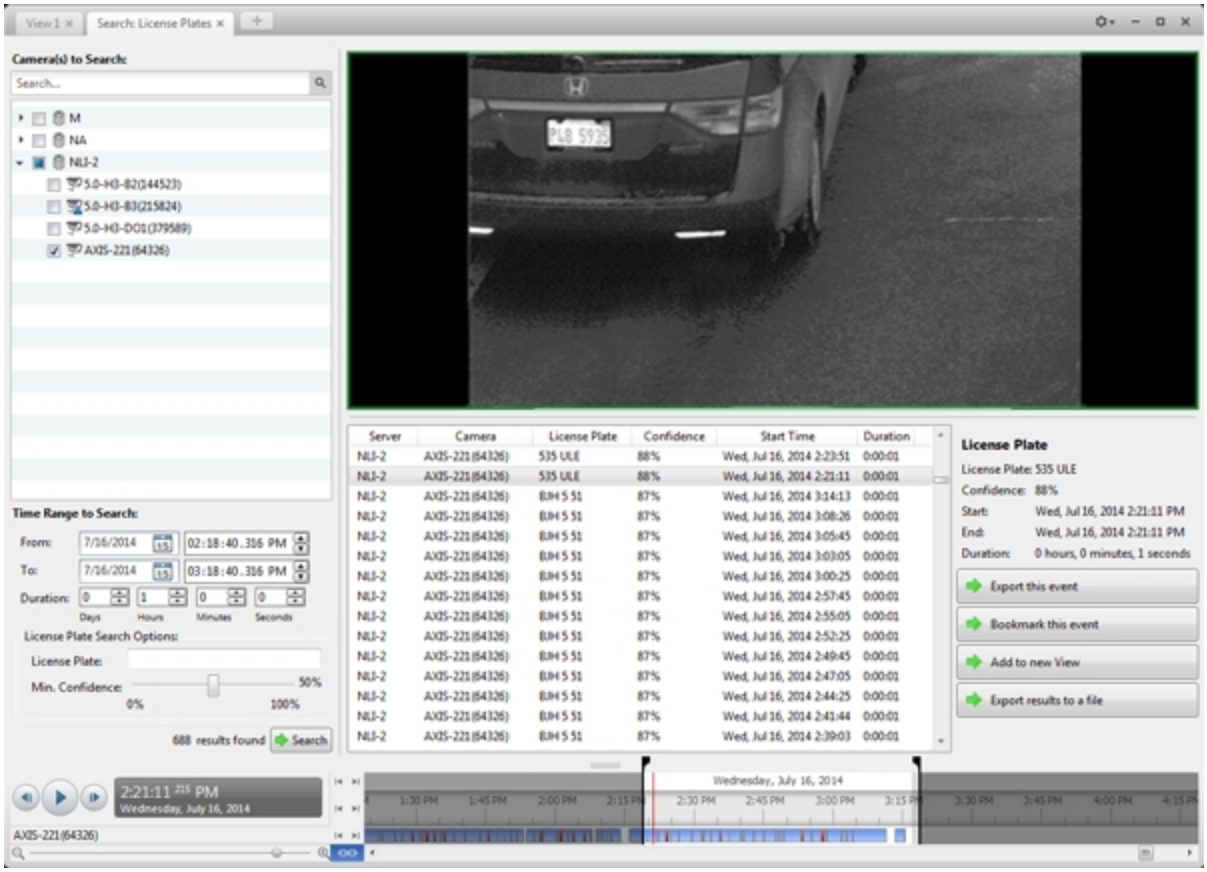


Figure 27: The Search: License Plates tab

2. In the **Camera(s) to Search:** area, select all the cameras you want to include in the search.
3. In the **Time Range to Search:** area, set the date and time range of your search. The time range is highlighted on the Timeline by the black time range markers. You can also drag the time range markers to modify the time range.
4. In the **License Plate Search Options:** area, enter the license plate you want to find and a minimum confidence of a match.
5. Click **Search**.

Viewing License Plate Search Results

1. In the **Search Results** area, select a search result. The event is highlighted on the Timeline and the video is displayed in the image panel. Details about the search result are displayed to the right.
2. Use the Timeline controls to review the event.

   For more information, see **Playing Back Recorded Video**.
3. If the search result is linked to multiple cameras, select a camera from the drop down list above the image panel to change the video that is displayed.
4. Click **Export this event** to export the selected event video.

   For more information, see **Export**.
5. To export all listed search results, click **Export results to a file** and save the file. The search results can be saved as either a CSV or Text file.

Performing a Pixel Search

The Pixel Search allows you to search for tiny pixel changes in specific areas in the camera's field of view.

1. In the New Task menu, click 

   The Search: Pixel tab is displayed.

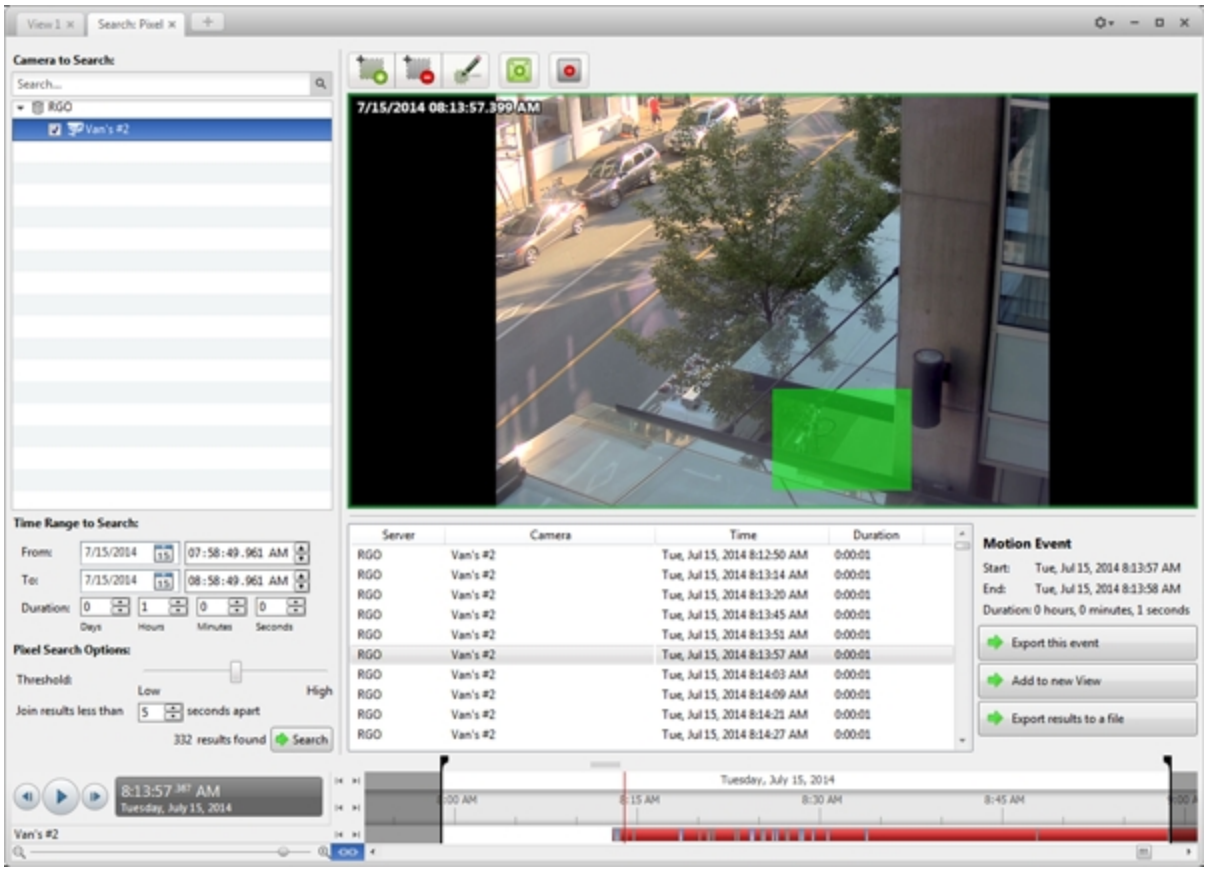


Figure 28: The Search: Pixel tab

By default, the entire search image panel is highlighted in green.

2. In the **Camera to Search:** area, select a camera.
3. In the **Time Range to Search:** area, set the date and time range of your search. The time range is highlighted on the Timeline by the black time range markers. You can also drag the time range markers to modify the time range.
4. Define the pixel search area by using the motion detection tools above the image panel.

   Tip: If you are looking for something very specific, limit the green area to a dot to find what you're looking for more quickly.
5. In the Pixel Search Options: area, drag the **Threshold:** slider to select the amount of motion required to return a search result.

   A high threshold requires more pixels to change before results are found.
6. Enter a number in the **Join results less than** field to set the minimum number of seconds between separate search results. You can enter any number between 1-100 seconds.
7. Click **Search**.

Viewing Pixel Search Results

1. In the **Search Results** area, select a search result. The event is highlighted on the Timeline and the video is displayed in the image panel. Details about the search result are displayed to the right.
2. Use the Timeline controls to review the event.

   For more information, see **Playing Back Recorded Video**.
3. Click **Export this event** to export the selected event video.

   For more information, see **Export**.
4. To export all listed search results, click **Export results to a file** and save the file. The search results can be saved as either a CSV or Text file.

Performing a POS Transaction Search

The POS Transaction Search allows you to search for specific transactions.

1. In the New Task menu, click  .

   The Search: POS Transactions tab is displayed.

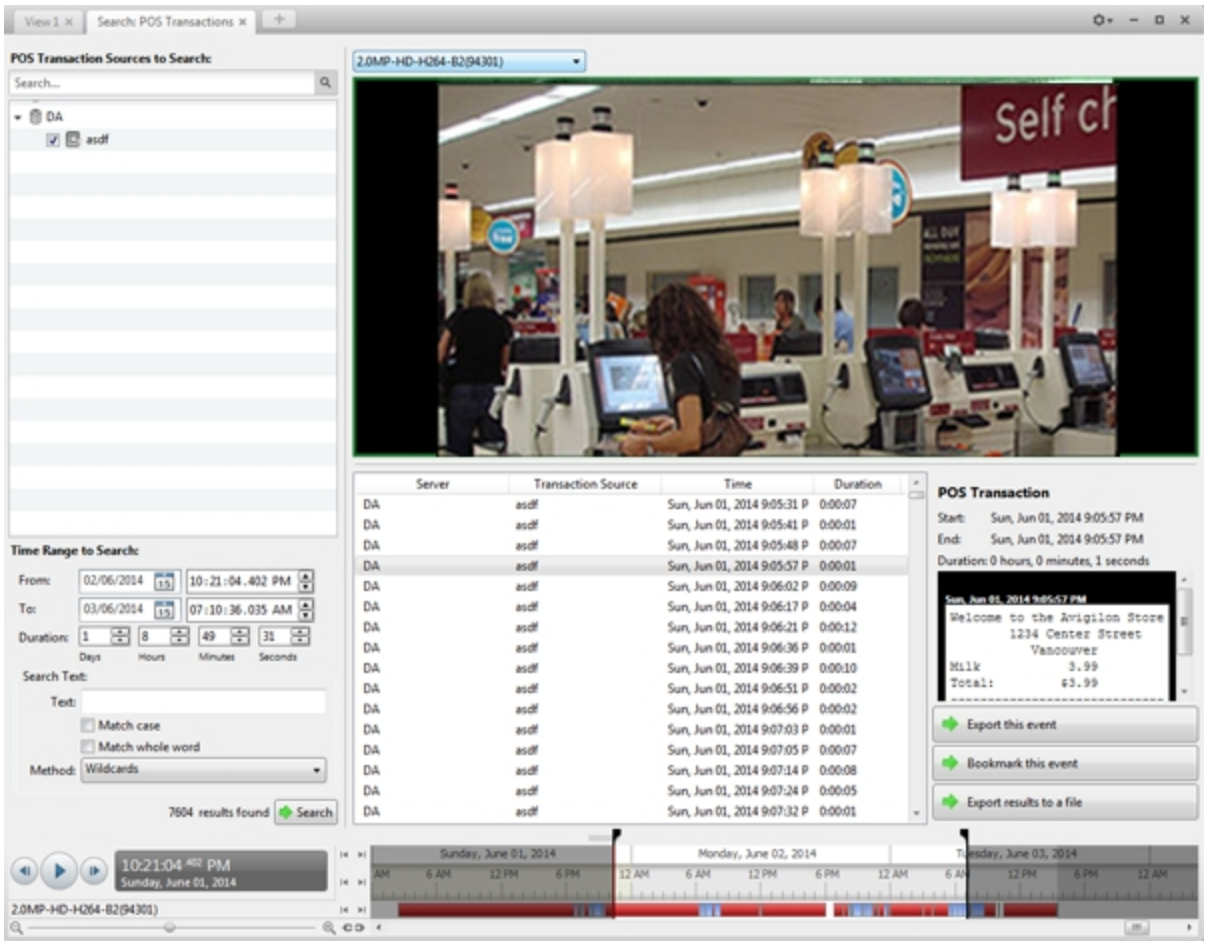


Figure 29: The Search: POS Transactions tab

2. In the **POS Transaction Sources to Search:** area, select all the POS transaction sources you would like to include in the search.
3. In the **Time Range to Search:** area, set the date and time range of your search. The time range is highlighted on the Timeline by the black time range markers. You can also drag the time range markers to modify the time range.
4. In the **Search Text:** area, enter any text that will help you filter the search results. For example, you can enter product names or transaction values.

   Use the **Wildcards** and **Regular expressions** search methods to find a range of results. Leave the **Text:** field blank to find all transactions.
5. Click **Search**.

Viewing POS Transaction Search Results

1. In the **Search Results** area, select a search result. The event is highlighted on the Timeline and the video is displayed in the image panel. Details about the search result are displayed to the right.
2. Use the Timeline controls to review the event.

   For more information, see **Playing Back Recorded Video**.

3. If the search result is linked to multiple cameras, select a camera from the drop down list above the image panel to change the video that is displayed.
4. Click **Export this event** to export the selected event video.

   For more information, see **Export**.
5. To export all listed search results, click **Export results to a file** and save the file. The search results can be saved as either a CSV or Text file.

Performing a Thumbnail Search

The Thumbnail Search is a visual search that displays search results as a series of thumbnail images.

1. In the New Task menu, click  .

   The Search: Thumbnails tab is displayed.

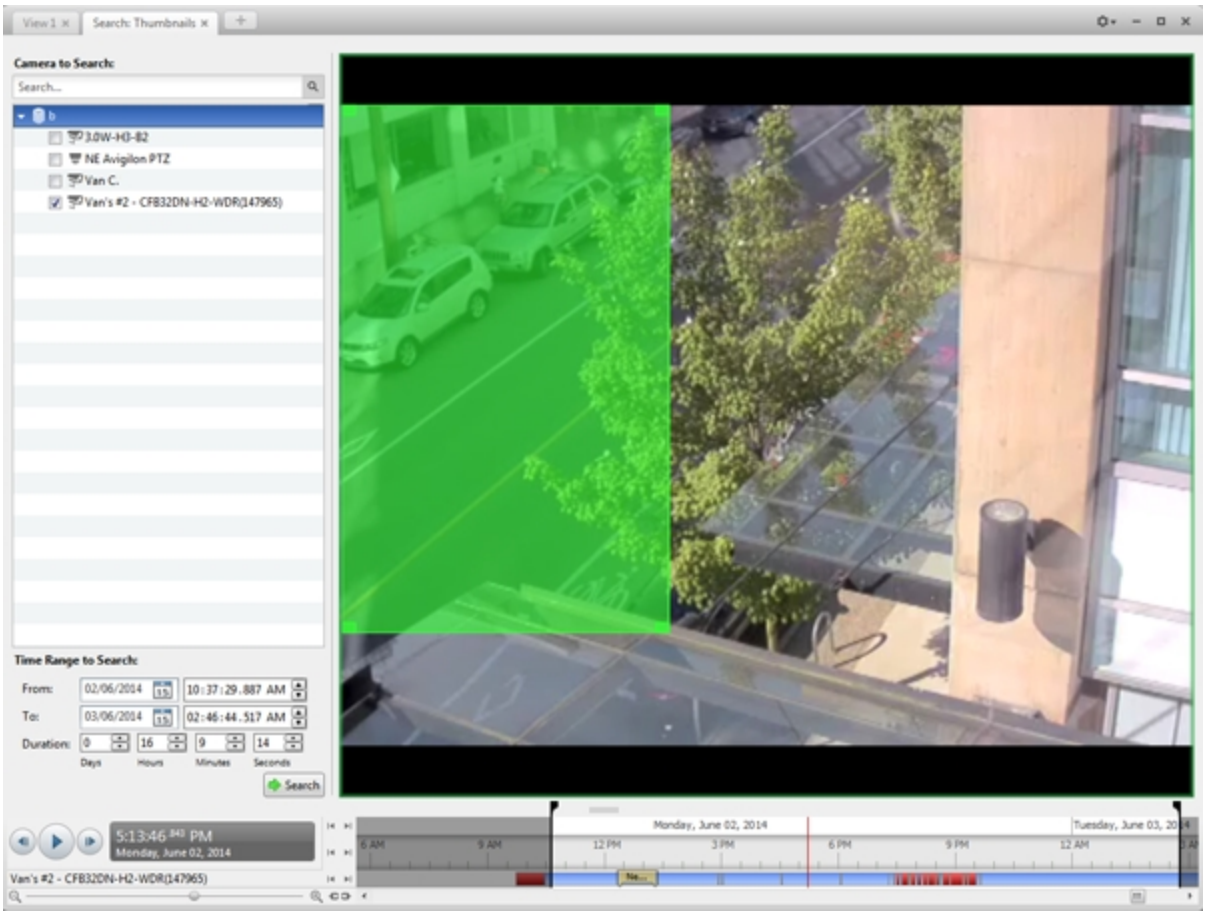


Figure 30: The Search: Thumbnails tab

2. In the **Camera to Search:** area, select a camera.
3. In the **Time Range to Search:** area, set the date and time range of your search. The time range is

highlighted on the Timeline by the black time range markers. You can also drag the time range markers to modify the time range.

4. In the image panel, move or drag the edges of the green overlay to focus the search on one area in the video image. Only the area highlighted in green will be searched.
5. Click **Search**.

Viewing Thumbnail Search Results

The search results display thumbnails at equal intervals on the Timeline.

1. To change the size of the search result thumbnails, select **Large Thumbnails**, **Medium Thumbnails**, or **Small Thumbnails** from the menu above the search results.

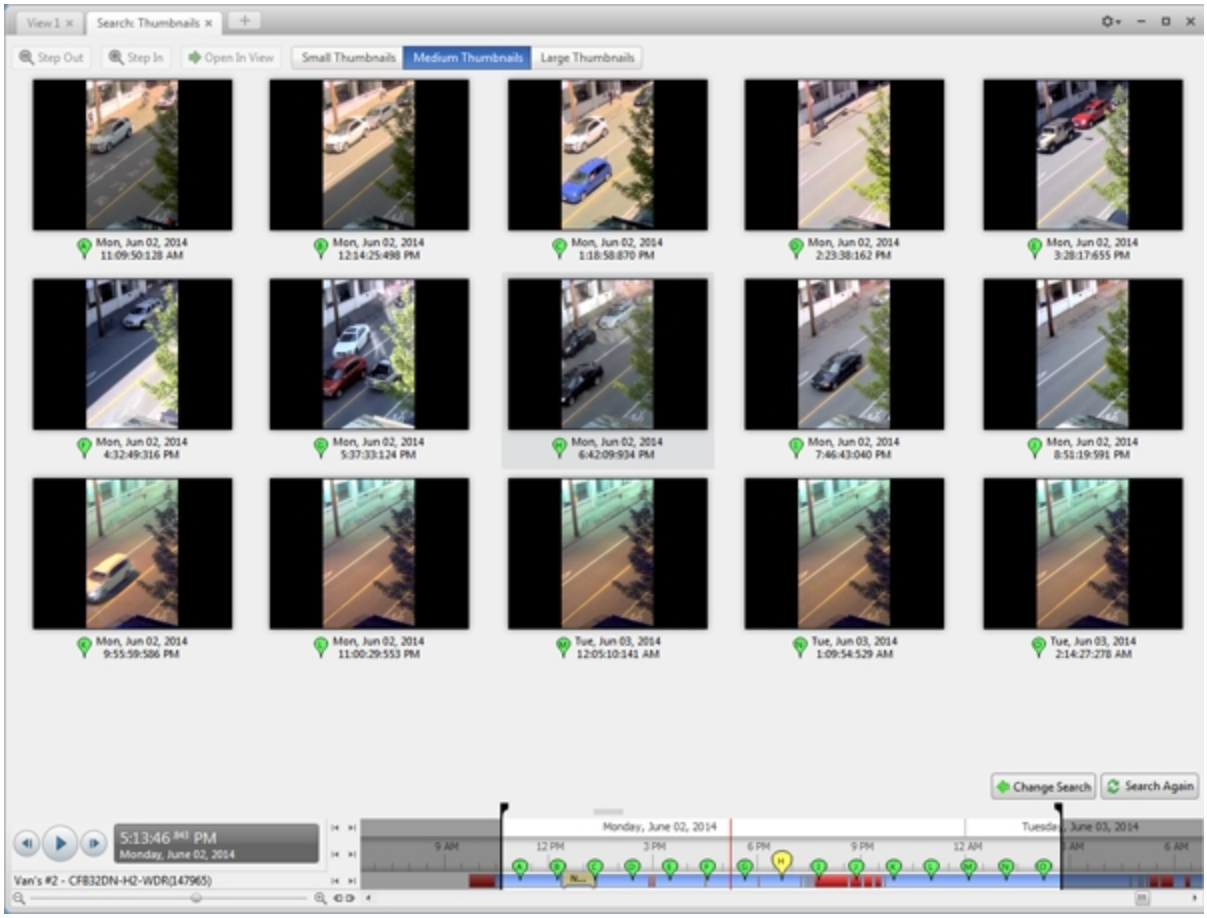


Figure 31: The Search: Thumbnails results tab

2. Select a thumbnail to highlight the video on the Timeline.
3. Click **Step In**, or double-click the thumbnail to perform another search around the thumbnail.

   Click **Step Out** to return to the previous results page.
4. Click **Open In View** (after selecting a thumbnail) to open the recorded video in a new View.
5. Click **Change Search** to change the search criteria.

Export

You can export video in multiple video and image formats. The Export tab can be accessed from bookmark options, the Alarms tab, the New Task menu, and any Search tab.

You can also export snapshots of an image panel as you monitor video.

It is recommended that you export video of individual events and back up video for your archives. For more information, see **Backup**.

Exporting Native Video

The Native (AVE) format is the recommended format for exporting video. You can export video from multiple cameras in a single file, and the video maintains its original compression. AVE video is played in the Avigilon™ Control Center Player, where the video can be authenticated against tampering and re-exported to other formats.

If there is audio linked to the video, the audio is automatically included in the export.

If you are exporting a large amount of video for your records, back up the video instead. For more information, see **Backing Up Recorded Video On Demand**.

1. In the New Task menu, click  . The Export tab opens.

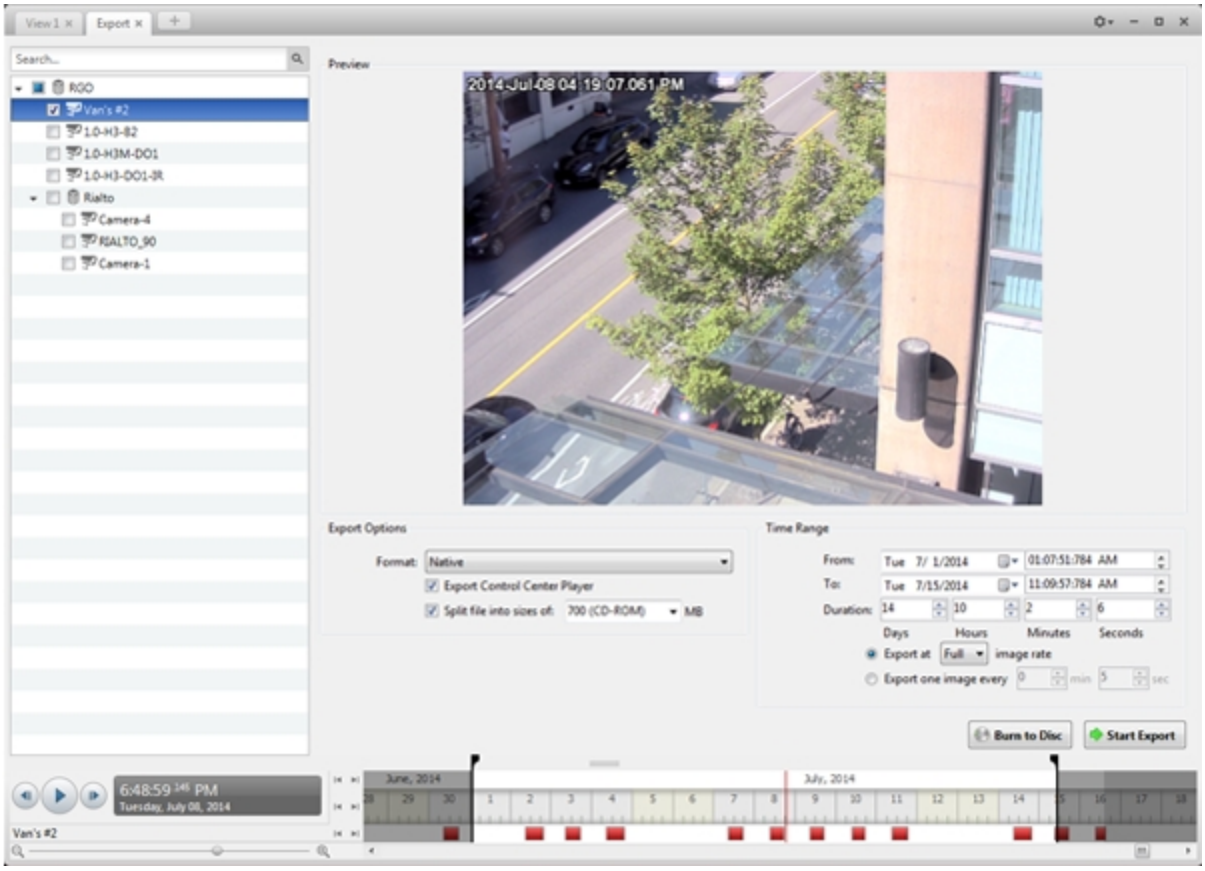


Figure 32: The Export tab for AVE export

2. In the **Format:** drop down list, select **Native**.
3. In the System Explorer, select the camera video you want to export.
4. To automatically divide the export into separate files, select the **Split file into sizes of:** check box, then select one of the options from the drop down list, or manually enter the size of each file in MB.

   This option allows you to export smaller files for storing in a flash drive or on optical media.

   This setting is automatically disabled if you choose to burn the export to disc because the system auto-detects the disc size.
5. Enter the **Time Range** you want to export. The **Time Range** is highlighted on the Timeline by black time range markers. You can also drag the time range markers to modify the time range.
6. Set the export image rate:

Option	Description
Export at _ image rate	Select this option to control how many images per second are exported. For example, the video is streaming at 30 images per second. If you select **1/2**, only

Option	Description
	15 images for that second will be exported.
Export one image every _ min _sec	Select this option to control the time between each exported video image. For example, if you enter *5* min. *0* sec., only one image will be exported for every 5 minutes of video.

7. Click one of the following:
   - **Start Export**: to save the file locally.
     - In the Save As dialog box, name the export file and click **Save**.
   - **Burn to Disc**: to burn the file directly to disc media.

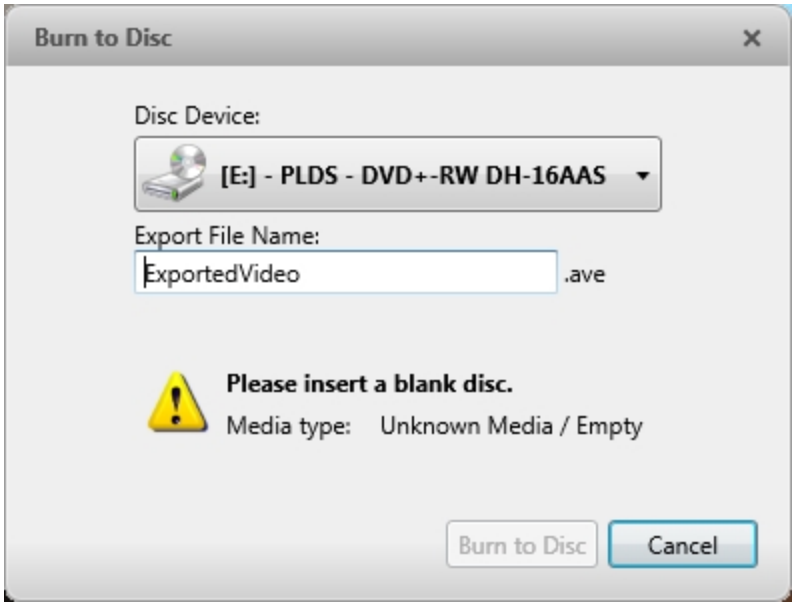


Figure 33: The Burn to Disc Dialog Box

   a. When the dialog box appears, insert a disc and select the media burning drive.
   b. Name the export file. The file name is automatically given a numbered suffix to help identify which file you are playing if the export spans multiple discs.
   c. Click **Burn to Disc** to start the export. If this button is disabled, the disc may be corrupt or full.
   d. Monitor the export progress to see if extra discs are required. When a disc is full, the export automatically pauses and you are asked to insert a new disc. After you insert a new disc, click **Resume Export**.

The number of discs required to export a video varies widely depending on the type of camera and disc used. Video is stored on the server with minimal compression to maximize the function of Avigilon's

HDSM™ technology, so the size of an export can be quite large due to the camera's high megapixel resolution and frame rate.

Generally, if you export a 2 minute video from a 2MP H.264 HD camera into AVE format, you will export a 93 MB file. To reduce the number of discs required, you can lower the frame rate or use a disc type with a larger capacity. Be aware that reducing the frame rate too much may cause the exported video to be jerky or missing data.

8. When the export is complete, click **OK**.

Exporting AVI Video

Video exported in Audio Video Interleave (AVI) format can be played in most media players. Be aware that you can only export one video at a time in this format.

1. In the New Task menu, click  . The Export tab opens.

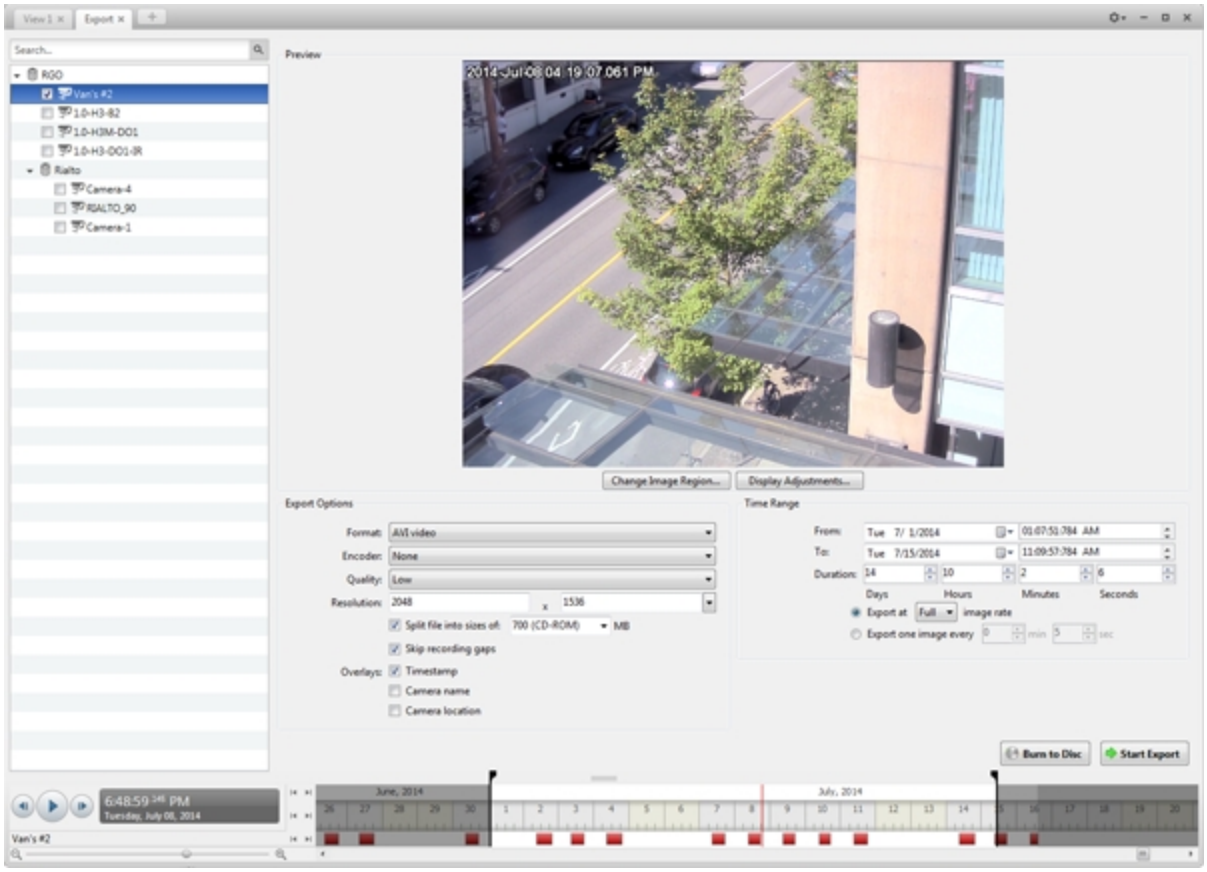


Figure 34: Export tab for AVI export

2. In the **Format:** drop down list, select **AVI video**.
3. In the System Explorer, select the camera video you want to export.
4. In the **Encoder:** field, select the compression used. The VC-1 (Windows Media Video) compression is

included by default because it is tailored for high-resolution AVI encoding.

If you are planning to burn the export to disc, it is important to select a compression method to help reduce the export size and maintain video quality.

5. In the **Quality:** drop down list, select the exported image quality level.
6. In the **Resolution:** field, select a resolution for the video image. You can manually enter the resolution or click the drop down arrow to select a standard resolution.

   NOTE: The Resolution: field automatically maintains the image aspect ratio.
7. To automatically divide the export into separate files, select the **Split file into sizes of:** check box, then select one of the options from the drop down list, or manually enter the size of each file in MB.

   This option allows you to export smaller files for storing in a flash drive or on optical media.

   This setting is automatically disabled if you choose to burn the export to disc because the system auto-detects the disc size.
8. Select the **Skip recording gaps** check box to avoid pauses in the video caused by gaps in the recording.
9. Select the image overlays you want: **Timestamp**, **Camera name**, and **Camera location**.

   Select the **Video Analytics Activity** overlay to include video analytics bounding boxes with the video. These boxes cannot be hidden or removed from the exported video.
10. Enter the **Time Range** you want to export. The **Time Range** is highlighted on the Timeline by black time range markers. You can also drag the time range markers to modify the time range.
11. Set the export image rate:

Option	Description
Export at _ image rate	Select this option to control how many images per second are exported. For example, the video is streaming at 30 images per second. If you select **1/2**, only 15 images for that second will be exported.
Export one image every _ min _sec	Select this option to control the time between each exported video image. For example, if you enter *5* min. *0* sec., only one image will be exported for every 5 minutes of video.

12. Click **Change Image Region...** to only export part of the video image. In the **Change Image Region...** dialog box, move and resize the green overlay to select the region you want to export, then click **OK**. Only areas highlighted in green will be exported.
13. Click **Display Adjustments...** to adjust the **Gamma:**, **Black Level:** and/or **White Level:**.
14. Click one of the following:

- **Start Export**: to save the file locally.
  - In the Save As dialog box, name the export file and click **Save**.
- **Burn to Disc**: to burn the file directly to disc media.

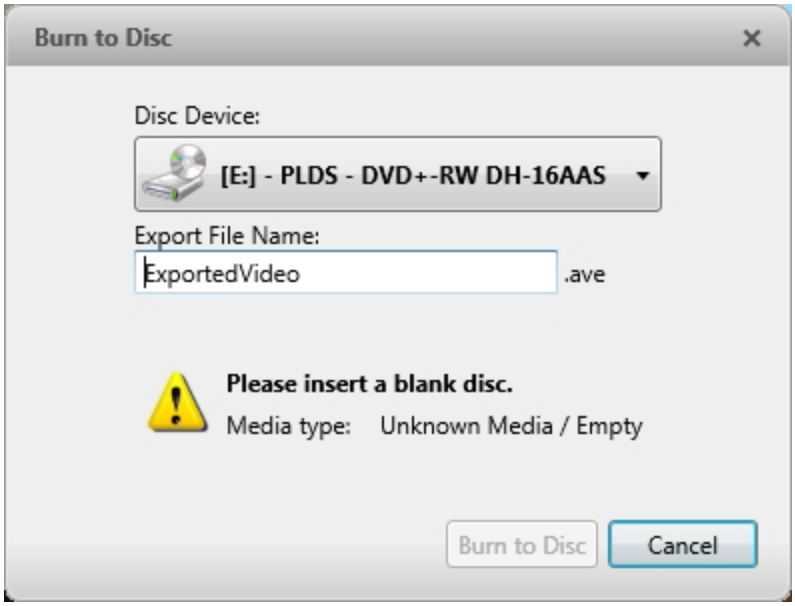


Figure 35: The Burn to Disc Dialog Box

a. When the dialog box appears, insert a disc and select the media burning drive.

b. Name the export file. The file name is automatically given a numbered suffix to help identify which file you are playing if the export spans multiple discs.

c. Click **Burn to Disc** to start the export. If this button is disabled, the disc may be corrupt or full.

d. Monitor the export progress to see if extra discs are required. When a disc is full, the export automatically pauses and you are asked to insert a new disc. After you insert a new disc, click **Resume Export**.

The number of discs required to export a video varies widely depending on the type of camera and disc used. Video is stored on the server with minimal compression to maximize the function of Avigilon's HDSM technology, so the size of an export can be quite large due to the camera's high megapixel resolution and frame rate.

Generally, if you export a 2 minute video from a 2MP H.264 HD camera into uncompressed AVI format, you will export a 2.7 GB file. If you select an **Encoder:** format and compress the video, you can export a 224 MB video at high quality. It is recommended that you always select an Encoder: format for AVI export to help significantly reduce the file size.

To further reduce the file size you can select a lower quality setting, lower the export frame rate, reduce the video resolution, or focus the export on a specific image region. Be aware that reducing each of the available settings too much may cause the export to be blurry or missing frames.

If it is important to have a high quality and full frame rate export, it is recommended that you use the AVE export format instead. AVE export intelligently compresses the video to create a smaller export file while

maintaining video data so that you can search, re-export video, and authenticate the video against tampering through the Avigilon Control Center Player software.

15. When the export is complete, click **OK**.

Exporting a Print Image

You can export a frame of video directly to your printer or as a PDF, and include notes related to the image.

To print a photo of the video you are currently watching, take a snapshot. For more information, see **Exporting a Snapshot of an Image**.

1. In the New Task menu, click  . The Export tab opens.

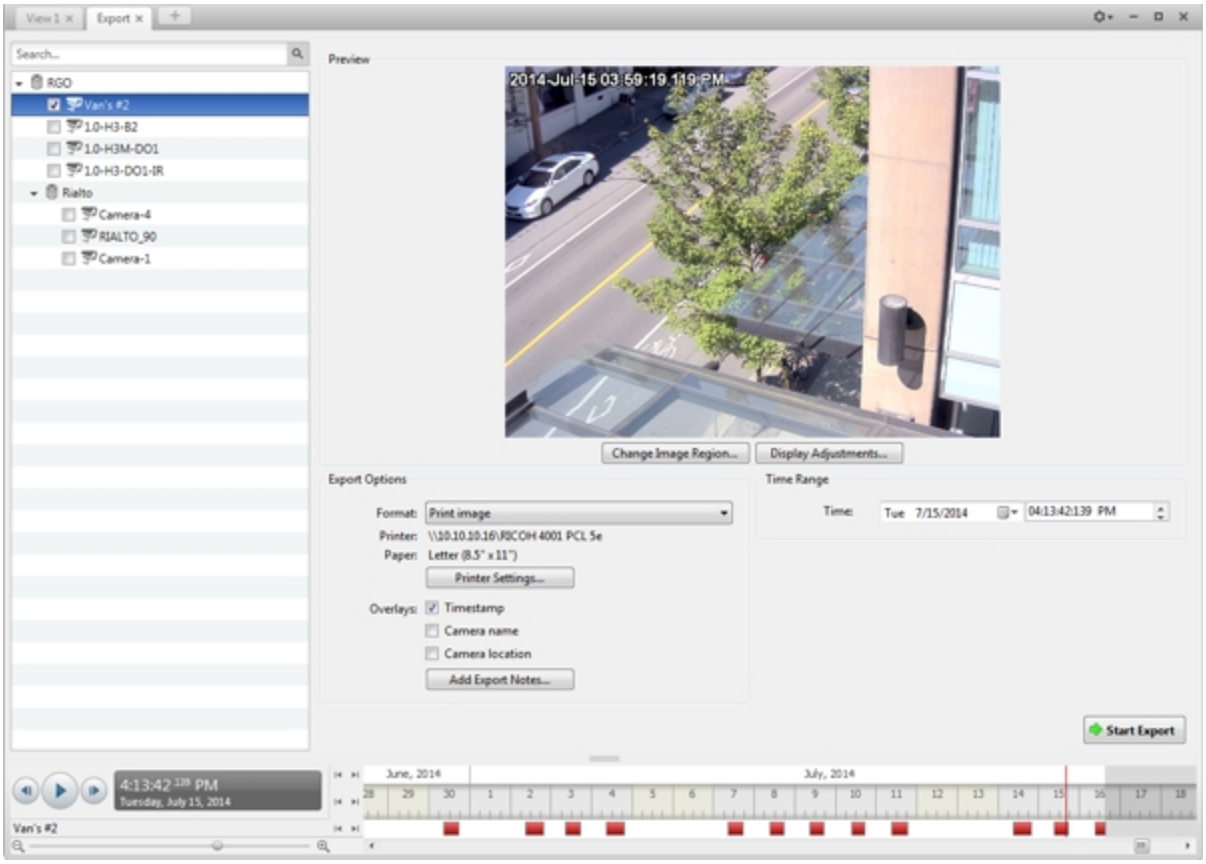


Figure 36: Export tab for print image export

2. In the **Format:** drop down list, select **Print image** or **PDF file**.
3. In the System Explorer, select the camera video you want to export.
4. (Print Image Only) Click **Printer Settings...** to change the printer and paper size that the image is printed on.
5. Select the image overlays you want: **Timestamp**, **Camera name**, and **Camera location**.

6. Click **Add Export Notes...** to add notes about the exported image. The notes are added below the image.
7. In the **Time Range** box, enter the exact date and time of the video image you want to export.
8. Click **Change Image Region...** to only export part of the video image. In the **Change Image Region...** dialog box, move and resize the green overlay to select the region you want to export, then click **OK**. Only areas highlighted in green will be exported.
9. Click **Display Adjustments...** to adjust the **Gamma:**, **Black Level:** and/or **White Level:**.
10. Click **Start Export**.
    - If you are exporting a Print image, the image is sent to the printer.
    - If you are exporting a PDF file, save the image.

    The Preview area displays the video you are exporting.
11. When the export is complete, click **OK**.

Exporting a Snapshot of an Image

You can export a snapshot of any image panel with video. When you export a snapshot, you are exporting what the image panel is currently displaying.

1. To export a snapshot, do one of the following:
    - In the image panel, click  .
    - Right-click the image panel and select **Save Snapshot**.

    The snapshot Export tab is opened, and the image you want to export is displayed.

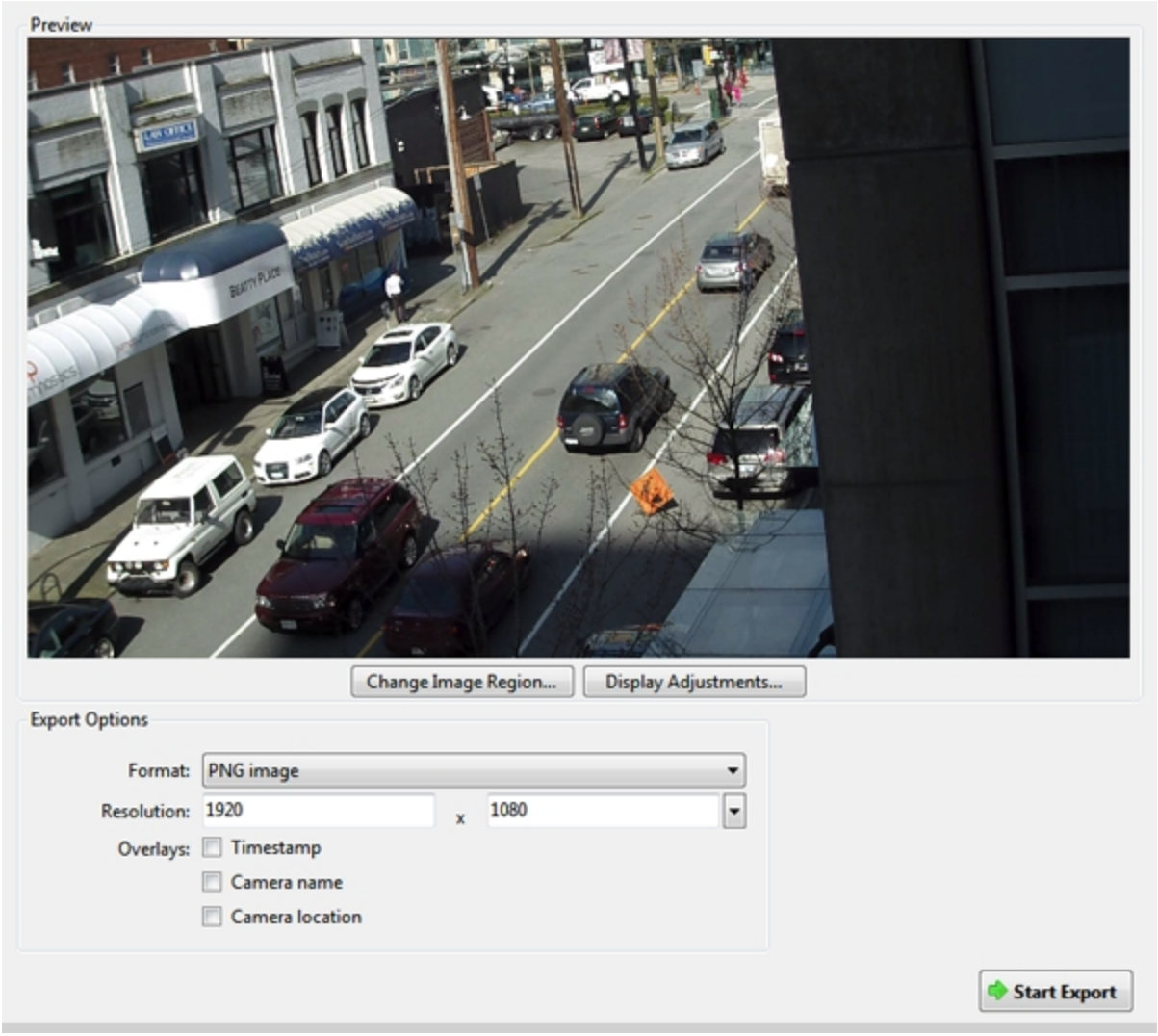


Figure 37: The Export tab for snapshot export

2. In the **Format:** drop down list, select an export format.
3. For the selected export format, define your preferences:

Format	Export options
Native **NOTE:** The Native format requires the Avigilon Control Center Player to view.	This is the recommended export format because the exported image maintains its original compression and can be authenticated against tampering in the Avigilon Control Center Player.
PNG image	1. In the **Resolution:** field, select a resolution for the video image. You can manually enter the resolution or click the drop down arrow to select a standard resolution. **NOTE:** The Resolution: field automatically maintains the image aspect ratio. 2. Select the image overlays you want: **Timestamp**, **Camera name**, and **Camera location**.

Format	Export options
	3. Click **Change Image Region...** to only export part of the video image. In the **Change Image Region** dialog box, move and resize the green overlay, then click **OK**. Only areas highlighted in green are exported. 4. Click **Display Adjustments...** to adjust the **Gamma:**, **Black Level:**, and/or **White Level:**.
JPEG image	1. In the **Quality:** drop down list, select the exported image quality level. 2. Set the image **Resolution:**. 3. Select the image overlays you want. 4. Click **Change Image Region...** to only export a part of the video image. 5. Click **Display Adjustments...** to modify the image quality.
TIFF image	1. Set the image **Resolution:**. 2. Select the image overlays you want. 3. Click **Change Image Region...** to only export a part of the video image. 4. Click **Display Adjustments...** to modify the image quality.
Print image	1. Click **Printer Settings...** to change the selected printer and paper size. 2. Select the image overlays you want. 3. Click **Add Export Notes...** to add notes about the exported image. The notes are printed below the image. 4. Click **Change Image Region...** to only export a part of the video image. 5. Click **Display Adjustments...** to modify the image quality.
PDF file	1. Select the image overlays you want. 2. Click **Add Export Notes...** to add notes about the exported image. 3. Click **Change Image Region...** to only export a part of the video image. 4. Click **Display Adjustments...** to modify the image quality.

4. Click **Start Export**.
5. In the Save As dialog box, name the export file and click **Save**. If you are printing the snapshot, the image is sent to your printer instead.

   The Preview area displays the snapshot you are exporting.
6. When the export is complete, click **OK**.

Exporting Still Images

Video can be exported as a series of still PNG images, JPEG images, or TIFF images. When you export a series of still images, you are exporting each frame of video as an independent file.

If you only want one photo of the video you are watching, take a snapshot. For more information, see **Exporting a Snapshot of an Image**.

1. In the New Task menu, click  . The Export tab opens.

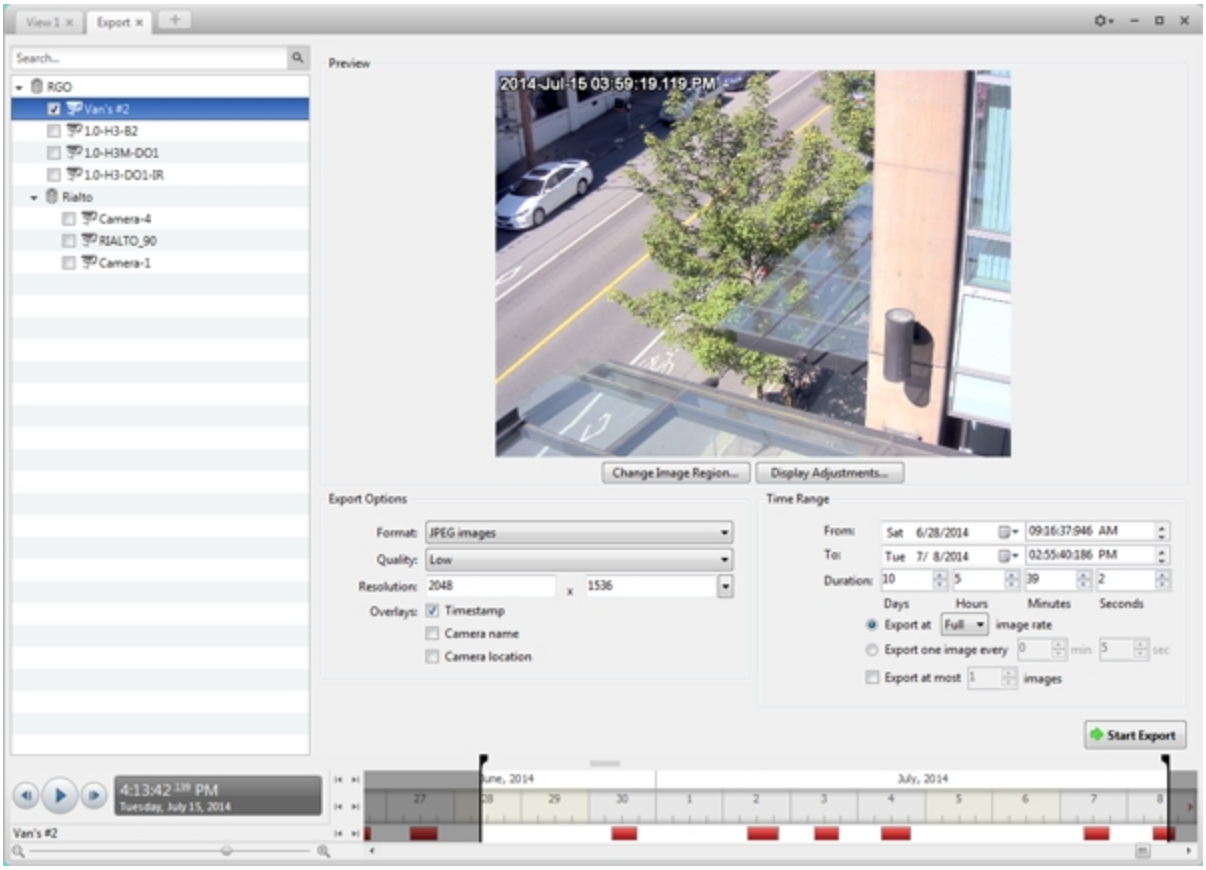


Figure 38: Export tab for still image export

2. In the **Format:** drop down list, select **PNG images**, **JPEG images**, or **TIFF images**.
3. In the System Explorer, select the camera video you want to export.
4. (JPEG only) In the **Quality:** drop down list, select the exported image quality level.
5. In the **Resolution:** field, select a resolution for the video image. You can manually enter the resolution or click the drop down arrow to select a standard resolution.

   NOTE: The Resolution: field automatically maintains the image aspect ratio.
6. Select the image overlays you want: **Timestamp**, **Camera name**, and **Camera location**.
7. Enter the **Time Range** you want to export. The **Time Range** is highlighted on the Timeline by black time range markers. You can also drag the time range markers to modify the time range.

8. Set the export image rate:

Option	Description
Export at _ image rate	Select this option to control how many images per second are exported. For example, the video is streaming at 30 images per second. If you select **1/2**, only 15 images for that second will be exported.
Export one image every _ min _sec	Select this option to control the time between each exported video image. For example, if you enter *5* min. *0* sec., only one image will be exported for every 5 minutes of video.

9. To limit the number of images that are exported, select the **Export at most _ images** check box and enter a number.
10. Click **Change Image Region...** to only export part of the video image. In the **Change Image Region...** dialog box, move and resize the green overlay to select the region you want to export, then click **OK**. Only areas highlighted in green will be exported.
11. Click **Display Adjustments...** to adjust the **Gamma:**, **Black Level:** and/or **White Level:**.
12. Click **Start Export**.
13. In the Save As dialog box, name the export file and click **Save**.

    The Preview area displays the video you are exporting.
14. When the export is complete, click **OK**.

Exporting WAV Audio

If you want to export audio with video, simply export the video in Native or AVI format. Any audio that is linked to the video is automatically included in the export file.

This procedure exports the audio alone.

1. In the New Task menu, click  . The Export tab opens.

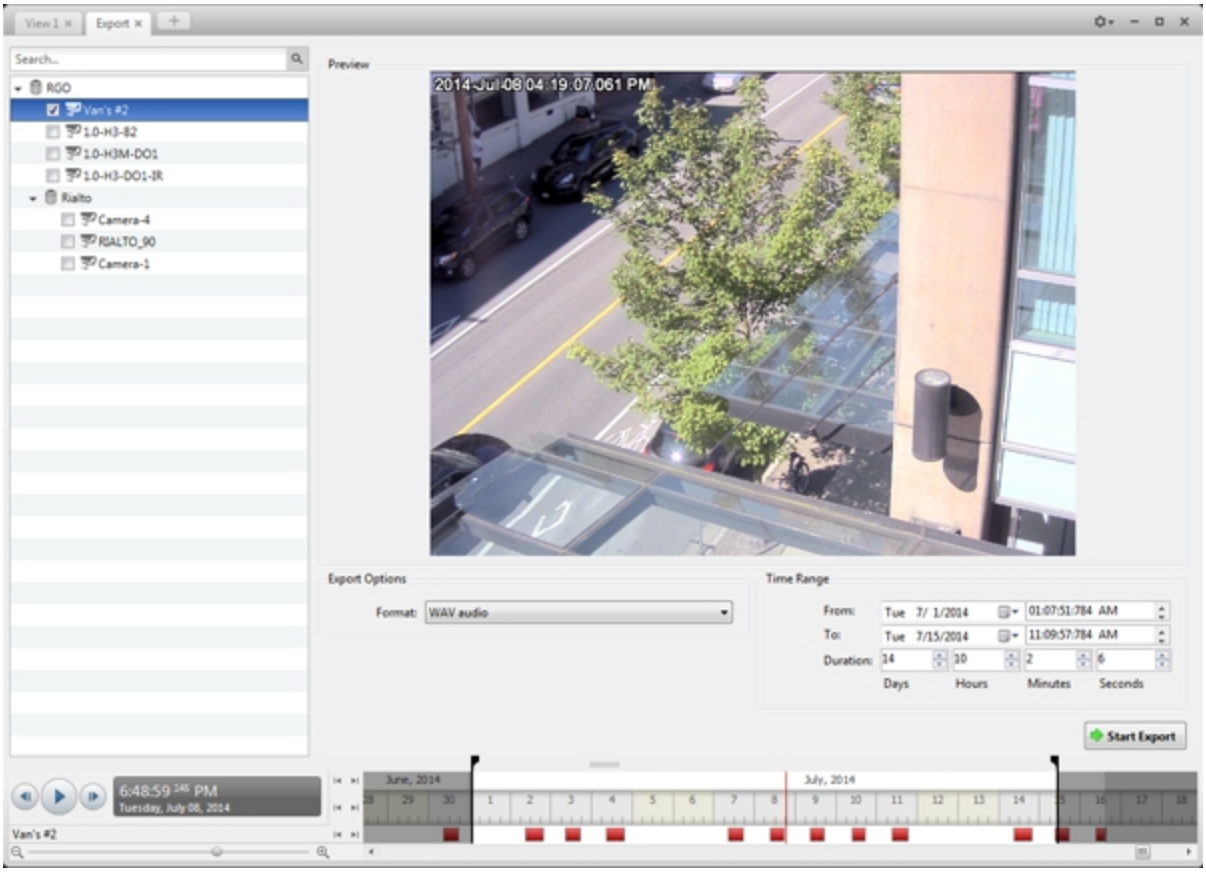


Figure 39: Export tab for audio export

2. In the **Format:** drop down list, select **WAV audio**.
3. In the System Explorer, select the camera that the audio is linked to.
4. Enter the **Time Range** you want to export. The **Time Range** is highlighted on the Timeline by black time range markers. You can also drag the time range markers to modify the time range.
5. Click **Start Export**.
6. In the Save As dialog box, name the export file and click **Save**.

   The Preview area displays the video linked to the audio you are exporting.
7. When the export is complete, click **OK**.

Backup

If you need to export a large amount of camera video, it is faster to back up the content into Avigilon Backup (AVK) format. AVK files can be opened in the Avigilon™ Control Center Player and re-exported as needed.

It is recommended that you export video of individual events and back up video for your archives. For more information, see **Export**.

Be aware that you can only back up video if the option is enabled in the Avigilon Control Center Admin Tool. For more information, see *The Avigilon Control Center Server User Guide*.

Backing Up Recorded Video On Demand

If you want a copy of the recorded video in your system, use the backup feature. Video is always backed up in Avigilon Backup (AVK) format. You can review the backed up video in the Avigilon Control Center Player.

The backup files are stored in a backup folder set by the Avigilon™ Control Center Admin Tool. For information about changing the backup folder, see *The Avigilon Control Center Server User Guide*.

1. In the application window, click  >  .

   The Backup tab is displayed.

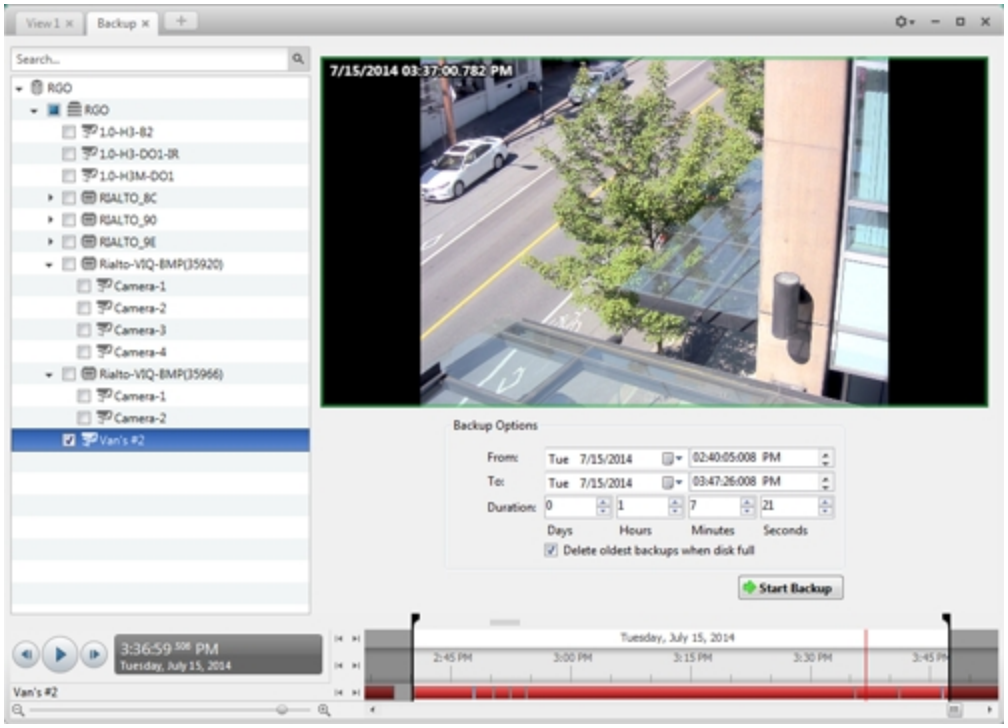


Figure 40: The Backup tab

2. In the System Explorer, select all the cameras you want to back up.

3. In the **Backup Options** area, set the time range you want to back up. The time range is highlighted on the Timeline by the black time range markers. You can also drag the time range markers to change the time range.
4. Select the **Delete oldest backups when disk full** check box to allow the application to automatically overwrite old backup files when the backup folder is full.
5. Click **Start Backup**.
6. When the backup is complete, click **OK**.

This Page Left Intentionally Blank

Avigilon™ Gateway Web Client User Guide

Version 5.4.2

Avigilon Corporation
http://www.avigilon.com

Revised: 2014-12-09

PDF-GATEWAYWC-E-Rev1

Table of Contents

Introduction

The Avigilon™ Gateway Web Client works with the Avigilon™ Control Center Gateway to give users remote access to your Avigilon™ Control Center system. The Gateway Web Client is a simplified web browser version of the Avigilon™ Control Center Client software that gives you access to Sites and cameras configured by the Gateway.

The Gateway Web Client differs from the Avigilon™ Control Center Web Client in that the Gateway Web Client accesses the Avigilon™ Control Center system through the Gateway to protect the security of the server. The Avigilon™ Control Center Web Client requires direct access to the server and may not be accessible outside of your local area network.

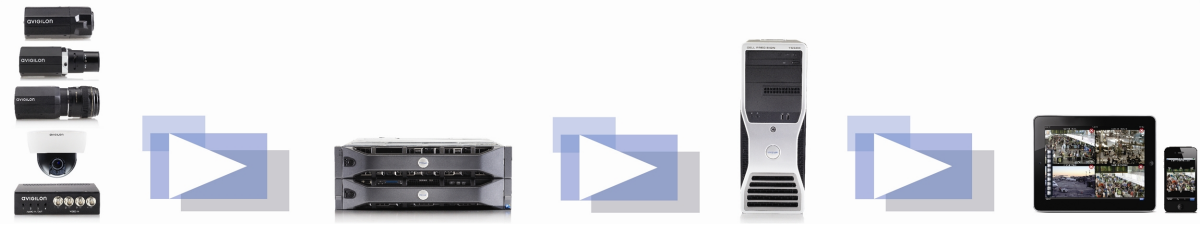


Figure 1: The Avigilon Control Center system workflow

Installation

The Gateway Web Client is part of the Gateway and is automatically installed with it. The Gateway is available for download from the Avigilon website: **http://avigilon.com/support-and-downloads**.

The Gateway must be installed on a computer that has network access to your Avigilon Control Center system. For more information, see *The Avigilon Control Center Gateway User Guide*.

For More Information

Visit Avigilon at **http://www.avigilon.com/** for additional product documentation.

The Avigilon Training Center

The Avigilon Training Center provides free online training videos that demonstrate how to set up and use the Avigilon Surveillance System. Register online at the Avigilon Partner Portal site to begin: **http://avigilon.force.com/login**

Support

For additional support information, visit **http://avigilon.com/support-and-downloads/**. The Avigilon Partner Portal also provides self-directed support resources - register and login at **http://avigilon.force.com/login**.

Regular Avigilon Technical Support is available Monday to Friday from 12:00 a.m. to 6:00 p.m. Pacific Standard Time (PST):

- North America: +1.888.281.5182 option 1
- International: +800.4567.8988 or +1.604.629.5182 option 1

Emergency Technical Support is available 24/7:

- North America: +1.888.281.5182 option 1 then dial 9
- International: +800.4567.8988 or +1.604.629.5182 option 1 then dial 9

E-mails can be sent to: **support@avigilon.com**.

Upgrades

Software and firmware upgrades will be made available for download as they become available. Check **http://avigilon.com/support-and-downloads/** for available upgrades.

Feedback

We value your feedback. Please send any comments on our products and services to **feedback@avigilon.com**

Using the Gateway Web Client

The Gateway Web Client allows you to access your Avigilon Control Center system from any web browser.

To access the Gateway Web Client, you will need the IP Address/Hostname:, User Name: and Password: of the Gateway software, and a user account in the Avigilon Control Center system.

1. In a supported web browser, enter the Gateway IP address in this format: http://<Gateway IP Address>/acc

   NOTE: Supported browsers are: Safari - Versions 6+, Firefox - Versions 15+, Chrome - Versions 20+, Internet Explorer - Versions 9+.

   NOTE: If you are using Firefox, you need to manually override automatic cache management to avoid using excessive amounts of memory. Do the following:

   a. Open Firefox.

   b. Click  >  > **Network**.

   c. Select the **Override automatic cache management** check box. Make sure it is checked.

   d. In the **Limit cache to __ MB of space** field, enter a low value like **10**.

   e. Click **OK**.

2. The browser will prompt you to enter the Gateway **User Name** and **Password**.

   After you log in, the System Explorer will list all the Sites that are connected to the Gateway.

3. Right-click a Site and select **Log In...**
4. In the following dialog box, enter your **User Name:** and **Password:** for the Site then click **Log In**.

All the cameras in the Site are listed in alphabetical order. You can control video like you would in the Avigilon Control Center Client.

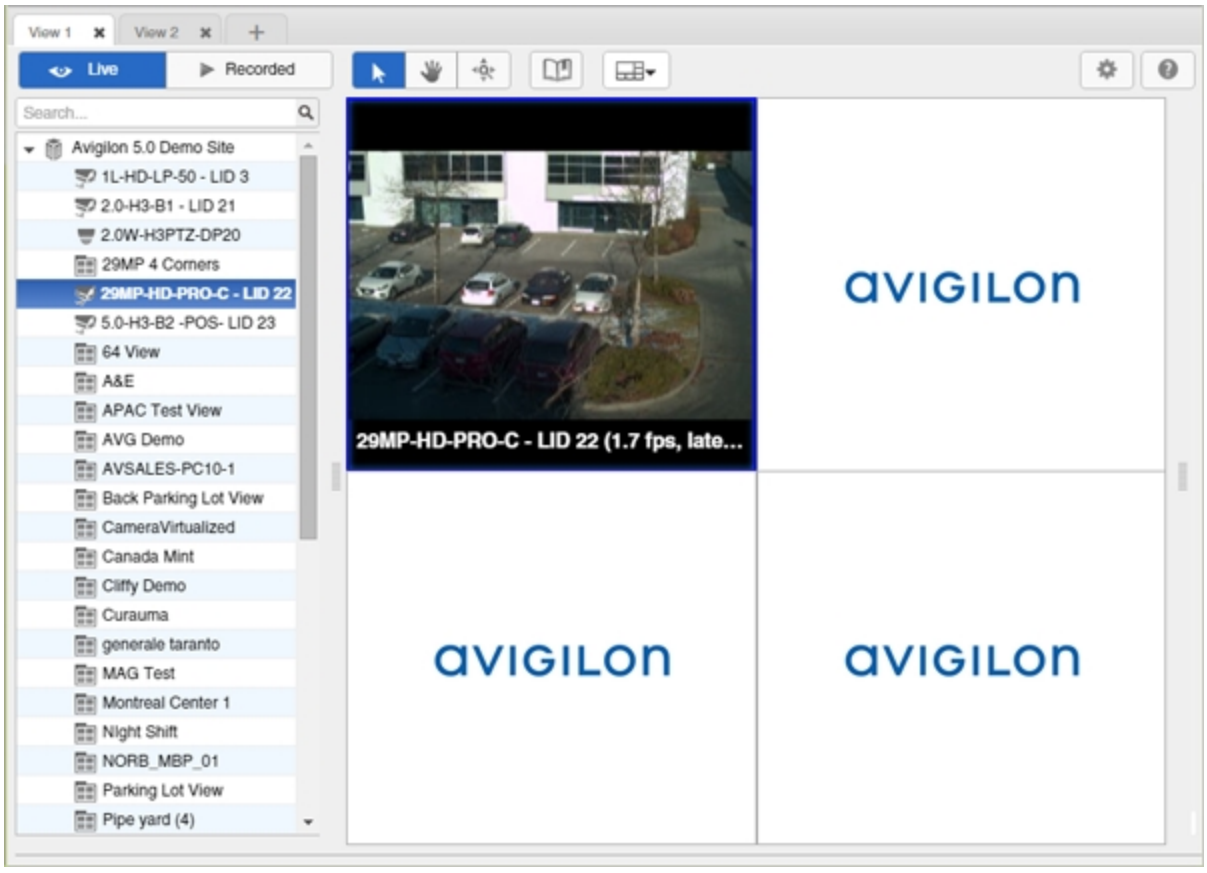


Figure 2: Gateway Web Client page

Logging In to and Out of a Site

After you log in to the Gateway, you will see a list of all the Sites that you have access to through the Web Client.

- To log in to a Site, right-click the Site in the System Explorer and select **Log In...**.
- To log out of a Site, right-click the Site and select **Log Out**.

If you choose to close the tab or the web browser rather than log out, be aware that you are still logged in to the Site. The session automatically times out after 5 minutes, but you will still be able to access your last session through the web browser history until then.

Navigating the Gateway Web Client

Once you log in, the Gateway Web Client application window is populated with all the features that are available to you.

NOTE: Some features are not displayed if the server does not have the required license, or if you do not have the required user permissions.

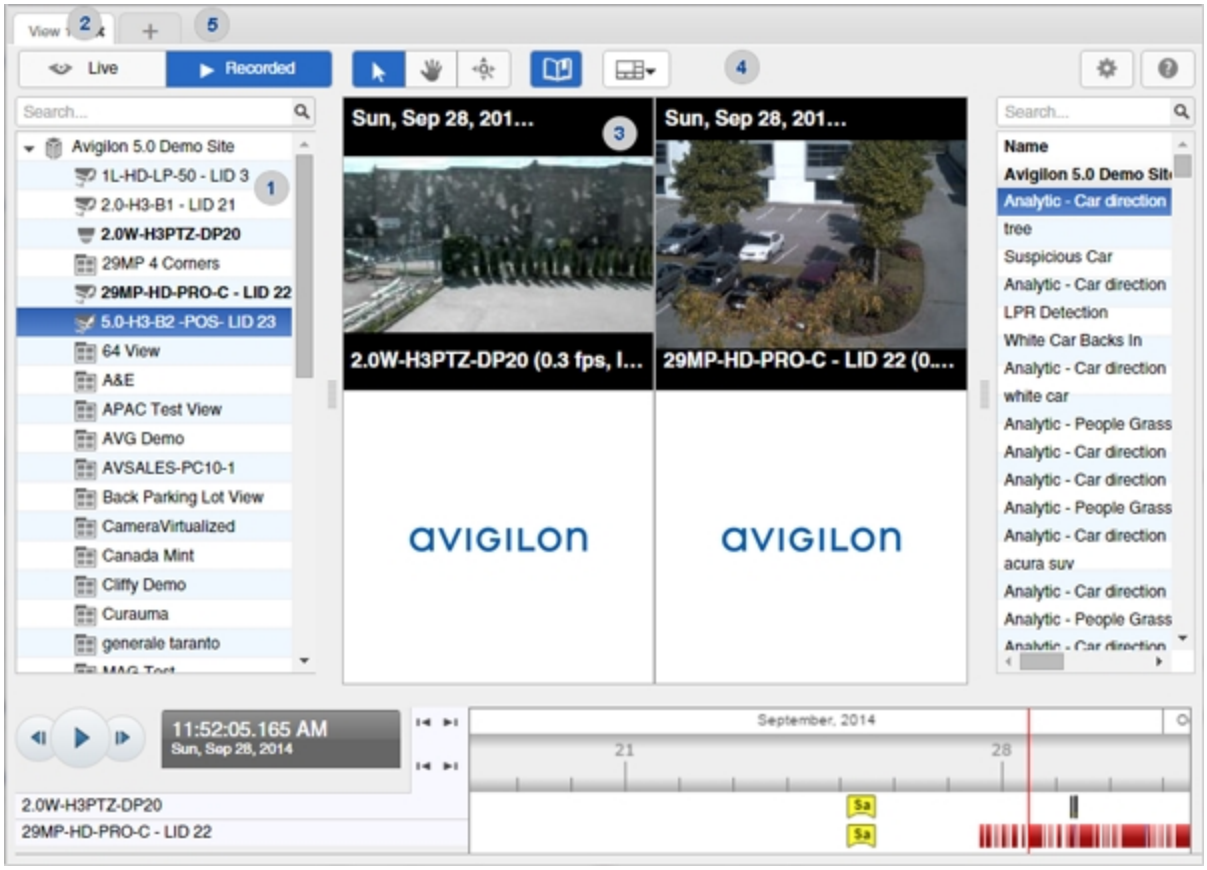


Figure 3: The Avigilon Control Center Gateway Web Client application window.

Application Window Features

	Area	Description
1	System Explorer	Displays all the elements in your surveillance system. Use the **Search...** bar to quickly locate anything that is available in the System Explorer. You can search for items by name, and devices can also be searched for by location, logical ID, serial number and IP address.
2	View tab	Allows you to monitor video and organize image panels. You can have multiple Views open at once.
3	Image panel	Displays live or recorded video from a camera. The video control buttons are displayed when you move your mouse into the image panel.

	Area	Description
4	Toolbar	Provides quick access to commonly used tools.
5	Task tabs	Displays all the tabs that are currently open.
	Add View tab button	To open a new View tab, click  . To close a View tab, click  .
	Image Display Settings menu	This menu gives you access to image display settings.

System Explorer Icons

Icon	Description
	A Site. Listed under a Site are connected devices and linked features in the system.
	A camera.
	A PTZ camera.

Adding and Removing Cameras

Adding a Camera to a View

Do one of the following:

- Drag the camera from the System Explorer to an empty image panel in the View tab.
- Double-click a camera in the System Explorer.
- In the System Explorer, right-click the camera and select **Add To View**.

  The camera is added to the next empty image panel in the View layout.

Tip: You can drag the same camera to multiple image panels to watch the video at different zoom levels.

Removing a Camera from a View

Do one of the following:

- Right-click the image panel and select **Close**.
- Inside the image panel, click ✕.

Viewing Live and Recorded Video

NOTE: Some features are not displayed if the server does not have the required license, or if you do not have the required user permissions.

When you monitor video, you can choose to watch live and recorded video in the same View, or only one type of video per View.

Once you've added cameras to the View, perform the following:

- To switch all of the image panels in the View between live and recorded video, click either  **Live** or  **Recorded** on the toolbar.
- To switch individual image panels between live and recorded video, right-click the image panel and select either **Live** or **Recorded**.

Adjusting Image Quality

If the video is not as clear as you would like, you can adjust the image quality.

- In the image panel, right-click and select **Image Quality:** then select a setting number.

An image quality setting of **1** will produce the highest quality video and require the most bandwidth. The default setting is **5**.

Controlling Recorded Video

The Timeline is displayed when you watch recorded video.

The colored bars on the Timeline show the camera's recording history:

- A red bar shows the camera has recorded a motion event.
- A blue bar shows the camera has recorded video.
- White areas show periods of time during which the camera has not recorded any video.
- An yellow bar is a bookmark in the camera's recording history.

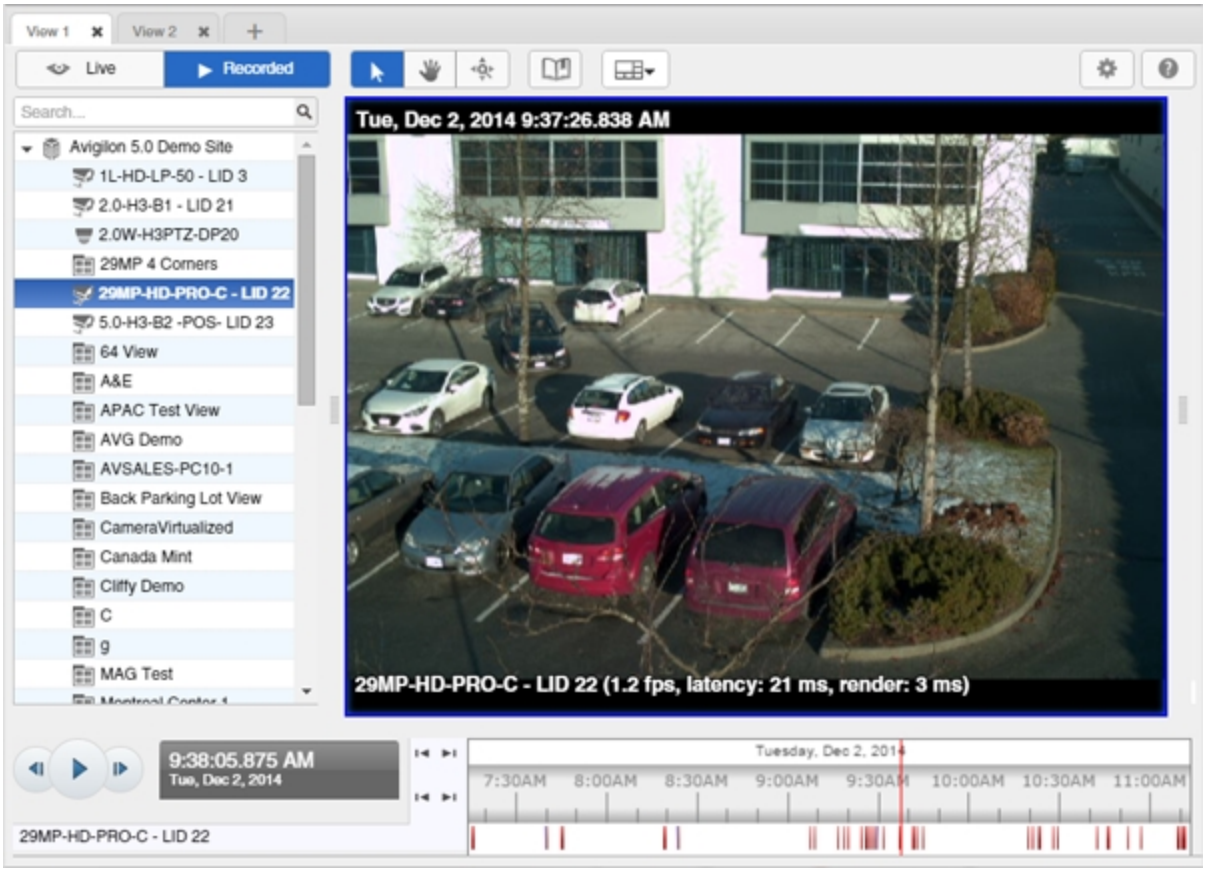


Figure 4: Recorded video and Timeline

To control recorded video, do any of the following:

- To select a playback time, click on a point in the Timeline.
- To start playback, click  .

- To stop playback, Click  .
    - Click  to step forward one frame.
    - Click  to step backward one frame.
- To zoom in or out on the Timeline, place your mouse over the Timeline and use the scroll wheel to zoom in or out. You can zoom in to a quarter of a second, and zoom out to see years.
- To pan the Timeline:
    - Click and drag the red time marker through the Timeline.
    - Right-click and drag the Timeline.

Controlling PTZ Cameras

If you have a pan, tilt, zoom camera connected to your Site, you can control the PTZ camera by using the on-screen controls in the image panel.

To display the PTZ on-screen controls, click  .

- In the image panel, drag your mouse from center to move the camera in that direction. The farther the cursor is from the center of the image panel, the faster the camera will move.

Figure 5: PTZ On-screen Controls

- If the camera supports Click to Center, click anywhere in the image panel to center the camera at that point.
- If the camera supports Drag to Zoom, click and drag on the image panel to create a green box to define the area you want to zoom in and see.

Zooming and Panning in a Video

Use the zoom and pan tools to focus on specific areas in the live or recorded video stream.

Using the Zoom Tools

There are two ways to digitally zoom in and zoom out of a video image:

- Move your mouse over the video image, then rotate your mouse wheel forward and backward.

Using the Pan Tools

There are two ways to pan through the video image:

- Right-click and drag inside an image panel
- On the toolbar, select  , then click and drag the video image in any direction inside the image panel.

Maximizing and Restoring an Image Panel

You can maximize an image panel to enlarge the video display.

Maximizing an Image Panel

Do one of the following:

- Right-click an image panel and select **Maximize**.
- Inside the image panel, click  .
- Double-click the image panel.

Restoring an Image Panel

In a maximized image panel, do one of the following:

- Right-click the maximized image panel and select **Restore Down**.
- Inside the image panel, click  .
- Double-click the image panel.

Selecting a Layout for a View

You can organize how video is displayed by selecting a View layout. The figure below shows the default View layouts.

- On the toolbar, select  , then select one of the following layout options.

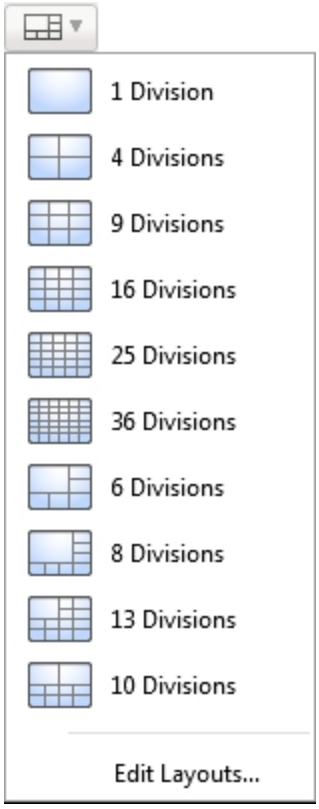


Figure 6: Layouts in the toolbar

Opening a Saved View

Do one of the following

- In the System Explorer, double-click the saved View.
- Drag the saved View from the System Explorer to the current View in the application.

Taking Snapshots

A snapshot allows you to save any image that is displayed in an image panel.

- In the image panel, click  .

The current image in the image panel is immediately downloaded through your browser.

Viewing Saved Bookmarks

You can view and search for saved bookmarks.

- On the toolbar, select  . The Bookmark Explorer opens.

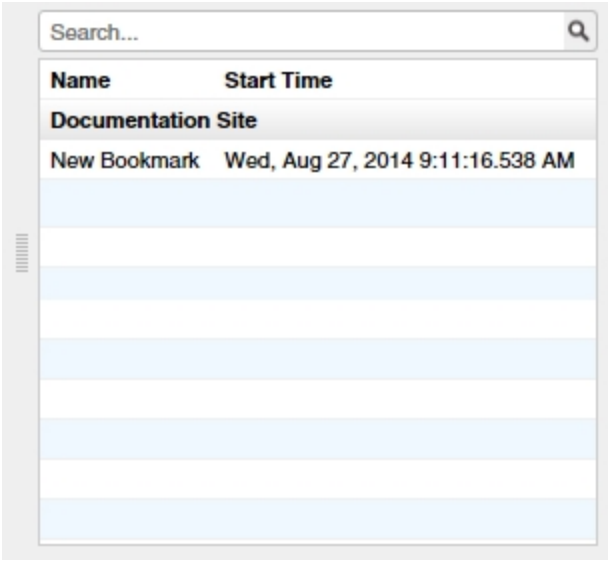


Figure 7: The Bookmark Explorer

The following information is grouped by Site. You can use it to search for a specific bookmark.:

- **Name** - the name of the bookmark.
- **Start Time** - the start time of the bookmark.

Double click on a bookmark to display its video in the View.

Click on a bookmark in the Timeline (highlighted in yellow) to view its Name, Start Time, and End Time.

This Page Left Intentionally Blank

Avigilon™ Control Center Enterprise Client User Guide

Version 5.4.2

Avigilon Corporation
http://www.avigilon.com

Revised: 2014-12-09

PDF-CLIENT5-E-Rev1

Table of Contents

What is the Avigilon™ Control Center Client?

The Avigilon™ Control Center Client software works with the Avigilon™ Control Center Server software to give you access and control of your Avigilon High Definition Stream Management (HDSM)™ surveillance system.

The Client software allows you to view live and recorded video, monitor events, and control user access to the Control Center. The Client software also gives you the ability to configure your surveillance system.

The Client software can run on the same computer as the Server software, or run on a remote computer that connects to the Site through a local area network (LAN) or a wireless area network (WAN).

What you can do in the Client software depends on the Server software edition. There are three editions of the Server software available: Core, Standard and Enterprise. Visit the Avigilon website for an overview of the features available in each edition: **http://avigilon.com/products/video-surveillance/avigilon-control-center/editions/**

A copy of the Client software can be downloaded from the Avigilon website or installed with the Server software.

System Requirements

	Minimum requirements	Recommended requirements
Monitor resolution	1280 x 1024	1280 x 1024
OS	Windows Vista, Windows 7, Windows 8 (32-bit or 64-bit), or Windows 8.1	Windows 7 (64-bit)
CPU	Intel Dual Core 2.0 GHz processor	Quad Core 2.0 GHz
System RAM	2 GB	2 GB
Video card	PCI Express, DirectX 10.0 compliant with 256 MB RAM	PCI Express, DirectX 10.0 compliant with 256 MB RAM
Network card	1 Gbps	1 Gbps
Hard disk space	500 MB	500 MB

For More Information

Visit Avigilon at **http://www.avigilon.com/** for additional product documentation.

The Avigilon Training Center

The Avigilon Training Center provides free online training videos that demonstrate how to set up and use the Avigilon Surveillance System. Register online at the Avigilon Partner Portal site to begin: **http://avigilon.force.com/login**

Support

For additional support information, visit **http://avigilon.com/support-and-downloads/**. The Avigilon Partner Portal also provides self-directed support resources - register and login at **http://avigilon.force.com/login**.

Regular Avigilon Technical Support is available Monday to Friday from 12:00 a.m. to 6:00 p.m. Pacific Standard Time (PST):

- North America: +1.888.281.5182 option 1
- International: +800.4567.8988 or +1.604.629.5182 option 1

Emergency Technical Support is available 24/7:

- North America: +1.888.281.5182 option 1 then dial 9
- International: +800.4567.8988 or +1.604.629.5182 option 1 then dial 9

E-mails can be sent to: **support@avigilon.com**.

Upgrades

Software and firmware upgrades will be made available for download as they become available. Check **http://avigilon.com/support-and-downloads/** for available upgrades.

Feedback

We value your feedback. Please send any comments on our products and services to **feedback@avigilon.com**

Getting Started

Once the Avigilon™ Control Center Client software has been installed, you can start using the Avigilon High Definition Stream Management (HDSM)™ surveillance system immediately. Refer to any of the procedures in this section to help you get started.

Starting Up and Shutting Down the Control Center Client

The Control Center Client software can be started or shut down at anytime - video recording is not affected because it is controlled separately by the Server software.

Starting Up the Client Software

Perform one of the following:

- In the Start menu, select **All Programs** or **All Apps > Avigilon > Control Center Client**.
- Double-click the  shortcut icon on the desktop.
- From the Avigilon Control Center Admin Tool, click **Launch Control Center Client**. For more information, see the *Avigilon Control Center Server User Guide*.

Log in to your Site when the Log In dialog box appears. For more information, see **Logging In to and Out of a Site**

Shutting Down the Client Software

1. In the top-right corner of the Client, select ⚙ **> Exit**.
2. In the confirmation dialog box that appears, click **Yes**.

Logging In to and Out of a Site

To access any of the features in your Avigilon High Definition Stream Management (HDSM)™ surveillance system, you must log in to a Site.

The default administrator access uses *administrator* as the username and no password. To maintain the security of the administrator account, it is recommended that your system administrator immediately create a password for this account after the first login. Your system administrator can then create user accounts for other users.

Logging In

1. Open the Log In dialog box. The Log In dialog box automatically appears when the Client software is launched.

   To manually access the Log In dialog box, do one of the following:

- In the top-right corner of the Client, select > **Log In...** to log in to all available Sites.
- In the System Explorer, right-click a Site and select **Log In...** to log in to the selected Site.

2. In the Log In dialog box, select a specific Site or select **All Sites** from the **Log in to:** drop down list.

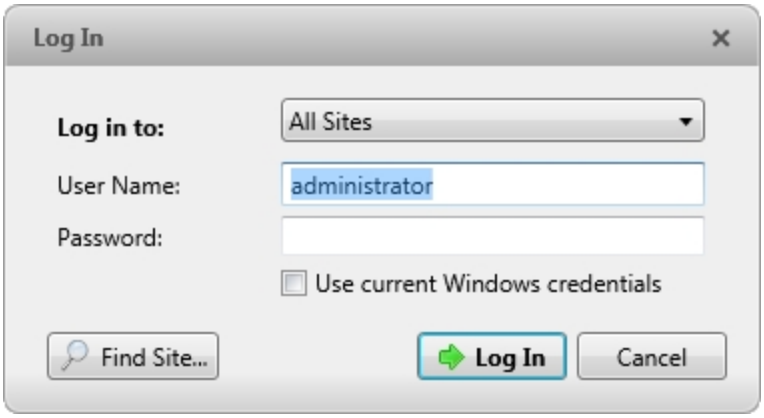


Figure 1: The Log In dialog box

Tip: If you accessed the Log In dialog box from a specific Site, you will not have the option of logging in to All Sites.

If the Site you want to log into is not shown, click to discover the Site. For more information, see **Discovering Sites**.

3. Enter your **User Name:** and **Password:**. Or, select the **Use current Windows credentials** check box to automatically use the same username and password as your computer.
4. Click **Log In**.

After logging in the first time, you can set up automatic login from the Client Settings... dialog box. For more information, see **General Settings**.

Logging Out

You can log out of one or all Sites at any time.

To...	Do this...
Log out of one Site	1. In the System Explorer, right-click the Site and select **Log Out**.
Log out of all Sites	1. In the top-right corner of the Client, select > **Log Out**. 2. In the confirmation dialog box, click **Yes**.

Navigating the Client

Once you log in, the Avigilon™ Control Center Client application window is populated with all the features that are available to you.

NOTE: Some features are not displayed if the server does not have the required license, or if you do not have the required user permissions.

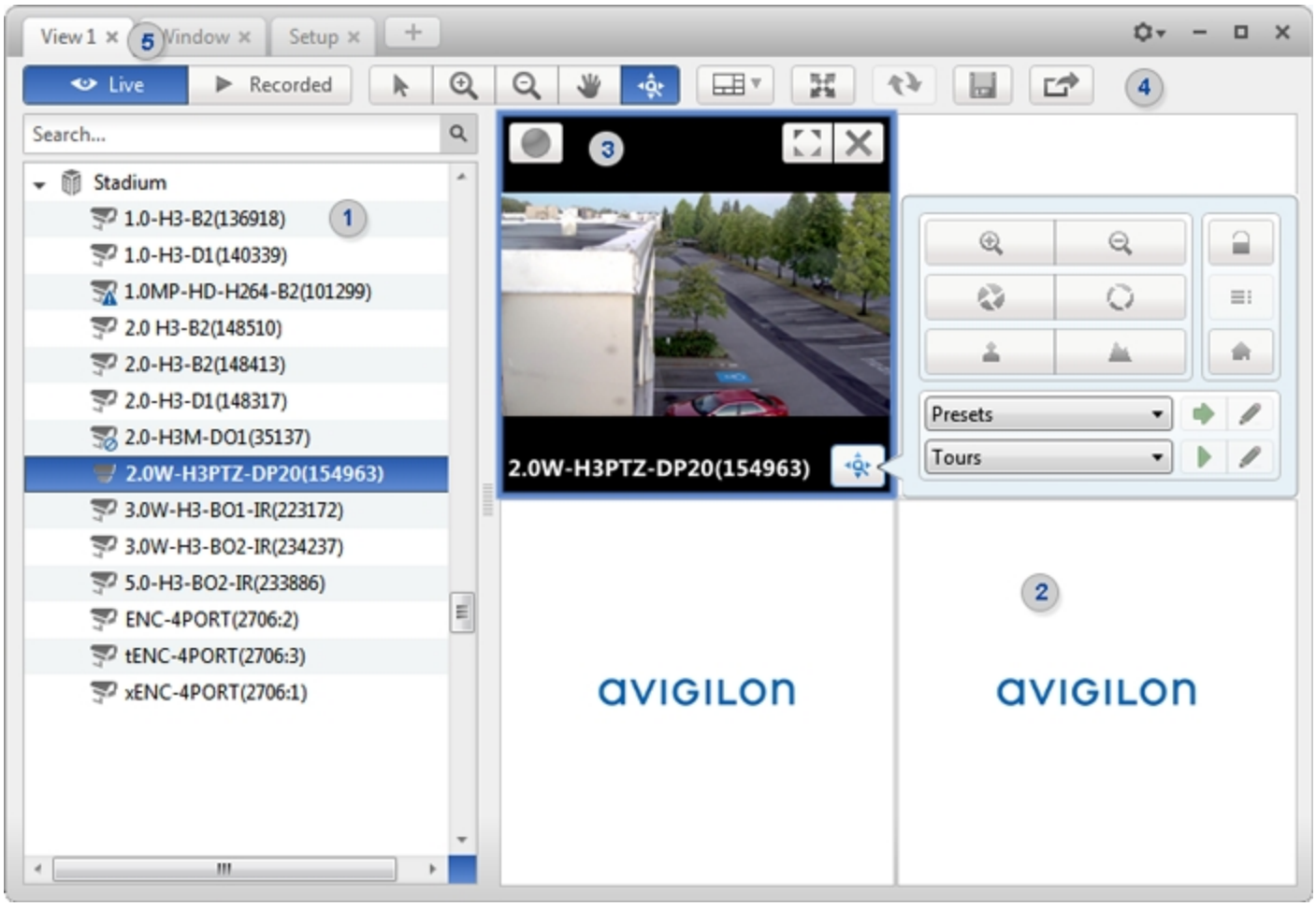


Figure 2: The Avigilon Control Center Client application window.

Application Window Features

	Area	Description
1	System Explorer	Displays all the elements in your surveillance system. Use the **Search...** bar to quickly locate anything that is available in the System Explorer. You can search for items by name, and devices can also be searched for by location, logical ID, serial number and IP address. **Tip:** The content of the System Explorer changes depending on the tab you have open. For example, servers are not listed in the View tab.
2	View tab	Allows you to monitor video and organize image panels. You can have multiple Views open at once.
3	Image panel	Displays live or recorded video from a camera. The video control buttons are displayed when you move your mouse into the image panel.
4	Toolbar	Provides quick access to commonly used tools.
5	Task tabs	Displays all the tabs that are currently open.

	Area	Description
	The New Task button	Opens the New Task menu so you can select and open new task tabs. You can access advanced tools like Search and Export, or system administrative features like Site Setup.
	The Application Menu menu	This menu gives you access to local application settings like Client Settings.... You can also open a new window from this menu.
	System message list	The highlighted number shows the number of system messages that need your attention. Click the number to display the list of messages. The highlight color indicates the severity of the most recent message. • **Red** = Error • **Yellow** = Warning • **Green** = Information

System Explorer Icons

Icon	Description
	A Site. Listed under a Site are all the connected devices and linked features in the system.
	A server.
	A camera.
	A PTZ camera.
	An encoder.
	A Virtual Matrix monitor.
	A saved View.
	A map.
	A web page.

Adding and Removing Cameras in a View

To monitor video, add a camera to a View. Camera video can be removed from a View at any time.

Adding a Camera to a View

Do one of the following:

- Drag the camera from the System Explorer to an empty image panel in the View tab.
- Double-click a camera in the System Explorer.
- In the System Explorer, right-click the camera and select **Add To View**.

  The camera is added to the next empty image panel in the View layout.

Tip: You can drag the same camera to multiple image panels to watch the video at different zoom levels.

Removing a Camera from a View

Do one of the following:

- Right-click the image panel and select **Close**.
- Inside the image panel, click  .

Viewing Live and Recorded Video

NOTE: Some features are not displayed if the server does not have the required license, or if you do not have the required user permissions.

When you monitor video, you can choose to watch live and recorded video in the same View, or only one type of video per View.

Once you've added cameras to the View, perform the following:

- To switch all of the image panels in the View between live and recorded video, click either  **Live** or  **Recorded** on the toolbar.
- To switch individual image panels between live and recorded video, right-click the image panel and select either **Live** or **Recorded**.

Image panels displaying recorded video have a **green** border.

Accessing the Setup Tab

The Setup tab is where you would configure the majority of your system – including Sites, servers and cameras.

Follow one of the following steps to open the Setup tab:

- At the top of the application window, click  to open the New Task menu. When the menu appears, click  .
- In the System Explorer, right-click the device you want to configure, then select **Setup**.

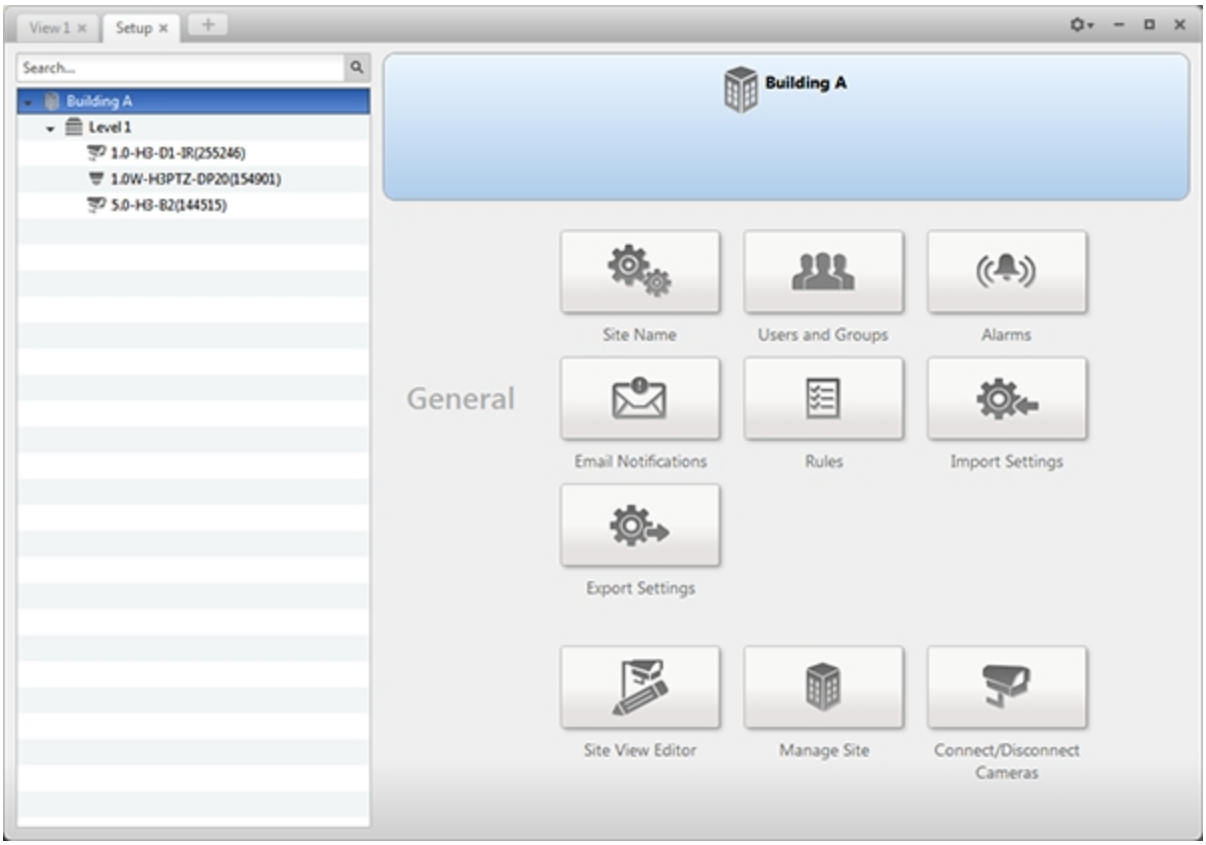


Figure 3: The Setup tab

In the Setup tab, the System Explorer is displayed on the left and the Setup options are displayed on the right. The Setup options change depending on the device that is selected in the System Explorer.

Managing a Site

NOTE: Some features are not displayed if the server does not have the required license, or if you do not have the required user permissions.

The default settings in the Avigilon™ Control Center Client software allow you to start using the application immediately after installation. However, you may want to customize and set up your Site to reflect how the system will be used in daily operations.

In Avigilon Control Center 5, servers are maintained in clusters called Sites. Each Site can contain multiple servers that share configuration settings across the entire Site.

At the Site level, you can manage your server and device connections, as well as set up Site-wide system events.

At the server level, you can manage the recording and bandwidth for each of the server's connected cameras.

At the device level, you can edit the camera image quality and other device-specific features.

All the Site, server and device settings can be configured from the Setup tab.

Sites and Servers

In the Avigilon Control Center software, servers are organized in clusters called Sites. By organizing the system into clusters, you are able to control user access and system wide events through the Site settings. Site settings are stored on the server, or across all servers in a multi-server system.

Depending on your system and license edition, you may have multiple servers in a Site. When there are multiple servers in a Site, the Site is able to distribute tasks and system data between the servers so that the system can continue running even if a server fails.

Within a Site, each individual server is responsible for managing the devices that are connected to it. Specifically, the server controls video recording. Through the server settings, you control when video is recorded, how long it is stored, and how much bandwidth is used to stream video.

Discovering Sites

If your computer is on the same network segment (subnet) as a Site, that Site is automatically discovered and displayed in the System Explorer.

If the Site you want to access is not listed, it is because the Site is on a different subnet and must be manually discovered. There is no limit to the number of Sites that can be discovered by the Client software.

By default, when a server is first connected to the system, it is added to a Site with the same name. To locate a new server, you need to search for its Site.

1. Open the Find Site dialog box.
   - In the top-right corner of the Client, select > **Log In...** . In the Log In dialog box, click .
   - Or, select > **Client Settings...** > **Site Networking**. In the Site Networking tab, click .

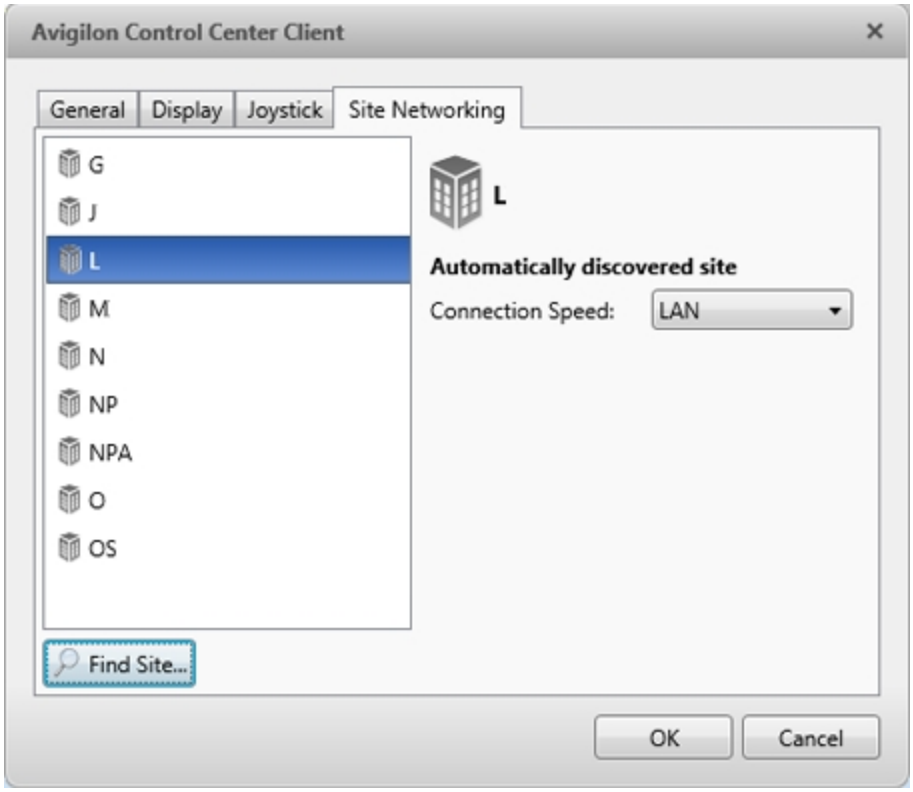


Figure 4: The Site Networking tab

2. In the dialog box, enter the **IP Address/Hostname:** and the **Base Port:** of the server in the Site you want to discover.

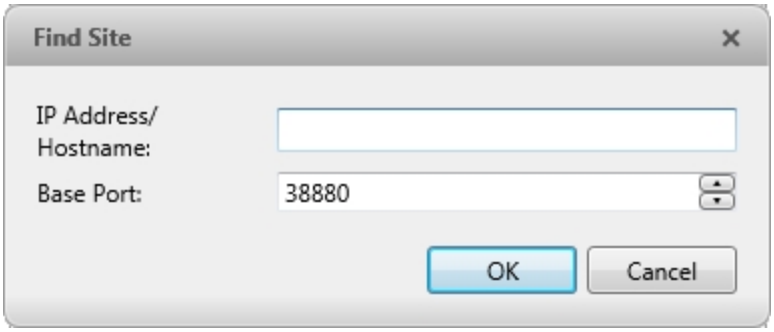


Figure 5: The Find Site dialog box

   The base port is 38880 by default. You can change the base port number in the Avigilon Control Center Admin Tool. For more information, see *The Avigilon Control Center Server User Guide*.

3. Click **OK**.

If the Site is found, it is automatically added to the Site list in the Site Networking tab.

If the Site is not found, check the following then try again:

- The network settings are configured correctly.
- The firewall is not blocking the application.
- The Avigilon Control Center Server software is running on the server you searched for in step 2.

Sharing Site Settings Between Client Users

When a user sets up Sites on an Avigilon Control Center Client or Virtual Matrix Application, the following global settings are shared for all users that are logged in to that machine:

- Sites that have been manually discovered in the Site Networking tab in the Client Settings... dialog box will be visible to all users. Users will not be able to access the manually discovered Sites if they do not have the required access permissions.
- A Site's **Connection Speed:** settings in the Site Networking tab will be common to all users.

User permissions are as follows:

- **Administrators** - Can always read and write global LAN/WAN settings and manually add Sites.
- **Standard Users** - Can always read global LAN/WAN settings and manually add Sites. Sites added manually by Standard Users will default to WAN. Standard Users cannot change this.

Managing Site Logs

The Site Logs record events that occur in the Avigilon Control Center. This can be useful for tracking system usage and diagnosing issues.

You can filter the items displayed in the log and save the log to a separate file for sending to Avigilon support.

NOTE: The Site Logs maintain a record of system events for as long as video data is available or 90 days, whichever is longer.

1. In the New Task menu, click  .

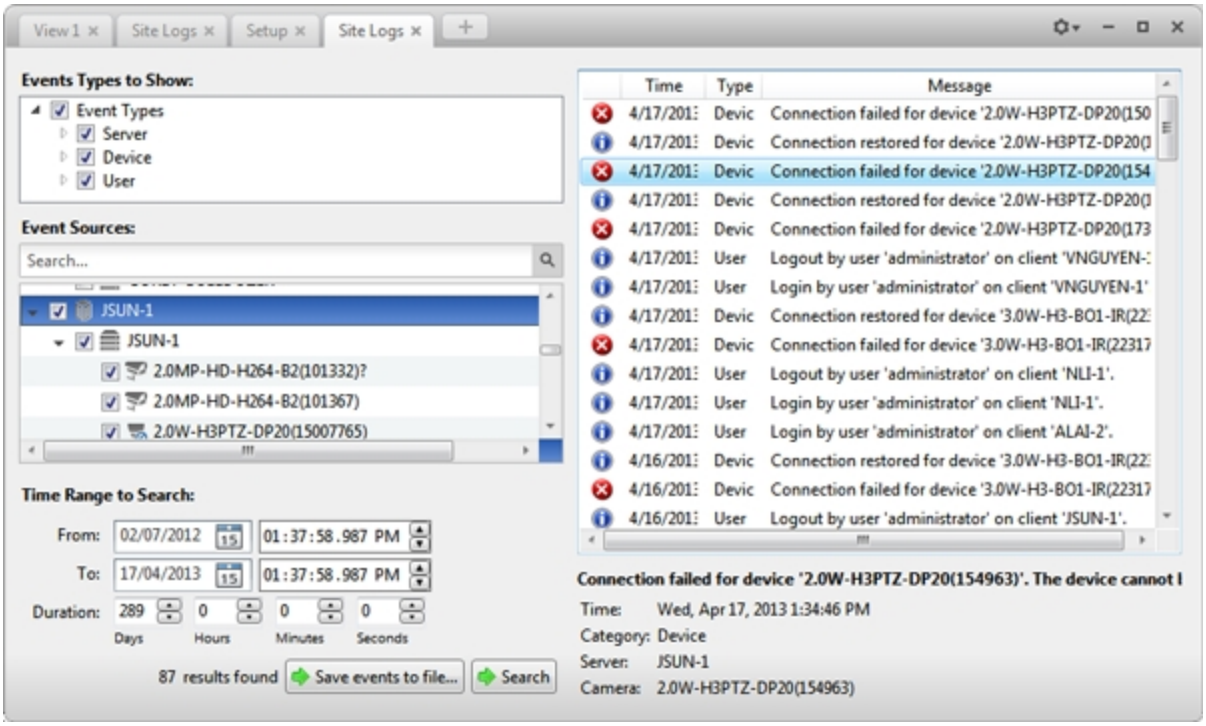


Figure 6: The Site Logs tab

2. In the Site Logs tab, select the **Event Types to Show:**.
3. Next, select the specific Sites, servers and devices whose logs you want to see.
4. In the **Time Range to Search:** area, set the date and time range of your search.
5. Click **Search**.
6. Select a result to display its event details.
7. To save the log search results, click **Save events to file...** and save the file. You can choose to save the search results as a text file or a CSV file.

Managing User Connections

If you find that too many users are logged in through the same username or inactive users are preventing active users from accessing a Site, you can force specific users to log out.

1. In the New Task menu, click  .
2. In the User Connections tab, select a Site from the System Explorer to display a list of all the current users on the right.

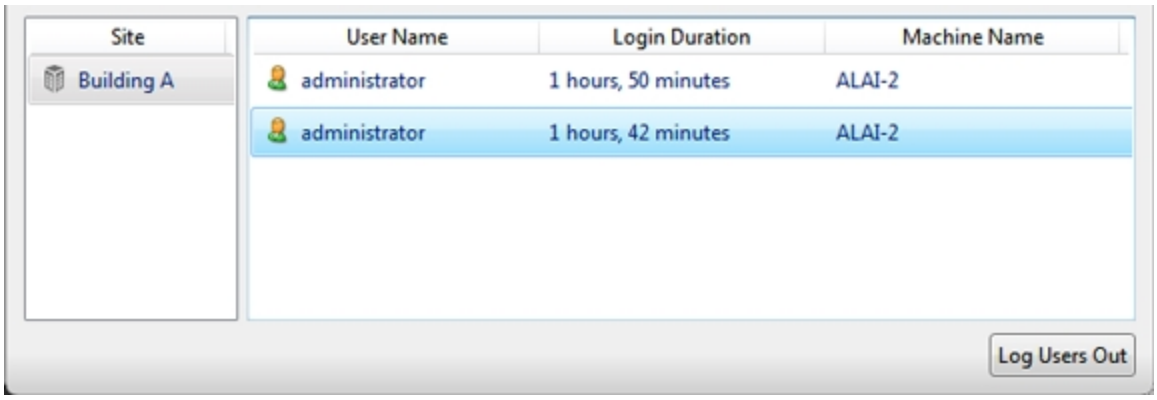


Figure 7: The User Connections tab

- The users are listed by username and computer name so that users that share a login are displayed separately.
- The Login Duration column lets you know exactly how long that user has been logged in to the Site.

3. To force a user to log out of a Site, select a user then click **Log Users Out**.

Monitoring Server Status

To help you monitor the health of your Site, you can access a quick overview in the Server Status tab.

- In the New Task menu, click  .

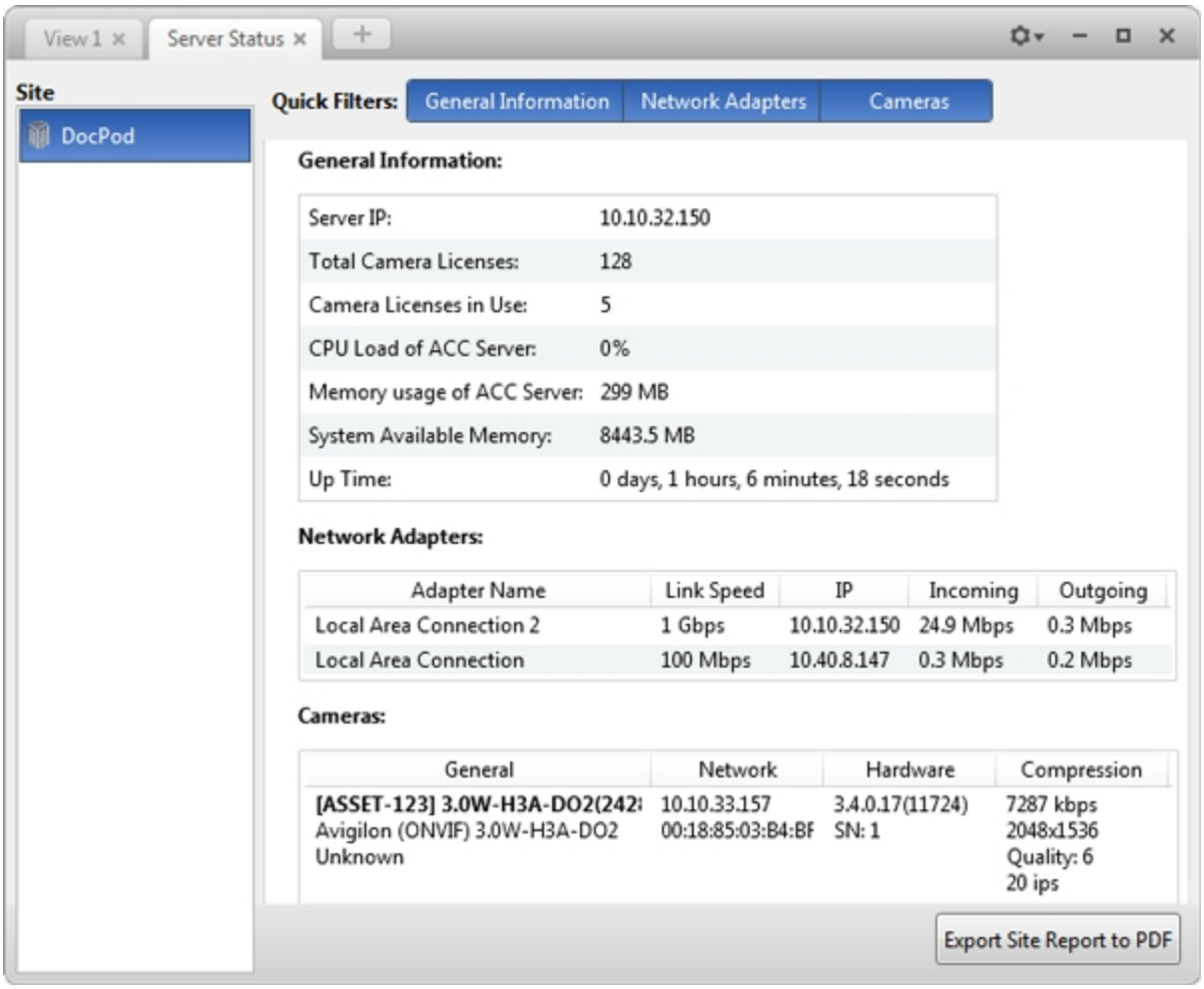


Figure 8: The Server Status tab

In the System Explorer, select a Site to display the statuses of the connected servers. At the top of the tab, click any of the **Quick Filters** to choose what type of information is displayed.

Listed information includes:

1. **General Information:** Information about the server you have selected.
    - **Server IP:** the server's IP address.
    - **Total Camera Licenses:** the total number of camera channel licenses that have been activated on the server.
    - **Camera Licenses in Use:** the number of cameras that are currently connected to the server.
    - **CPU Load of ACC Server:** the percentage of server processing power used by the AvigilonControl Center server software.
    - **Memory usage of ACC Server:** the amount of memory used by the AvigilonControl Center Server software.
    - **System Available Memory:** the amount of storage available for video recording.
    - **Up Time:** the amount of time the server has been running since it was last rebooted.

- **Network Adapters:** the networks that the server is connected to, including the IP address of the network connection, the network speed, and the amount of data passing through the connection.

2. **Network Adapters:**
   - **Adapter Name:** the name of the network adapter.
   - **IP:** the IP address of the network adapter.
   - **Incoming:** the speed of incoming data.
   - **Outgoing:** the speed of outgoing data.
3. **Cameras:** The devices that are connected to this server.
   - **General:** the name, model number, and location of the device.
   - **Network:** the IP and MAC addresses of the device.
   - **Network:** the serial number of the device.
   - **Compression:** the video compression rate, resolution, quality, and images per second (ips) of video streamed from the device.

Click **Export Site Report to PDF** to export the listed server information.

Site Settings

The settings stored at the Site level impact all users and devices within the Site.

These settings include alarms, rules, user account information and email notifications. This is also where you can set up how the System Explorer is laid out, and where you can add or remove servers and devices in a Site.

NOTE: Some features are not displayed if the server does not have the required license, or if you do not have the required user permissions.

Naming a Site

Give the Site a meaningful name so that it can be easily identified in the System Explorer. Otherwise, the Site uses the name assigned to the server it was originally discovered with.

1. In the Site Setup tab, click  .
2. In the dialog box that appears, give the Site a name.

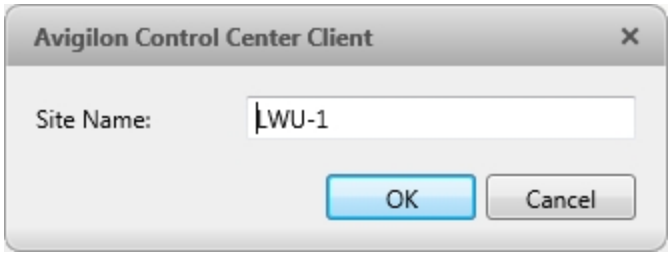


Figure 9: The Site Name: dialog box

Editing the Site View

You can edit the way your Site is organized in the View tab so that it reflects how your system is set up.

Through the Site View Editor, you can organize the System Explorer to display cameras by location, group maps, and saved Views for convenience, or hide cameras that are not relevant to an ongoing investigation.

By default, all cameras are listed in alphabetical order by Site in the System Explorer.

NOTE: These settings only affect the System Explorer in the View tab.

1. In the Site Setup tab, click  .

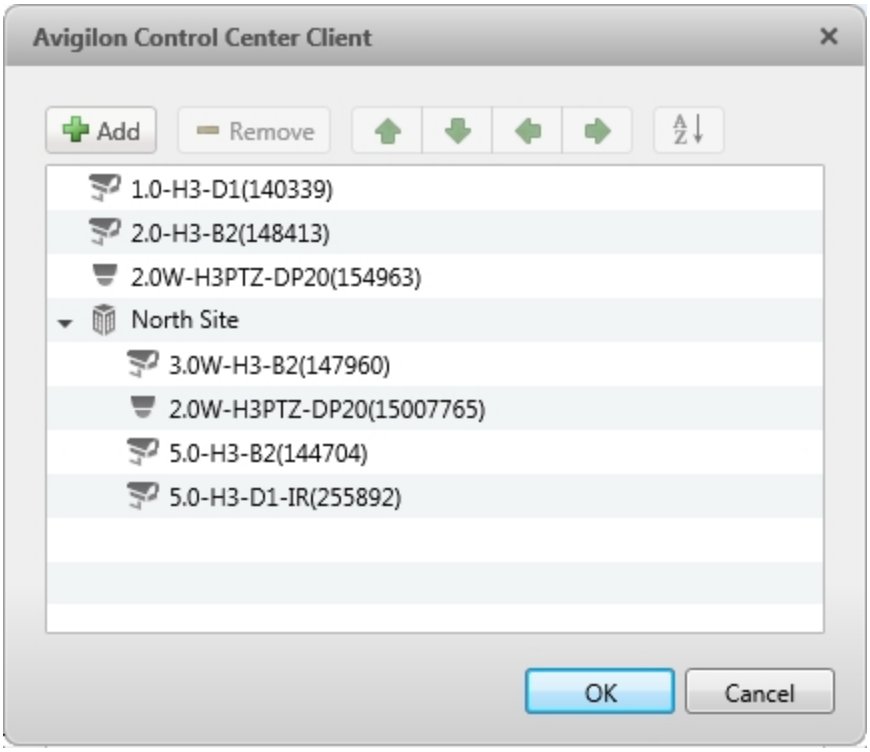


Figure 10: The Site View Editor dialog box

2. In the Site View Editor dialog box, you can perform the following:
   - Select any of the listed elements and use the green arrows to move it up and down the list, or move it under a Site folder.
   - Click  to sort the list in alphabetical order.
   - Click  to add a new Site. The new Site is a virtual folder for organizational purposes only and will not have any Setup options.

     Double-click the new Site to change the default name.
   - Click to delete a Site folder.
3. Click **OK** to save your changes.

When you open a new View tab, your changes will be displayed in the System Explorer.

Exporting Site Settings

You can export Site settings so that they can be backed up or used on a different Site.

NOTE: Some features are not displayed if the server does not have the required license, or if you do not have the required user permissions.

1. In the Site Setup tab, click 
2. Select the settings you want to export.

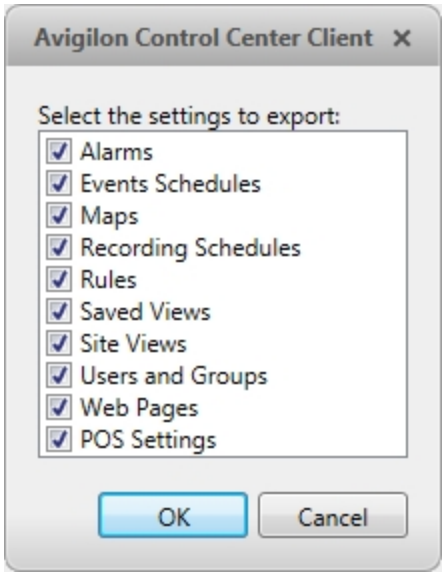


Figure 11: The Export Settings dialog box

3. Click **OK**.
4. In the Save As dialog box, name and save the file.

   Exported client settings can only be saved in Avigilon Settings File (.avs) format.

Importing Site Settings

You can import and use settings that were previously exported from a Site.

1. In the Site Setup tab, click 
2. In the Select File to Import dialog box, find the Avigilon Settings File (.avs) you want to import then click **Open**.

   NOTE: .avc files are not compatible with this version of the Avigilon Control Center Client software.
3. Select the settings you want to import. Only the settings included in the .avs file are displayed.

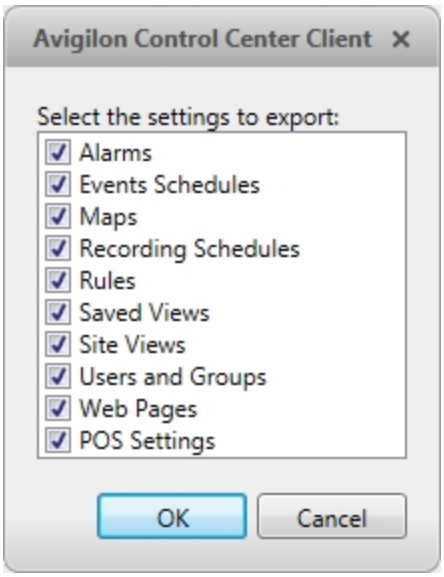


Figure 12: The Import Settings dialog box

4. Click **OK**.

   The settings are merged.

   - Unique settings are added to the Site.
   - If the settings are identical, only the current Site version is kept.
   - If an import setting and a Site setting have the same name but are configured differently, the import setting is added to the Site and renamed in this format: *<setting name>* (Import), like Email1 (Import).
     - In the rules engine, the Notify users (default) rule is always added and renamed, even if the settings are the same. The import version is enabled and the Site version is disabled by default.
   - The two Site Views are combined.
     - The import settings take precedence.

       For example, a map from the import file is already used in the Site. Currently, the map is stored at the top of the Site View. But in the import file, the map is kept at the bottom. After the import settings are merged with the current Site settings, the map is moved to the bottom.
     - Unorganized elements from the import file are listed at the bottom of the Site View.
   - User permission groups are merged.
     - If groups have the same name, the import settings are used and the users from both the import file and the current Site are added to the group.
     - Groups added from the import file automatically gain access to all the new devices that were added since the settings were exported.
   - Users with the same name will use the import settings, including passwords.

Managing Servers in a Site

A Site can contain multiple servers to share settings and tasks across all the servers. For example, users and groups that are added to the Site will automatically have access to all linked servers.

By default, when a server is first discovered on the network, it is added to the System Explorer as a server in a Site of the same name. You can move the server to a different Site to share resources.

1. In the Site Setup tab, click  .
2. The Site Management tab lists all the Sites you can access and all the servers connected to each Site.

   If you do not see the Site or server you want to configure, see **Discovering Sites** for more information.

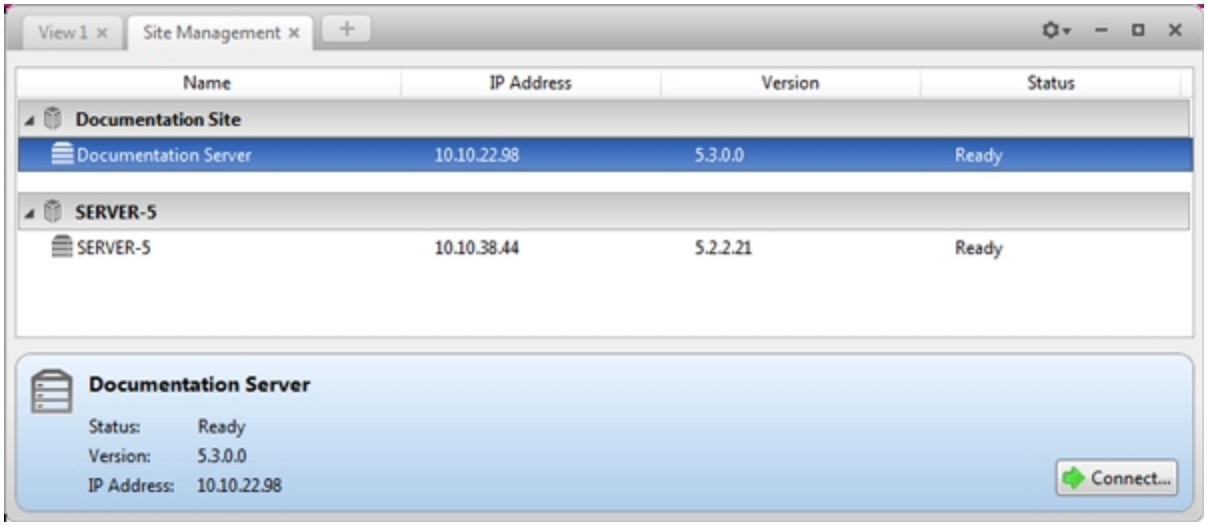


Figure 13: The Site Management tab

3. When you select a server, you will see the available options at the bottom of the screen.
4. To move a server:
   - Select the server and drag it to a different Site.
   - Or, select the server then click **Connect**. In the dialog box that appears, select the Site you want the server to connect to.

   NOTE: Sites without any servers are automatically removed from the list.

   Once the server is connected to the Site, the settings are merged.
   - Unique settings from the server are added to the Site.
   - If the settings are identical, only the Site version is kept.
   - If a server setting and a Site setting have the same name but are configured differently, the server setting is added to the Site and renamed in this format: *<setting name> (server name),* e.g. Email1 (Server2F).

        - In the rules engine, the *Notify users (default)* rule is always added and renamed, even if the settings are the same. The Site version remains enabled but the added rule is disabled by default.
    - The two Site Views are combined.
        - The Site settings take precedence.

          For example, a map from the Site was copied to the server in the past. In the server, the map was placed at the top of the Site View. But in the Site, the same map is placed at the bottom. After the server is connected to the Site, the map takes the position used by the Site (the bottom).
        - New, unorganized elements from the server are listed at the bottom of the Site View.
    - User permission groups are merged.
        - If groups have the same name, the Site settings are used and the users from both the Site and the server are added to the group.
        - Groups that are new to the Site automatically get access to all the devices in the Site.
        - Groups that are new to the server automatically get access to all the devices that are connected to the server.
    - Users with the same name will use the settings configured in the Site (including passwords), and gain group permissions from the server.
    - If the Site is connected to a Windows Active Directory, the server must be connected to the same Active Directory domain or the connection will fail. For more information, see **Importing Active Directory Groups**.
5. If the Site has multiple servers, you can choose to disconnect a server from the current Site and re-assign the server to its own Site.
    - Select a server from the Site then click **Disconnect from Site...**.

    When a server is disconnected, it retains all the settings it received from its previous Site.

Site Families

Child Sites can be connected to a parent Site to create a site family. Once set up, all ranked user and group privileges on the parent Site are pushed to the child Sites, and controlled from the parent Site. The child Site can still define local users and groups.

NOTE: A parent Site can have multiple child Sites, but a child Site can only have one parent Site. You must be logged in to both your desired parent and child Sites before you can connect them.

Only Enterprise Sites can be parent Sites. Each parent Site can have up to 1 Core Site, 24 Standard Sites and unlimited Enterprise Sites as child Sites.

Connecting a Child Site to a Parent Site

1. In the Site Setup tab, click  .

   The Site Management tab is displayed.

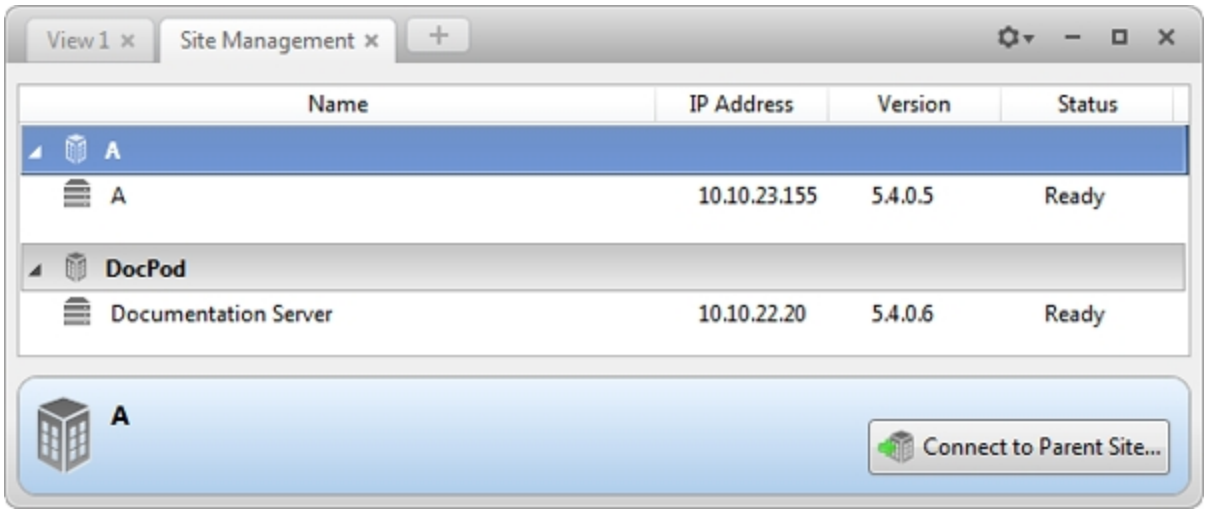


Figure 14: The Site Management tab

2. Select the Site you want to connect as a child Site.
3. In the bottom right corner of the tab, click  .

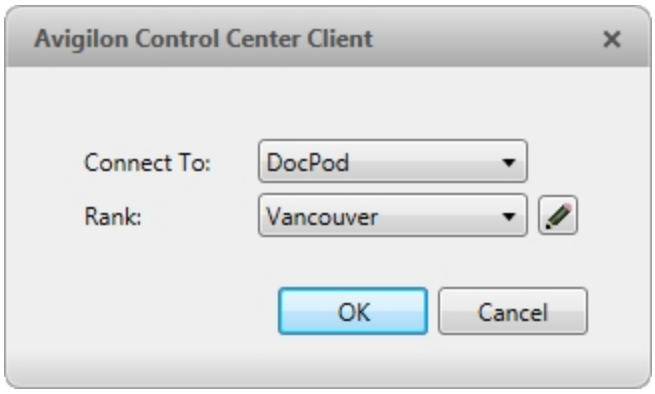


Figure 15: The Parent-Child Setup dialog box

4. In the following dialog box, select the parent Site from the **Connect to:** drop down list.
5. In the **Rank:** drop down list, select a rank for the child Site. To edit or view the entire Corporate Hierarchy, click  . For more information, see **Setting Up a Corporate Hierarchy**.
6. Click **OK**.
7. In the confirmation dialog box, click **Yes**.

Disconnecting Site Families

If a child Site needs to be removed from or moved in the Corporate Hierarchy, you can disconnect it from the parent Site. The child Site can then function independently, be reconnected to the parent Site, or be connected to a new parent Site.

You can also revoke a child Site's access from the parent Site.

Disconnecting a Child Site from a Parent Site

1. In the Site Setup tab, click  .
2. Select the child Site you want to disconnect.
3. In the bottom right corner of the tab, click  .
4. When the confirmation dialog box appears, click **OK**.

   NOTE: If a network issue occurs while you are disconnecting the child Site, you need to also revoke access from the parent Site.

Revoking Parent Site Access to a Child Site

1. In the Site Setup tab, click  .
2. Select the parent Site whose child Site you want to disconnect.
3. In the bottom right corner of the tab, click  .
4. From the drop down list, select the child Site you want to disconnect.
5. When the confirmation dialog box appears, click **OK**.

Connecting/Disconnecting Cameras and Devices

Cameras and other devices are connected to a Site through the linked servers. The server manages and stores the camera's recorded video, while the Site manages the events that can be linked to the camera's video.

You can connect and disconnect cameras and devices through the Connect/Disconnect Cameras... tab.

A camera's connection status is indicated by the icon beside the camera name in the System Explorer. The status icons may appear over any device icon in the System Explorer.

Icon	Definition
 **Camera Connected**	The camera is connected to the server.
 **Camera Upgrading**	The camera is connected to the server and is currently upgrading its firmware.
	The camera cannot connect to a server. This may be because the camera is no longer on the network or there is a

Icon	Definition
Camera Connection Error	network conflict
 **Camera Disconnected**	The camera is disconnected but recorded video from the camera remains on the server.
No Icon	The camera is disconnected and no recorded video from the camera remains on the server.

Discovering a Device

When devices are connected to the network, they should be automatically discovered by the Client.

If a device is not automatically discovered, you can try to manually discover the device.

- In the Site Setup tab, click  .

  In the Connect/Disconnect Cameras... tab, all Avigilon and ONVIF cameras that are connected to the same network segment (subnet) are automatically detected and appear in the Discovered Cameras list.

If the device you want to connect to is on a different subnet, or is manufactured by a third-party, do the following:

1. At the top of the Connect/Disconnect Cameras... tab, click **Find Camera...**.
2. In the Find Camera dialog box, complete the following fields:

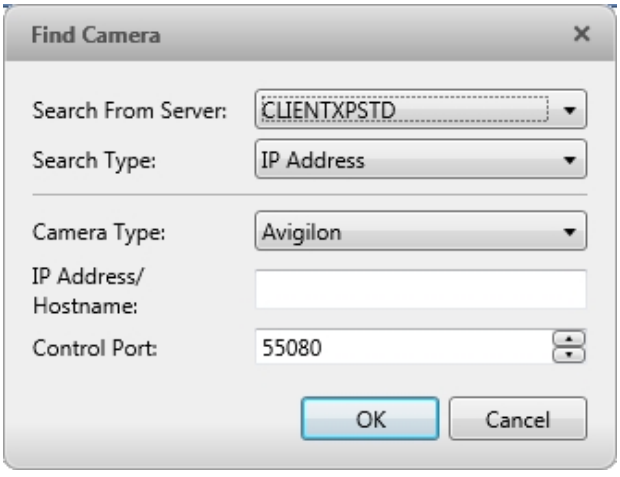


Figure 16: The Find Camera dialog box: Search Type - IP Address

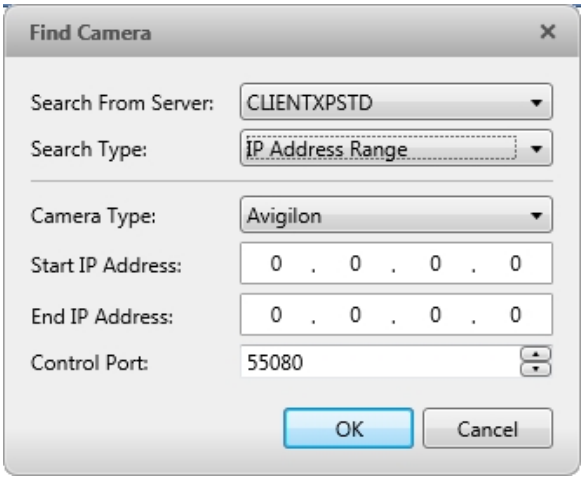


Figure 17: The Find Camera dialog box: Search Type - IP Address Range

- **Search From Server:** select the server that you want the device to connect to.
- **Search Type:** select a search type.
- **Camera Type:** select the device's brand name.

  Tip: Select ONVIF to discover devices that are ONVIF complaint.

- **IP Address/Hostname:** (For IP Address search only) enter the device's IP address or hostname. The device and server's gateway IP address must be set correctly for the device to be found.
- **Start IP Address:** and **End IP Address:** (For IP Address Range search only) enter the start and end IP addresses. Only addresses in that range will be searched for the selected device type.
- **Control Port:** enter the device control port.
- Provide the **User Name:** and **Password:** for the device if required.

3. Click **OK**.

If the device is discovered, it will appear in the Discovered Cameras list. You can now connect the device to a server.

Connecting a Device to a Server

NOTE: Some features are not displayed if the server does not have the required license, or if you do not have the required user permissions.

To access a device from a Site, it must be connected to server within the Site. The server manages and stores a camera's recorded video, while the Site manages the events that can be linked to a camera's video.

Once a device has been discovered on the network, it can be connected to the server. If you do not see a device you want to connect, see **Discovering a Device**.

1. In the Site Setup tab, click  .

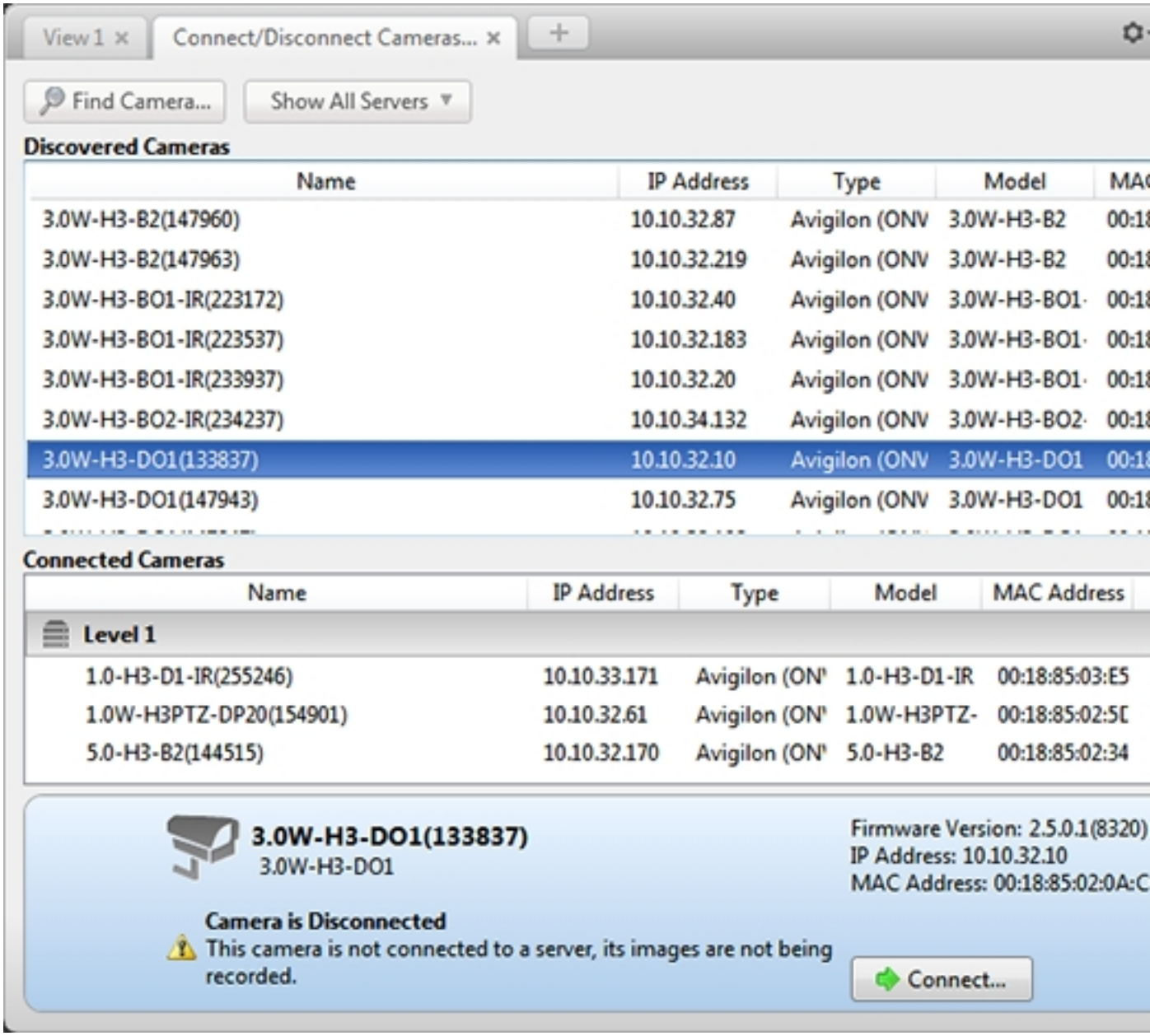


Figure 18: The Connect/Disconnect Cameras... tab

2. In the Discovered Cameras area, select a device then click **Connect...**.

   Tip: You can also drag the device to a server on the Connected Cameras list.

3. In the Connect Camera dialog box, select the server you want the device to connect to.

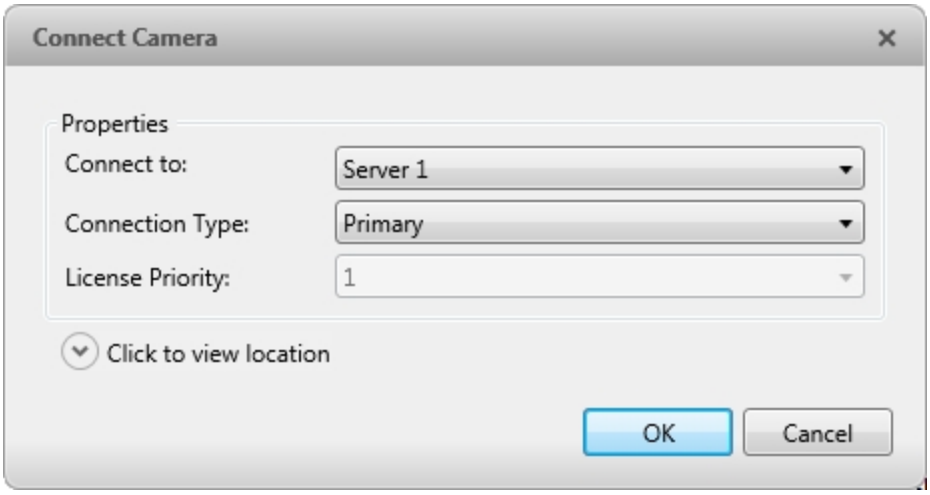


Figure 19: The Connect Camera dialog box

4. If you are connecting a third-party device, you may choose to connect the device by its native driver. In the **Camera Type:** drop down list, select the device's brand name. If there is only one option in the drop down list, the system only supports one type of driver from the device.
5. In the **Connection Type:** drop down list, select **Primary**. The device will automatically connect to this server if they are in the same network.

   If you plan to create failover connections, see **Failover Connections** for more information.
6. In the **License Priority:** drop down list, select the appropriate license priority. The highest priority is **1** and the lowest priority is **5**.

   NOTE: This option is only available if you are connecting to a secondary or tertiary server.

   The License Priority: setting decides the order that devices are connected to the server. The server will try to connect cameras with a higher priority before cameras with lower priority. If the server does not have enough camera channel licenses, low priority devices may not be connected. A camera channel license is only used when the device actually connects to the server.
7. Click to choose where the device appears in the System Explorer.
   - If your Site includes virtual sub-sites, select a location for the device. The list on the right updates to show what is stored in that directory.
   - In the Site directory, drag the device up and down to set where it is displayed.

   Tip: If the Site you want is not listed, you may need to connect the device to a different server. Make sure the selected server is connected to the Site you want.
8. Click **OK**.
9. If the device is password protected, the Camera Authentication dialog box appears. Enter the device's username and password, then click **OK**.

Connecting Cameras to a Video Analytics Appliance

If you have an IP model of the video analytics appliance, you do not need to physically connect the camera to the appliance, you can do so through the Video Analytics Configuration dialog box.

If you have an analog model of the video analytics appliance, the cameras are automatically associated with video analytics appliance channels. You do not need to connect cameras to video analytics appliance channels through the Video Analytics Configuration dialog box.

NOTE: The connecting camera and video analytics appliance must be on the same server.

1. Add the video analytics appliance to the server. For more information, see **Editing the Device Connection to a Server**.
2. Connect the required cameras to the same server as the video analytics appliance.
3. In the Setup tab, select a video analytics appliance camera channel.
4. Click  . The Video Analytics Configuration dialog box opens.

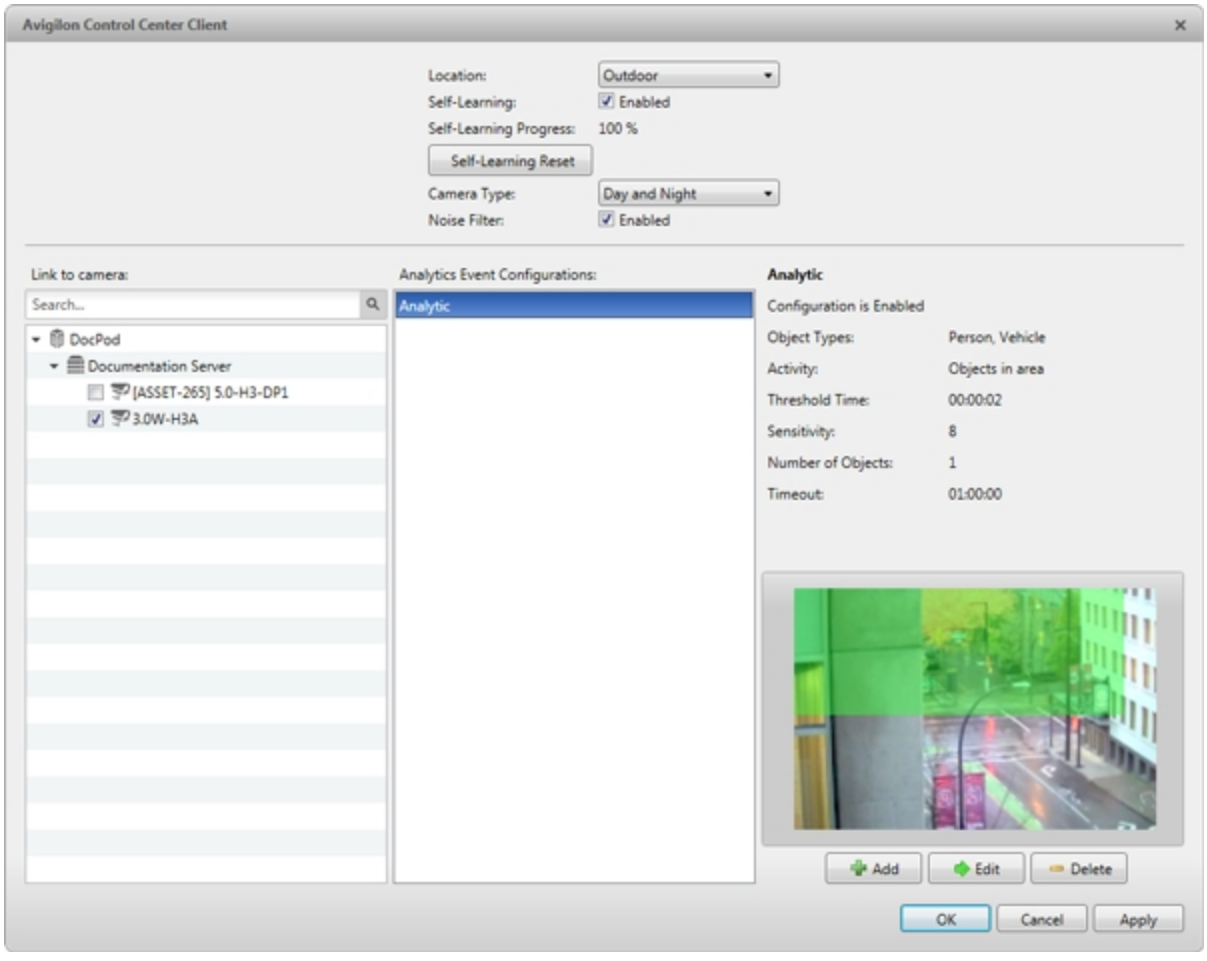


Figure 20: The Video Analytics Configuration dialog box

5. Select the check box beside the camera you want to assign to this camera channel.

   Tip: After connecting or disconnecting a camera to a video analytics appliance, you will need to reboot the video analytics appliance before making any further configuration changes to the device. This process will take about 5-10 minutes. It is recommended that you make all required connection changes before rebooting. For more information, see **Rebooting a Device**.

6. Click **OK**.

If the camera you link to has a resolution higher than 2.0 MP, the video analytics appliance will use the camera's secondary video stream.

NOTE: The video streamed from the video analytics appliance may not be in high definition because the video analytics appliance cannot stream video with a resolution higher than 2.0 MP. This does not affect the resolution of recorded video.

Editing the Device Connection to a Server

NOTE: You can only edit manually discovered device connections.

1. In the Site Setup tab, click  .
2. In the Connect/Disconnect Cameras... tab, select the device connection you want to edit from the Connected Cameras list.
3. Click **Edit...**. For details about the editable options, see **Connecting a Device to a Server**.
4. Click **OK**.

Failover Connections

You can set up failover connections so that if a server fails, the devices connected to it will automatically connect to a backup server and continue recording.

NOTE: Failover connections can only be made between servers within the same Site.

Failover connections are set up in the Connect/Disconnect Cameras... tab and are defined by the Connection Type: setting and the License Priority: setting.

The Connection Type: determines when the device will connect to a server:

- **Primary:** the device will automatically connect to this server if they are in the same network.
- **Secondary:** if the Primary server is not available, the device will try to connect to this server.
- **Tertiary:** if the Primary and Secondary servers are not available, the device will try to connect to this server.

The License Priority: setting decides the order that devices are connected to the server — **1** is the highest and **5** is the lowest. The server will try to connect devices with a higher priority before devices with lower priority. If the server does not have enough camera channel licenses, low priority devices may not be connected. A camera channel license is only used when the device actually connects to the server.

Setting Up a Failover Connection

1. In the Connect/Disconnect Cameras... tab, select a device that is currently connected to its Primary server.
2. At the bottom of the application window, click **Connect...**.
3. When you see the Connect Camera dialog box, select a different server within the same Site and set the **Connection Type:** as either **Secondary** or **Tertiary**.
4. Select a **License Priority:** for the failover connection.
5. Click **OK**.
6. Repeat this procedure until all the required failover connections have been made.

The following is an examples of how failover will work in the event of server failure.

Example

Cameras A, B, C, D, E and F have failover connections set up to two different servers. Assume each server has 6 camera channel licenses, and the license priority is set to 1 for each connection.

Connection Type	NVR 1	NVR 2	NVR 3
Primary	A B	C D	E F
Secondary	E F	A B	C D
Tertiary	C D	E F	A B

Figure 21: Primary connections

When the server NVR1 fails, cameras A and B from NVR 1 automatically connect to their Secondary server, NVR 2.

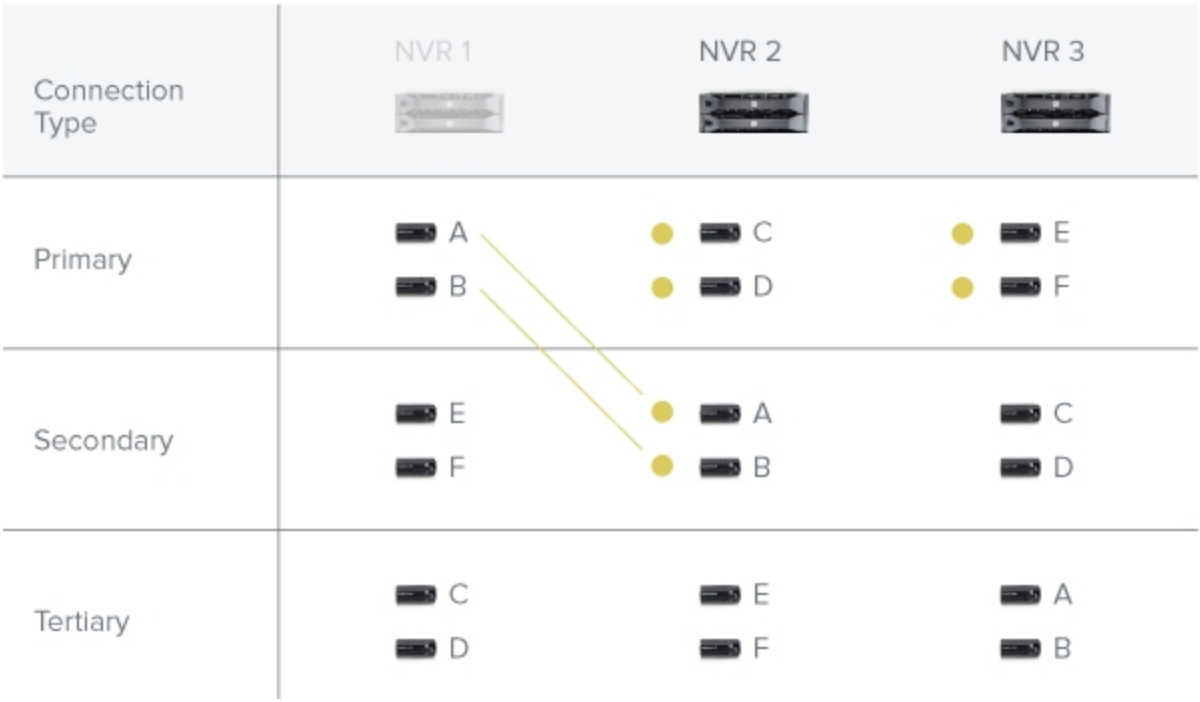


Figure 22: NVR 1 fails

When the server NVR3 fails, cameras E and F automatically connect to their Tertiary server, NVR 2.

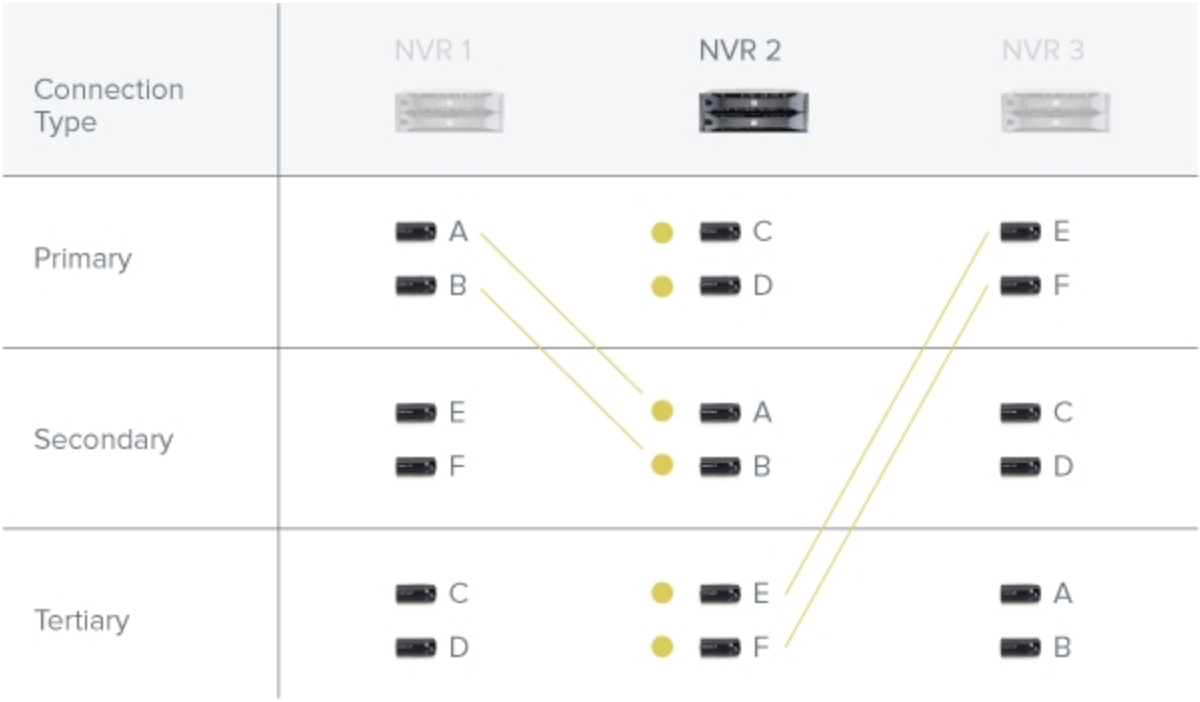


Figure 23: NVR 3 fails

Disconnecting a Device from a Server

1. In the Site Setup tab, click  .
2. In the Connect/Disconnect Cameras... tab, select the device you want to disconnect from the Connected Cameras list, then do one of the following:
   - Click **Disconnect**. The device will be disconnected from the server and moved to the Discovered Cameras list.
   - Drag the device into the **Discovered Cameras** list.

Upgrading Camera Firmware

Camera firmware updates are typically included with the Avigilon™ Control Center Server update packages. Camera firmware updates are automatically downloaded and installed to the camera.

When the camera firmware is being upgraded, video from that camera cannot be displayed and the System Explorer will display  beside the camera name.

When the firmware upgrade is complete, the System Explorer will display  again and video from the camera will display.

Users and Groups

When users are added to the Avigilon Control Center, they are assigned to a group that defines their access permissions in a Site. Use the Users and Groups dialog box to create and manage users and groups.

Managing Users and Groups Across Multiple Sites

When you have a large organization, you need detailed user access permissions to manage how the system is used each day.

The Avigilon Control Center system offers several features to help you manage large organizations:

- **Active Directory Support:** The system can synchronize with Windows Active Directory to quickly import large number of users. For more information, see **Importing Active Directory Groups**.
- **Group Privileges:** Users must be added to at least one group that defines what they can access within the system. This includes system features and specific devices. Only users with **Setup user and group settings** permission are able to edit other users and groups at all. For more information, see **Adding Groups**.

  To help you manage groups across the system, here are some features to help you maintain secure group access:

  - **Corporate Hierarchy:** Create a Corporate Hierarchy to determine which groups have control over other groups. For more information, see **Corporate Hierarchy**.
  - **Site Families:** You can connect multiple child Sites to an Enterprise parent Site. You can then control group settings for all of the Sites from the parent Site. For more information, see **Site Families**.

Best Practices

Listed here are some recommendations for maintaining an efficient and secure system:

- Change the default administrator password. The default administrator user has control over all aspects of the system, so adding a password to the account is highly recommended. By default, there is no password for the administrator account.
- Create a secondary user for the Administrator group. It is recommended that you do not use the default administrator user account, instead create a secondary user account with the same privileges so that the default administrator user can still be used in the rare event that the system becomes compromised.

Tip: If you forget your administrator user password, the alternate administrator user can be used to reset the password. This will avoid the need for a system-wide reset to restore the default administrator user password.

- Assign a rank to all groups. Unranked groups have access over all other groups, so it is recommended that any groups with users be assigned a rank to further define their access privileges. The default Administrators group is Unranked by default, but you can create a new group with same permissions and assign a rank to the new group. For more information, see **Corporate Hierarchy** .
- Limit the number of users in the default Administrator group. The Administrator group is the oversight group that should only be used for system maintenance. For example, users in the default Administrator group are the only ones who can see or remove private bookmarks made by all users.
- Always check that the device access permissions are correct after a child Site has been connected to a parent Site. Ranked groups from the parent Site whose rank is above or equal to the child Site retain their permissions on the child Site. These groups automatically gain access to all devices, maps, saved Views, and web pages on the child Site.
- Always check group access permissions after a new server has been merged into the Site.
    - If groups have the same name, the Site settings are used and the users from both the Site and the server are added to the group.
    - Groups that are new to the Site automatically get access to all the devices in the Site.
    - Groups that are new to the server automatically get access to all the devices that are connected to the server.
- Always check group access permissions after new users and groups settings are imported into the Site.
    - If groups have the same name, the import settings are used and the users from both the import file and the current Site are added to the group.
    - Groups added from the import file automatically gain access to all the new devices that were added since the settings were exported.

Corporate Hierarchy

You can set up a Corporate Hierarchy to reflect your organization's structure.

The Corporate Hierarchy can only be accessed by users belonging to a group with the Setup sites and Setup corporate hierarchy privileges. Users cannot see groups of equal or higher rank than the group they belong to, unless they are part of an Unranked group. If users belong to multiple groups of different ranks, they will be able to view all ranks below the highest rank they belong to.

Sites can also be combined together as Site families to reflect the defined Corporate Hierarchy. This further defines what devices and events users can control.

Adding and Editing Ranks

When you see the **Edit Corporate Hierarchy** option while configuring a group or adding a child Site, you can select an existing Corporate Hierarchy or create a new Corporate Hierarchy.

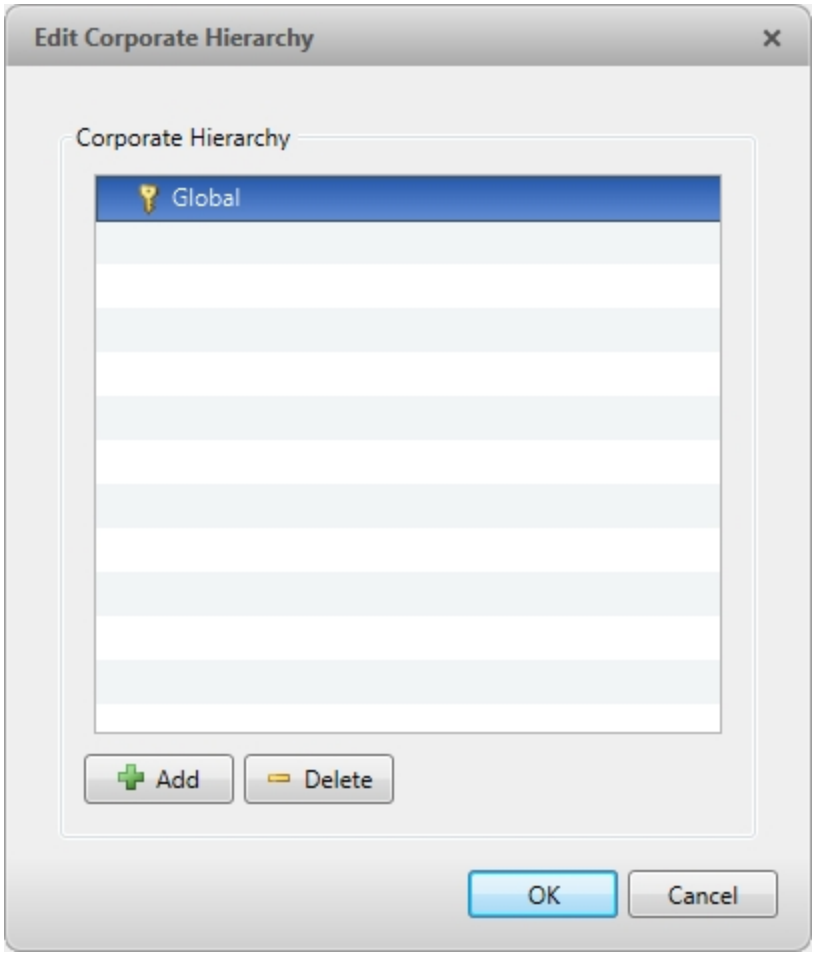


Figure 24: The Edit Corporate Hierarchy dialog box

NOTE: If you have not yet created a Corporate Hierarchy, a message will appear prompting you to create a new one. Click **Yes** to create a Corporate Hierarchy for this Site.

The default rank is **Global**. It is the highest rank in the Corporate Hierarchy.

6. To create a new rank, select **Global** and click . A **Add rank** will be created.

   NOTE: The Global rank cannot be deleted. It can only be renamed.

7. To rename a rank, double-click the name and enter a new name in the text field. Click anywhere outside the text field to save the new name.

8. Selecting a rank and clicking will create a new rank immediately below the rank you selected.

   NOTE: Ranks can only be added or deleted. They cannot be moved within the Corporate Hierarchy.

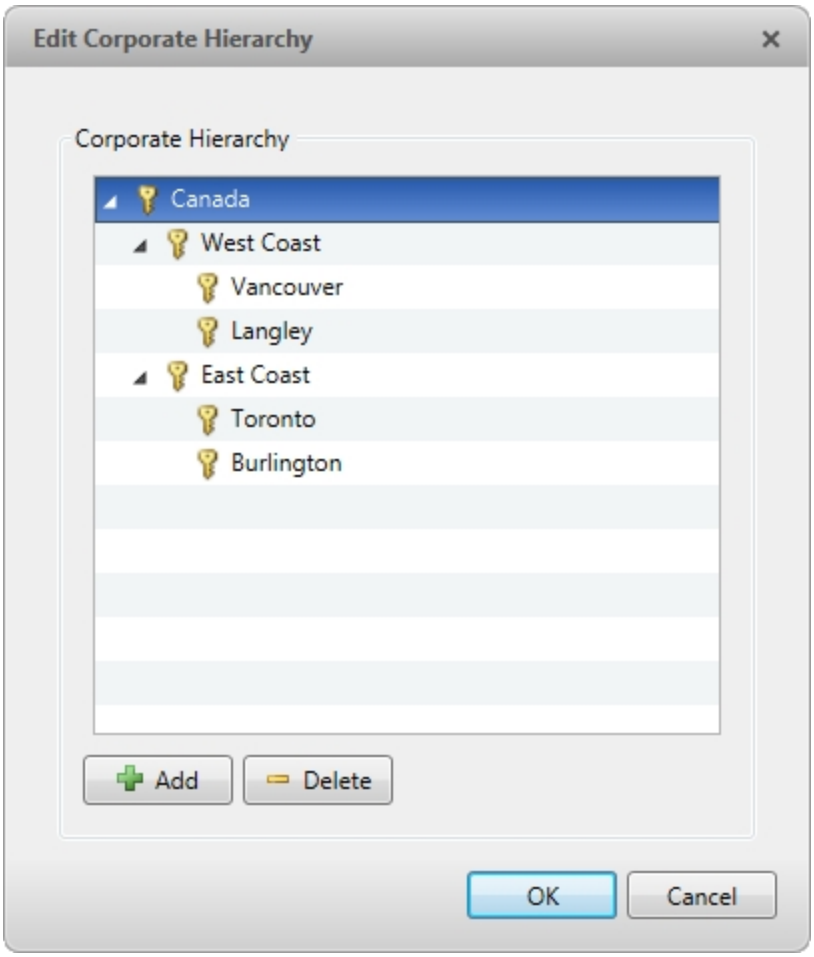


Figure 25: An example of a Corporate Hierarchy with multiple ranks that share a level. **Canada** is the highest, Global rank. **West Coast** and **East Coast** are of equal rank to each other, and one rank below **Canada**. Users belonging to **East Coast** cannot edit ranks below **West Coast** and vice versa.

Now that you've set up the Corporate Hierarchy, you can assign ranks to permission groups to define what users can access within the system. For more information, see **Users and Groups**.

Deleting Ranks

If a rank is deleted, groups in this rank are removed from the hierarchy and assigned an orphaned rank. An orphaned rank is the lowest rank possible and is only visible to Unranked and Global users.

Unranked and Global users can reassign group ranks at any time. Members of the orphaned rank have no Setup user and group settings privileges but still retain other privileges, e.g. viewing live video.

Deleting a rank will also delete all the ranks below it in the Corporate Hierarchy. Remotely synchronized users and groups may become inaccessible.

- To delete a rank, select it in the Corporate Hierarchy and click .

Unranked Groups

The Unranked groups are not part of the Corporate Hierarchy. The Unranked rank cannot be deleted or edited.

Users belonging to Unranked groups are able to create and edit any ranked or Unranked groups and users if they have the **Setup user and group settings** privilege.

The default groups Administrators, Power Users, Restricted Users, and Standard Users are Unranked.

Ranking Site Families

The Corporate Hierarchy is configured through the parent Site. The Global rank is associated with the parent Site. To edit the Corporate Hierarchy, a user on the parent Site must have the **Setup corporate hierarchy** privilege. A child Site is assigned a rank in the Corporate Hierarchy through the parent Site. For more information, see **Site Families**.

A child Site's rank determines the access rights of groups and users that are pushed to it from the parent Site. Any pushed group whose rank is higher than the child Site's can access the child Site. Pushed groups and users are controlled by the parent Site.

Adding a User

NOTE: This procedure describes adding individual users to the system. If you are managing users through Windows Active Directory, add new users directly through Active Directory.

1. In the Site Setup tab, click  .
2. In the Users tab, click  .

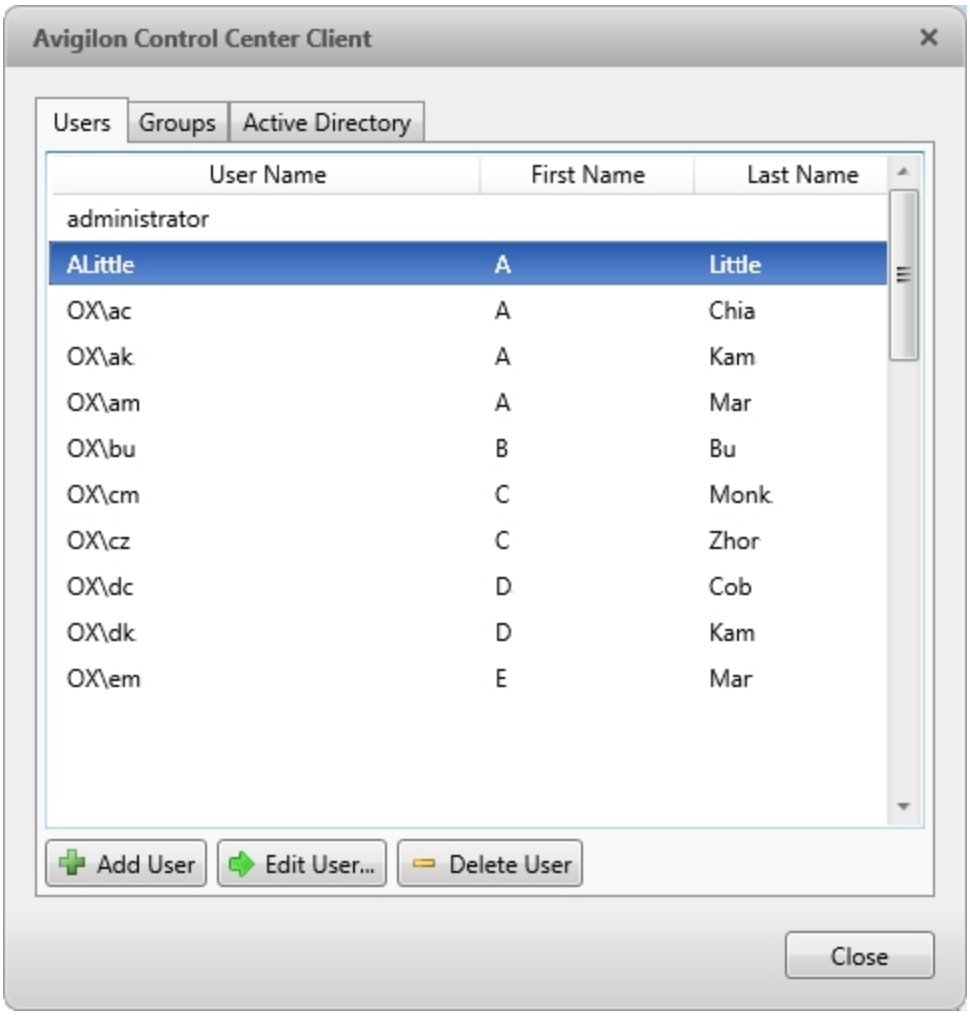


Figure 26: The Users and Groups dialog box

3. When the Add User dialog box appears, complete the User Information area.

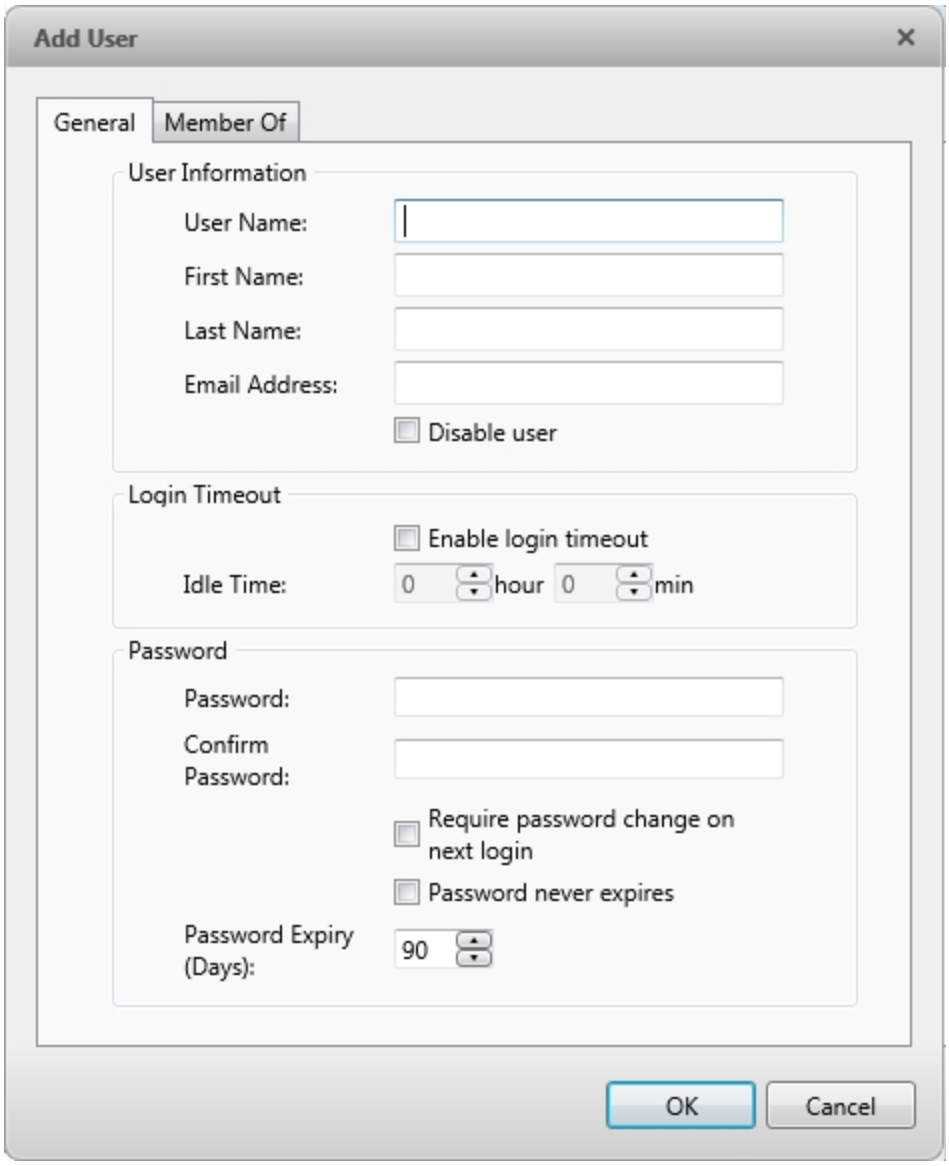


Figure 27: The Add User dialog box, General tab

4. If you don't want this user to be active yet, select the **Disable user** check box. Disabled users are in the system but cannot access the Site.
5. In the Login Timeout area, select the **Enable login timeout** check box to limit the amount of time the user can be logged in while the Client is idle.
6. In the Password area, complete the following fields:
   - **Password:** enter a password for the user.
   - **Confirm Password:** re-enter the password.
   - **Require password change on next login:** select this check box if the user must replace the password after the first login.

- **Password Expiry (Days):** specify the number of days before the password must be changed.
- **Password never expires:** select this check box if the password never needs to be changed.

7. In the Member Of tab select the check box beside each access group the user belongs to.

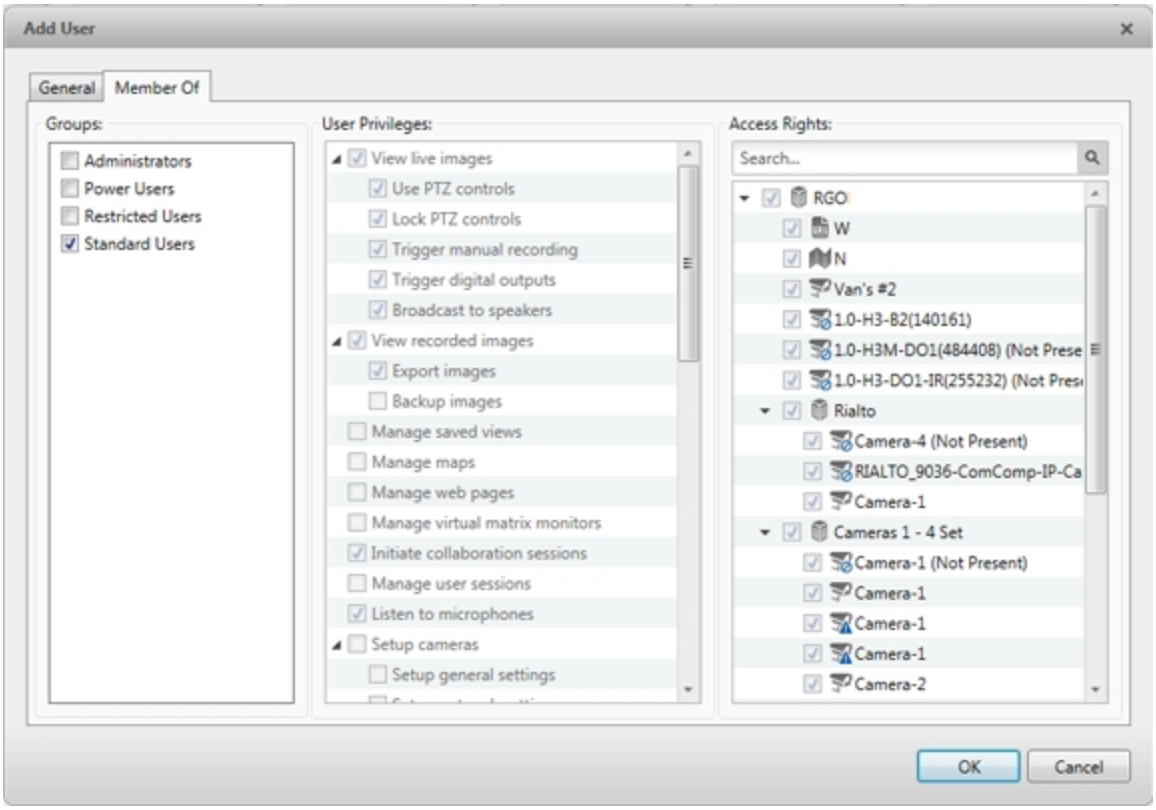


Figure 28: The Add User dialog box, Member Of tab

The other two columns display the permissions linked to the selected group.

8. Click **OK**. The user is added to the Site.

Editing and Deleting a User

You can edit and delete users as needed.

NOTE: Be aware that you cannot edit or delete users that belong to the same ranked group as you or higher. This also means that you cannot edit your own user account unless you are part of an Unranked group.

Tip: If a user has access to more than one Site, the changes to the user need to be made on each Site.

1. In the Site Setup tab, click  .
2. In the Users tab, select a user then perform one of the following:
   - To edit the user's information, click  . For details about the editable options, see **Adding a User**.
   - To delete the user, click .

     NOTE: Users imported through the Active Directory tab cannot be deleted, only disabled.

Importing Active Directory Groups

You can import Windows Active Directory groups to the Site so users can log in using their Windows credentials. Members of an imported Active Directory group are automatically added as users to the Site.

Changes to member accounts in the Active Directory are automatically synchronized with user accounts in the Avigilon Control Center.

1. In the Site Setup tab, click  .
2. Select the Active Directory tab.

Figure 29: The Users and Groups dialog box

3. If it says *Active Directory Synchronization is Disabled* at the top, you need to enable the feature first.
    a. Click **Change...**.
    b. In the dialog box, select the **Enable Active Directory synchronization** check box.
    c. Enter your username and password for the network domain.
    d. Click **OK**.
4. Click  .
5. Assign a set of permissions to the Active Directory group, then click **OK**. You can edit the permissions for the group later.

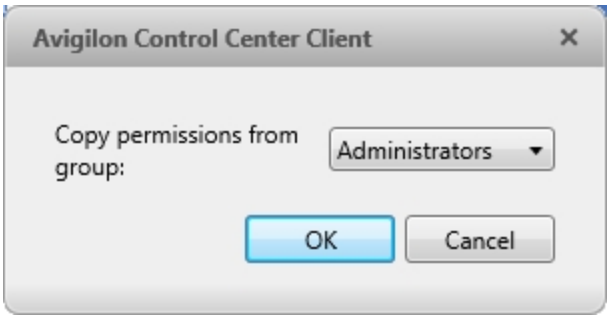


Figure 30: Copy Permissions dialog box

6. In the Select Groups dialog box, locate the Windows group you want to import by doing one of the following:
   - Enter the name of the Windows group in the **Enter the object names to select** field and click **OK**.
   - Click the **Advanced** button and search for the group you want.

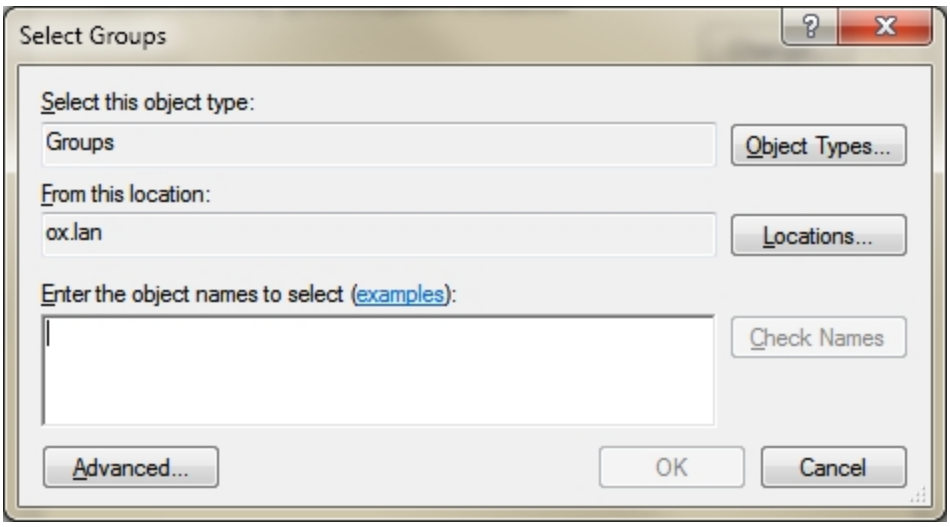


Figure 31: Select Groups dialog box

Once located, the group is automatically added to the Active Directory Groups: list and the Groups list. All the users in the group are imported into the Users list.

Members of an imported Active Directory group can now be added to any existing ranked user group in the Avigilon Control Center Client. and will be treated like other users.

Imported user information, including login credentials, is maintained by the Active Directory. In the Users and Groups dialog box, you can only disable an imported user or configure the Login Timeout settings. For more information see **Editing and Deleting a User**.

Adding Groups

Groups define what features users have access to. Create new groups to change what users can access.

1. In the Site Setup tab, click  .
2. Select the Groups tab and click

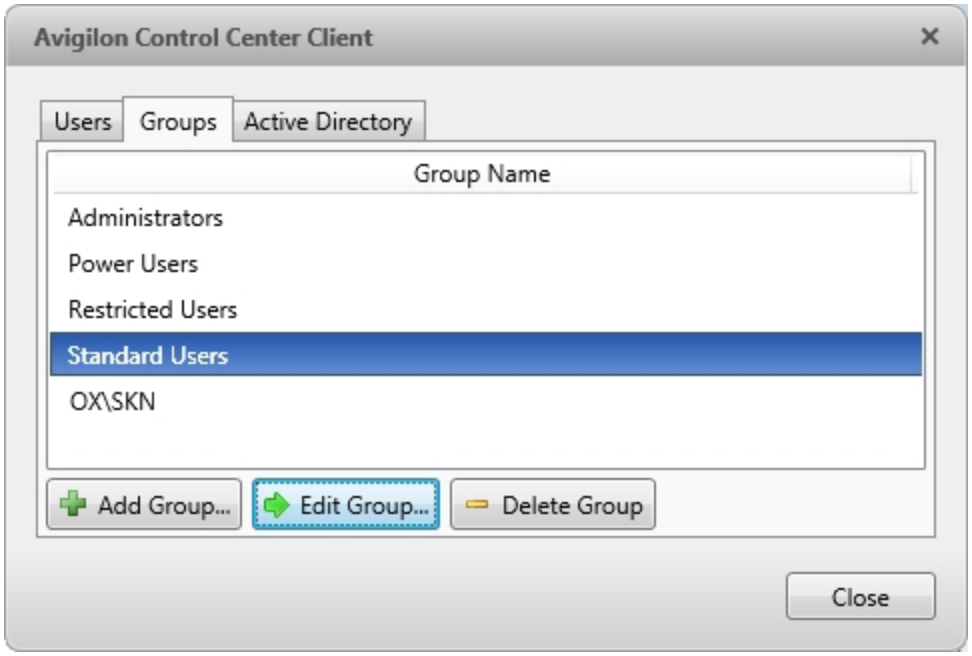


Figure 32: The Groups tab

3. Select an existing group to use as a template for your new group, then click **OK**.

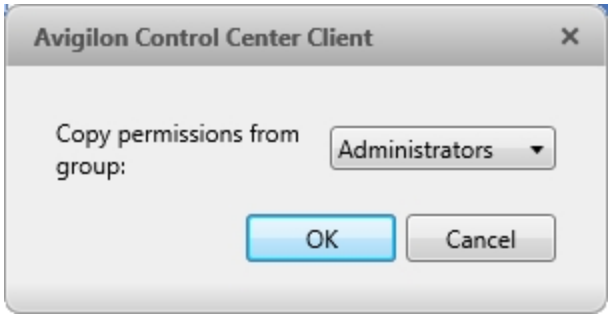


Figure 33: The Copy permissions from group: dialog box

4. In the Edit Group dialog box, complete the following:

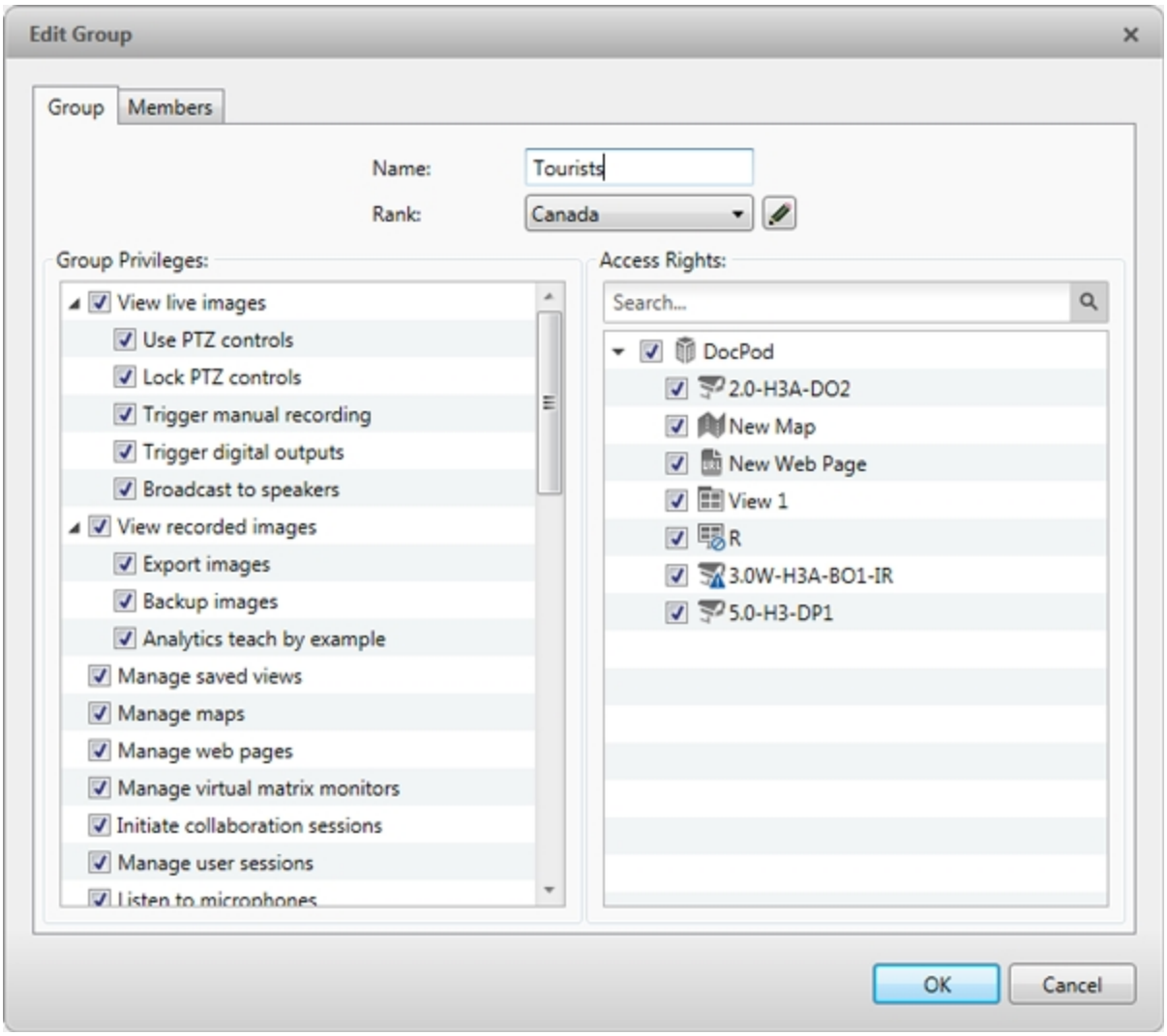


Figure 34: The Edit Group dialog box: Group tab

a. Give the new group a name.

b. Choose a rank for the group from the Rank: drop down list. To edit or view the entire Corporate Hierarchy, click  . For more information, see **Setting Up a Corporate Hierarchy** .

c. Select the **Group Privileges:** and **Access Rights:** for the group. Clear the check box of any feature or camera you do not want the group to access.

5. Select the Members tab to add users to the group. If a user is added to the group through the Add User dialog box, the user is automatically added to the group's Members list. For more information, see **Adding a User**.

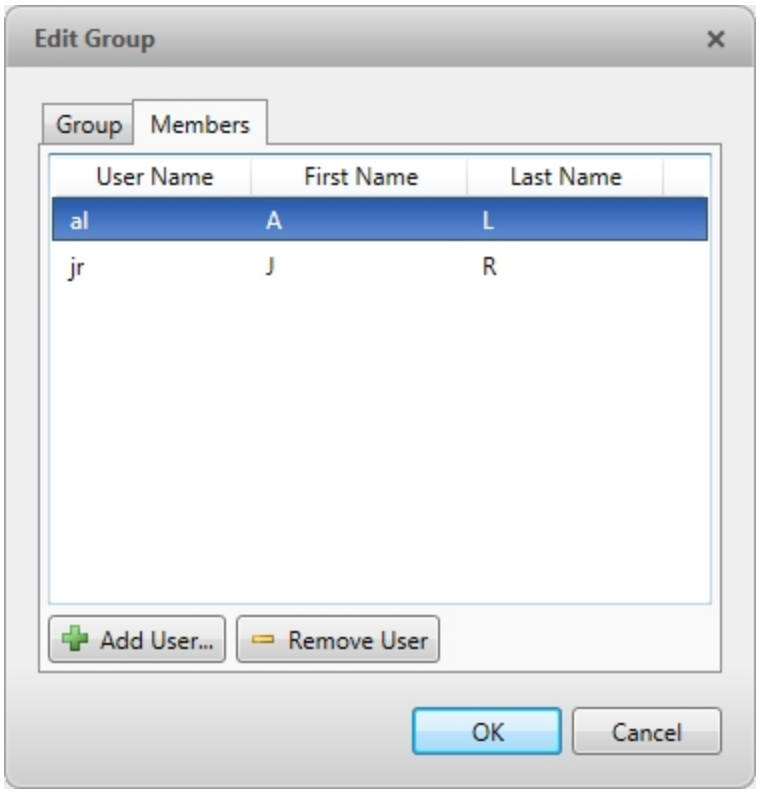


Figure 35: The Edit Group dialog box: Members tab

a. Click .

b. Select the users that should be part of this new group. Only users that have been added to the Site are displayed.

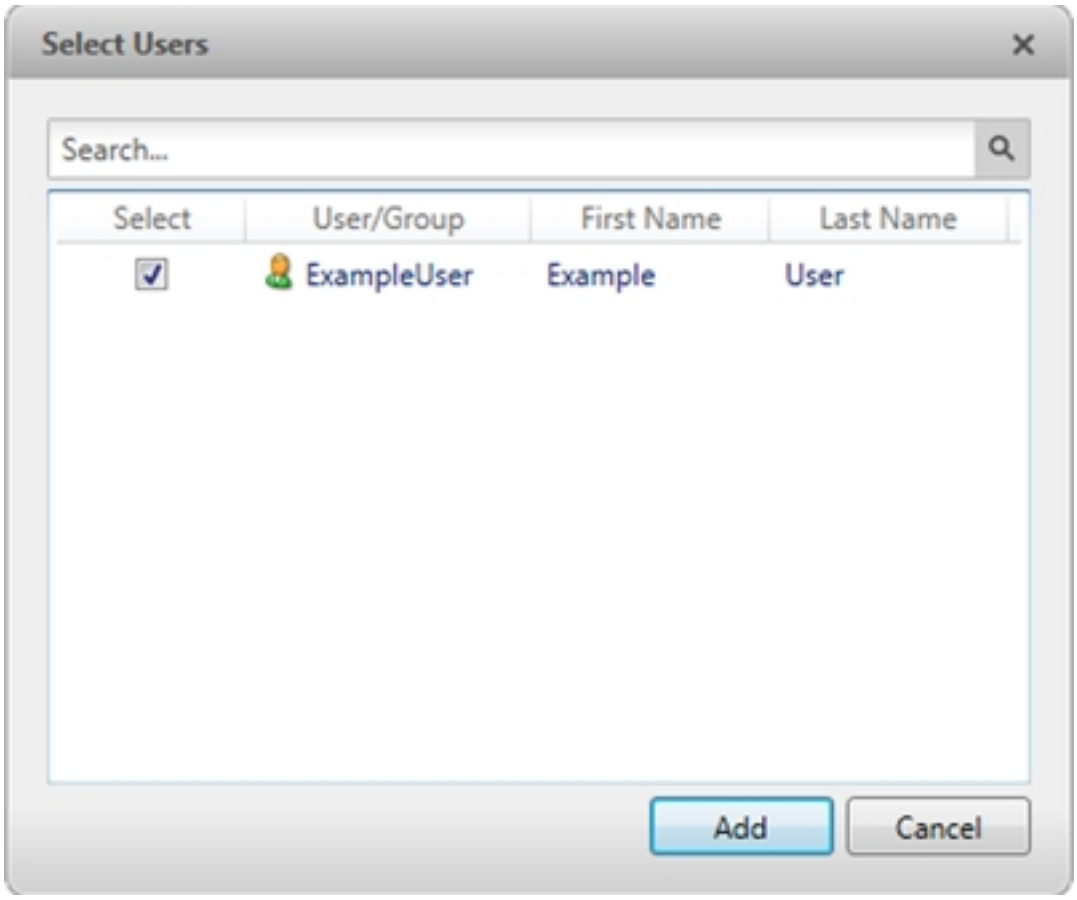


Figure 36: The Select Users dialog box

c. Click **Add**. The users are added to the Members list.

6. Click **OK** to save the new group.

Editing and Deleting a Group

You can change the access permissions for a set of users by editing their access group.

1. In the Site Setup tab, click  .
2. Select the Groups tab.
3. Select a group and do one of the following:
   - To edit the group, click  . For details about the configurable options, see **Adding Groups**.
   - To delete the group, click .

     NOTE: Default groups cannot be deleted.

Alarms

Use the Alarms dialog box to create and manage alarms. Once an alarm has been created, you can monitor alarm events in the Alarms tab. For more information, see **Accessing the Alarms Tab**.

Adding a New Alarm

Alarms need to be added to the Site before they can be monitored in the Alarms tab.

1. In the Site Setup tab, click  .
2. In the Alarms dialog box, click  .
3. Select an **Alarm Trigger Source:** . Click  when you are ready to continue. The alarm trigger options are:
    - **Motion Detection** - movement has been detected within a camera's field of view.
    - **Video Analytics Event** - a video analytics event has been detected.

      NOTE: A Video Analytics Event can only be detected on a video analytics camera or on a camera that is connected to a video analytics appliance.
    - **Digital Input Activation** - a digital input connected to a device has been activated.
    - **License Plate Watchlist Match** - a license plate on the Watch List has been detected.
    - **POS Transaction Exception** - a transaction exception has been detected at a POS transaction source.
    - **Camera Error** - a camera error has occurred.
    - **System Error** - a system error has occurred.
    - **External Software Event** - an event generated by third-party integration software has occurred.

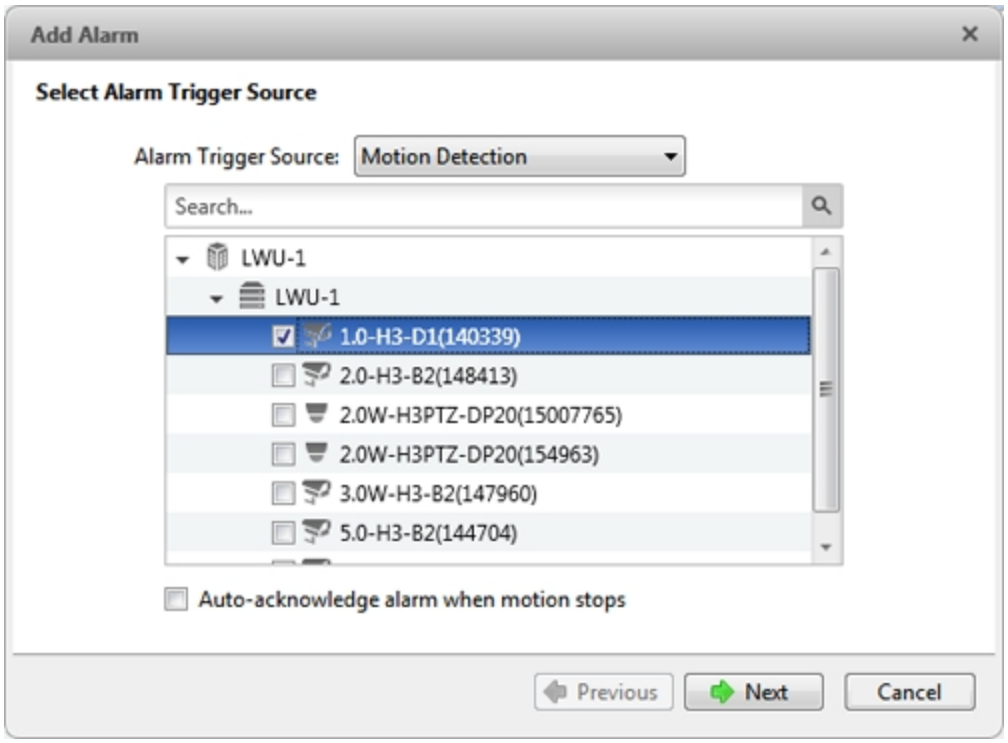


Figure 37: The Select Alarm Trigger Source dialog box

4. Select the cameras to link to this alarm, then complete the following:

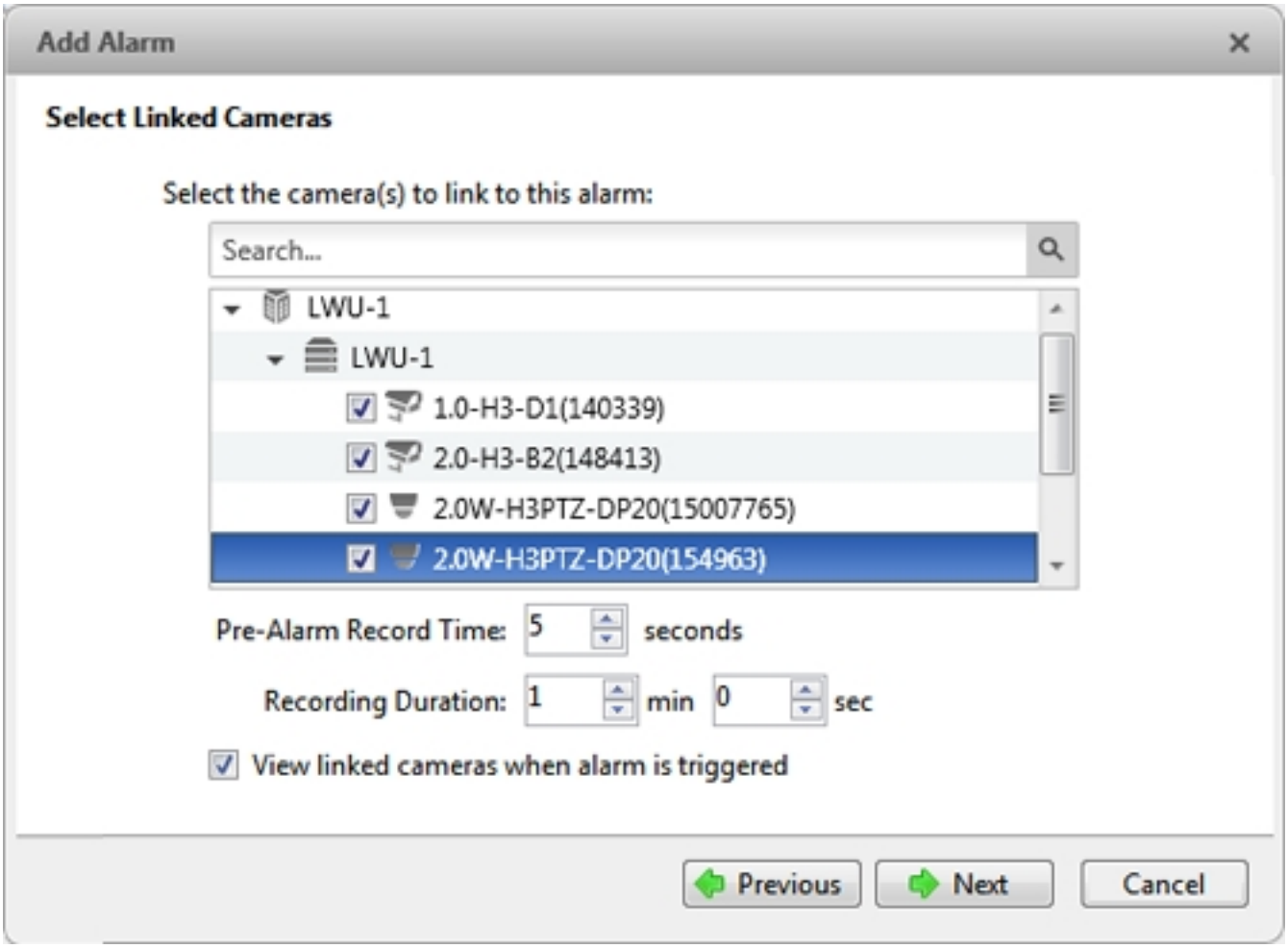


Figure 38: The Select Linked Cameras dialog box

   a. Set the **Pre-Alarm Record Time:** and the **Recording Duration:**.

   b. Select the **View linked cameras when alarm is triggered** check box to automatically display the alarm video in a View when the alarm is triggered.

   c. Click .

5. Select the groups and users that need to receive alarm notifications. You can create an escalation workflow to determine who is notified next if the alarm is not acknowledged.

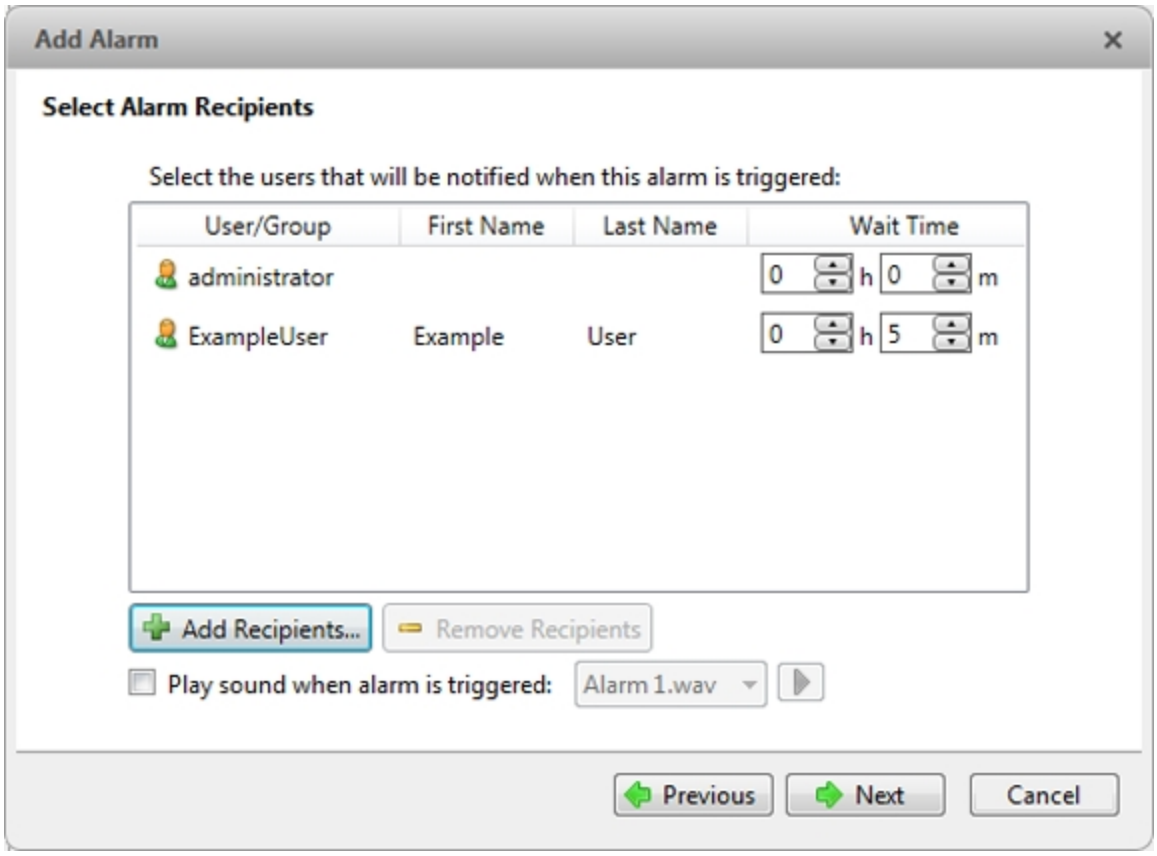


Figure 39: The Select Alarm Recipients dialog box

a. Click to add the users or groups that will be notified of this alarm. By default, the list is empty and you must add at least one user to continue.

b. In the dialog box that appears, select all the required users ( ) and groups ( ). Use the search bar at the top of the window to quickly find the user/group you want.

c. Click **Add**.

d. Assign each user a **Wait Time**. The Wait Time determines when the user or group will be notified of the alarm. If a user is assigned 0h 0m, the user will be notified immediately after the alarm occurs. If the next user is assigned a wait time of 1h 0m, that user is notified in one hour if the alarm is not acknowledged in that time. If the first user acknowledges the alarm within one hour, the second user is never notified of the alarm.

   In the Alarms tab, only users who are notified will see the live alarm trigger. All potential alarm recipients will see the alarm once it has been acknowledged.

6. Select the **Play sound when alarm is triggered:** check box to play a sound when the alarm is triggered. The sound is played in the Client only, and will be used to notify the selected users. Select the sound you want to use for the alarm from the drop down list.

7. Click .

8. (Optional) Set the actions that must occur when an alarm is acknowledged.

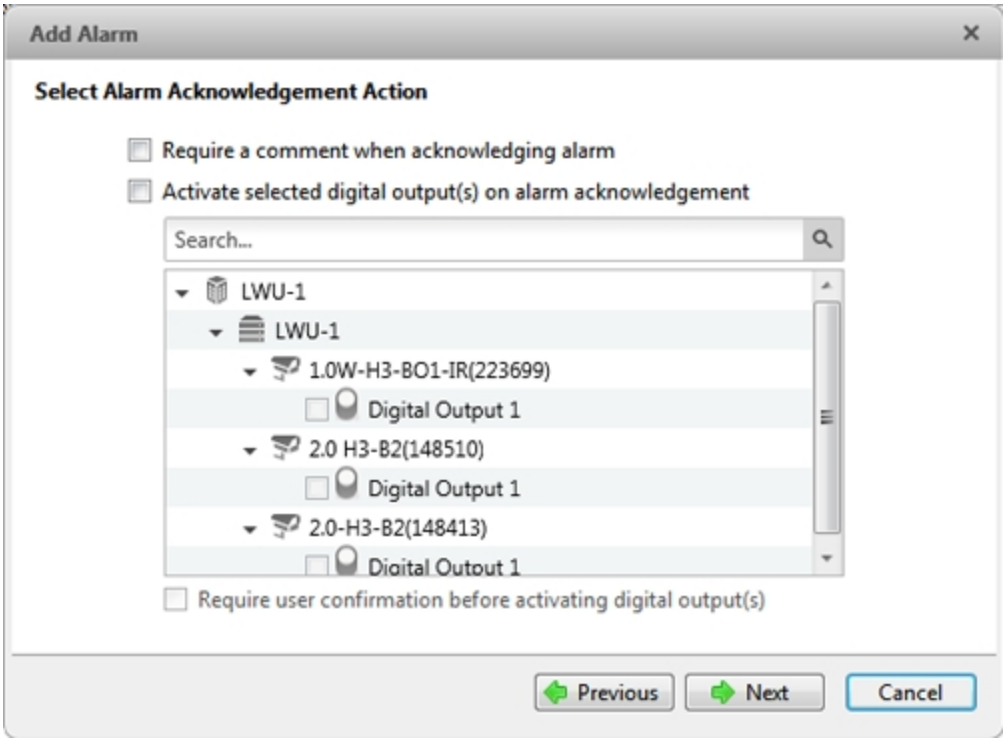


Figure 40: The Select Alarm Acknowledgement Action dialog box

a. If the user must add comments about the alarm, select the **Require a comment when acknowledging alarm** check box.

b. If a digital output must be activated when the alarm is acknowledged, select the **Activate selected digital output(s) on alarm acknowledgement** check box. Then, select the digital outputs to be activated.

c. If the digital output should only be activated when confirmed by a user, select the **Require user confirmation before activating digital output(s)** check box.

d. Click .

9. On the last page, complete the following:

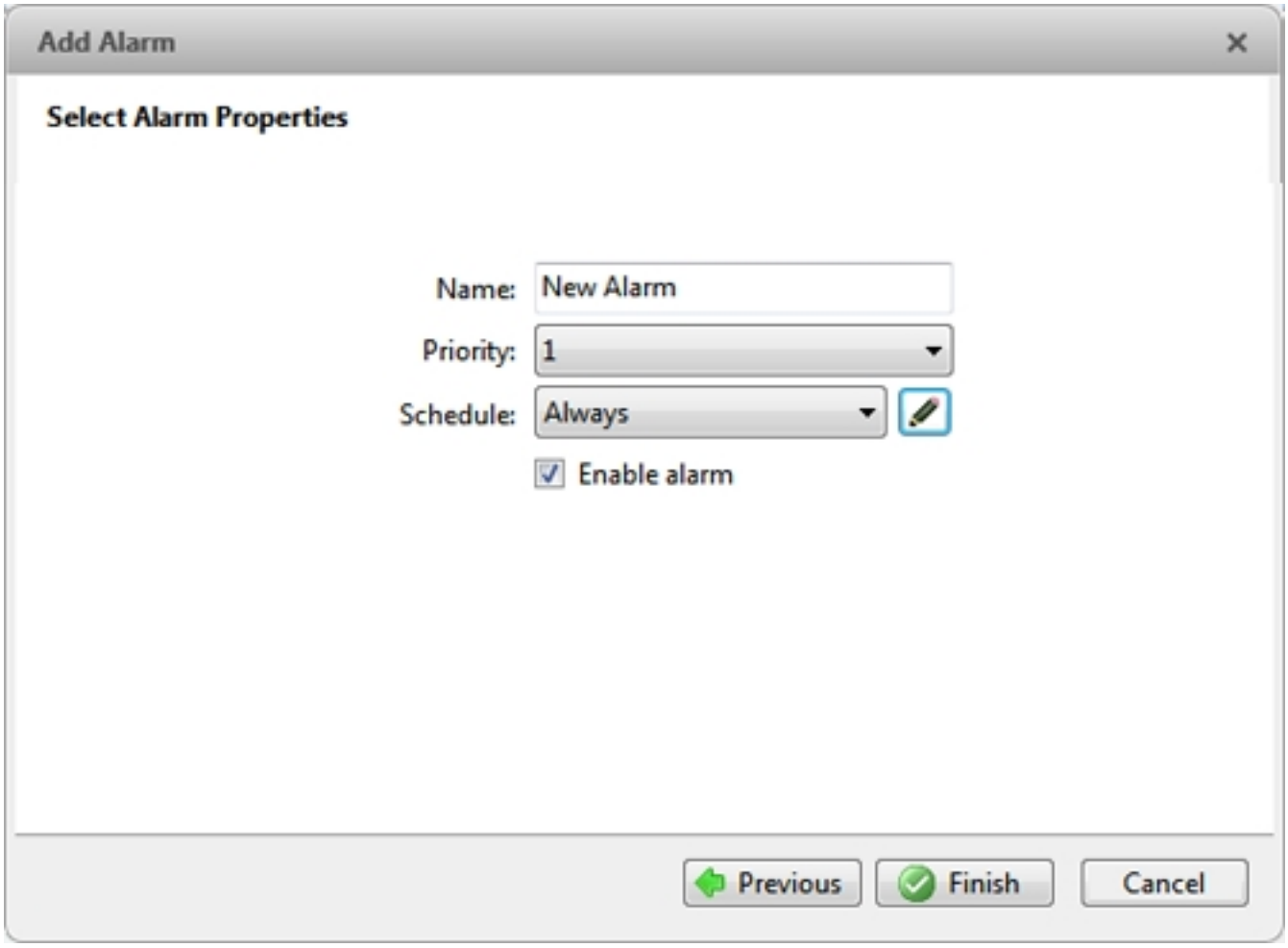


Figure 41: The Select Alarm Properties dialog box

   a. Enter a **Name:** for the alarm.
   b. Select a **Priority:** for the alarm. Priority: **1** is the highest alarm priority.
   c. Select a **Schedule:** for the alarm. For more information, see **Scheduling Site Events**.
   d. Make sure the **Enable alarm** check box is selected to enable the alarm.

10. Click .

Editing and Deleting Alarms

1. In the Site Setup tab, click .
2. In the Alarms dialog box, select an alarm, then do one of the following:
   - To edit the alarm, click . Go through the Add Alarm wizard and make the required changes on each page. On the last page, click to save your changes. For details about the editable options,

see **Adding a New Alarm**.

- To delete the alarm, click .

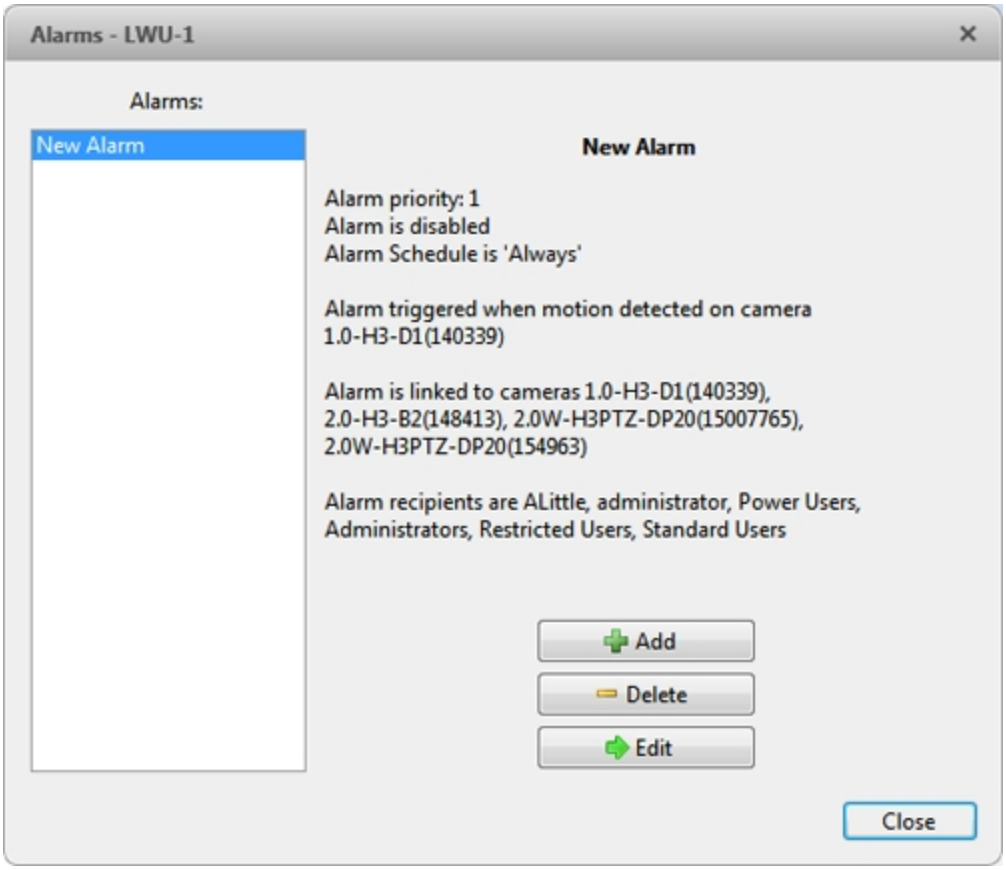


Figure 42: The Alarms dialog box: alarm properties

Email Notifications

Use the Email Notifications dialog box to set up the Site to send email in response to specific events. You can choose what events require email notifications and who receives the emails.

Setting Up the Email Server

To send email notifications, the Site must be given access to an email server.

1. In the Site Setup tab, click  .
2. Select the Email Server tab.

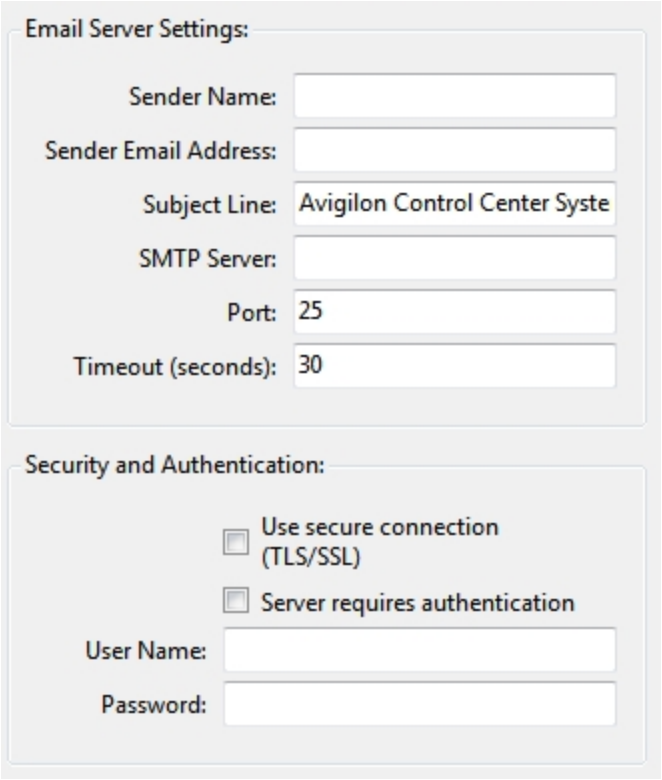


Figure 43: The Email Notifications dialog box: Email Server tab

3. In the Email Server Settings: area, complete the following:
    a. **Sender Name:** enter a name to represent the Site in all email notifications.
    b. **Sender Email Address:** enter an email address for the Site.
    c. **Subject Line:** enter a subject line for all emails sent from the Site. The default subject is *Avigilon Control Center System Event*.
    d. **SMTP Server:** enter the SMTP server address used by the Site.
    e. **Port:** enter the SMTP port.
    f. **Timeout (seconds):** enter the maximum amount of time the server will try to send an email before it quits.
4. (Optional) If the email server uses encryption, you can select the **Use secure connection (TLS/SSL)** check box.
5. (Optional) If the email account has a username and password, select the **Server requires authentication** check box.
    a. Enter the **User Name:** and **Password:** for the email account.
6. Click **OK**.

Configuring Email Notifications

In the Email Notifications dialog box, you can create email notification groups to specify who will receive email notifications when certain events occur.

NOTE: Some features are not displayed if the server does not have the required license, or if you do not have the required user permissions.

1. In the Site Setup tab, click  .
2. In the Email Notifications dialog box, make sure the Email Notifications tab is selected.
3. Click  .

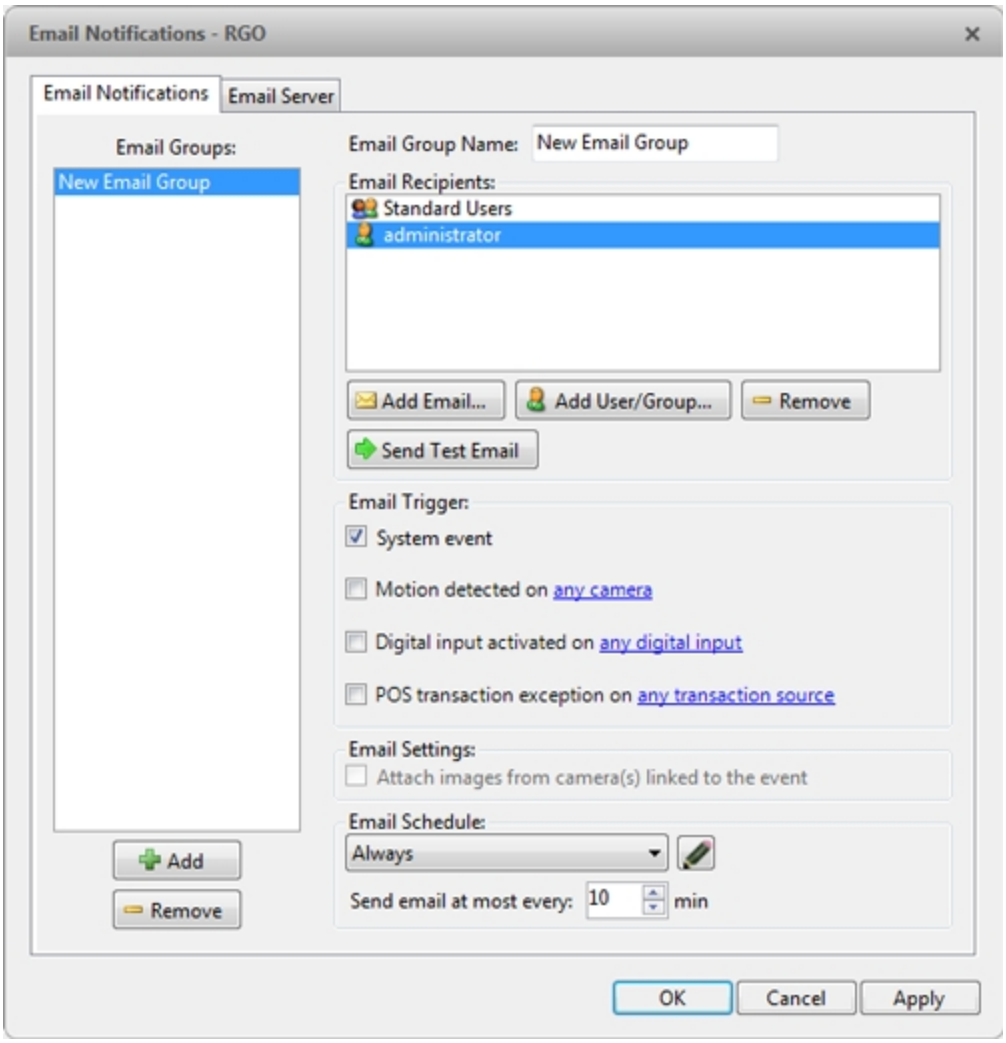


Figure 44: The Email Notifications dialog box

4. Enter an **Email Group Name:**.
5. In the **Email Recipients:** area, add all the user, group, and individual emails that are part of this email group. Do any of the following:

- Click  to add a Site user or access group. In the dialog box, select all the required users and groups then click **OK**.
- Click  to add individual emails. In the dialog box, enter the email address, then click **OK**.

Tip: Make sure the Site users in the Email Recipients: list have a valid email in their user account.

6. Click  to send a test email to everyone on the Email Recipients: list.
7. In the **Email Trigger:** area, select all the events that will trigger an email for this email group. Click the blue underlined text to define the event requirements.

   Tip: If you require other events or more specific requirements, you can also configure email notification in the rules engine. For more information, see **Rules**.
8. To attach a snapshot of the email notification event, select the **Attach images from camera(s) linked to the event** check box.

   NOTE: This option is disabled if *Motion Detect* is not selected because there are no images associated with system events, digital inputs, or POS transaction exceptions.
9. In the **Email Schedule:** area, select a schedule for the email notification. For more information, see **Scheduling Site Events**.
10. To limit the number of emails sent, enter the minimum amount of time between each email in the **Send email at most every:** field.
11. Click **OK**.

Editing and Deleting an Email Notification

You can edit or delete email notifications as needed.

1. In the Site Setup tab, click  .
2. In the Email Notifications tab, do one of the following:
   - To edit the email notification, select the Email Group from the **Email Groups:** list, then make the required changes. For details about the configurable options, see **Configuring Email Notifications**.
   - To delete the email notification, select the Email Group from the **Email Groups:** list, then click .

Rules

The Rules engine allows you to trigger specific actions when a certain event, or set of events, occurs.

For example, you can create a rule that starts a live stream when the back door is opened.

If the default email notification options are insufficient for your needs, you can use the Rules engine to set up more specific trigger events.

Adding a Rule

1. In the Site Setup tab, click  .
2. In the Rules dialog box, click  .
3. Select the events that will trigger the rule. If blue underlined text appears in the rule description, click on the text to further define the event.

   When the trigger event is defined, click  .

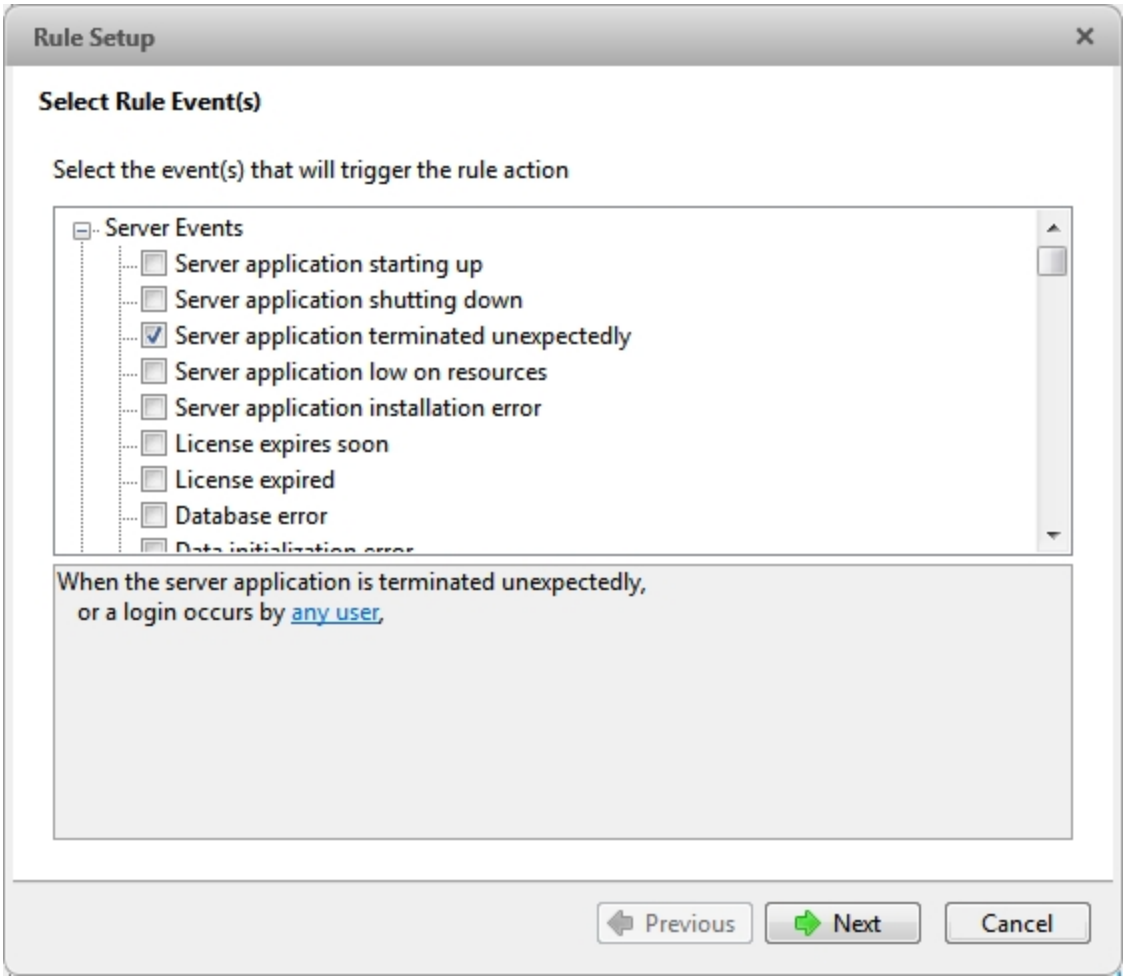


Figure 45: The Select Rule Event(s) page

4. Select the actions that will occur when the rule is triggered. If any blue underlined text appears in the rule description, click on the text to further define the action.

   When the action is defined, click  .

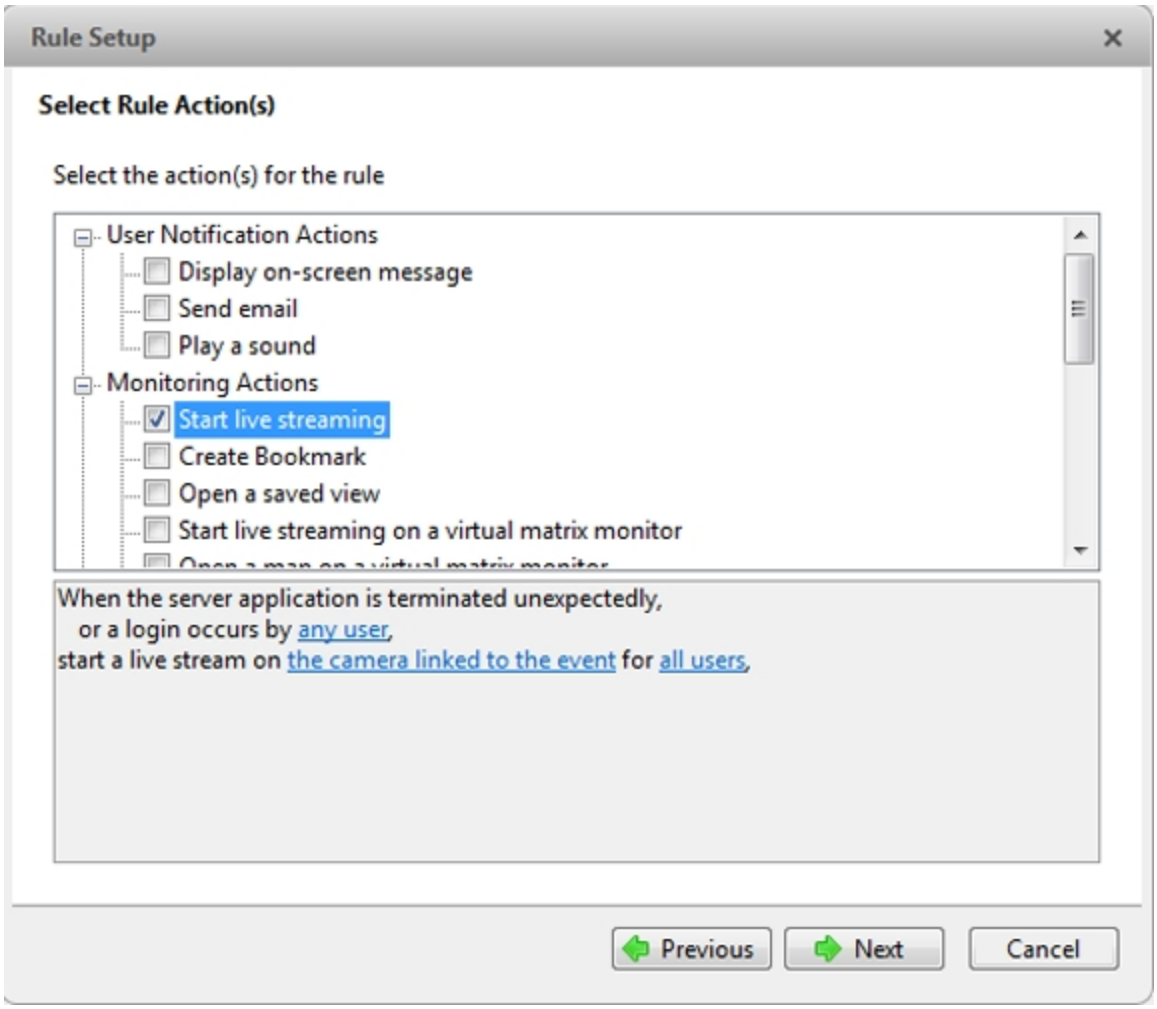


Figure 46: The Select Rule Action(s) page

5. Complete the following:
    a. Enter a **Rule Name:** and a **Rule Description:**.
    b. Select a **Schedule:** for the rule. For more information, see **Scheduling Site Events**.
    c. Make sure the **Rule is enabled** check box is selected to enable the rule.

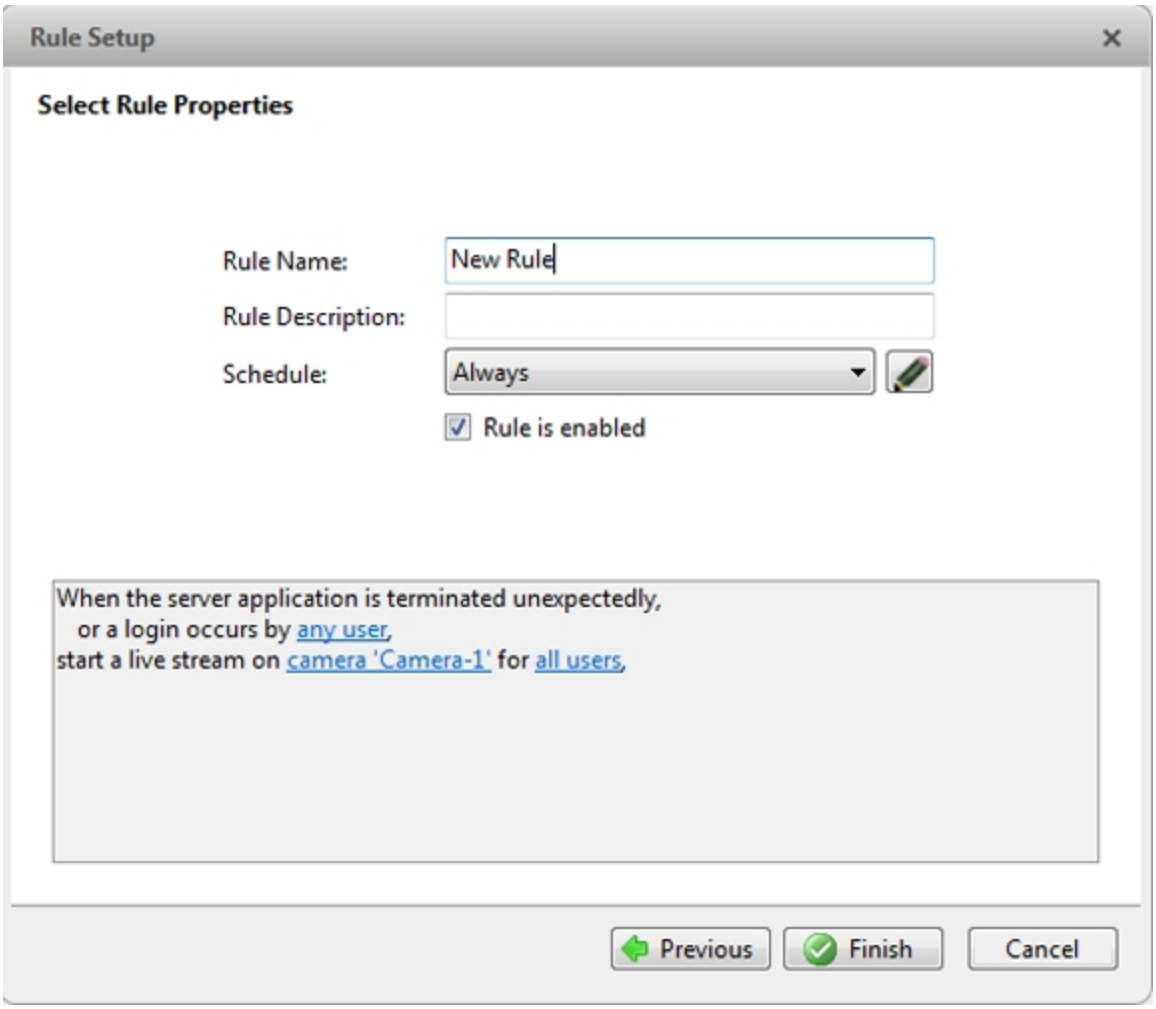


Figure 47: The Select Rule Properties page

6. Click .

Editing and Deleting a Rule

1. In the Site Setup tab, click  .
2. In the Rules dialog box, select a rule, then do one of the following:

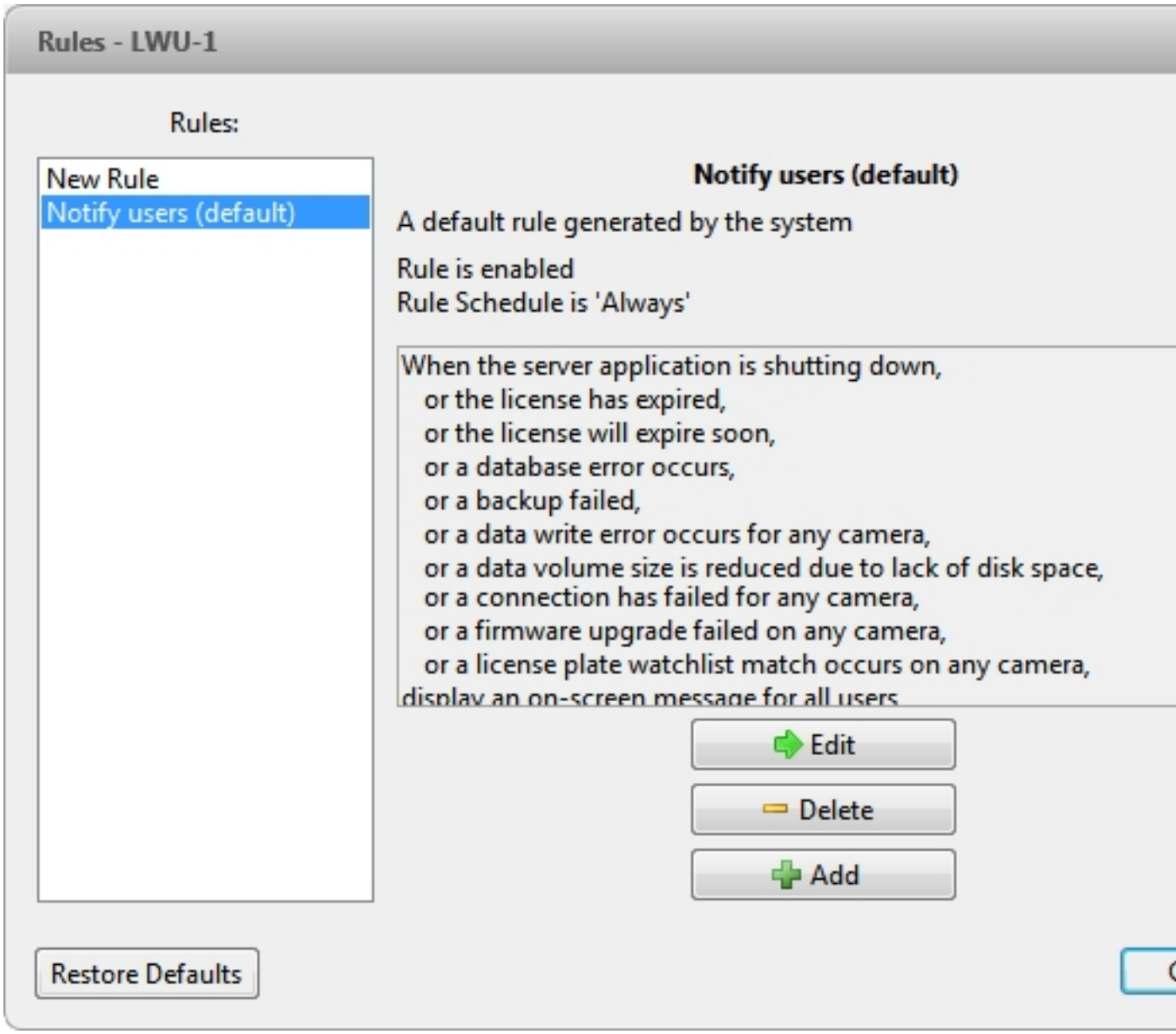


Figure 48: The Rules dialog box

- To edit the rule, click  . Go through the **Rule Setup** wizard and make the desired changes on each page. On the last page, click to save your changes.

  For details about the editable options, see **Adding a Rule**.

- To delete a rule, click . When the confirmation dialog box appears, click **OK**.

Scheduling Site Events

Site events are actions that can affect the entire Site, like email notifications. When you configure a Site event, you are given the option to assign a schedule to the event. Schedules control when events can occur — at specific times during a day or only on specific days.

When you see the **Schedule** option while configuring an event, you can select an existing schedule or create a new schedule.

NOTE: Schedules are shared across a Site.

Figure 49: Schedule option

- To use a preconfigured schedule, select an option from the drop down list. The default option is *Always*, which allows the event to run constantly.
- To change a schedule, select the schedule then click and select .
- To delete a schedule, select the schedule then click and select .
- To create a schedule, click then select . When you see the Edit... dialog box, complete the following steps:

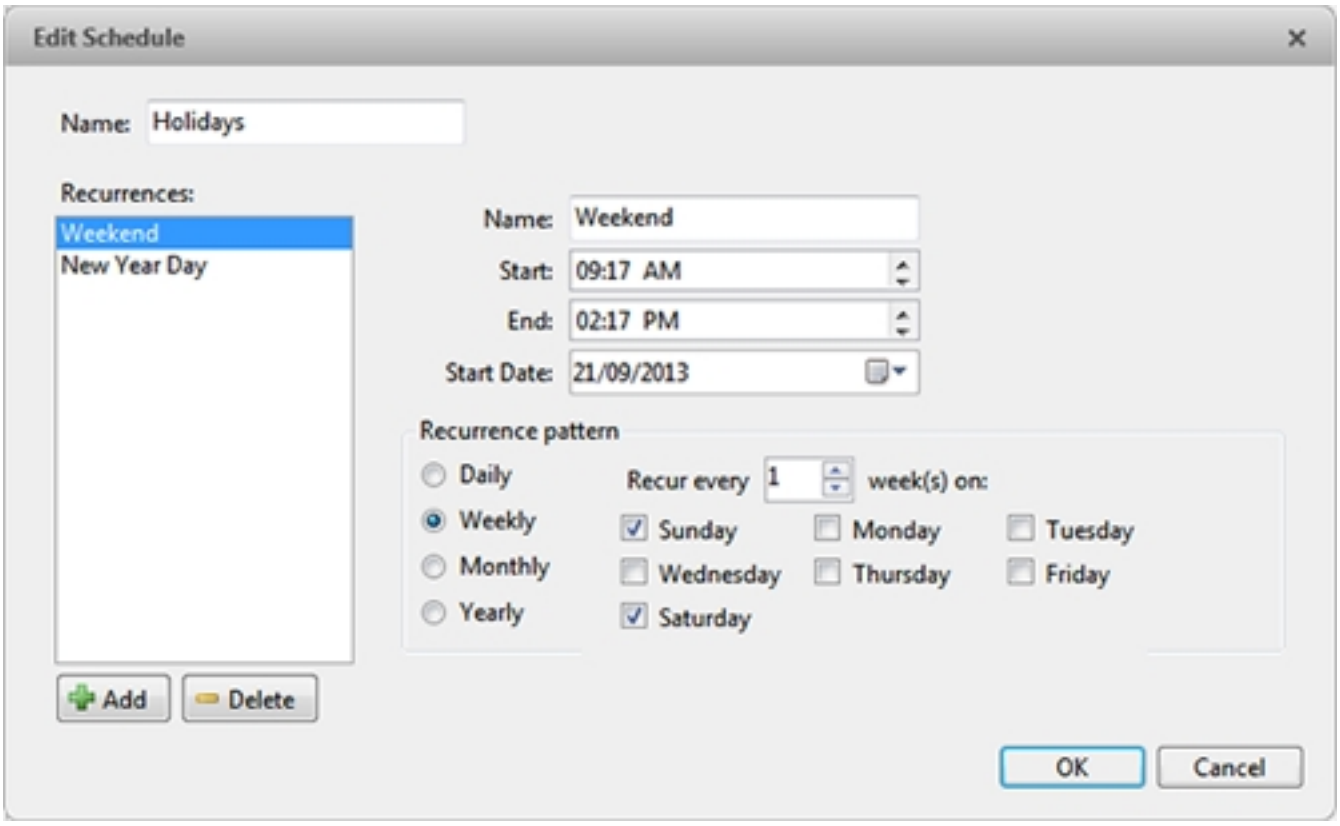


Figure 50: The Edit... dialog box.

1. Give the new schedule a name.
2. Give the recurrence a name.

   You can add multiple recurrences to create a detailed schedule. For example, you could create one recurrence to cover every weekend, plus extra recurrences to cover public holidays.

   - To add a recurrence, click  .
   - To delete a recurrence, select the recurrence then click .
3. In the **Start:** and **End:** fields, enter the time the recurrence will cover.

   Be aware that if you enter an End: time that is earlier than the Start: time, the event will span two days. For example, if the schedule is set to start at 12:00pm and end at 11:59am, the event is automatically enabled from 12:00pm on day 1 and will end at 11:59am on day 2.
4. In the **Start Date:** field, enter when the recurrence should begin.
5. In the Recurrence pattern area, schedule how often the event will be enabled during this recurrence.

Option	Description
Daily	The event is enabled during the same time every day. • Select the number of days between each schedule recurrence.
Weekly	The event is enabled during the same day and time every week. • Select the day(s) of the week, then select the number of weeks between each schedule recurrence.
Monthly	The event is enabled during the same day and time every month. • Select the specific day or weekday, then select the number of months between each schedule recurrence.
Yearly	The event is enabled during the same day and time every year. • Select the specific day or weekday and month, then select the number of years between each schedule recurrence.

6. Complete any other recurrences that have been added to the schedule.
7. Click **OK** to save the new schedule.

Server Settings

Server settings are related to video recording. This includes configuring the recording schedule, data aging, and bandwidth usage, as well as POS transactions and scheduled video backups.

NOTE: Some features are not displayed if the server does not have the required license, or if you do not have the required user permissions.

Naming a Server

Give the server a meaningful name so that it can be easily identified in the System Explorer. Otherwise, the server uses the name that is assigned by Windows.

1. In the server Setup tab, click  .
2. In the dialog box that appears, give the server a name.

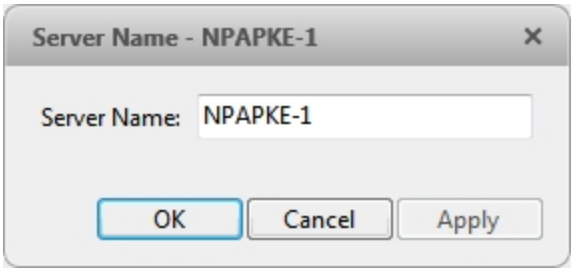


Figure 51: The Server Name dialog box

3. Click **OK**.

Recording Schedule

Use the Recording Schedule dialog box to set the recording schedule for cameras connected to the server. By default, the server is set to record motion and configured events when they occur.

Once the recording schedule is set, video is recorded automatically.

Setting Up a Weekly Recording Schedule

You can set up a weekly recording schedule by applying templates to cameras for each day of the week.

1. In the server Setup tab, click  .
2. In the Recording Schedule dialog box, select a template from the Templates: pane.
3. In the Default Week area, click the days of the week this template applies to for each camera.

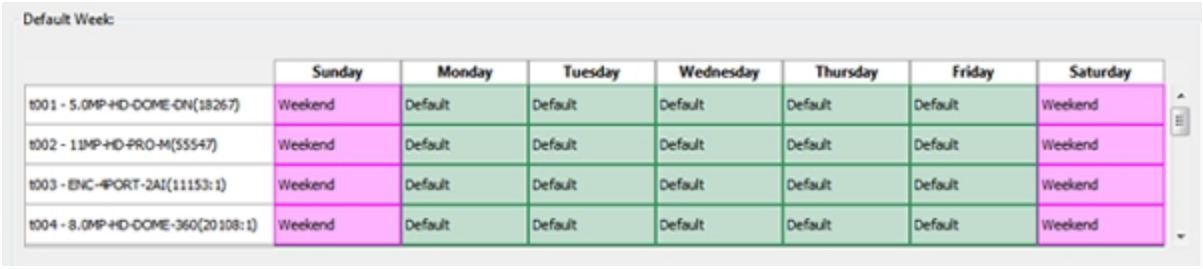


Figure 52: The Recording Schedule dialog box: Default Week

4. Click **OK**.

Using Templates to Modify the Recording Schedule

The recording schedule is set by using templates that tell cameras when and what to record. For example, you can create one recording schedule template for weekdays and another for weekends.

NOTE: Recording templates are shared across a Site.

Adding a Template

NOTE: Some features are not displayed if the server does not have the required license, or if you do not have the required user permissions.

1. In the server Setup tab, click  .
2. In the Recording Schedule dialog box, click **Add Template** below the Templates: pane.

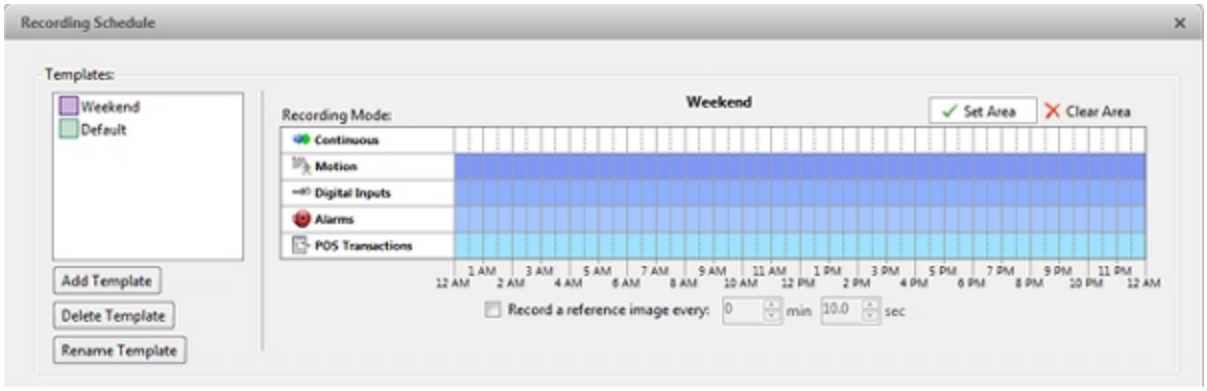


Figure 53: The Recording Schedule dialog box

3. Enter a name for the **New Template**.
4. Click the **Set Area** button, then click or drag the cursor across the **Recording Mode:** timeline to set the types of events that the cameras will record throughout the day. Individual rectangles on the Recording Mode: timeline will be colored if they have been selected.

Record Mode	Definition
Continuous	Record video constantly.
Motion	Only record video when motion is detected.
Digital Inputs	Only record video when a digital input is activated.
Alarms	Only record video when an alarm is activated.
POS Transactions	Only record video when a point of sale (POS) transaction is made.
License Plates	Only record video when a license plate is detected.

5. To disable recording in parts of the template, click the **Clear Area** button, then click or drag the cursor across the timeline to remove the set recording areas.
6. If cameras are *not* recording in Continuous mode all day, you can set cameras to record reference images between events in the recording schedule.

- Select the **Record a reference image every:** check box then set the time between each reference image.

Editing and Deleting a Template

1. In the Setup tab, select the server you want to edit, then click  .
2. In the Recording Schedule dialog box, select a template from the Templates: pane and do one of the following:
   - To edit a template, modify the schedule.
   - To rename a template, click **Rename Template** and enter a new name.
   - To delete a template, click **Delete Template**.
3. Click **OK** to save your changes.

Recording and Bandwidth

While the Recording Schedule dialog box sets when and what cameras record, the Recording and Bandwidth dialog box sets how long recorded video is stored.

In the Recording and Bandwidth dialog box, you can change the Data Aging settings and set the maximum record time for each connected camera.

1. In the server Setup tab, click  .

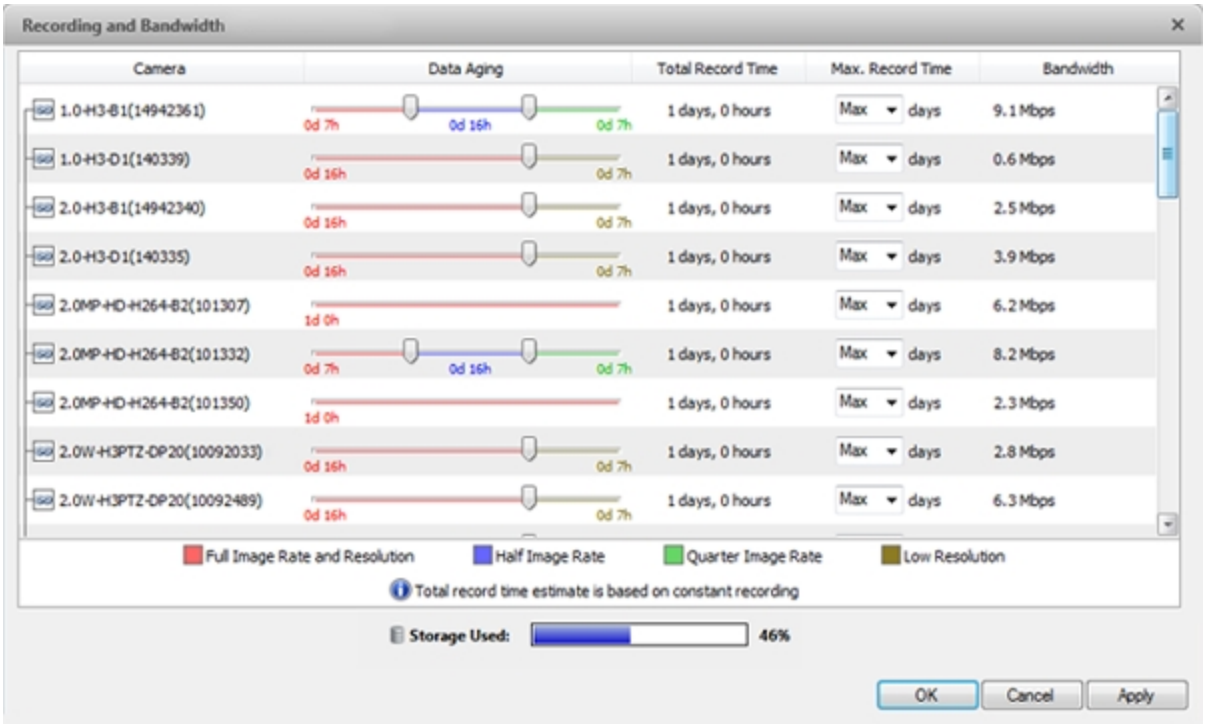


Figure 54: The Recording and Bandwidth dialog box

The Data Aging column shows an estimate of the recording time that is available at each image rate, given the amount of space on the server.

- For JPEG2000 or JPEG compression cameras, Data Aging is available at three rates:
  - **Full Image Rate and Resolution** keeps recordings at their original quality.
  - **Half Image Rate** discards half of the recorded data to make room for new recordings.
  - **Quarter Image Rate** keeps 1/4 of the original recorded data so that you can still see older video.
- For H.264 cameras that support Data Aging, Data Aging is available at two rates:
  - **Full Image Rate and Resolution** keeps the original high quality video and the secondary stream of low resolution video.
  - **Low Resolution** only keeps the secondary stream of low resolution video.

  NOTE: The Data Aging can only occur when the secondary stream is enabled.
- For H.264 cameras that *do not* support Data Aging, only the **Full Image Rate and Resolution** video is kept.

2. In the Data Aging column, move the sliders to adjust the amount of time video is stored at each image rate.
   - To change the data aging settings for all linked cameras, move the slider for one linked camera and all linked cameras will be updated.
   - To change the data aging setting for one camera, break the camera's link to other cameras by clicking the icon to the left of its name, then make your changes.
3. In the **Max. Record Time**, manually enter a maximum record time or select one of the options from the drop down list for each camera.

   NOTE: If the time estimated in the Total Record Time column is shorter than what is set in the Max. Record Time column, the camera's actual recording time will be shorter than the Max. Record Time.
4. Click **OK**.

Scheduled Backup

Video backup must be enabled in the Avigilon™ Control Center Admin Tool before Scheduled Backup settings can be set in the Client. The Admin Tool is also where you manually set the backup file location. For more information, see *The Avigilon Control Center Server User Guide*.

Files are always backed up in Avigilon Backup (AVK) format. You can review backed up video in the Avigilon Control Center Player.

Once backups are enabled, you can schedule the application to automatically back up recorded video.

1. In the server Setup tab, click  .

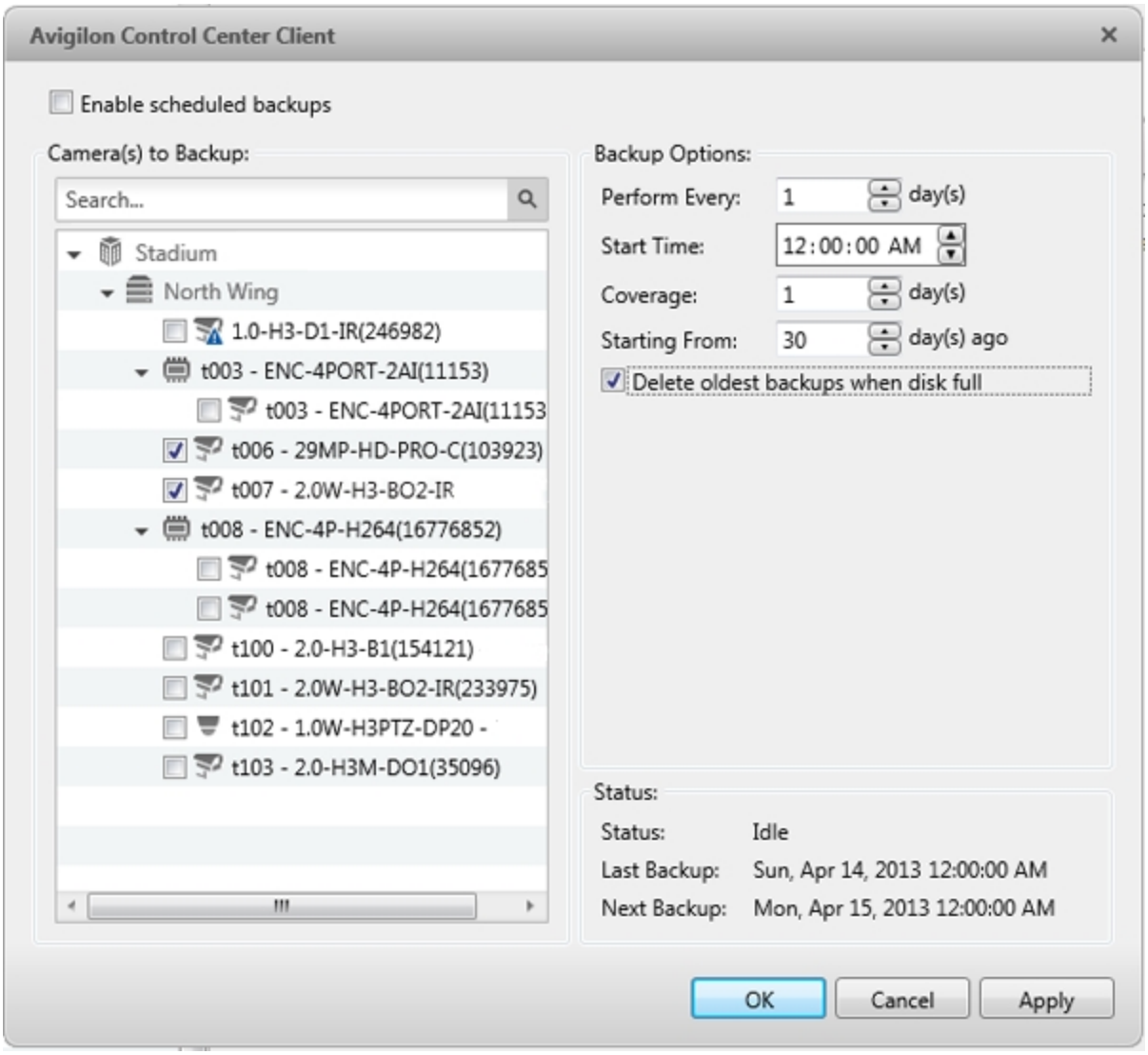


Figure 55: Scheduled Backup Setup dialog box

2. Select the **Enable scheduled backups** check box.
3. In the Camera(s) to Backup: list, select all the devices to back up.
4. In the Backup Options: area, complete the following:
   - **Perform Every: <X> day(s):** specify the number of days between backups
   - **Start Time:** the time when backup occurs
   - **Coverage:** the amount of recorded image data that is backed up
   - **Starting From:** starting point for the backup

- **Delete oldest backups when disk full:** select this check box to automatically delete the oldest backups when the backup storage location is full

For example in the figure above, the Scheduled Backup is configured to occur every day at 12 am. Video from 30 days ago is backed up and will cover 1 day of video, so only the 30th day is backed up to the remote server each night.

5. Click **OK**.

   The Status area displays when the next backup will be.

License Plate Recognition

License Plate Recognition (LPR) is a licensed feature that allows users to read and store vehicle license plate numbers from any video streamed through the Avigilon Control Center.

The License Plate Recognition options will only appear if you have the feature licensed and installed on the server.

Setting Up License Plate Recognition

1. In the server Setup tab, click  .

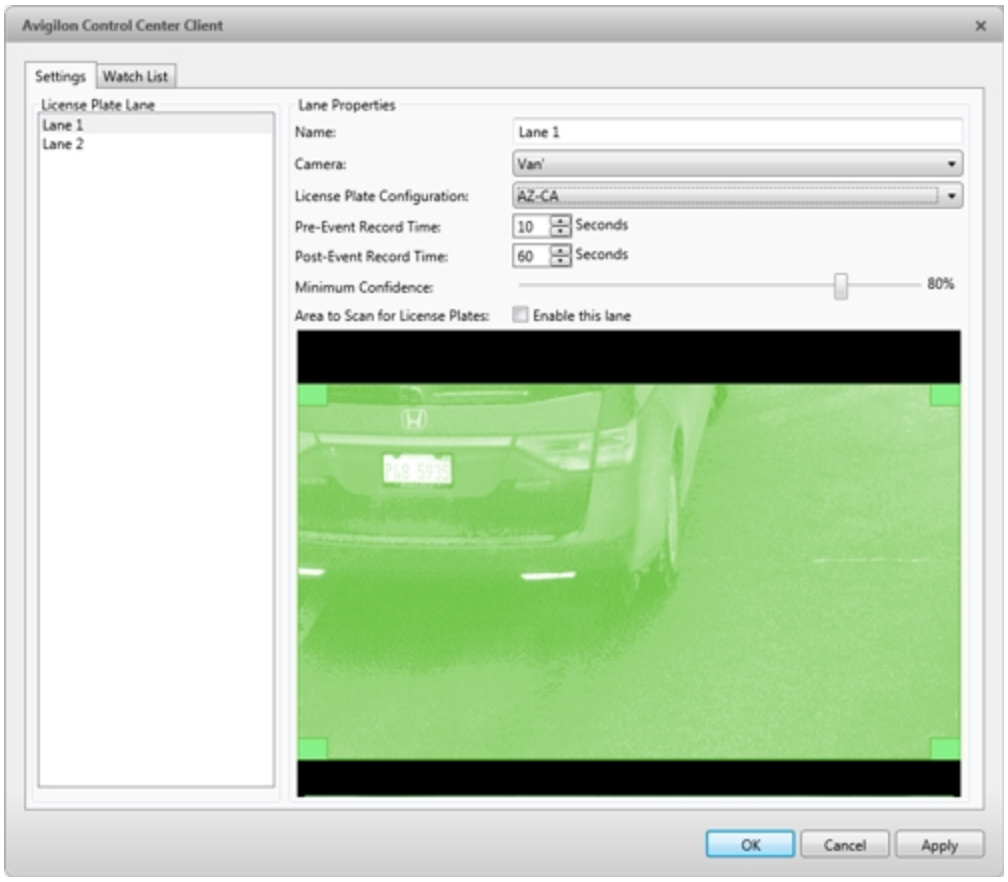


Figure 56: License Plate Recognition Setup dialog box

2. Select a lane from the left pane.

   The number of lanes listed is determined by the number of License Plate Recognition (LPR) channels that are licensed.

3. Complete the following fields:

   - **Name:** enter a name for the lane.
   - **Camera:** select the camera that will perform LPR. One camera can be used for multiple lanes.
   - **License Plate Configuration:** select the regional license plate format that needs to be recognized by the camera. For more information, see **Supported License Plates**.
   - **Pre-Event Record Time:** enter the amount of time that video is recorded before the license plate is recognized.
   - **Post-Event Record Time:** enter the amount of time that video is recorded after the license plate is recognized.
   - **Minimum Confidence:** move the slider to set the minimum confidence required for a detected license plate to be recognized. The default value is 80%.
   - **Enable this lane:** select this check box to enable LPR on this lane.

4. Move and adjust the size of the overlay to define the area where license plates are detected by the camera.

   NOTE: License plates are only detected when the overlay is green. If the overlay is red, the license plate detection area is too large.

5. Click **OK**.

Configuring the Watch List

The License Plate Recognition (LPR) Watch List identifies license plates that are of special interest. When a license plate on the Watch List is detected, an event is generated to notify you of the license plate and can be used to trigger an action in the Rules engine.

You can manually add each license plate that needs to be recognized, or import a list of license plates into the Client.

Adding Licenses to the Watch List

1. In the server Setup tab, click  .
2. When the License Plate Recognition dialog box appears, select the **Watch List** tab.

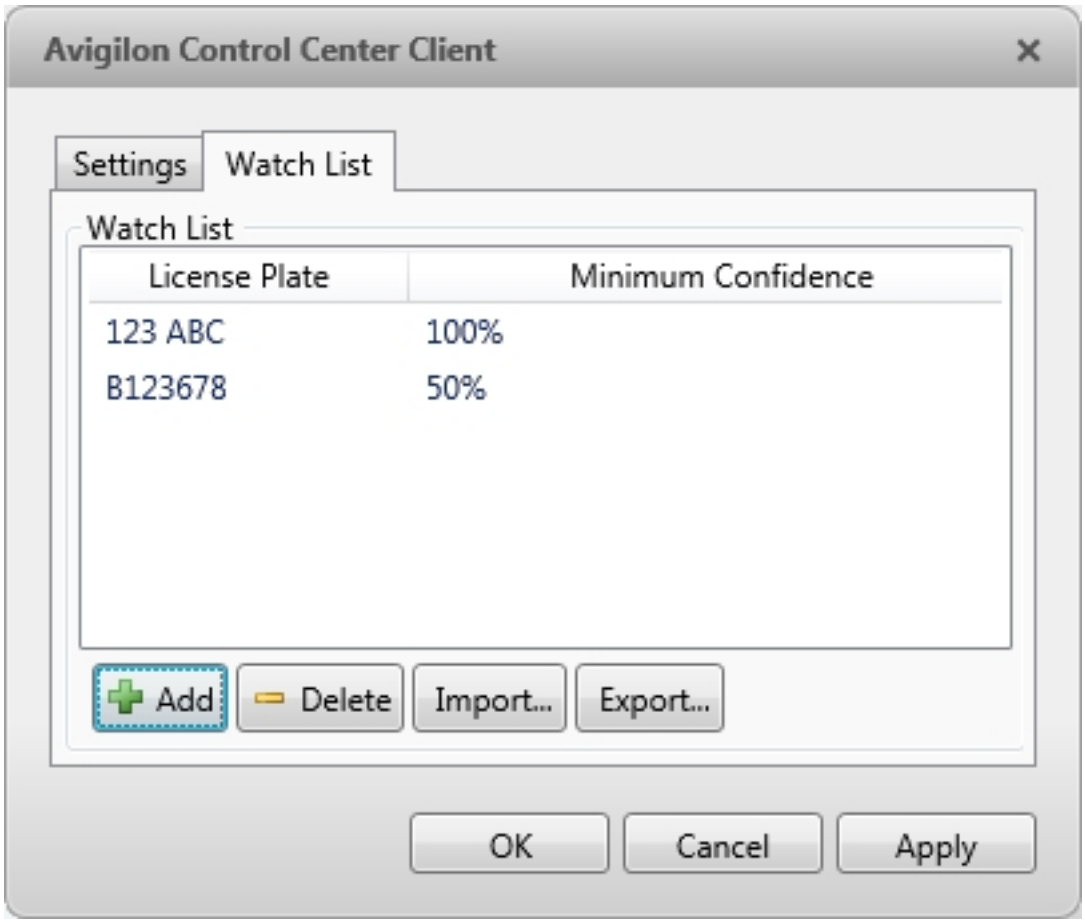


Figure 57: License Plate Recognition dialog box: Watch List tab

3. Click **Add...**. The Add License Plate dialog box appears.

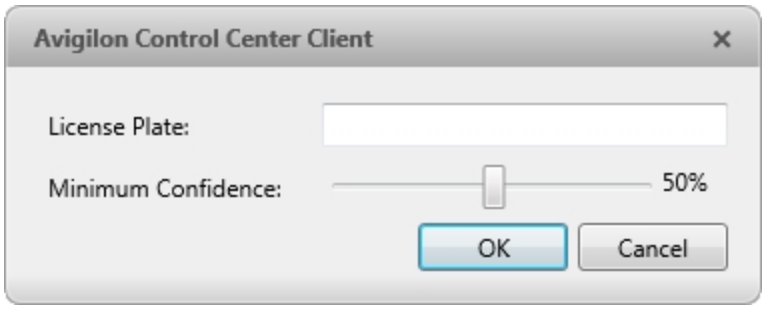


Figure 58: Add License Plate dialog box

4. Enter the license plate number you want to watch for.
5. Move the **Minimum Confidence** slider to determine how similar the detected license plate must be before it is considered a match.

   For example, if a license plate on your Watch List is ABC 123 and the Avigilon Control Center detects an ABC 789 license plate, the system will be 50% confident that it has found a match. If the system detects ABC 129, it will be 83% confident that it has found a match.

6. Click **OK**.

Deleting a License Plate from the Watch List

1. In the License Plate Recognition dialog box, select the **Watch List** tab.
2. Select the license plate from the Watch List, and click **Delete**.

Exporting a Watch List

1. In the License Plate Recognition dialog box, select the **Watch List** tab.
2. Click **Export...**.
3. In the Save As dialog box, name the file and click **Save**.

The Watch List can be exported as a text file or a comma-separated values (CSV) file.

Importing a Watch List

1. In the License Plate Recognition dialog box, select the **Watch List** tab.
2. Click **Import...**.
3. In the Import dialog box, locate the Watch List file and click **Open**.

POS Transactions

The Point of Sale (POS) Transaction Engine is a licensed feature that records raw data from POS transaction sources. You can link cameras to specific POS transaction sources, and set up the system to make note of transaction exceptions.

Once POS transactions have been set up, you can see live and recorded POS transaction data in the View tab while watching any linked video.

To monitor live POS transactions, see **Monitoring Live POS Transactions**.

To review recorded POS transactions, see **Reviewing Recorded POS Transactions**.

Adding a POS Transaction Source

1. In the server Setup tab, click  .
2. In the POS Transactions dialog box, click  .
3. Enter the **Hostname/IP Address:** and the **Port:** number for the POS transaction source device, then click  .

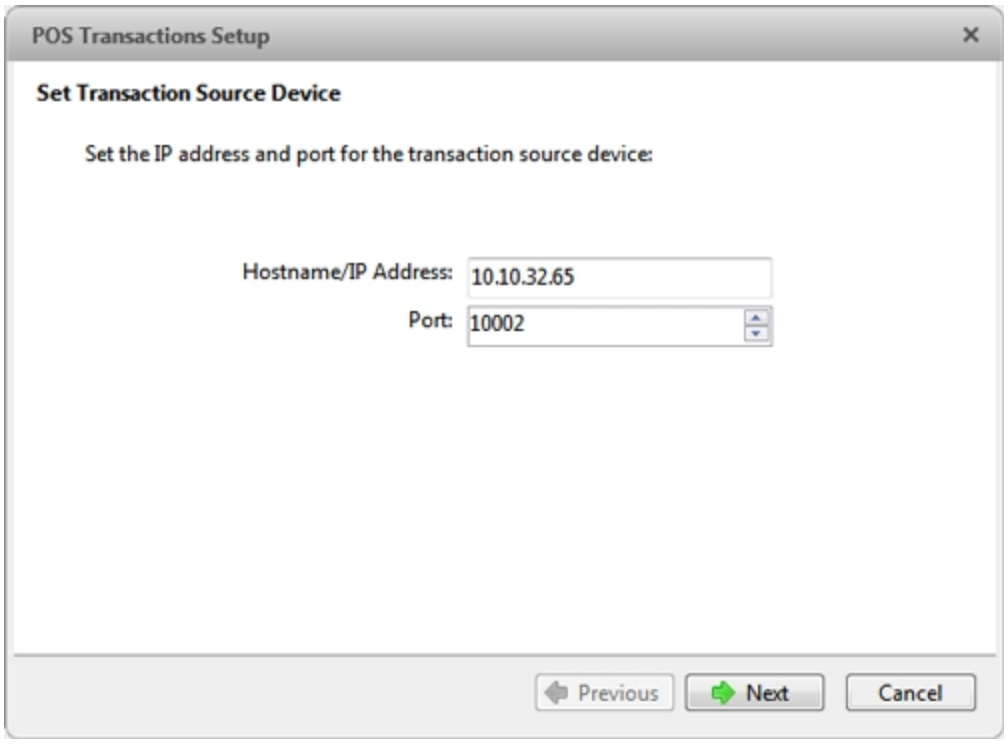


Figure 59: The Set Transaction Source Device page

4. Select a Transaction Source Data format, then click **Next**.

   If the source data format needs to be added or edited, click or **Edit**. Alternatively, click **Copy From** to create a new data format based on the selected data format. For more information, see **Adding a Transaction Source Data Format**.

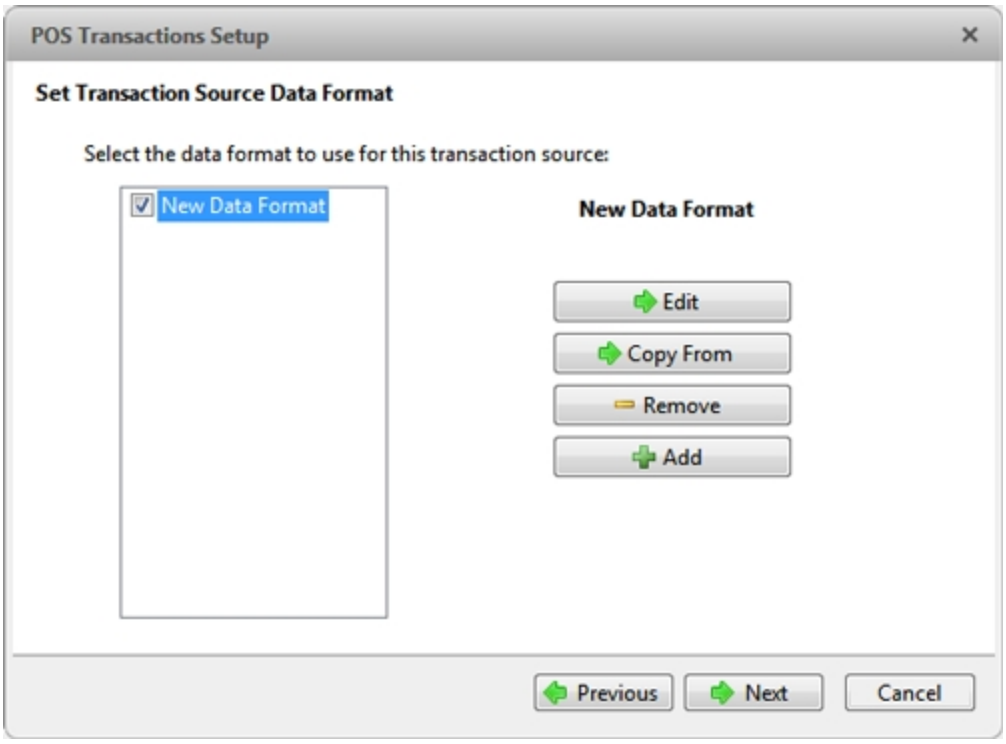


Figure 60: The Set Transaction Source Data Format page

5. On the Set Transaction Exceptions page, select any exceptions that need be monitored, then click **Next**. If you do not need to monitor for exceptions, just click **Next**.

   Click to add an exception or **Edit** to edit an existing exception. For more information, see **Adding a Transaction Exception**.

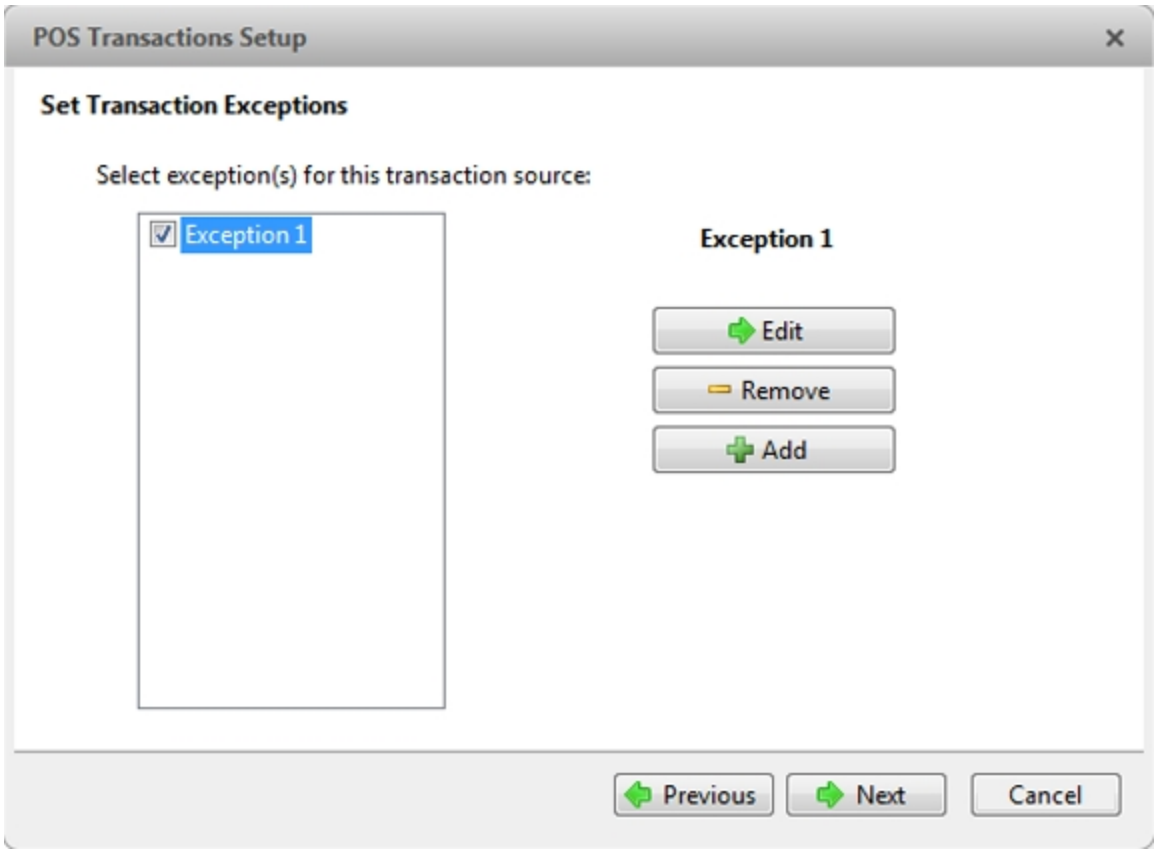


Figure 61: The Set Transaction Exceptions page

6. Select any cameras you want to link to the transaction source, and set the amount of time video needs to be recorded before and after each transaction. Then click .

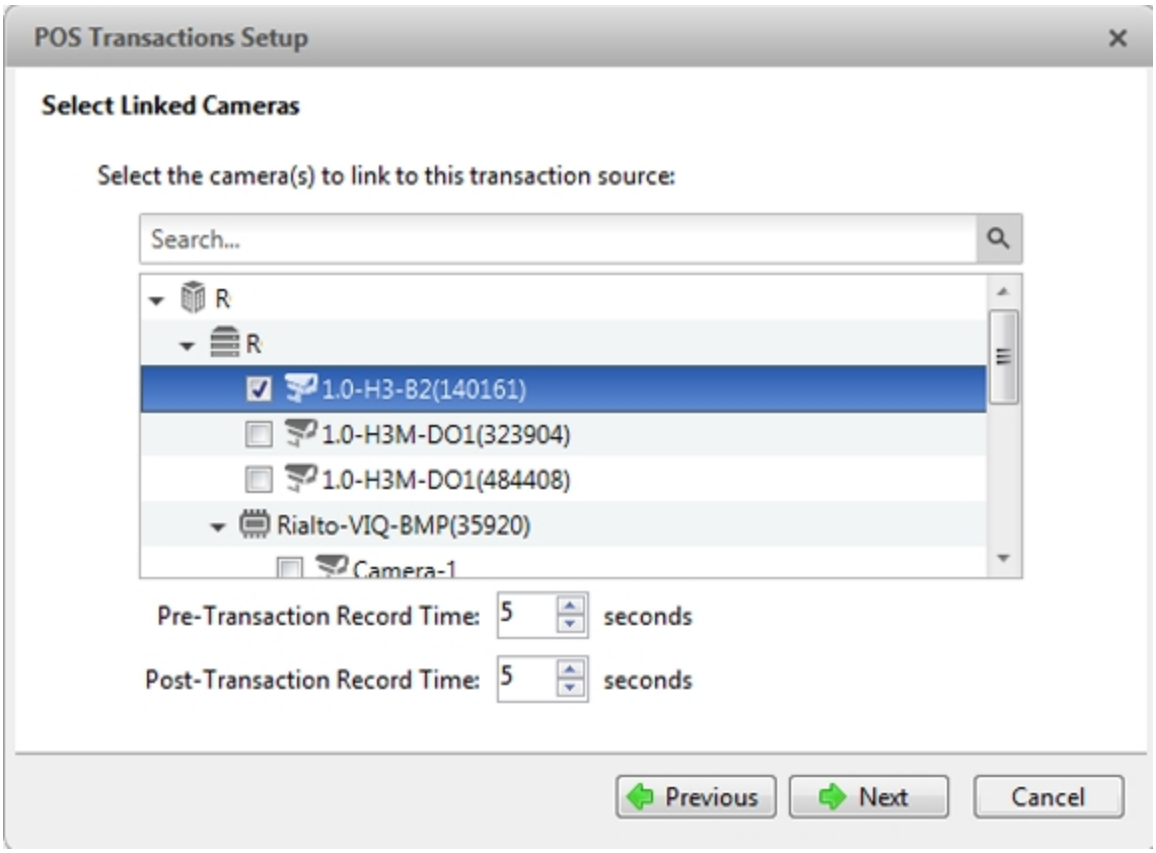


Figure 62: The Select Linked Cameras page

7. Enter a name and description for the transaction source, then select **Enable transaction source** to start receiving data from the transaction source.

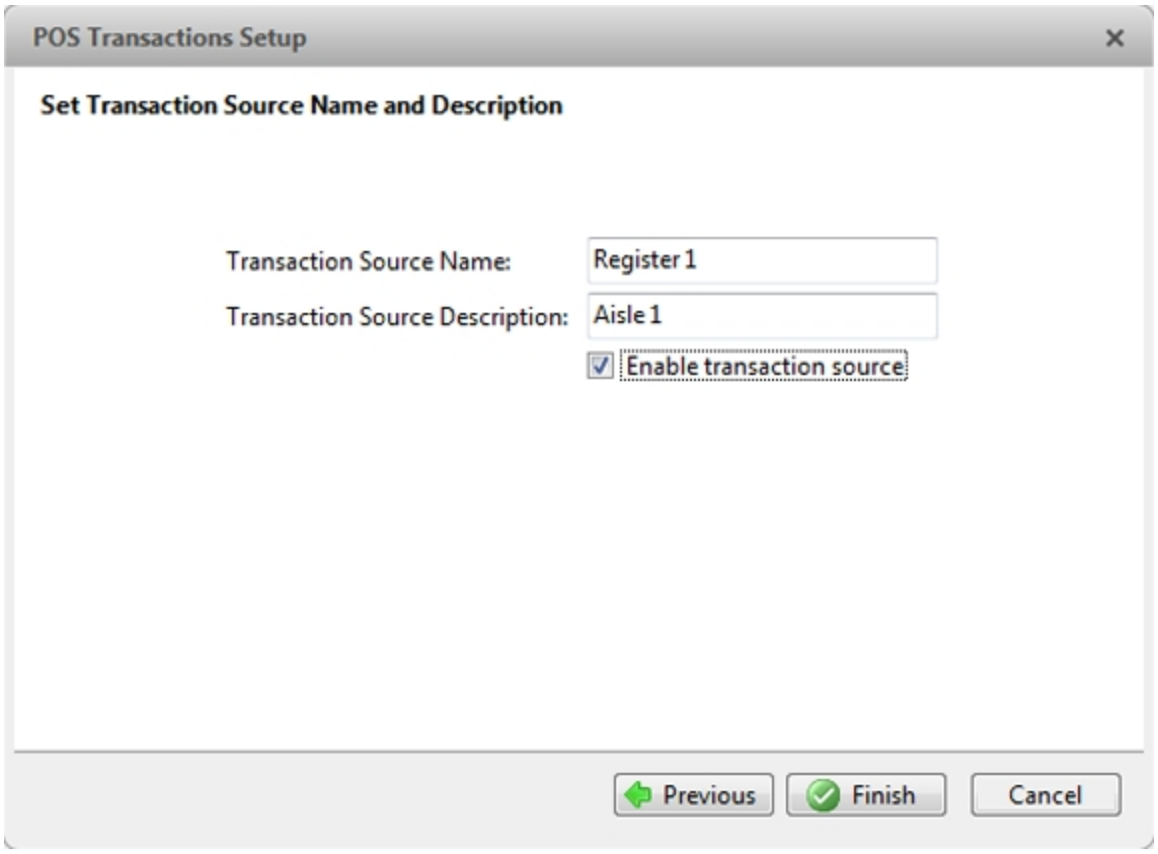


Figure 63: The Set Transaction Source Name and Description page

8. Click .

Adding a Transaction Source Data Format

NOTE: POS transaction source data formats are shared across a Site.

When you add a new POS transaction source, be aware that the transaction source must have a source data format.

In the POS Transactions Setup wizard, click when you arrive on the Set Transaction Source Data Format page. When the Configure Data Format dialog box appears, complete the following procedure:

1. In the Properties area, specify the following:

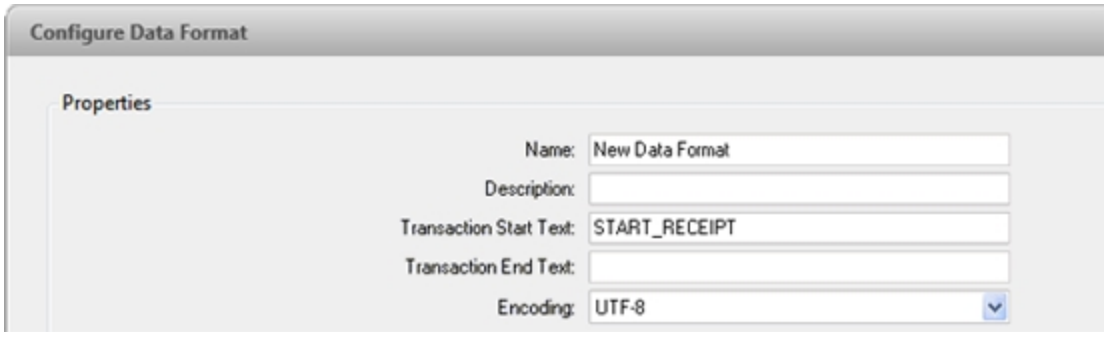


Figure 64: The Configure Data Format dialog box

- **Name:** enter a name for the data format.
- **Description:** enter a description of the data format.
- **Transaction Start Text:** (required) enter the text that identifies the start of each transaction from the POS transaction source.
- **Transaction End Text:** (optional) enter the text that identifies the end of each transaction.
- **Encoding:** Select the encoding used by the POS transaction source.

2. The following figure shows raw transaction data on the left and filtered transaction data on the right. Perform any of the following to capture raw data for the source data format:

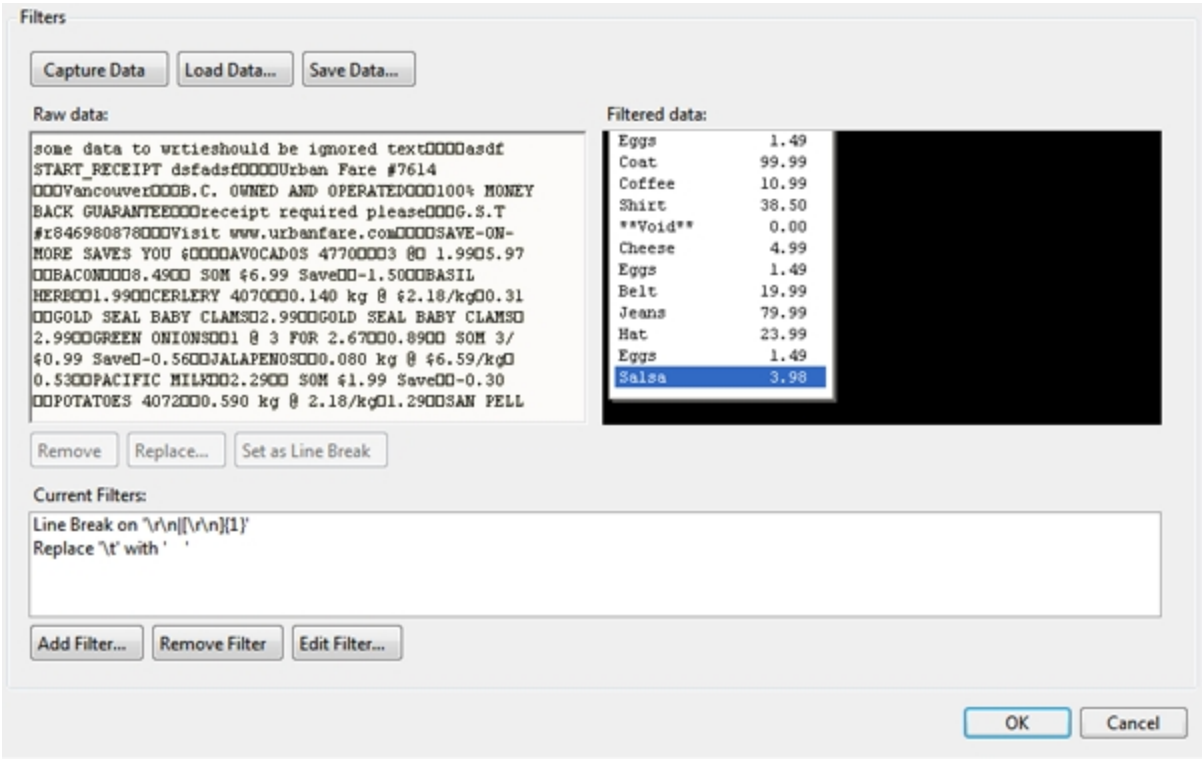


Figure 65: The Configure Data Format dialog box

- Click **Capture Data** to start capturing a raw transaction data sample.
- Click **Stop Capture** to stop capturing transaction data.
- Click **Load Data...** to load raw transaction data from a file.
- Click **Save Data...** to save a copy of the transaction data that has been captured.

3. (Optional) Click **Add Filter...** to create a new filter for the raw transaction data file.

   There are two default filters in the Current Filters: area: one to create line breaks and the other to delete extra white space at the beginning of each line. If you do not need extra filters, skip this step.

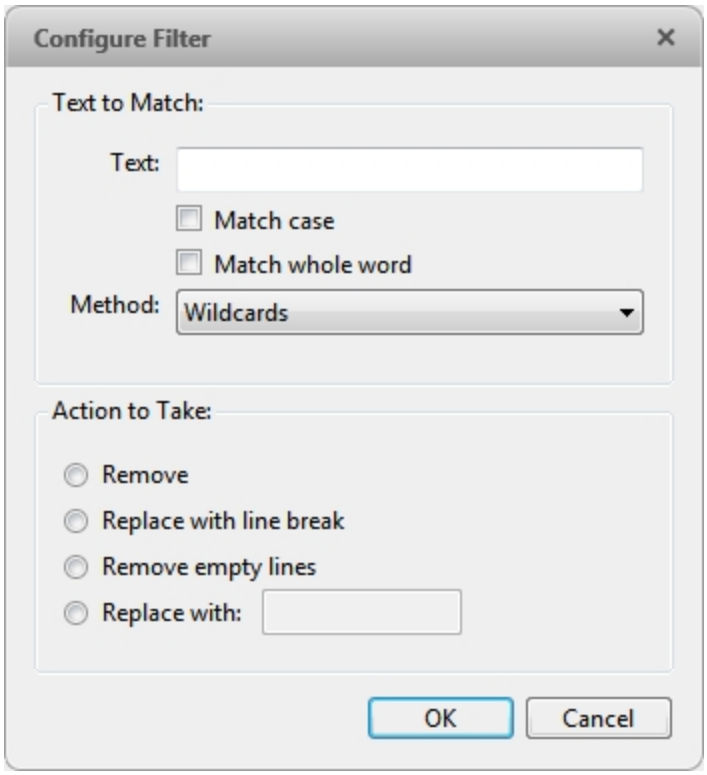


Figure 66: The Configure Filter dialog box

a. In the **Text:** field, enter text for the filter to search for.

b. Select the **Match case** and/or **Match whole word** check box to focus the text filter to only find text with the same capitalization or an exact match.

c. In the **Method:** drop down list, select a search method. You can choose to filter text found through a **Normal** search, **Wildcards** search, or **Regular expressions** search.

d. In the **Action to Take:** area, select which action to take when the filter finds a match to your text criteria.

e. Click **OK**.

4. On the Configure Data Format screen, click **OK** to add the new data format to the data format list.

Adding a Transaction Exception

NOTE: POS transaction exceptions are shared across a Site.

To help monitor unusual transactions, you can set up transaction exceptions. Transaction exceptions can help you identify unauthorized discounts, fake returns, and manual price overrides.

In the POS Transactions Setup tab, select the camera you want to edit and go through the setup wizard. Click when you arrive on the Set Transaction Exceptions page. When the Configure Exception dialog box appears, complete the following procedure:

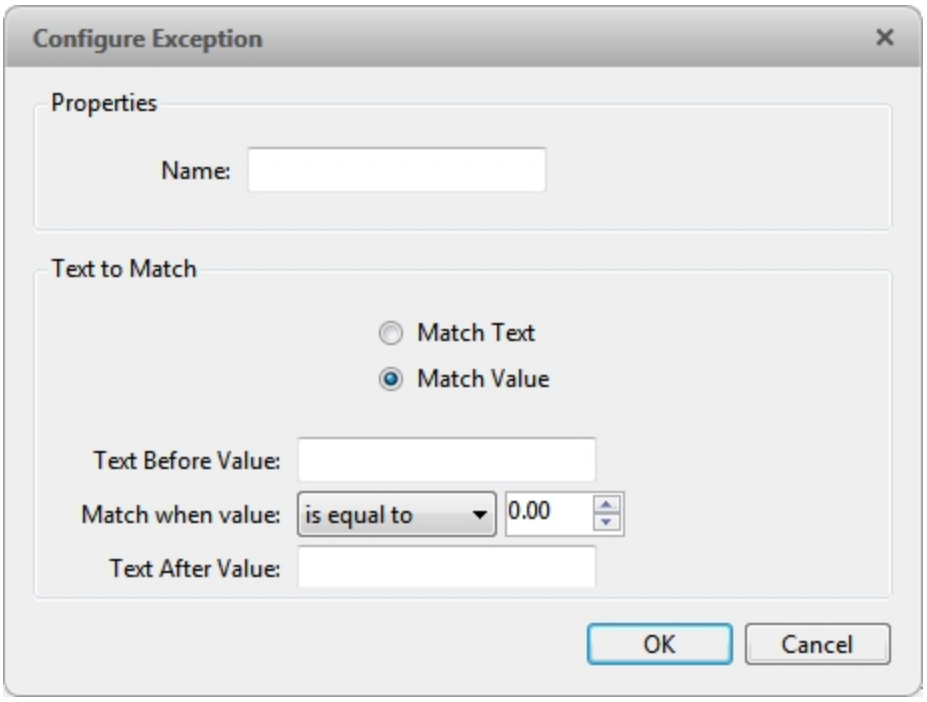


Figure 67: The Configure Exception dialog box

1. Enter a name for the exception.
2. Select one of the Text to Match options:

Select	And do this...
Match Text	Enter text for the exception to search for. The exception will monitor all transactions for the text entered in the **Text to Match** field.
Match Value	Enter the value that triggers the exception, and enter the text that may appear around the value. The exception will monitor all transactions for values that match what you enter in the **Text Before Value:**, **Match when value:**, and **Text After Value:** fields

3. Click **OK.**

Editing and Deleting a POS Transaction Source

1. In the server Setup tab, click  .

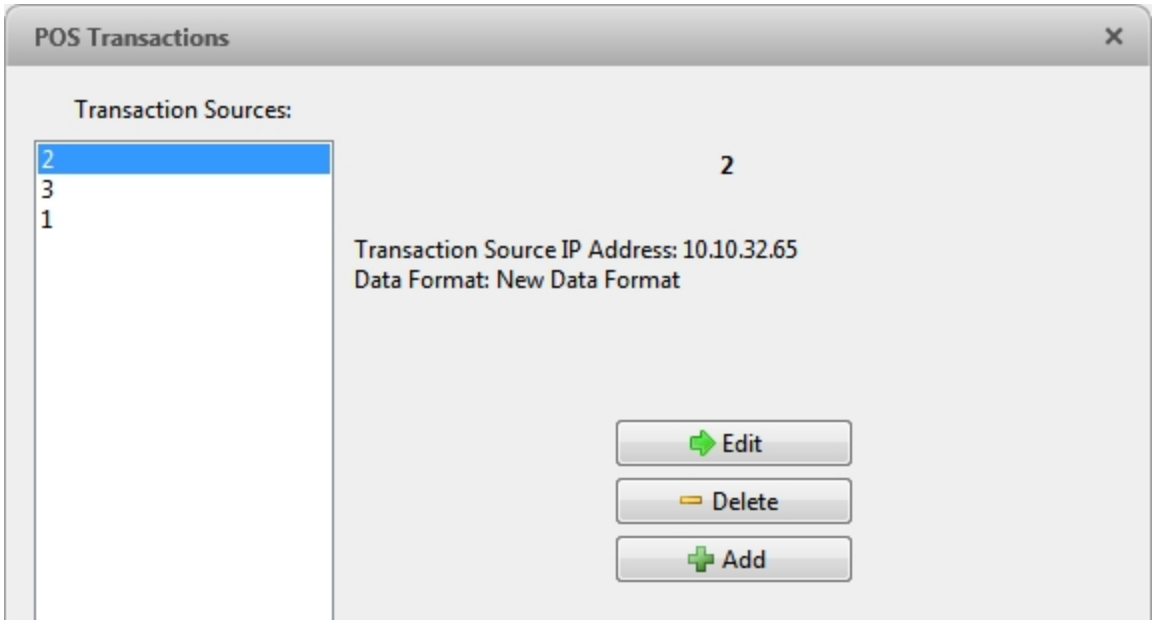


Figure 68: The POS Transactions dialog box

2. In the POS Transactions dialog box, select a POS transaction source, then do one of the following:

   - To edit the POS transaction source, click . Go through the POS Transactions Setup wizard and make the required changes on each page. On the last page, click to save your changes. For details about the editable options, see **Adding a POS Transaction Source**.

   - To delete the POS transaction source, click . When the confirmation dialog box appears, click **Yes**.

Device Settings

Device settings are used to adjust video quality and set up devices that can be connected to cameras and video analytics appliances. These settings include adjusting camera display quality, video compression, and image rate, as well as digital and audio inputs/outputs.

NOTE: Some features are not displayed if the server does not have the required license, or if you do not have the required user permissions.

NOTE: The dialog box may appear differently depending on the device. Options that are not supported by the device will be disabled or hidden.

General

Use the device General dialog box to set a device's identity and configure device PTZ settings. You can also reboot the device through the General dialog box.

Setting a Device's Identity

In a device's General dialog box you can give the device a name, describe the device's location, and give the device a logical ID. The logical ID is needed to control the device through keyboard and joystick commands.

NOTE: The dialog box may appear differently depending on the device. Options that are not supported by the device will be disabled or hidden.

1. In the device Setup tab, click 
2. In the **Camera Name:** field, give the device a meaningful name to help you identify it. By default, the device model number is used as the device's name.
3. In the **Camera Location:** field, describe the device's location.
4. In the **Logical ID:** field, enter a unique number to allow the Client and integrations to identify this device.
5. (Cameras only) To disable the LEDs on a device, select the **Disable camera status LEDs**. This may be required if the device is installed in a covert location.
6. (Cameras only)If a device has a motorized zoom and focus lens, the **Enable PTZ controls** check box will be displayed. For more information, see **Configuring PTZ**.
7. Click **OK**.

Configuring PTZ

Use the camera General dialog box to enable and configure the motorized pan, tilt, zoom (PTZ) devices that may be connected to Avigilon™ cameras. PTZ devices are connected to Avigilon cameras through the RS-485 inputs.

Third-party PTZ camera controls cannot be configured through the Control Center software.

1. In the camera Setup tab, click  .
2. In the PTZ area, select the **Enable PTZ controls** check box.

   NOTE: If the following options are not displayed, the camera only has a motorized zoom and focus lens that can be controlled through the PTZ Controls pane. Other PTZ controls will not be available.
3. In the **Protocol:** drop down list, select the appropriate PTZ protocol. The available protocols include:
   - AD Sensormatic
   - AXSYS
   - AXSYS DCU
   - Ernitec ERNA
   - Honeywell Diamond
   - Kalatel ASCII
   - Pelco D
   - Pelco P
   - TEB Ligne
   - Videotec MACRO
   - Videotec Legacy
   - Vicon extended
   - Vicon normal
   - JVC JCBP
4. Enter the **Dip Switch Address:**, **Baud Rate:**, and **Parity:** for the PTZ device.
5. Click **OK**.

Once PTZ has been configured, you can use the camera's PTZ Controls while you watch the camera's live video stream. For more information, see **Controlling PTZ Cameras**.

Rebooting a Device

You can restart all Avigilon devices through the device's General dialog box. This feature is not available for third party devices.

1. In the device Setup tab, click  .
2. Click **Reboot Camera...**.

The device will disconnect from the Avigilon Control Center and shut down. When the device starts up again, the device should automatically reconnect with the Avigilon Control Center.

Network

Use the device Network dialog box to change how a device connects to the server network.

NOTE: Some features are not displayed if the server does not have the required license, or if you do not have the required user permissions.

1. In the device Setup tab, click  .
2. In the Network dialog box, select how the device obtains an IP address:

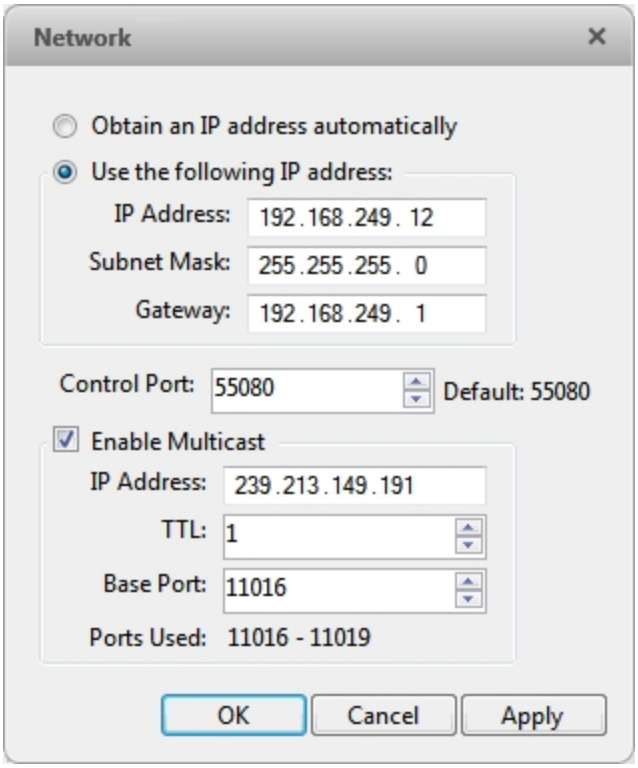


Figure 69: The Network dialog box

- **Obtain an IP address automatically:** select this option for the device to connect to the network through an automatically assigned IP address.

  The device will attempt to obtain an address from a DHCP server. If this fails, the device will obtain an address through Zero Configuration Networking (Zeroconf) and select an address in the 169.254.0.0/16 subnet.

- **Use the following IP address:** select this option to manually assign a static IP address to the device.

  Enter the **IP Address:**, **Subnet Mask:**, and **Gateway:** you want the device to use.

3. Select the **Control Port:** for connecting to the device. This port is also used for manually discovering the device on the network.
4. (Cameras only) Select the **Enable Multicast** check box to enable multicast streaming from the device. You

must Enable Multicast to set up redundant recording to multiple servers.

Use the default generated **IP Address:**, **TTL:**, and **Base Port:**, or enter your own values.

5. Click **OK**.

Image and Display

Use the Image and Display dialog box to control a camera's display settings for live and recorded video.

NOTE: The dialog box may appear differently depending on the device. Options that are not supported by the device will be disabled or hidden.

Changing Image and Display Settings

NOTE: The dialog box may appear differently depending on the device. Options that are not supported by the device will be disabled or hidden.

1. In the camera Setup tab, click  .
2. In the Image and Display dialog box, make the required changes to adjust the camera's image settings. A preview of your changes is displayed in the image panel.

   Tip: Use the **Maximum Exposure:**, **Maximum Gain:**, and **Priority:** options to control low light behavior.

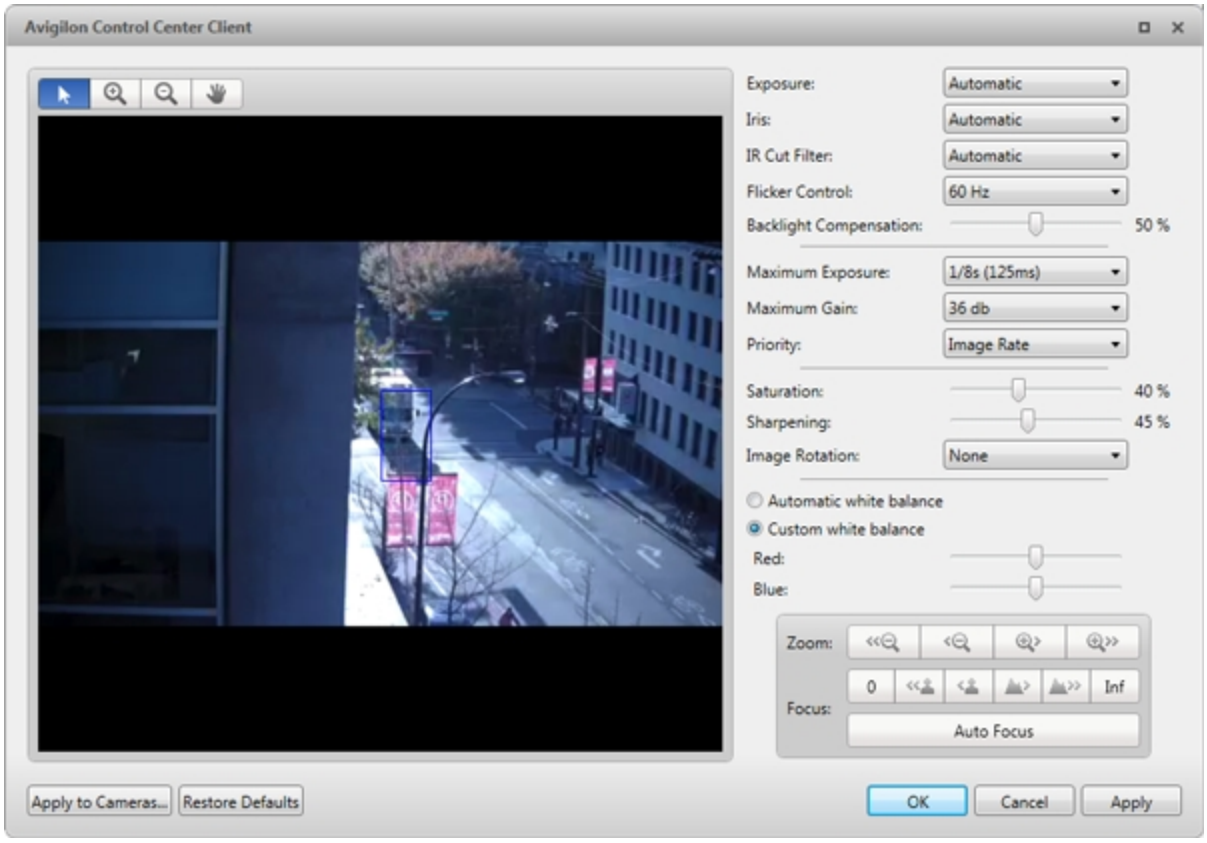


Figure 70: The Image and Display dialog box

Option	Description
Exposure:	You can allow the camera to control the exposure by selecting **Automatic**, or you can set a specific exposure rate. **NOTE:** Increasing the manual exposure time may affect the image rate.
Iris:	You can allow the camera to control the iris by selecting **Automatic**, or you can manually set it to **Open** or **Closed**.
IR Cut Filter:	You can allow the camera to control the infrared cut filter by selecting **IR Cut Filter:**, or set the camera to **Color** or **Monochrome** mode.
Flicker Control:	If your video image flickers because of the fluorescent lights around the camera, you can reduce the effects of the flicker by setting the **Flicker Control:** to the same frequency as your lights. Generally, Europe is **50 Hz** and North America is **60 Hz**.
Backlight Compensation:	If your scene has areas of intense light that cause the overall image to be too dark, move the **Backlight Compensation:** slider until you achieve a well exposed image.
Enable Wide Dynamic Range	Select this box to enable automatic color adjustments through Wide Dynamic Range (WDR). This allows the camera to adjust the video image to accommodate scenes where bright light and dark shadow are clearly visible.
Maximum Exposure:	You can limit the automatic exposure setting by selecting a **Maximum Exposure:** level. By setting a **Maximum Exposure:** level for low light situations, you can control the camera's exposure time to let in the maximum amount of light without creating blurry images.
Maximum Gain:	You can limit the automatic gain setting by selecting a **Maximum Gain:** level. By setting a **Maximum Gain:** level for low light situations, you can maximize the detail of an image without creating excessive noise in the images.
Priority:	You can select **Image Rate** or **Exposure** as the priority. When set to **Image Rate**, the camera will maintain the set image rate as the priority, and will not adjust the exposure beyond what can be recorded for the set image rate. When set to **Exposure,** the camera will maintain the exposure setting as the priority, and will override the set image rate to achieve the best image possible.
Saturation:	You can adjust the video's color intensity by moving the **Saturation:** slider until the video image meets your requirements.
Sharpening:	You can adjust the video sharpness to make the edges of objects more visible. Move the **Sharpening:** slider until the video image meets your requirements.
Image Rotation:	You can change the rotation of captured video. You can rotate the video 90,

Option	Description
	180, or 270 degrees clockwise.
White Balance	You can control white balance settings to adjust for differences in light. You can allow the camera to control the white balance by selecting **Automatic white balance**, or select **Custom white balance** and manually set the **Red:** and **Blue:** settings.

3. To focus the camera, see **Zooming and Focusing the Camera Lens**.
4. Click **Apply to Cameras...** to apply the same settings to other cameras of the same model.
5. Click **OK**.

Zooming and Focusing the Camera Lens

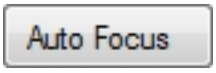
If the camera has remote zoom and focus capabilities, you can control the camera's zoom and focus through the Image and Display dialog box.

1. In the camera Setup tab, click  .
2. If the camera has a built-in auto-focus feature, you can choose one of the following:
   - **Continuous Focus:** the camera will automatically focus itself whenever the scene changes. Skip the following steps.
   - **Manual Focus:** you can manually focus the camera through the **Focus:** buttons. Once the focus is manually set, it will not change.
3. While you watch the preview in the image panel, complete the following steps to zoom and focus the camera:

   Tip: For Avigilon™ HD Professional Cameras, the lens must be set to auto-focus (AF) mode on the camera. If the camera does not detect the lens, the Focus: buttons are not displayed.

   a. Use the **Zoom:** buttons to zoom in to the distance you want to focus.
4. In the **Iris:** drop down list, select **Open**. When the iris is fully open, the camera's depth of field is the shortest.
5. Use the **Focus:** buttons until the image becomes clear.

Focus Buttons

Button	Description
	The camera will automatically focus one time.
	The camera will focus as close to zero as possible.

Button	Description
	Large step toward zero.
	Small step toward zero.
	Small step toward infinity.
	Large step toward infinity.
	Infinity.

6. Click **Apply to Cameras...** to apply the same settings to other cameras of the same model.
7. Click **OK**.

Dewarping a Panomorph Lens

If your camera uses a fisheye or panomorph lens, you may choose to dewarp the image through the Avigilon™ Control Center software.

NOTE: The dialog box may appear differently depending on the device. Options that are not supported by the device will be disabled or hidden.

1. In the camera Setup tab, click  .
2. In the Image and Display dialog box, select the **Lens Type:** used by the camera.

   If the Lens Type list is empty, contact Avigilon Technical Support and request that support for your camera and lens model be added to the application.

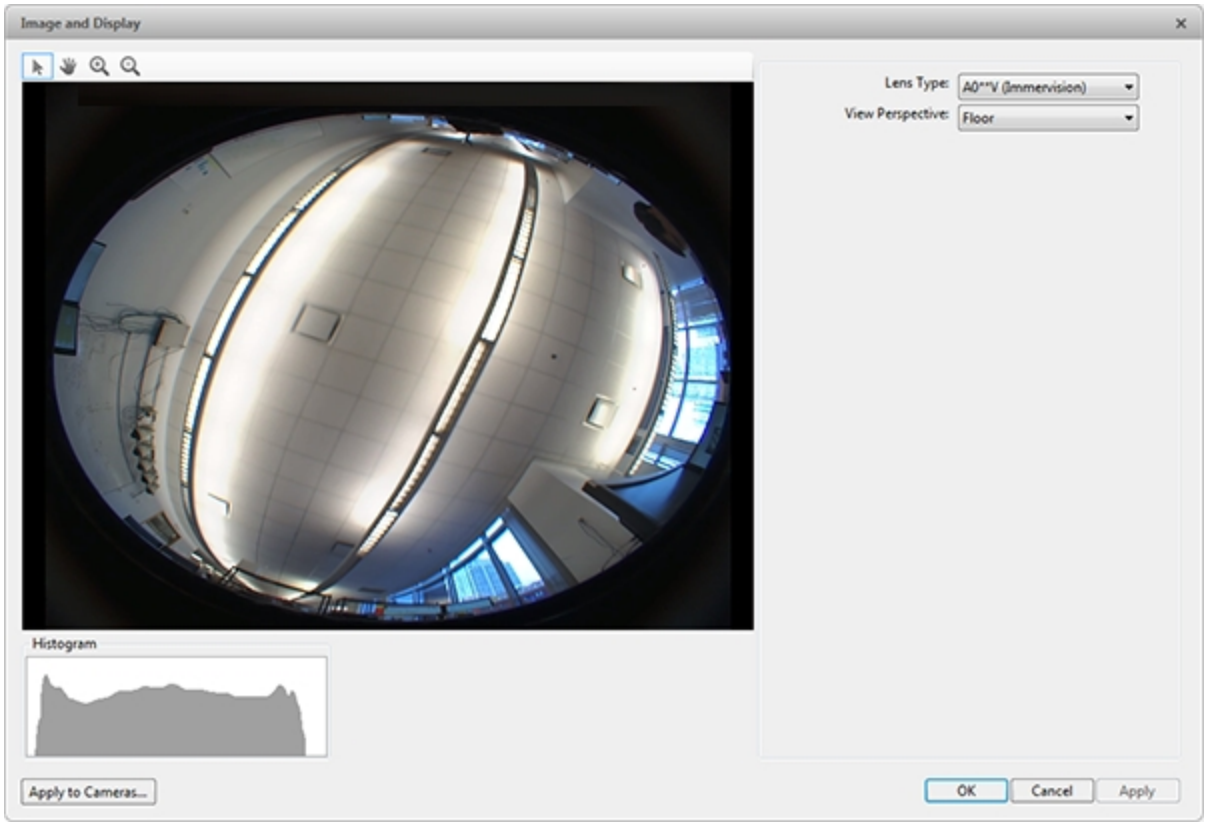


Figure 71: The Image and Display dialog box for panoramic lens configuration

3. In the **View Perspective:** drop down list, select one of the following options:
    - **Floor:** select this option if the camera is installed to look up.
    - **Ceiling:** select this option if the camera is installed to look down.
    - **Wall:** select this option if the camera is installed to look at the horizon.
4. If available, edit the image and display settings that are supported by the Lens Type:.
5. Click **OK**.

The system dewarps the lens image based on the way it is installed. You will be able to control how video is display in an image panel through the PTZ controls.

Compression and Image Rate

Use the camera Compression and Image Rate dialog box to modify the camera's frame rate and image quality settings for sending image data over the network.

NOTE: The dialog box may appear differently depending on the device. Options that are not supported by the device will be disabled or hidden.

For more information about the supported compression technologies, see the **Understanding Compression Technologies for HD and Megapixel Surveillance** white paper on the Avigilon website.

1. In the camera Setup tab, click 

.

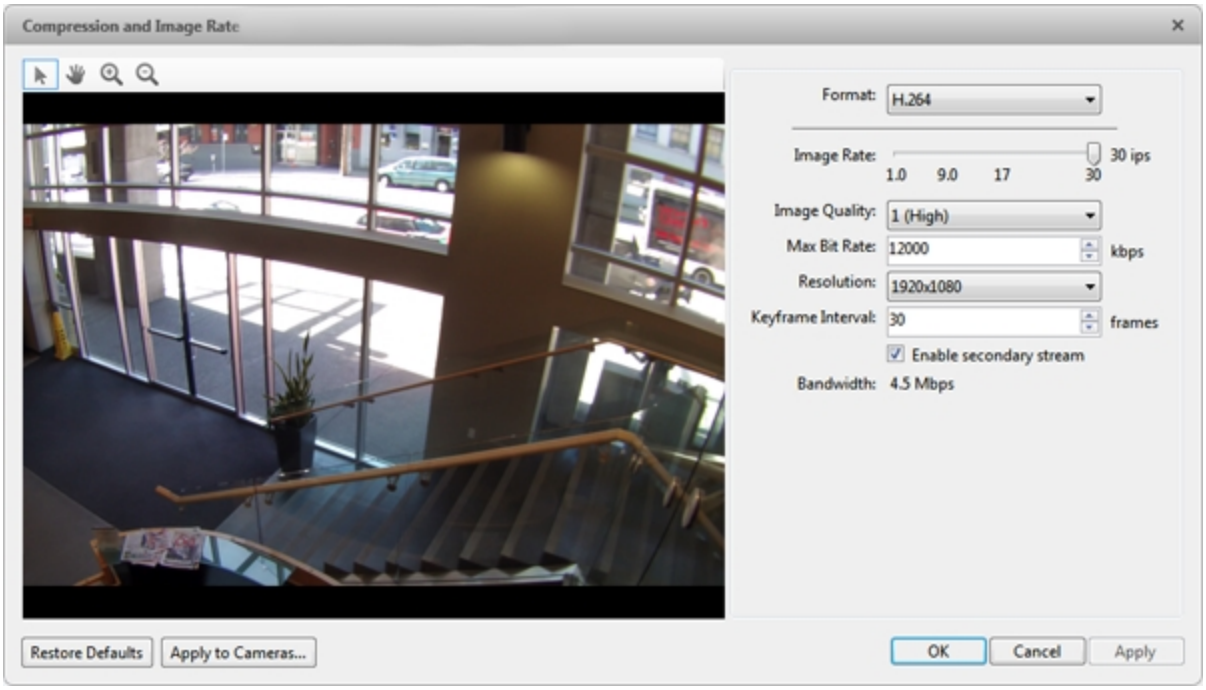


Figure 72: The Compression and Image Rate dialog box.

The Bandwidth: area gives an estimate of the bandwidth used by the camera with the current settings. Adjust the settings as required.

NOTE: For cameras capable of maintaining multiple streams, the settings in this dialog box only affect the primary stream.

2. In the **Format:** drop down list, select the preferred streaming format.
3. In the **Image Rate:** bar, move the slider to select the number of images per second (ips) you want the camera to stream over the network.

   For H.264 cameras and encoders, the image rate setting must be divisible by the maximum image rate. If you set the slider between two image rate settings, the application will round to the closest whole number.

4. In the **Image Quality:** drop down list, select an image quality setting. An image quality setting of **1** will produce the highest quality video and require the most bandwidth. The default setting is **6**.
5. In the **Max Bit Rate:** drop down list, select the maximum bandwidth the camera can use in kilobits per second (kbps).
6. In the **Resolution:** drop down list, select the preferred image resolution.
7. In the **Keyframe Interval:** drop down list, enter the preferred number of frames between each keyframe.

   It is recommended that you have at least one keyframe per second. So, if the image rate is set to 30 ips, you should enter **30** for the Keyframe Interval: setting.

8. If your camera supports multiple video streams, you can select the **Enable secondary stream** check box.

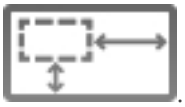
   When enabled, the secondary stream is a lower resolution video stream that is used by Avigilon's HDSM feature to maximize bandwidth and storage efficiencies.

9. Click **Apply to Cameras...** to apply the same settings to other cameras of the same model.
10. Click **OK**.

Image Dimensions

Use the Image Dimensions dialog box to set the image dimensions for the camera. You can crop the video image to help reduce bandwidth and increase the maximum image rate.

NOTE: This feature is only available for JPEG2000 cameras.

1. In the camera Setup tab, click  .
2. In the Image Dimensions dialog box, adjust the image dimensions by doing one of the following:
   - Drag the edges of the image until the video is cropped to fit your requirements.
   - Change the values for the **Top:**, **Left:**, **Width:**, and **Height:** fields.

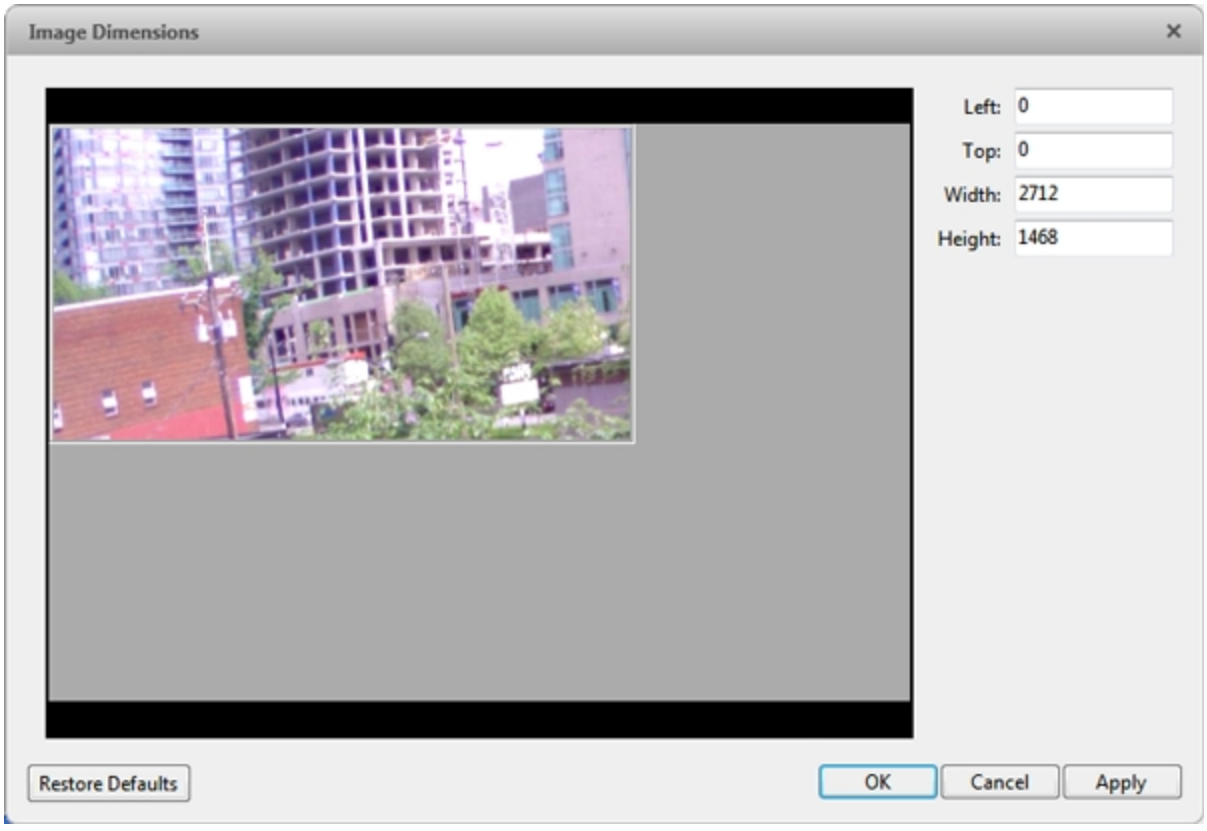


Figure 73: The Image Dimensions dialog box

3. Click **OK**.

Motion Detection

In the Motion Detection dialog box you can define specific pixel motion detection areas and configure the camera's sensitivity and threshold for pixel motion.

If you have a video analytics device, you can configureclassified object motion detection. For more information, see **Setting Up Classified Object Motion Detection**.

Selecting a Pixel Motion Detection Area

In the Motion Detection dialog box, you can set the green pixel motion detection areas in the camera's field of view. Pixel motion detection is ignored in the areas not highlighted in green.

1. In the camera Setup tab, click  .
2. Use the tools below the image panel to define the green pixelmotion detection area:
   -  **:** Click this button then draw green rectangles to define the pixel motion detection areas. You can draw multiple rectangles to create your pixel motion detection area.
   -  **:** Click this button and draw rectangles to erase sections from the pixel motion detection area.
   -  **:** Click this button and manually draw pixel motion detection areas with your mouse. This tool allows you to be very specific and highlight unusual shapes.
   -  **:** Click this button to highlight the entire image panel for pixel motion detection.
   -  **:** Click this button to clear the image panel of all pixel motion detection areas.

   Tip: Avoid areas with continuous pixel motion, like a TV or computer monitor, so that the camera is not constantly detecting unimportant pixel motion events.

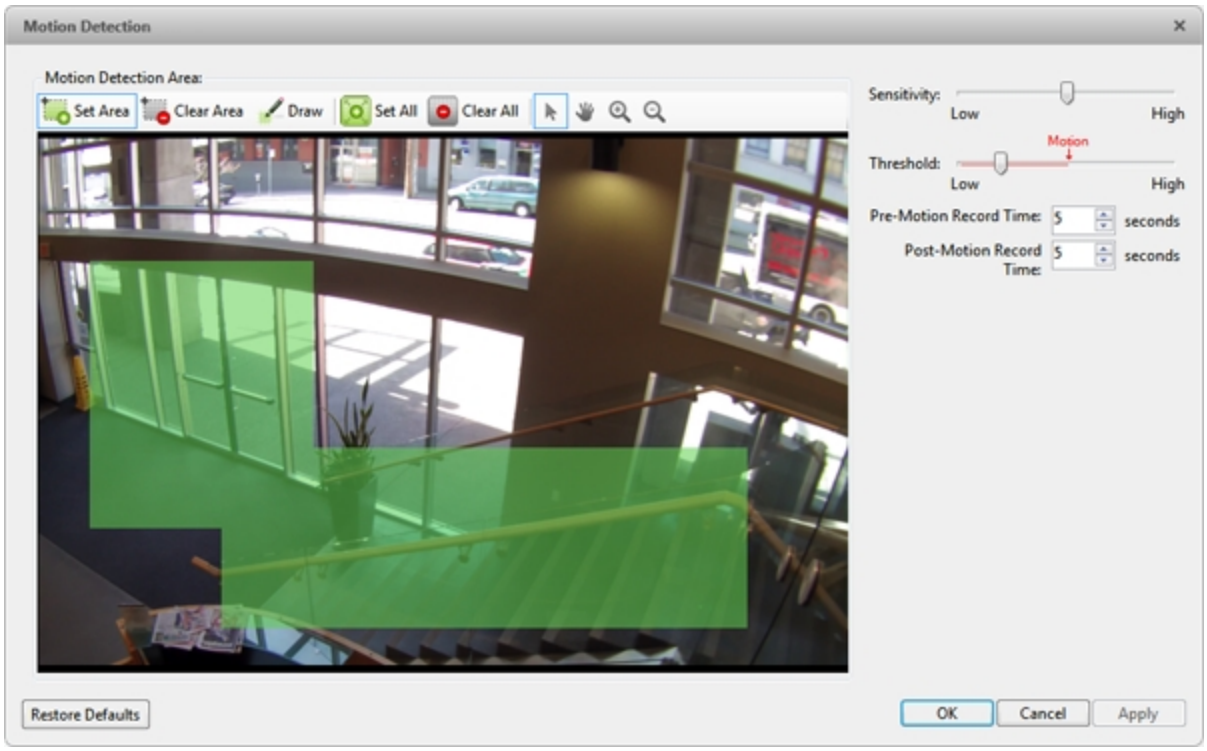


Figure 74: The Motion Detection dialog box

3. Click **OK**.

To define the sensitivity and threshold of the pixel motion detection area, see **Controlling Pixel Motion Sensitivity and Threshold**.

Controlling Pixel Motion Sensitivity and Threshold

In the Motion Detection dialog box, you can control the camera's sensitivity and threshold for pixel motion. You can also define how long video is recorded before and after each pixel motion event.

1. In the camera Setup tab, click  .

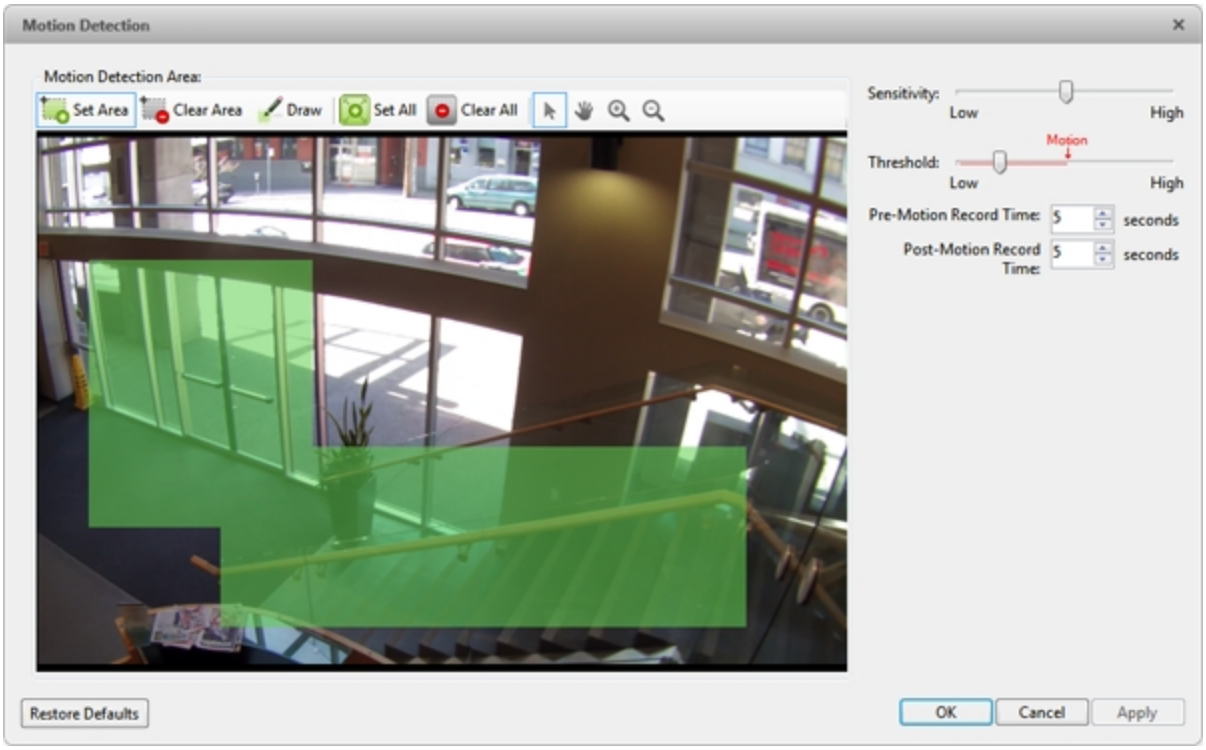


Figure 75: The Motion Detection dialog box

2. Move the **Sensitivity:** slider to adjust how much each pixel must change before it is considered in motion.

   When the sensitivity is High, even small movements are detected - like dust floating immediately before the camera lens.

   Move the slider to Low to avoid triggering pixel motion detection.

3. Move the **Threshold:** slider to adjust how many pixels must change before the image is considered to have pixel motion.

   When the threshold is High, only large motions are detected - like a truck driving across the scene.

   Tip: The **Motion** indicator above the Threshold: slider will move to indicate how much motion is occurring in the current scene. Only when the Motion indicator moves to the right of the Threshold: marker will the camera detect the pixel motion.

4. In the **Pre-Motion Record Time:** and **Post-Motion Record Time:** fields, specify how long video is recorded before and after the pixel motion event.
5. Click **OK**.

Adaptive Video Analytics

Adaptive video analytics is available on adaptive video analytics devices, including Rialto™ Video Analytics Appliances and Avigilon™ cameras with adaptive video analytics.

Configuring Video Analytics Device Location

NOTE: Changing the location of a video analytics device deletes existing teach data for that device.

1. In the device Setup tab, click  .

   The Video Analytics Configuration dialog box opens.

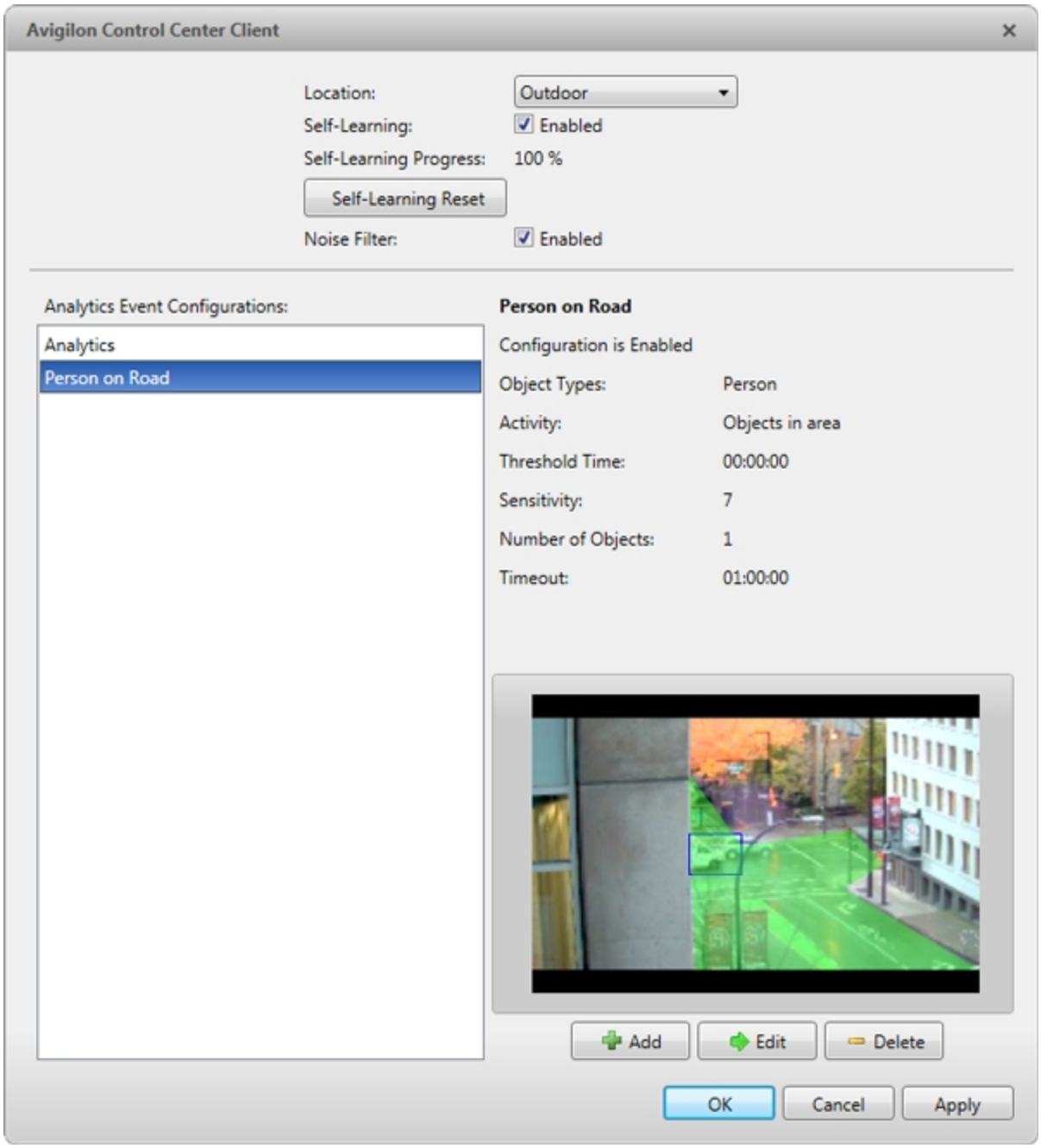


Figure 76: The Video Analytics Configuration dialog box

2. From the **Location:** drop down menu, select one of the following options:

- **Outdoor** - Use for outdoor scenes. This setting detects humans and vehicles.
- **Large Indoor Area** - Use for indoor scenes with a width of 1.5 m (5 ft) or more. Vehicle detection is disabled.
- **Indoor Overhead** - Use when camera is mounted overhead, with its field of view capturing the tops of people's heads. This setting is useful for counting people. Vehicle detection is disabled.

Configuring the Camera Type

To improve the analytics detection accuracy of a video analytics appliance, you can choose the type of video sent by each connected camera to the appliance.

1. In the device Setup tab, click  .

   The Video Analytics Configuration dialog box opens.

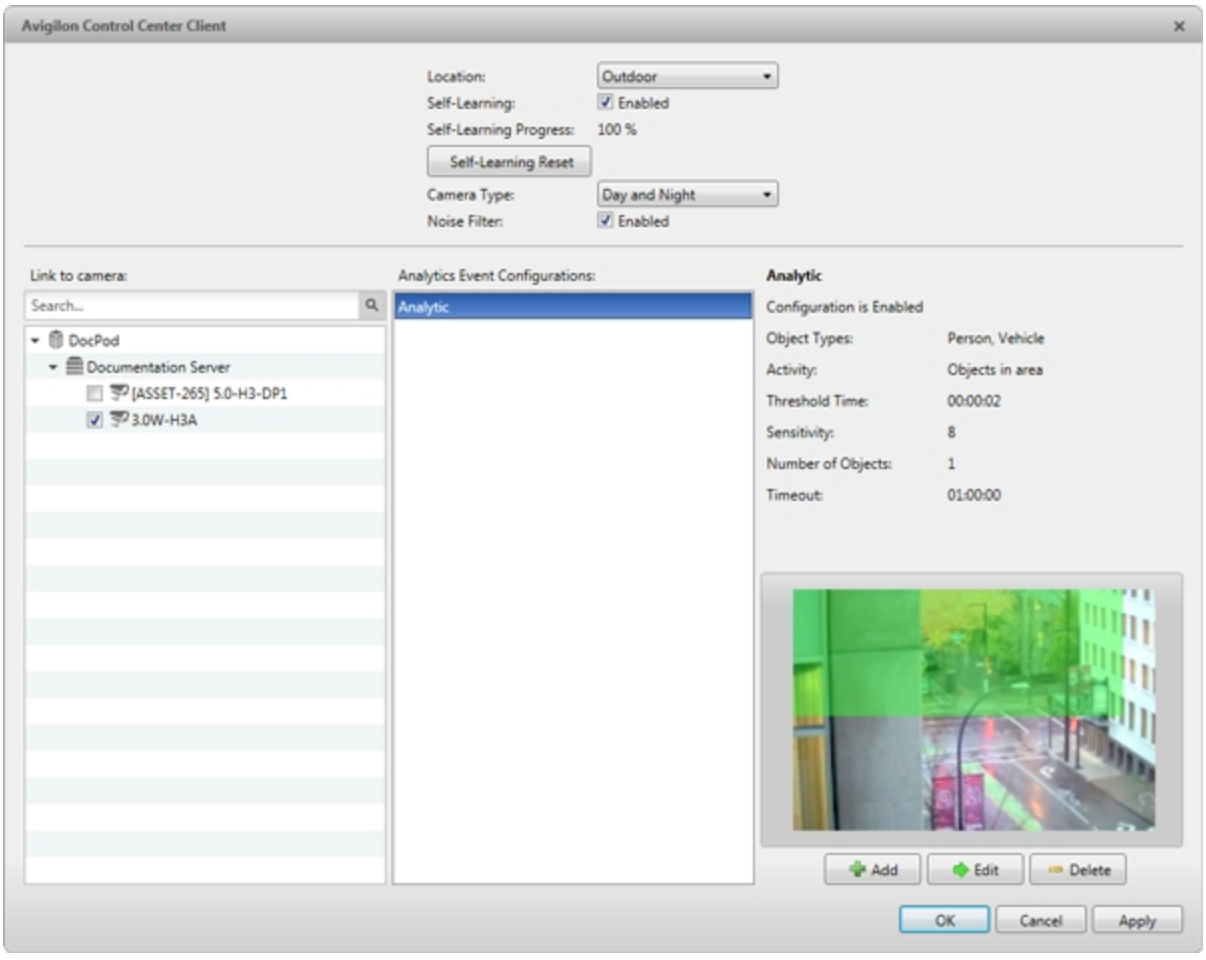


Figure 77: The Video Analytics Configuration dialog box

2. In the **Camera Type:** drop down list, choose one of the following options:
   - **Day and Night** - the video analytics appliance automatically detects if the video is in color or black and white.

- **Color** - the video analytics appliance is configured to analyze color video. It automatically detects if the video is daytime or nighttime.

  If the camera location is configured as Large Indoor Area or Indoor Overhead, the video analytics appliance is configured to analyze daytime video.

- **Black and White** - the video analytics appliance is configured to analyze black and white video.
- **FLIR** - the video analytics appliance is configured to analyze forward looking infrared (FLIR) video.

Using the Color Noise Filter

If the video analytics device is too sensitive and falsely detects motion as classified objects, enable the color noise filter. This is helpful for scenes with a lot of light and small, irrelevant motion, such as tree leaves on a sunny day.

- At the top of the Video Analytics Configuration dialog box, select the **Noise Filter:** check box. Make sure the check box is checked.

If the video analytics device is not sensitive enough and does not detect relevant classified objects, disable the color noise filter.

- At the top of the Video Analytics Configuration dialog box, select the **Noise Filter:** check box. Make sure the check box is unchecked.

Configuring Video Analytics Device Self-Learning

When self-learning is enabled, the video analytics device will perform initial self-calibration for the scene in its field of view. This can significantly improve classification accuracy of humans and vehicles.

NOTE: Enabling and disabling self-learning does not affect the Teach By Example feature.

Enabling Self-Learning

1. In the device Setup tab, click  .

   The Video Analytics Configuration dialog box opens.

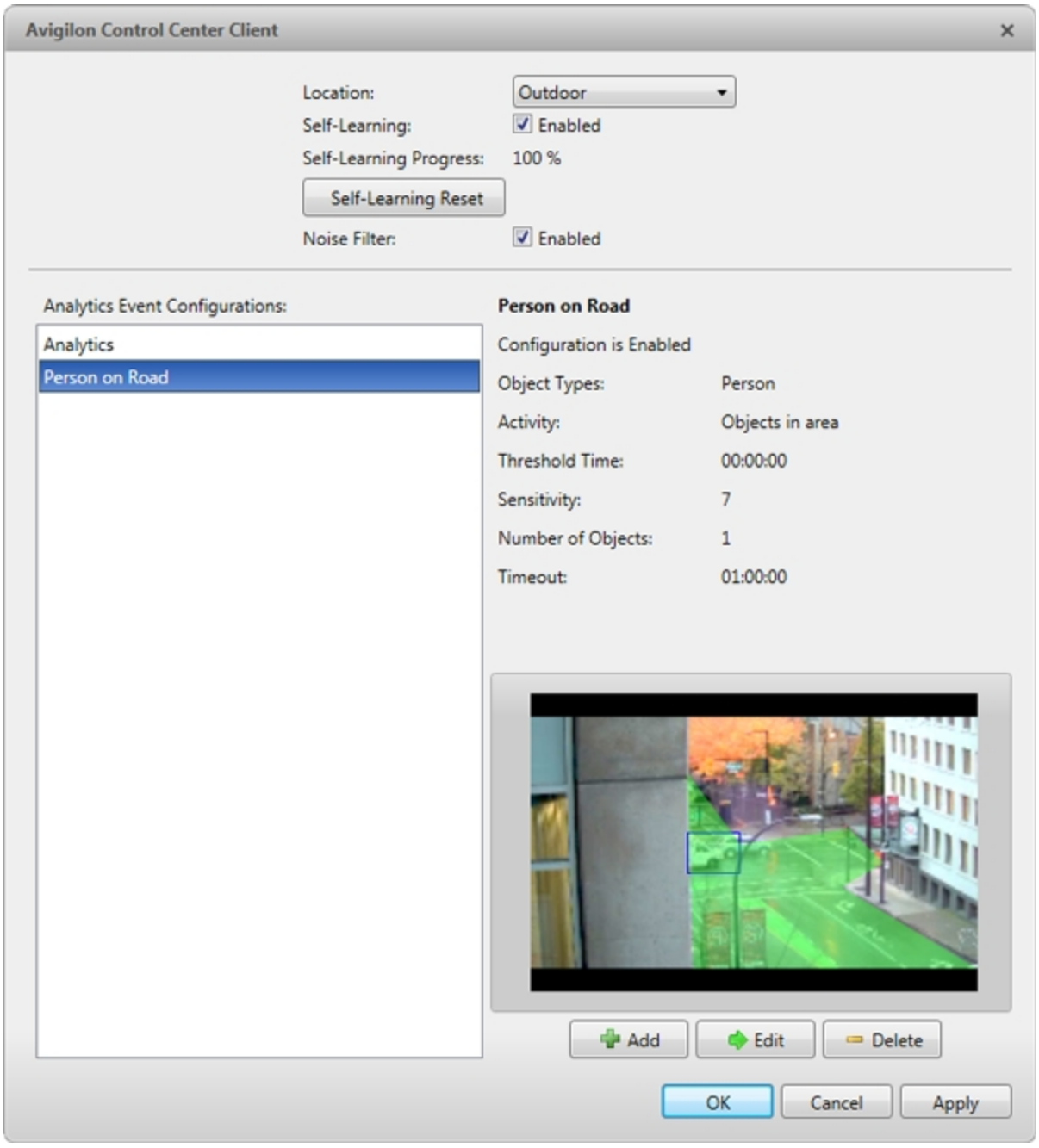


Figure 78: The Video Analytics Configuration dialog box

2. At the top of the dialog box, select the **Self-Learning:** check box. Make sure the check box is checked.

Self-Learning Progress

- **0% - 33%** - The device is in the initial learning stage where it begins to gather information on the scene.
- **34% - 66%** - The device is calibrating itself using the data it has gathered on the average person and average vehicle in the scene.
- **67% - 100%** - The device has established a high level of classified object detection accuracy based on its self-learning.

Tip: To further improve the detection accuracy of the device, use the Teach By Example feature. For more information, see **Teach By Example**.

NOTE: If after the device has reached a 100% Self-Learning Progress: level it has low classified object detection accuracy, an error may have occurred during installation. Contact Avigilon Technical Support.

Disabling Self-Learning

NOTE: Disabling self-learning may result in more classified objects being falsely detected.

You should disable self-learning in the following situations:

- If you do not expect any humans or vehicles in the device's field of view.
- If humans and vehicles in the field of view move at multiple height levels, such as people on a staircase.

1. In the device Setup tab, click  .

   The Video Analytics Configuration dialog box opens.

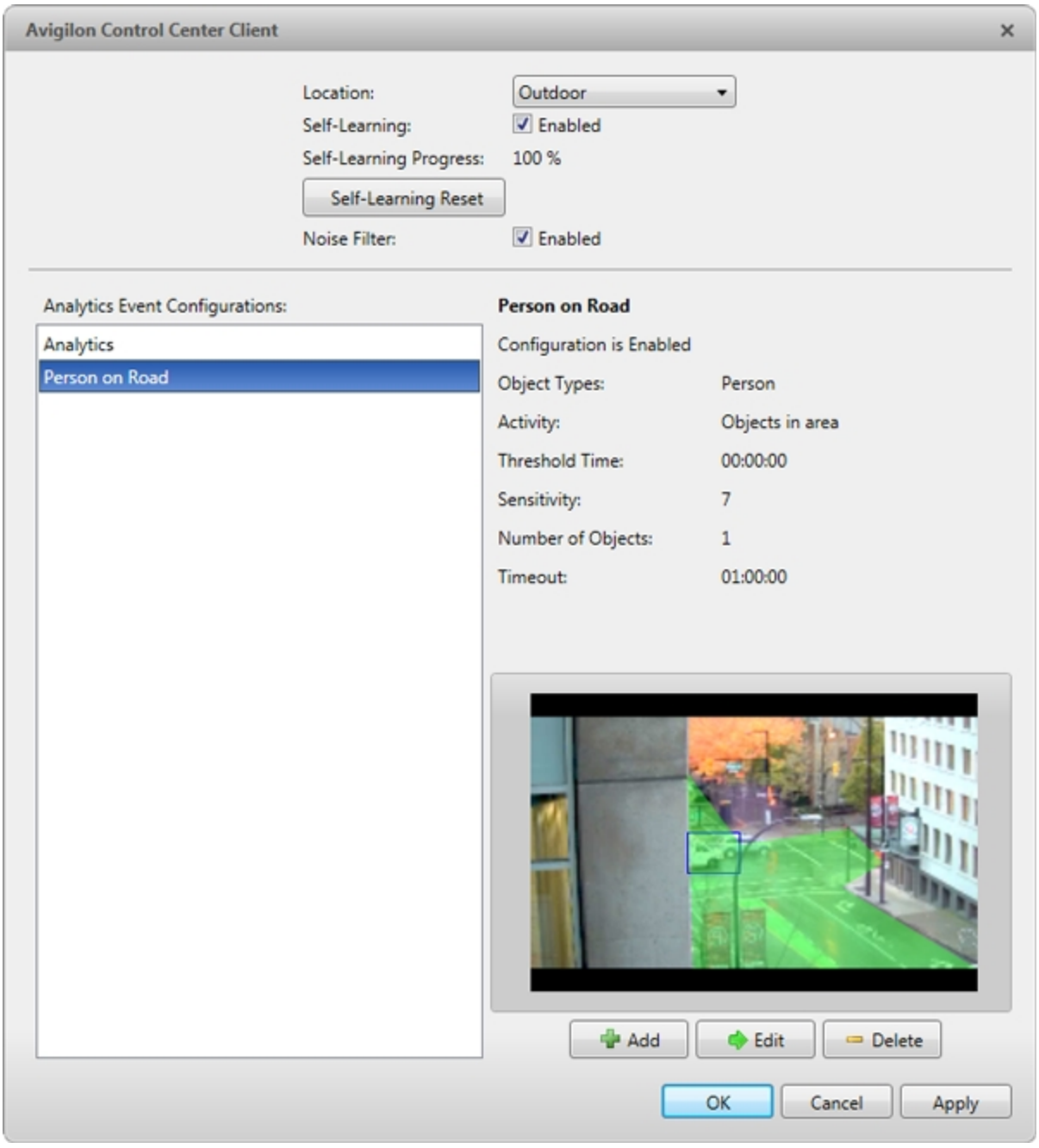


Figure 79: The Video Analytics Configuration dialog box

2. At the top of the dialog box, select the **Self-Learning:** check box. Make sure it is unchecked.

Resetting Self-Learning

When self-learning is reset, all previous self-learning data for the device is deleted.

You should reset self-learning when the field of view of the device is changed to ensure classified object detection accuracy.

1. In the device Setup tab, click  .

   The Video Analytics Configuration dialog box opens.

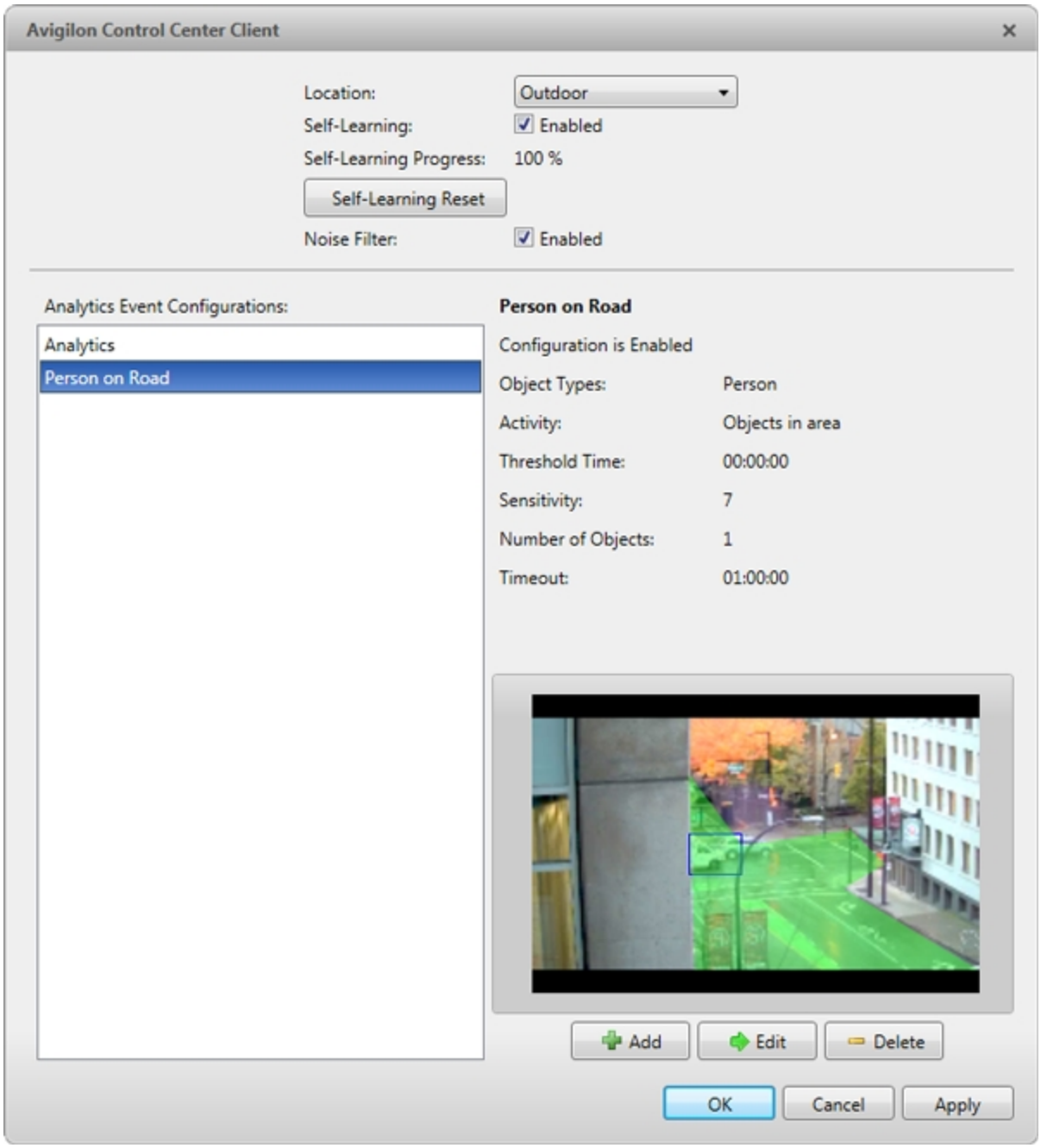


Figure 80: The Video Analytics Configuration dialog box

2. At the top of the dialog box, click **Self-Learning Reset**.
3. In the confirmation dialog box that appears, click **Yes**.

Resetting self-learning creates an event that appears in the Site Logs.

Setting Up Classified Object Motion Detection

The Avigilon™ adaptive video analytics devices use adaptive video analytics to intelligently detect relevant motion, such as a person or vehicle, while ignoring irrelevant movement, such as a moving tree. This allows you to receive events, trigger alarms and rules, and record video only when human or vehicle motion requires your attention.

1. In the device Setup tab, click  .

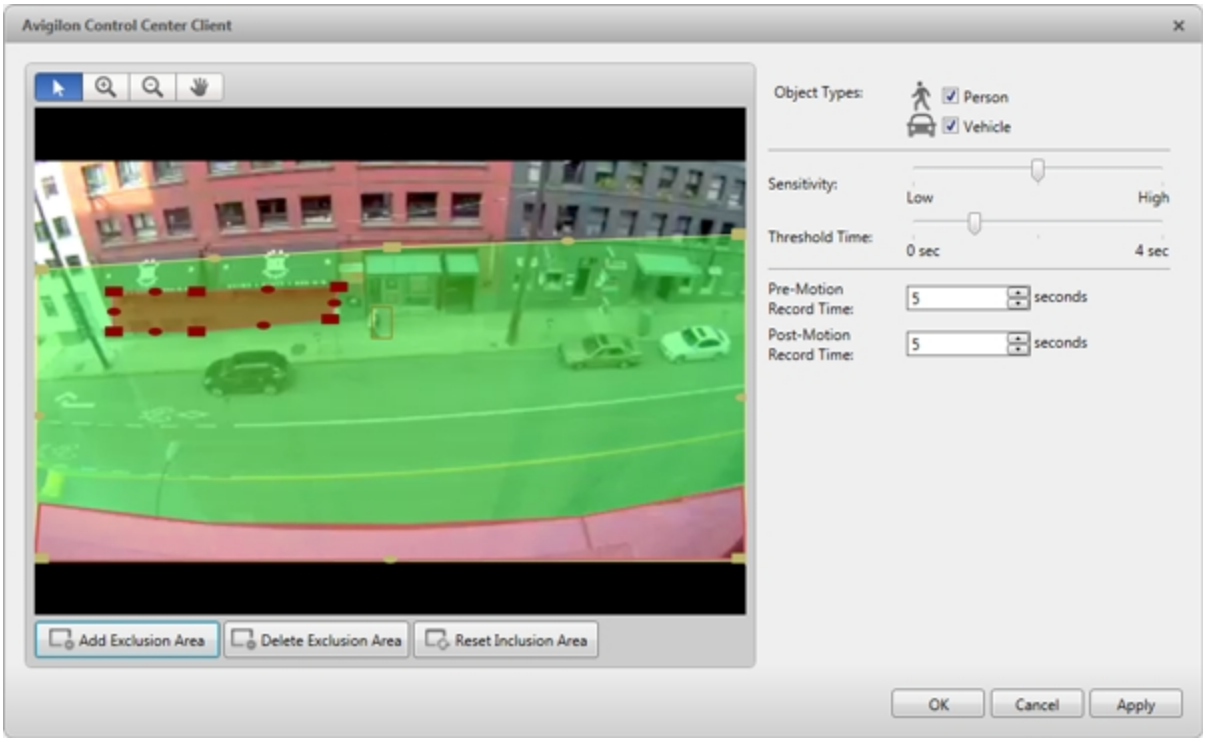


Figure 81: The Classified Object Motion Detection dialog box

2. To configure classified object motion detection, do the following:

Configuring Classified Object Motion Detection Settings

1. Select the **Person** and/or **Vehicle** check boxes to enable the detection of people and/or vehicles.
2. Move the **Sensitivity:** slider to adjust how sensitive the video analytics device is to the detection of classified objects.
3. Move the **Threshold Time:** slider to adjust how long an object must be moving before it triggers Classified Object Motion Detection.
4. In the **Pre-Motion Record Time:** and **Post-Motion Record Time:** fields, specify how long video is recorded before and after a classified object motion detection event.
5. Click **Apply** to save your settings.

Next, define the Classified Object Motion Detection area.

Selecting the Classified Object Motion Detection Area

By default, the camera's entire field of view is highlighted in green. You can set the camera's Classified Object Motion Detection area by changing the green overlay. Feet or wheels in the green overlay will trigger Classified Object Motion Detection. Classified object motion will not be detected in areas not highlighted in green.

1. Use the image panel tools to define the green overlay:
    - To change the shape or size of the green overlay, click and drag any of the yellow markers on the border. Extra markers are automatically added to help you fine tune the shape of the overlay.
    - To move the green overlay, place the cursor over the green overlay until the cursor changes into a hand or pan symbol. Then, click and drag the green area to the desired location.
    -  : Click this button to add an exclusion area. The exclusion area is added inside the green overlay.
        - Classified object motion in the exclusion area will not be detected. The exclusion area can be modified in the same way as the green overlay.
        - To set an exclusion area, move and resize the exclusion area as required then click anywhere on the green overlay.
        - To edit an exclusion area, double-click the exclusion area then modify as required.
    -  : Select an exclusion area then click this button to remove the exclusion area.
    -  : Click this button to restore the default green overlay.
2. Click **OK**.

Video Analytics Event Configuration

On each Avigilon™ adaptive video analytics device, you can set up specific video analytics events to detect a variety of human and vehicle activity within a scene.

Adding Video Analytics Events

Before you can add video analytics events to rules and alarms, they must first be created for each video analytics device.

1. In the device Setup tab, click  .

    The Video Analytics Configuration dialog box opens.

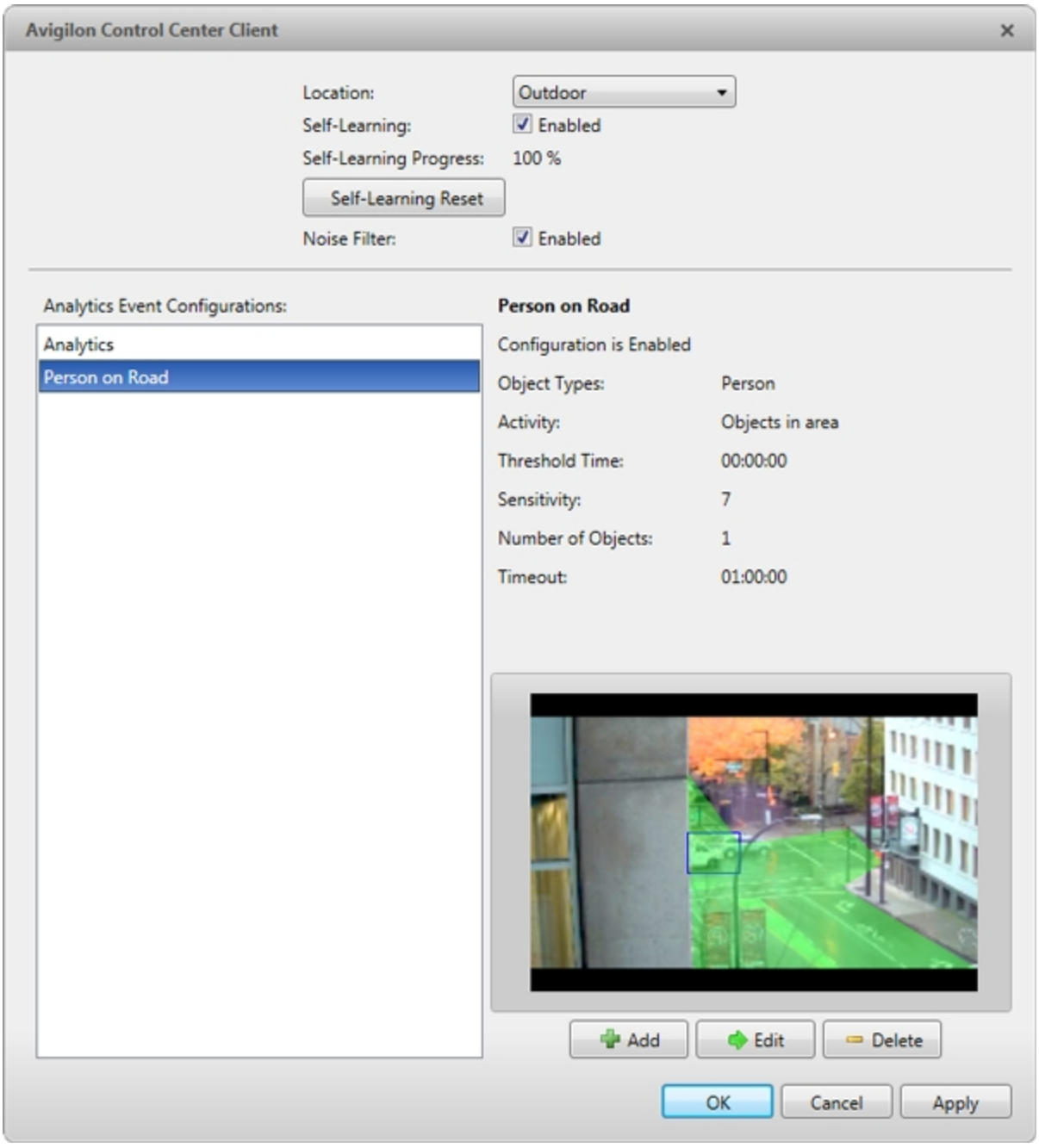


Figure 82: The Video Analytics Configuration dialog box

2. Click . The Add a Video Analytics Event dialog box opens.

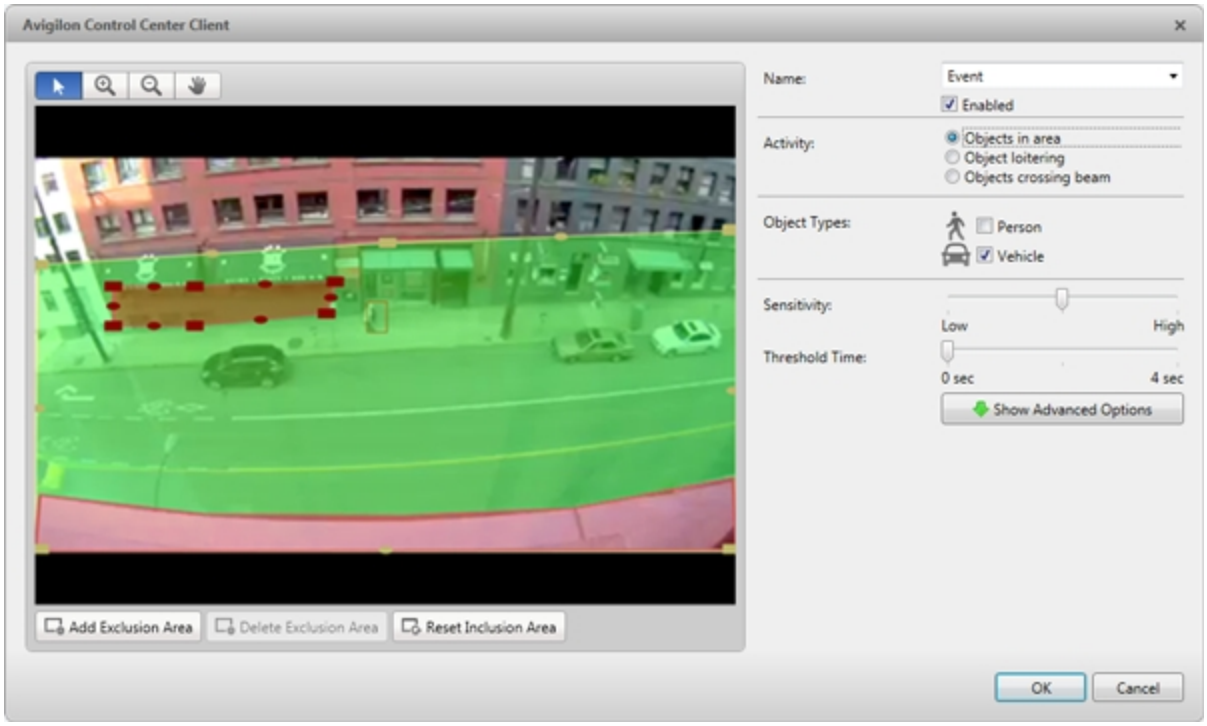


Figure 83: The Add a Video Analytics Event dialog box.

3. Enter a name for the video analytics event.
4. Select the **Enabled** check box. If the check box is clear, the video analytics event will not detect or trigger any events.
5. In the Activity: area, select one of the following options:
   - **Objects in area** – the video analytics event will only trigger when a selected object moves in the specified region of interest.

     In the image panel, define the region of interest. The green overlay can be configured like the Classified Object Motion Detection feature. For more information, see **Setting Up Classified Object Motion Detection**.
   - **Object loitering**– the video analytics event will only capture people or vehicles that stay within the region for an extended amount of time.

     In the image panel, define the specific area of interest. The green overlay can be configured like the Classified Object Motion Detection feature. For more information, see **Setting Up Classified Object Motion Detection**.
   - **Objects crossing beam** – the video analytics event will only trigger when people or vehicles cross the green beam in the pointed direction.

     In the image panel, move or resize the green beam as needed:

- To move the line, click and drag the green beam in any direction.
- To change the length or rotate the beam, click one end of the beam and stretch or rotate the beam.
- To change the direction of the beam, click  .
- To detect objects traveling in either direction of the beam, click  .

Depending on the selected video analytics activity, some of the following options may not be available.

6. To view more Activity: options, click  .For a description of each Activity: option, see **Video Analytics Event Descriptions**.
7. In the **Object Types:** area, select  and/or  .
8. Move the **Sensitivity:** slider to adjust how sensitive the video analytics device is to the detection of classified objects.
9. Move the **Threshold:** slider to adjust how long an object must be moving before it triggers a video analytics event.
10. In the **Number of Objects:** field, enter the minimum number of persons or vehicles that must be in the scene to trigger the video analytics event.
11. In the **Timeout:** field, enter the maximum length of a video analytics event. After this time, if the event is still active it will trigger a new event.
12. Click **OK**.

Editing and Deleting Video Analytics Events

1. In the device Setup tab, click  .
2. In the following dialog box, select a video analytics event from the Analytics Event Configurations: list and do one of the following:

   The dialog box may look different depending on the type of video analytics device.

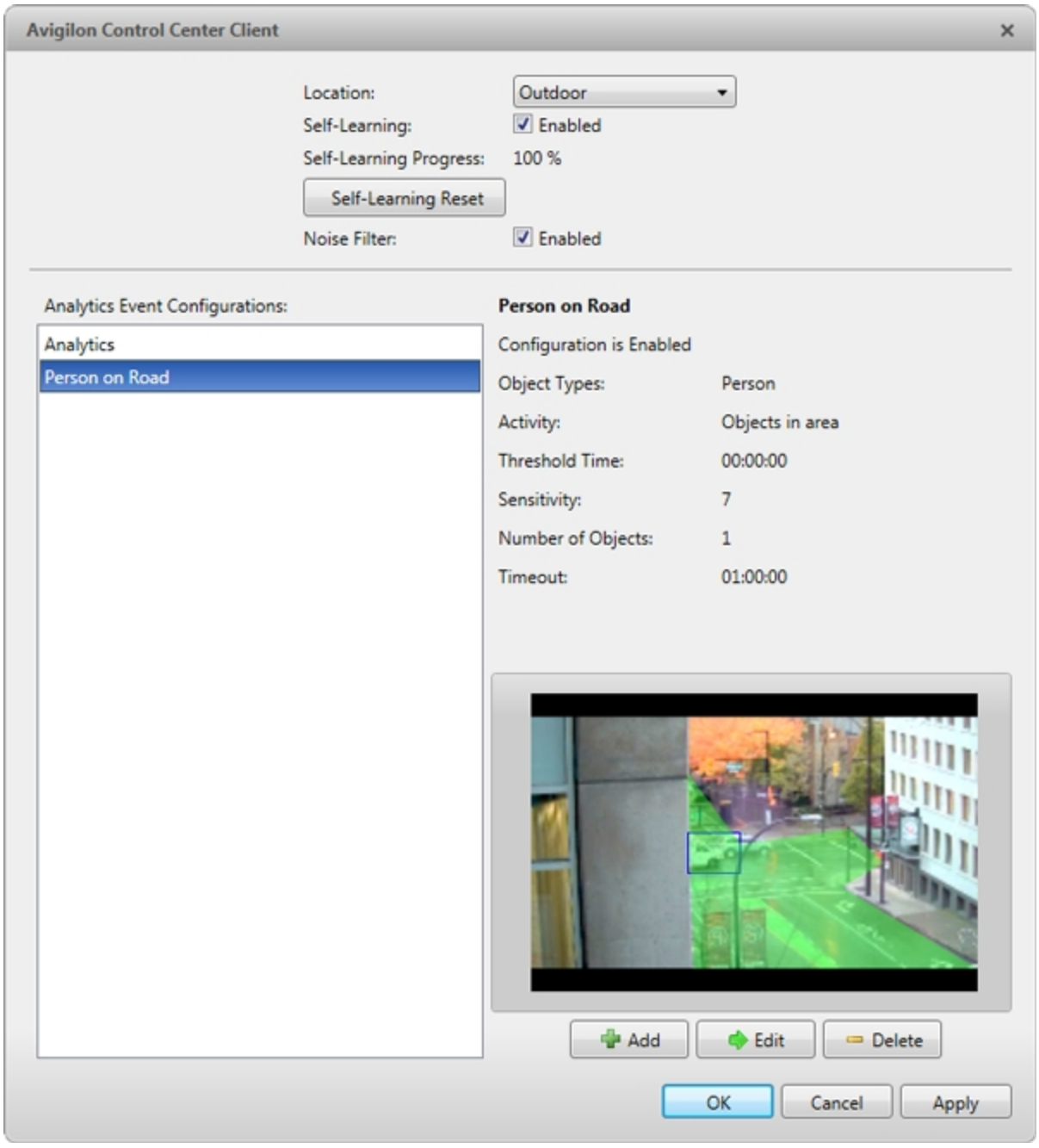


Figure 84: The Video Analytics Configuration dialog box for a video analytics camera.

- To edit the video analytics event, click . In the following dialog box, make the required changes. For more information, see **Adding Video Analytics Events**.

  NOTE: If you change the name of the event, any rules or alarms linked to the event may no longer function.

- To delete the video analytics event, click .

Teach By Example

You can improve the accuracy of classified object detection by using the Teach By Example feature. You can assign true or false Teach Markers to the objects detected by an Avigilon™ adaptive video analytics device, then apply the Teach Markers to train the video analytics engine of the Avigilon™ adaptive video analytics device.

NOTE: The Teach Markers are local to a single server and are created for individual cameras. They are not shared between servers or cameras.

Accessing the Teach By Example Tab

NOTE: To access the Teach By Example tab, a user must belong to a group with the Teach by example permission.

From the Teach By Example tab, you can assign and apply Teach Markers.

1. In the device Setup tab, click  .

   The Teach By Example tab opens.

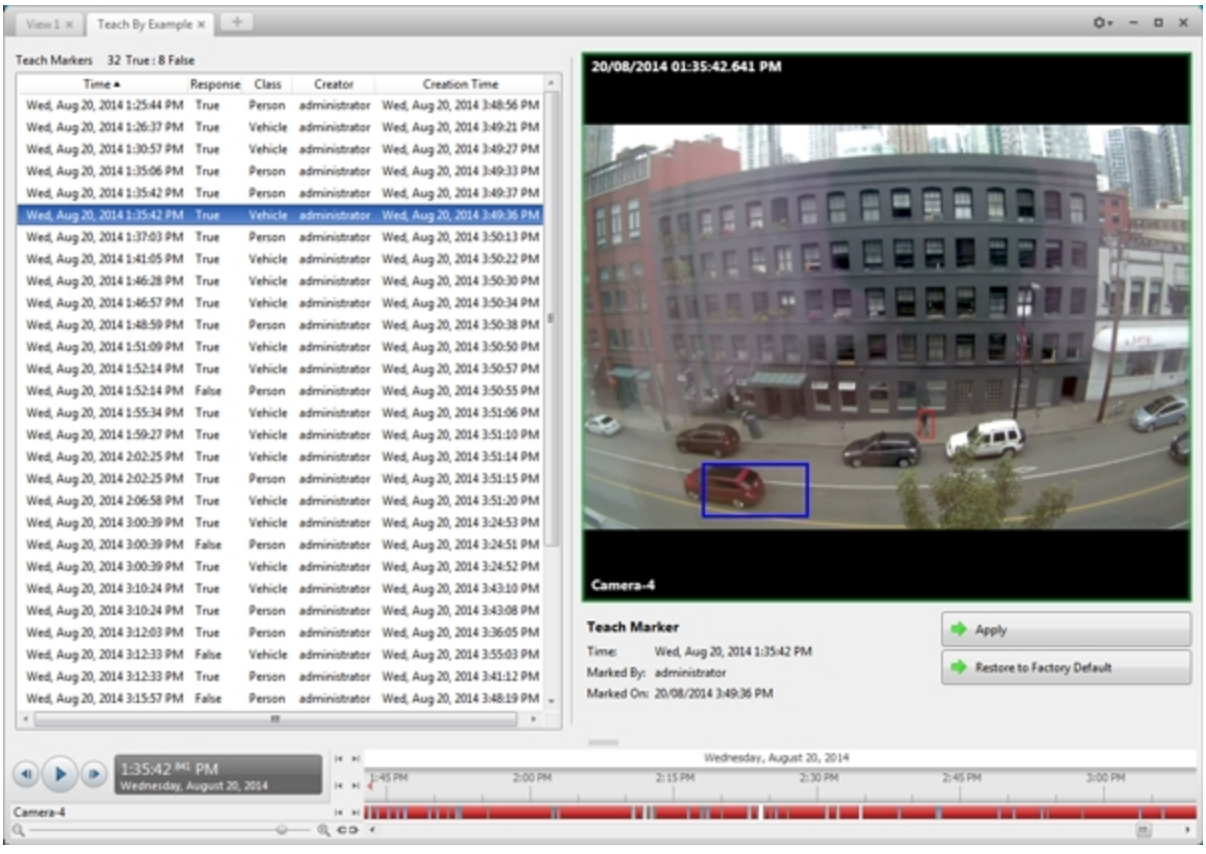


Figure 85: The Teach By Example tab

Assigning Teach Markers

In the Teach By Example tab, recorded video is shown in the image panel. Objects detected by the video analytics device are outlined in red bounding boxes (for humans) or blue bounding boxes (for vehicles).

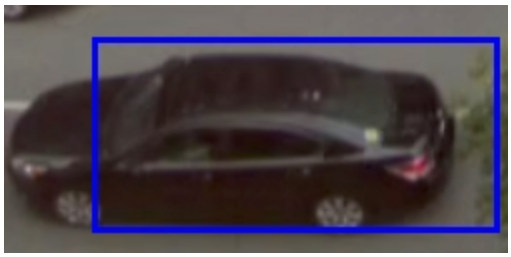


Figure 86: A detected classified object outlined in a blue bounding box.

1. Click inside a bounding box to open the object's Teach Markers menu.

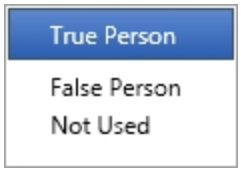


Figure 87: A Teach Markers menu

2. Select one of the following options:

   The options differ depending on whether the object has been classified as a vehicle or a person.

   - **True Person/True Vehicle** - Select this option if the video analytics device has correctly identified this object as a person or vehicle.
   - **False Person/False Vehicle** - Select this option if the video analytics device has incorrectly identified this object as a person or vehicle.
   - **Not Used** - Select this option if you do not want to use this object as a teaching sample.

   You can change Teach Markers at any time. The newest rating will override previous ones.

You can have a maximum of 50 true Teach Markers and 50 false Teach Markers per camera at a time. You need at least 30 true Teach Markers and 30 false Teach Markers per camera to teach a video analytics device.

The number of true and false Teach Markers already marked is displayed above the **Teach Markers** list.

Applying Teach Markers

NOTE: The user who assigns the Teach Markers can be different from the user who applies them to the video analytics device.

In the Teach By Example tab, you can apply Teach Markers to teach the video analytics device.

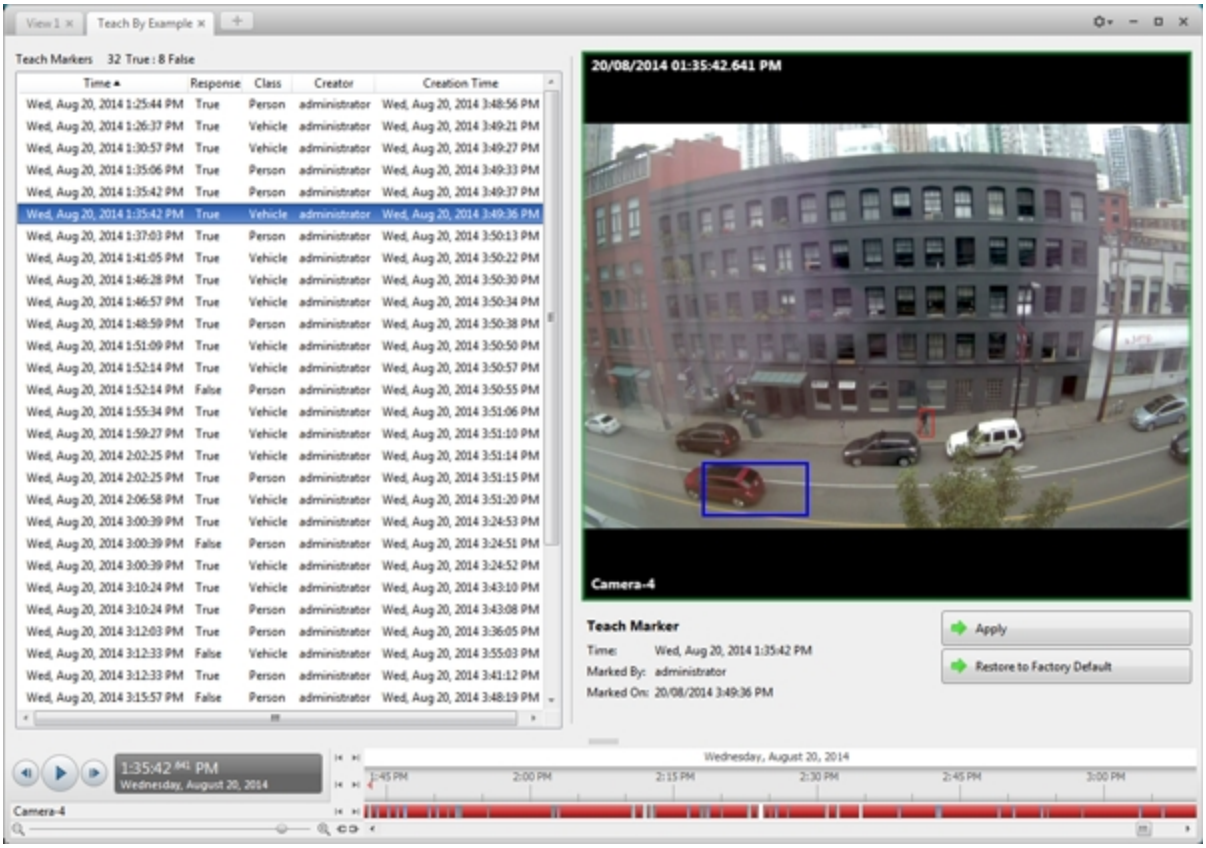


Figure 88: The Teach By Example tab

- Select a marker from the Teach Markers list to view it. The associated video is displayed in the image panel. The details are displayed below.

  You can sort the Teach Markers in ascending or descending order by **Time**, **Response**, **Class**, **Creator**, or **Creation Time** by clicking the column headings.

- To apply Teach Markers to a video analytics device, click **Apply**. The video analytics device will now use the listed markers to improve its classified object detection accuracy.

  NOTE: To apply Teach Markers, you need a minimum of 30 true Teach Markers and 30 false Teach Markers. If you do not have the minimum required, you will see an error message.

  When you apply Teach Markers, they are removed from the Teach Markers list.

- To reset the video analytics device's teach state click **Restore to Factory Default**. This will not delete any Teach Markers from the Teach Markers list, only clear the settings that were applied to the video analytics device.

Privacy Zones

You can set privacy zones in the camera's field of view to block out areas that you do not want to see or record, like bathroom entrances and other private areas.

Adding a Privacy Zone

NOTE: You can add up to 4 privacy zones per camera.

1. In the camera Setup tab, click  .
2. In the Privacy Zones dialog box, click  and a green box will appear on the image panel.

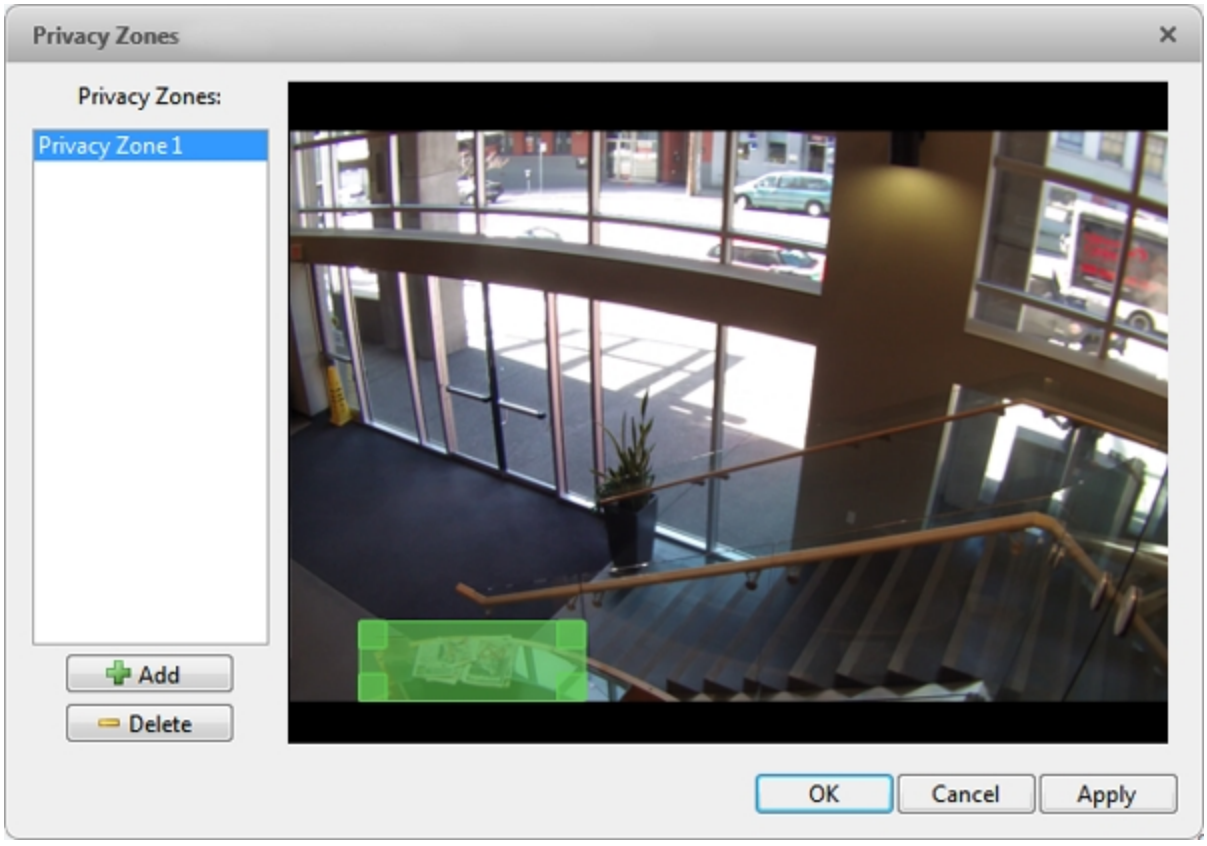


Figure 89: The Privacy Zones dialog box

3. Move and resize the green box until it covers the area you want to block out.
4. Click **OK**.

Editing and Deleting a Privacy Zone

1. In the camera Setup tab, click  .
2. In the Privacy Zones dialog box, select a privacy zone from the Privacy Zones: list and do one of the following:
   - To edit the privacy zone, adjust the green box in the image.
   - To delete the privacy zone, click .
3. Click **OK** to save your changes.

Manual Recording

When you trigger manual recording in an image panel, you are telling the camera to record video outside of its recording schedule. Manual recording continues until it is stopped, or until the maximum manual recording time is reached.

To set the maximum manual recording time, follow these steps:

1. In the camera Setup tab, click  .

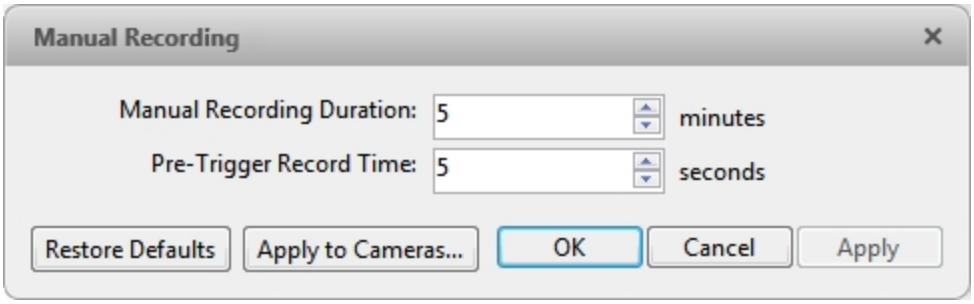


Figure 90: The Manual Recording dialog box

2. Specify the following:
   - **Manual Recording Duration:** enter how long the camera should record if recording is not manually stopped.
   - **Pre-Trigger Record Time:** enter the amount of time video is recorded before manual recording is activated.
3. Click **Apply to Cameras...** to apply the same settings to other cameras of the same model.
4. Click **OK**.

For more information on manually recording video, see **Triggering Manual Recording**.

Digital Inputs and Outputs

Use the Digital Inputs and Outputs dialog box to set up external digital input and output devices that are connected to the device (a camera or video analytics appliance).

The external devices can be used to create alarms or trigger recording events and specific actions through the Rules engine. For more information, see **Rules**.

Setting Up Digital Inputs

1. In the device Setup tab, click  .
2. In the **Digital Inputs:** area, select an input.

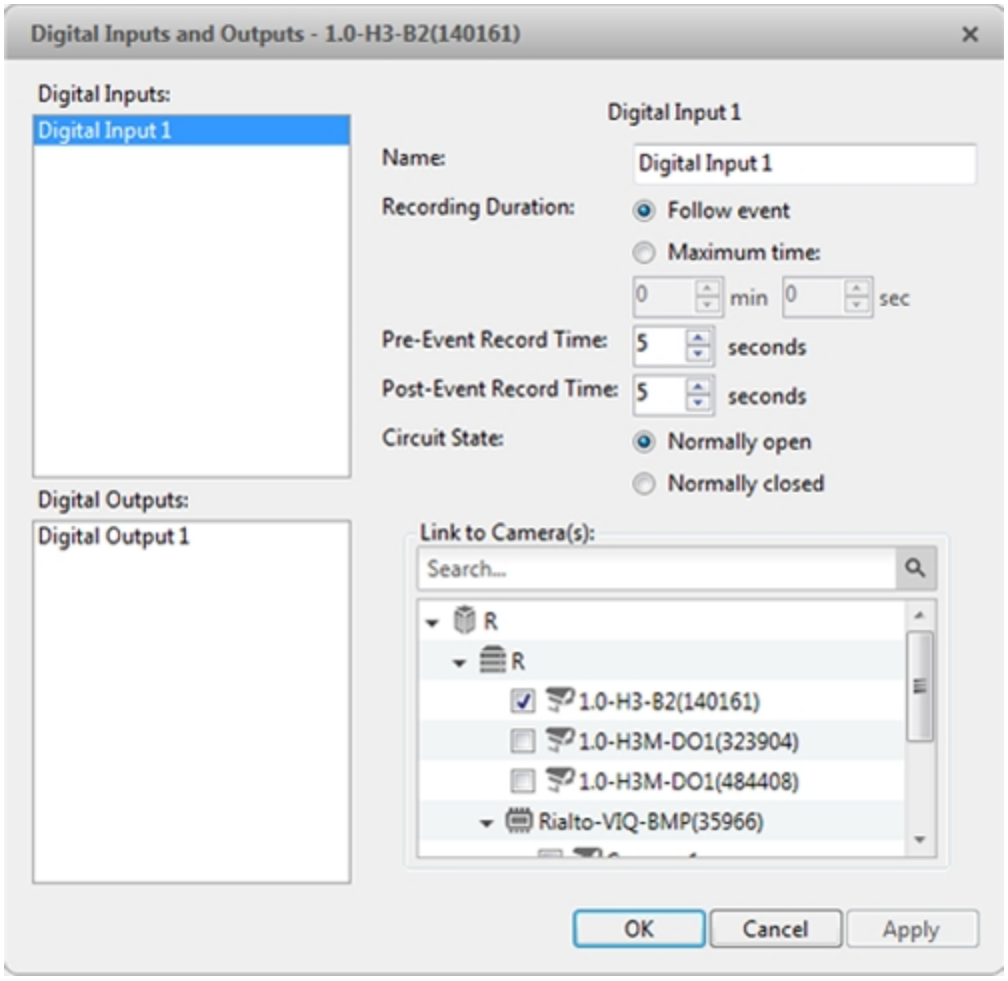


Figure 91: The Digital Inputs and Outputs dialog box

3. Enter a **Name:** for the digital input.
4. In the **Recording Duration:** area, select one of the following:
   - Select **Follow event** to record the entire digital input event.
   - Select **Maximum time:** to limit the recording time.
5. Enter the **Pre-Event Record Time:** and **Post-Event Record Time:**.
6. Select the digital input's default **Circuit State:**.
7. Select cameras to link to this digital input.

   If the Recording Schedule is configured to record digital inputs, the cameras selected in the **Link to**

Camera(s): area are used to record the events triggered by this digital input.

8. Click **OK**.

Setting Up Digital Outputs

Once a digital output is configured, you can manually trigger the digital output in an image panel. For more information, see **Triggering Digital Outputs**.

NOTE: The dialog box may appear differently depending on the device. Options that are not supported by the device will be disabled or hidden.

1. In the device Setup tab, click  .
2. In the **Digital Outputs:** area, select an output.

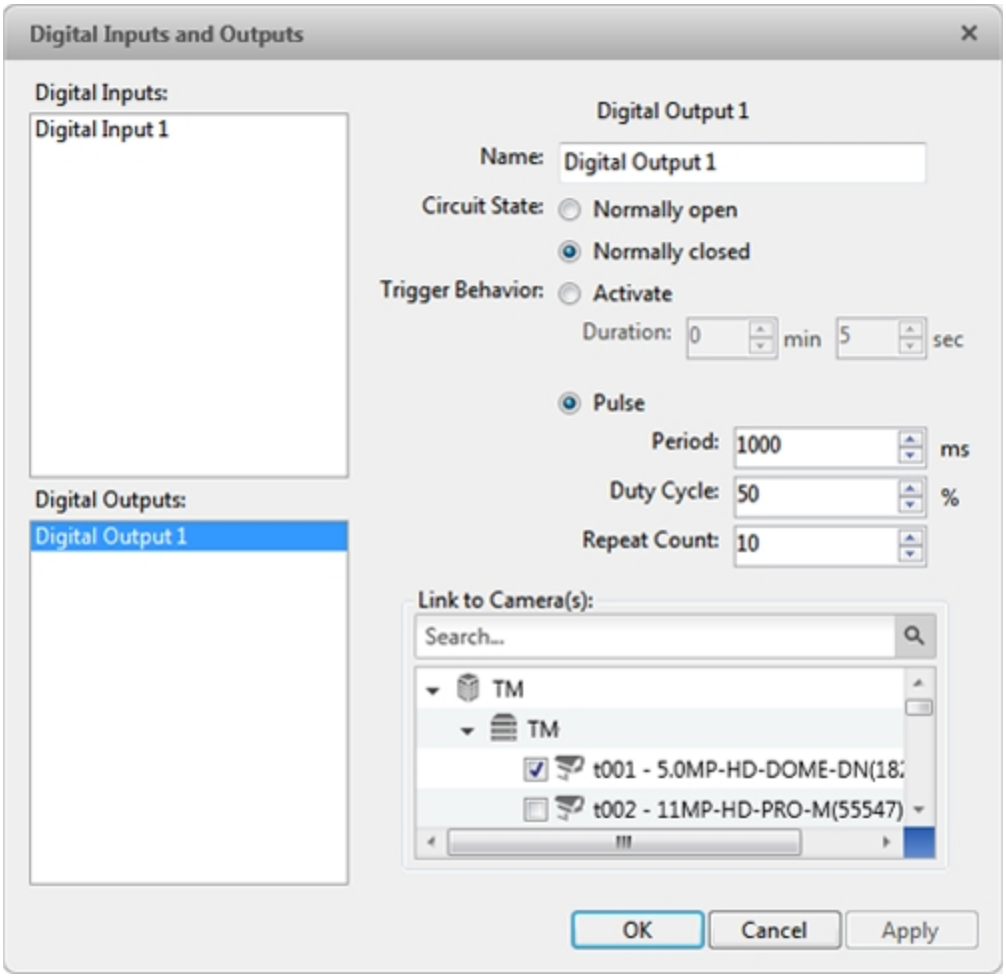


Figure 92: The Digital Inputs and Outputs box: Digital Output Settings

3. Enter a **Name:** for the digital output.
4. Select the digital output's default **Circuit State:**.

5. The **Trigger Behavior:** options define what occurs when the digital output is activated.
    - Select **Activate** to enable the digital output in continuous mode. The **Duration:** fields allow you to specify how long the digital output should be active for.
    - Select **Pulse** to enable the digital output in pulse mode. Specify the **Period:**, **Duty Cycle:**, and **Repeat Count:** for the pulse.
6. Alternatively, there may only be a **Trigger Duration:** field. Specify the trigger duration in minutes and seconds.
7. Select the cameras that should be linked to this digital output.

    When the digital output is triggered, all the cameras linked to this digital output will begin recording.
8. Click **OK**.

Microphone

Use the Microphone dialog box to change the settings for any audio input device that is connected to a camera or video analytics appliance. You can also link the audio to other cameras.

To use this feature, a microphone must be connected to the device.

NOTE: The dialog box may appear differently depending on the device. Options that are not supported by the device will be disabled or hidden.

1. In the device Setup tab, click  .

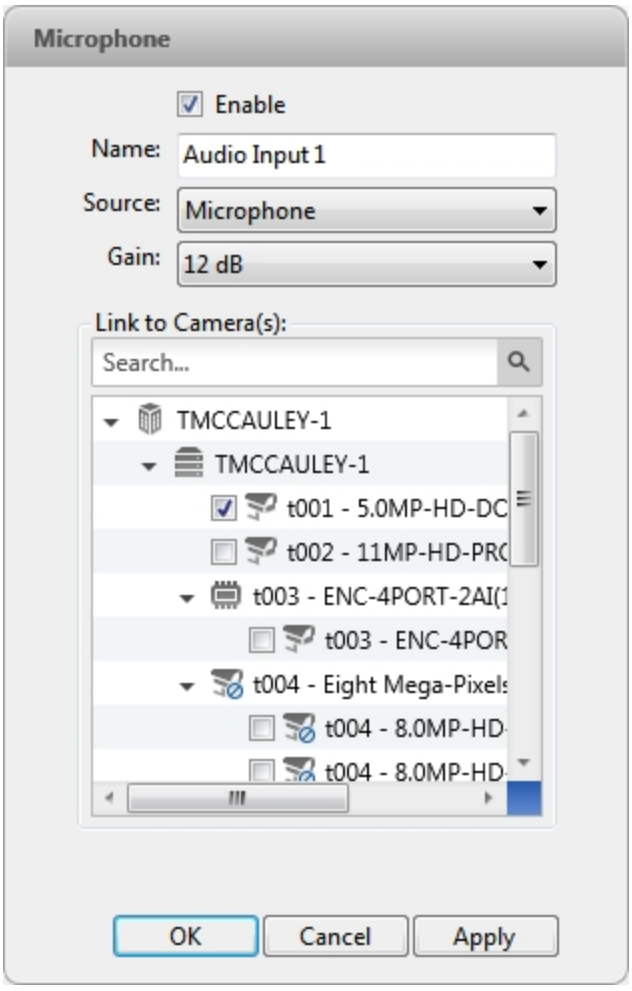


Figure 93: The Microphone dialog box

2. If multiple **Microphone Inputs:** are listed, select the one you want to edit.
3. Select the **Enable** check box to enable audio recording from microphones connected to the device.
4. Enter a name for the microphone.
5. In the **Source:** drop down list, select the audio input source.
6. In the **Gain:** drop down list, select the amount of analog gain that is applied to the audio input. The higher the dB setting, the louder the volume.
7. In the **Link to Camera(s):** area, select cameras to link to this audio.
8. Click **OK**.

Speaker

Use the Speaker dialog box to change the settings for any audio output that is connected to a device (a camera or video analytics appliance). You can also link the audio to other devices.

To use this feature, speakers must be connected to the device and a microphone must be connected to your local Client.

NOTE: The dialog box may appear differently depending on the device. Options that are not supported by the device will be disabled or hidden.

1. In the device Setup tab, click  .

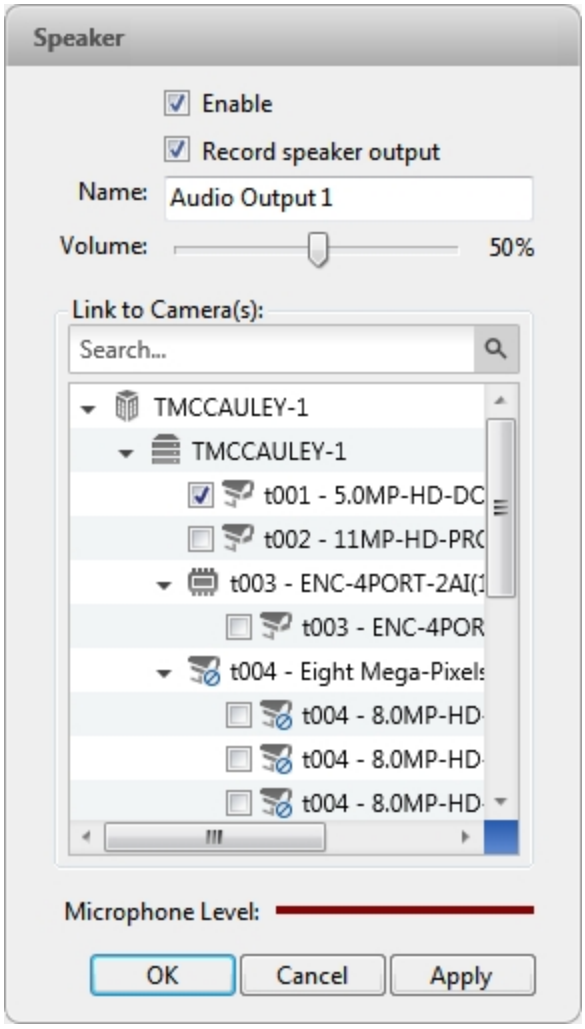


Figure 94: The Speaker dialog box

2. If multiple **Speaker Outputs:** are listed, select the one you want to edit.
3. Select the **Enable** check box to enable audio broadcasting. Speakers connected to the device will broadcast audio from the microphone that is connected to the local Client.
4. Select the **Record speaker output** check box to record what is broadcast.
5. Enter a name for the speaker.
6. The **Volume:** slider controls the volume of the speakers.
7. In the **Link to Camera(s):** area, select cameras to link to the speakers.
8. To test the **Microphone Level:**, speak into the microphone. The red bar will move to show the audio input

level.

9. Click **OK**.

If you want to enable two-way audio, see **General Settings** for the local Client.

Client Settings

The Client Settings... are used to set your preferences for your local copy of the Client software. This includes saving your password, setting the language, saving your last window layout, configuring your joystick, and manually adding and removing Sites.

General Settings

Use the General settings to set your local Client preferences. Any changes you make will only affect this copy of the Client software.

NOTE: Some features are not displayed if the server does not have the required license, or if you do not have the required user permissions.

1. In the top-right corner of the Client, select > **Client Settings...**.
2. In the General tab, make any required changes:

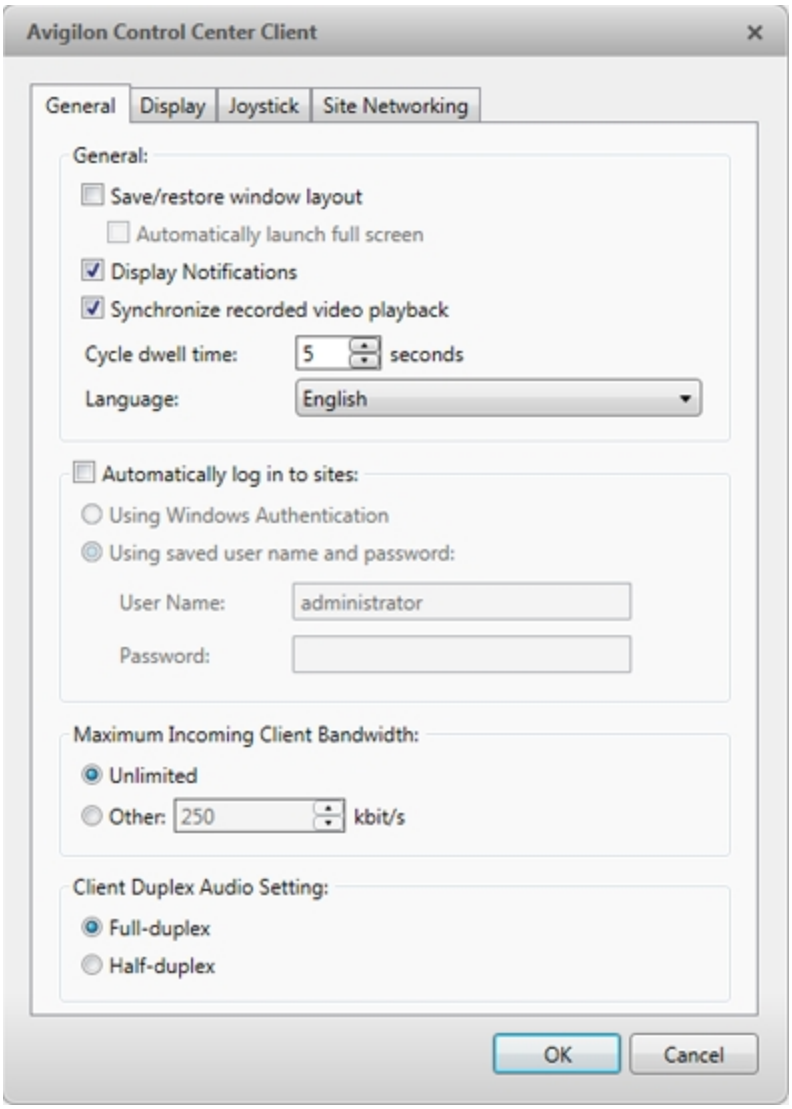


Figure 95: The Client Settings... dialog box

- **Save/restore window layout:** Select this check box if you want the Client to remember your layout preferences.
- **Automatically launch full screen:** Select this check box if you want the Client to automatically launch in full screen mode each time it starts.
- **Display Notifications:** Select this check box if you want the Client to display system messages. System messages are listed in the red box at the top-right corner of the Client - click the red box to see the messages. System messages notify you of Site events, system events and possible device connection issues.

  If this check box is cleared, all system messages are hidden.
- **Cycle dwell time:** Enter the number of seconds the Client waits before it cycles to a different View tab. For more information, see **Cycling Through Views**.

- **Language:** Select a language from the drop down list to change the Client language. Select **Windows Default** for the Client to use the same language as the operating system.
- **Automatically log in to sites:** Select this check box to automatically log in to all Sites you can access. Select the type of login you use:
  - Select **Using Windows Authentication** if you use your Windows login to access Sites.
  - Select **Using saved user name and password:** if you use your Avigilon Control Center username and password.
- In the **Maximum Incoming Client Bandwidth:** area, you can set how much bandwidth is received by the client. This includes video streaming.

  You can select **Unlimited** or **Other:**, and specify the maximum bandwidth allowance in kilobits per second (kbit/s).
- In the **Client Duplex Audio Setting:** area, decide if you want to enable two-way audio. This allows people in the video to talk with the operator monitoring the video.

  You have the option of **Full-duplex** audio, which allows simultaneous communication, or **Half-duplex**, which only allows communication from one side at a time. To use this feature, you need to set up microphones and speakers to cameras. For more information, see **Microphone** and **Speaker**.

3. Click **OK** to save your changes.

Joystick Settings

There are two types of joysticks supported by the Client: standard Microsoft DirectX USB joysticks and the Avigilon USB Professional Joystick Keyboard.

Access the Joystick settings to install the required drivers and configure your joystick options.

Configuring an Avigilon™ USB Professional Joystick Keyboard For Left-Hand Use

The Avigilon USB Professional Joystick Keyboard is a USB add-on that contains a joystick for controlling zooming and panning within image panels, a jog shuttle for controlling the Timeline, and a keypad programmed with the Client's keyboard commands. Refer to **Keyboard Commands** for the keypad commands that control the Client.

By default, the keyboard is installed in right-hand mode. Change the Joystick settings to configure it for left-hand mode.

1. Connect the keyboard.
2. In the top-right corner of the Client, select > **Client Settings...** > **Joystick**.

   If the keyboard is not automatically detected, an error message will appear. Click **Scan for Joysticks...**.

   Otherwise, the following option is displayed.

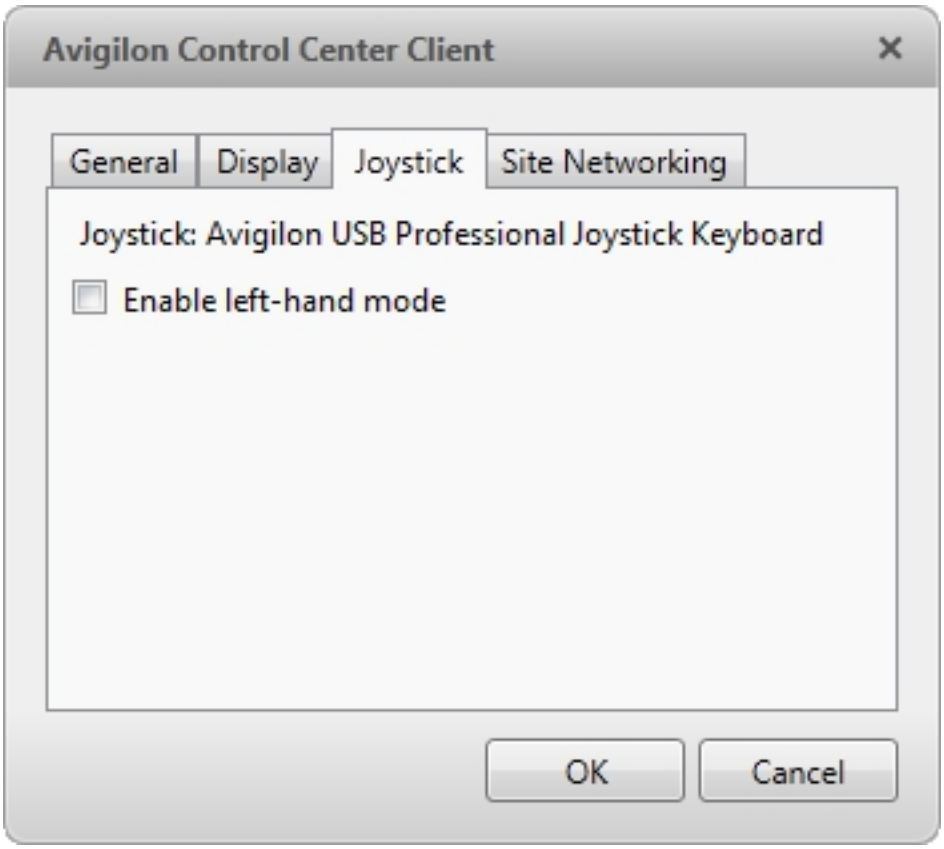


Figure 96: The Joystick dialog box

3. Select the **Enable left-hand mode** check box.
4. Click **OK**. The keyboard is now configured for left-hand mode.
5. Rotate the keyboard until the joystick is on the left and the jog shuttle is on the right. Reinstall the keypad cover with the View button labels at the top.

For more information about the Avigilon USB Professional Joystick Keyboard, see the installation guide included with the device.

Configuring a Standard USB Joystick

Use the Joystick settings to configure the buttons used in your standard Microsoft DirectX USB joystick.

1. Connect the joystick. In the top-right corner of the Client, select > **Client Settings** > **Joystick**.
2. If the joystick is not automatically detected, an error message will appear. Click **Scan for Joysticks...**.

   Otherwise, the following options are displayed:

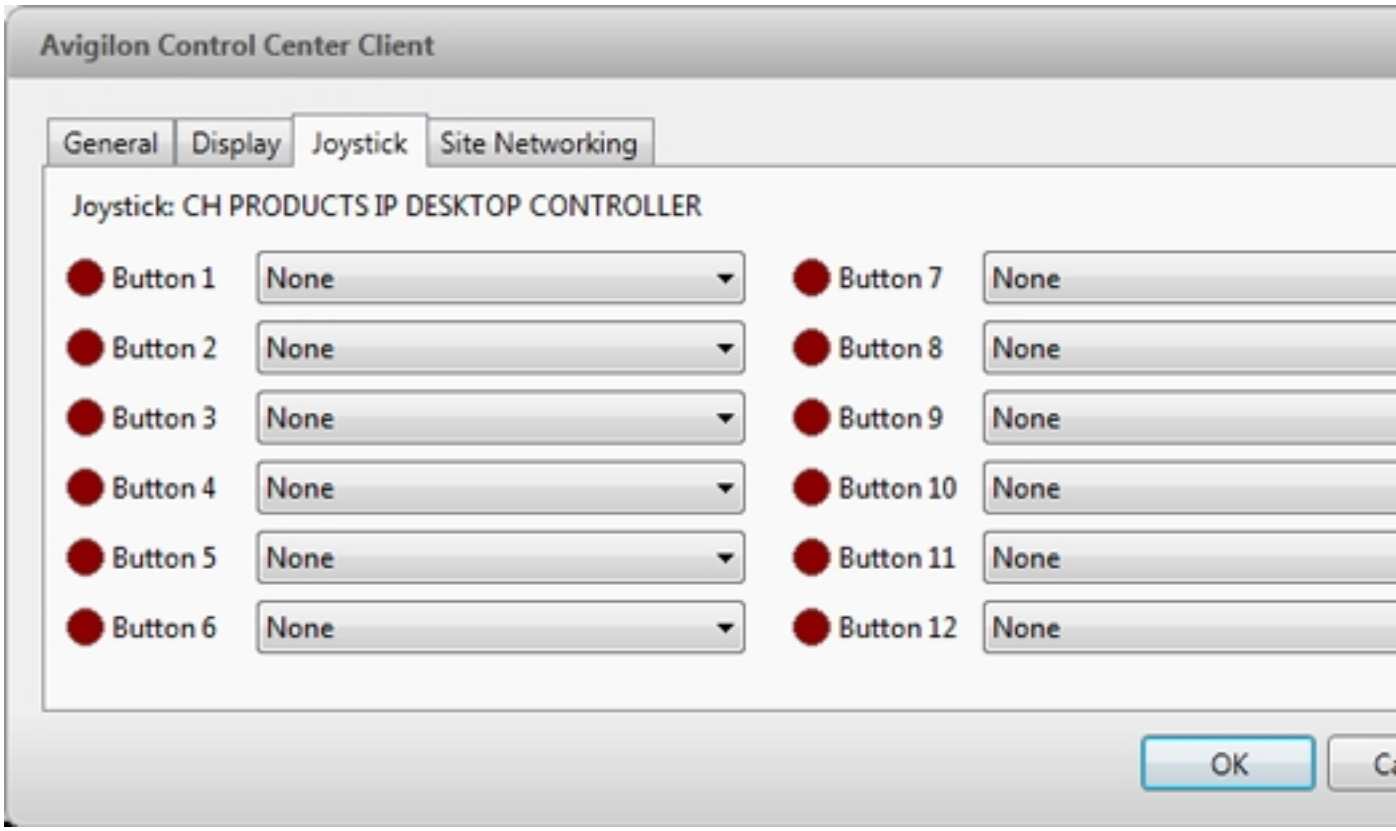


Figure 97: The Joystick dialog box

3. Choose an action for each button on the joystick:
    a. Press a button on the joystick to highlight its label in the dialog box.
    b. Select an action for the button from the drop down list.

        Options include ways to control recorded video, Views, image panels, instant replay, audio, snapshots and PTZ.

    c. Repeat this procedure for each button on the joystick.
4. Click **OK**.

Video Display Settings

You can adjust the Client Display settings to improve how video is displayed on your monitor.

NOTE: Some features are not displayed if the server does not have the required license, or if you do not have the required user permissions.

1. In the top-right corner of the Client, select ⚙ > **Client Settings...** > **Display**.

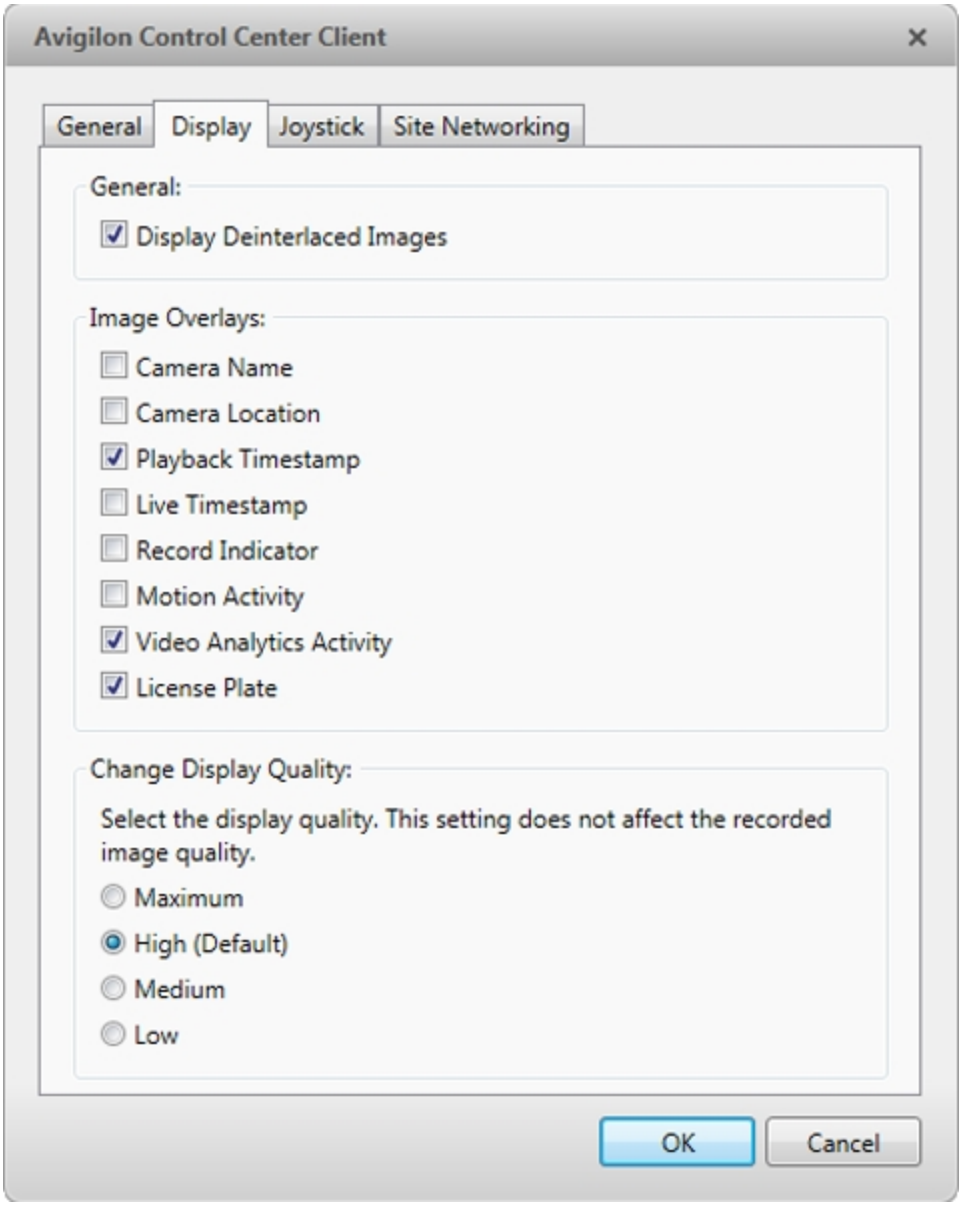


Figure 98: The Display Settings tab

2. Follow any of the following procedures to adjust how video is displayed in image panels.

Displaying Analog Video in Deinterlaced Mode

Select the **Display Deinterlaced Images** check box if the analog video you are watching is showing interfacing artifacts. This setting will help improve video image and smooth out some of the artifacts.

Displaying Image Overlays

Select any of the Image Overlays: options to set the type of information that is displayed over video.

Overlay	Description
Camera Name	Displays the name assigned to the camera.
Camera Location	Displays the location assigned to the camera.
Playback Timestamp	(Recorded video only) Displays the exposure timestamp for the video.
Live Timestamp	(Live video only) Displays the current system date and time to the millisecond.
Record Indicator	(Live video only) Displays the recording status of a camera. The recording status is indicated by the round icon on the top left corner of the image panel. The color of the icon shows the camera's recording status. •  : recording triggered by a motion event •  : recording •  : not recording. Click this icon at any time to begin manual recording.
Motion Activity	Highlights motion in red.
Video Analytics Activity	Bounding boxes outline objects detected in the video. The color of the bounding box identifies the object type: • Red - a person • Blue - a vehicle The Video Analytics Activity overlay is only activated for video from a video analytics device.
License Plate	(Live video only) Displays license plate numbers as they are detected. **NOTE:** This feature is only available if the *License Plate Recognition* feature is installed.

Changing Display Quality

If your computer does not have enough network bandwidth or processing power, you may not be able to watch video at its full image rate and quality. You can configure the image panels to display video in high quality and low frame rate, or low quality and high frame rate.

Select a higher display quality setting if you need to see specific details or faces in the scene. Select a lower display quality setting if it's more important to see moving events as they occur.

The Change Display Quality: settings only affect the image panel display and do not affect the actual video quality or image rate between the camera and the server. Therefore, you can review recorded footage later to confirm what you saw in the image panel.

In the Change Display Quality: area, select one of the following options:

- **Maximum:** displays video at full resolution with the lowest image rate.
- **High (Default):** displays video at 1/4 resolution.
- **Medium:** displays video at 1/16 resolution.
- **Low:** displays video at 1/64 resolution with the highest image rate.

What are Views?

A View tab is where you watch camera video. Inside the View tab is a set of image panels that allows you to organize how video is displayed.

You can arrange image panels into different layouts to take advantage of different camera angles and save View layouts that you like.

You can share Views with other users during investigations, and organize how video is displayed across multiple monitors.

For more information on controlling live and recorded video, see **Monitoring Video**.

Adding and Removing a View

View tabs allow you to customize how you monitor video. You can open a new View in the current window or open a View in a new window to make use of multiple monitors. Views can also be removed as required.

If you want to make use of a large number of monitors, like a video wall, see **Virtual Matrix**.

To...	Do this...
Open a new View tab	Click  >  .
Close a View tab	On the View tab, click  .
Open a new window	Select  > **New Window** A new window appears. You can now position this window to make use of multiple monitors.
Close a window	In the top-right corner of the window, click  . **NOTE:** If you see a confirmation dialog box, it is because there is only one window open and closing this window will also close the application.

View Layouts

You can organize how video is displayed through View layouts. You can choose to display video in 1 - 64 image panels. You can also customize the shape of image panels to accommodate cameras that are installed vertically to capture long hallways.

There are 10 pre-configured layouts that you can edit to fit your needs.

Selecting a Layout for a View

You can organize how video is displayed by selecting a View layout. The figure below shows the default View layouts.

- On the toolbar, select  , then select one of the following layout options.

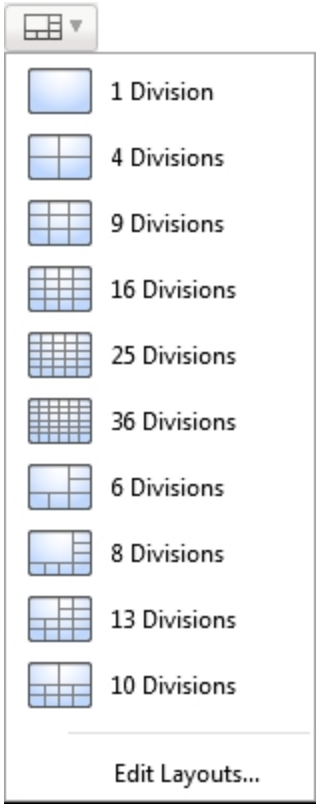


Figure 99: Layouts in the toolbar

Editing a View Layout

If the default View layouts do not fit your surveillance requirements, you can customize a View layout.

1. On the toolbar, select  > **Edit Layouts...**.

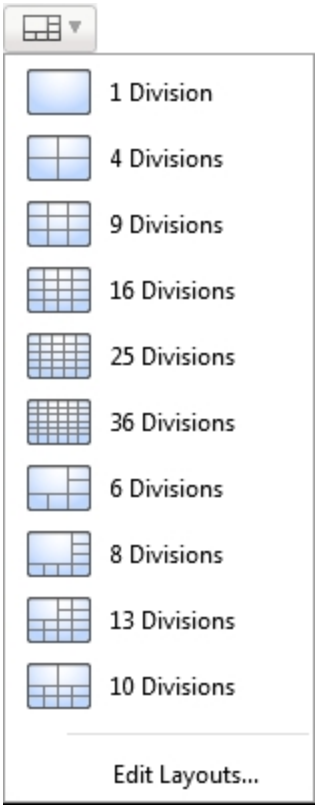


Figure 100: Layouts in the toolbar

2. In the Edit Layouts dialog box, select the layout you want to change.
3. Enter the number of **Columns:** and **Rows:** you want in your layout.

4. In the layout diagram, do any of the following to further customize the layout.

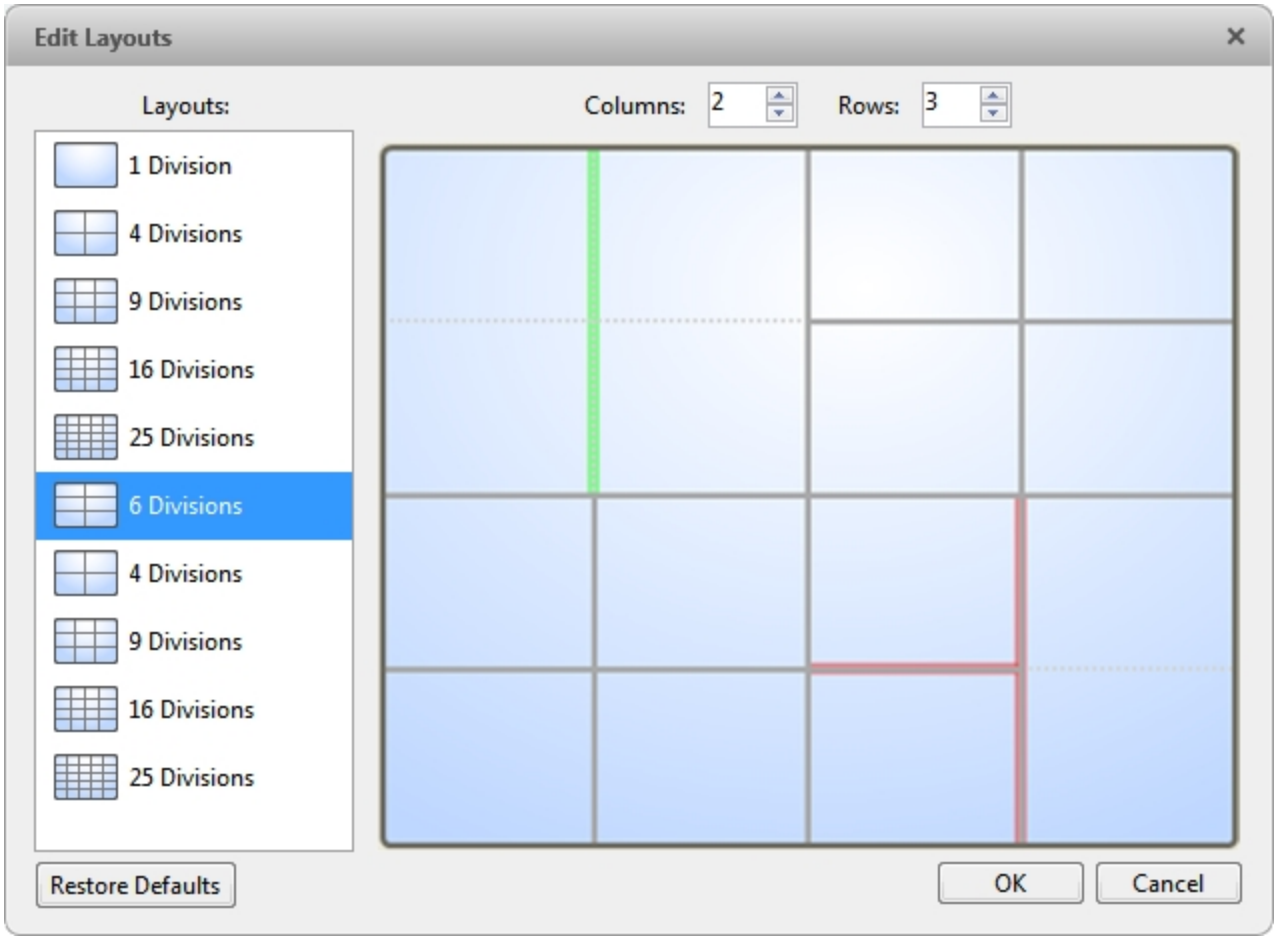


Figure 101: The Edit Layouts dialog box

- To create a larger image panel, select a gray line to delete the border between two image panels. When a line is highlighted in red, the line can be deleted.
- To restore an image panel, select a dotted line to divide a larger image panel into two. When a dotted line is highlighted in green, the line can be restored.
- To restore all default View layouts, click **Restore Defaults**. All custom layouts in the Layouts: list will be replaced.

NOTE: You can only add or subtract lines to create a rectangular shape.

5. Click **OK** to save your changes. The previous View layout has been replaced with your customized layout.

Tip: The keyboard commands used to access View layouts are linked to the layout's position in the Layouts: list. For example, if your custom layout is placed at the top of the Layouts: list (layout 1), you can press Alt + 1 to use that layout.

Making a View Full Screen

You can maximize a View to fill an entire monitor screen.

- On the toolbar, click  .

Ending Full Screen Mode

- While the View is in full screen mode, click  .

Cycling Through Views

If you have multiple Views open, you can cycle through the View tabs by displaying each one for a few seconds. This is useful when monitoring a large number of cameras.

- To activate the Cycle Views feature, click  .

To change the amount of time each View is displayed for, change the Cycle dwell time: setting. For more information, see **General Settings**.

Saved Views

Once you have set up a View you like, you can save the View to share with other users in the Site. A saved View remembers the current View layout, the cameras displayed in each image panel, and the image panel display settings.

Saving a View

1. In the toolbar, click  .
2. In the dialog box which appears, complete the following:

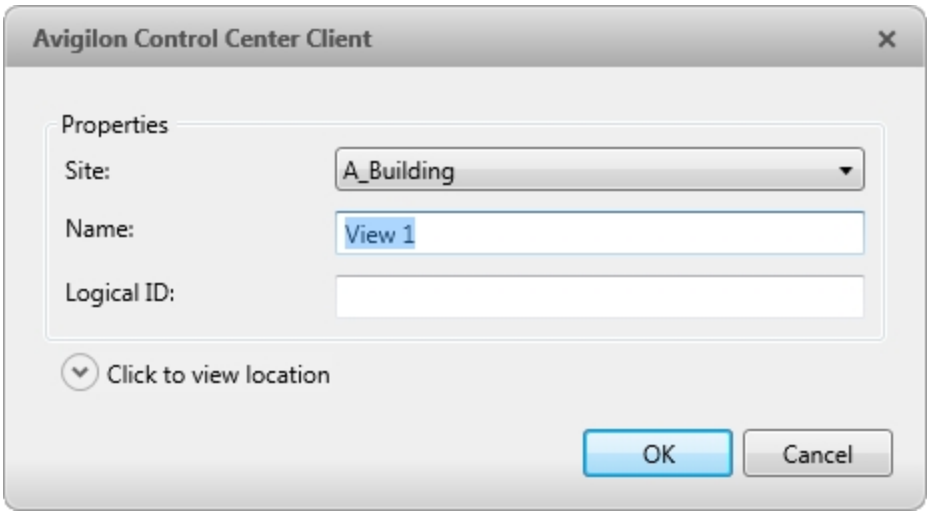


Figure 102: Edit View dialog box

a. Select the Site that the View should be added to.

b. Give the saved View a name.

c. Assign a **Logical ID:** to the View. The logical ID is a unique number that is used to open the saved View through keyboard commands.

d. Click  to choose where the saved View appears in the System Explorer.

- If your Site includes virtual sub-sites, select a location for the saved View. The list on the right updates to show what is stored in that directory.
- In the Site directory, drag the saved View up and down to set where it is displayed.

e. Click **OK**.

Your saved View is added to the System Explorer under the selected Site. You can now manage the saved View as a part of your Site.

Opening a Saved View

Do one of the following

- In the System Explorer, double-click the saved View.
- In the System Explorer, right-click the saved View and select **Open**.
- Drag the saved View from the System Explorer to the current View in the application or new window.

Editing a Saved View

1. Open a saved View.
2. Make any required changes to the View tab.
3. Click  .

Renaming a Saved View

1. In the System Explorer, right-click the saved View and select **Edit...**.
2. In the Edit View dialog box, enter a new name or logical ID and click **OK**.

Deleting a Saved View

1. In the System Explorer, right-click the saved View and select **Delete**.
2. In the confirmation dialog box, click **Yes**.

Collaborating

If you want to show another user an incident or need help investigating an event, you can share your current View with another user. You will both be able to control the View and show each other your findings.

Sharing a View

1. In the toolbar, click  .
2. In the following dialog box, select the user you want to collaborate with, then click **OK**.

   The users are listed by username and computer name. The computer name is used to help you identify a specific user if the username is shared by several people. Only users who are currently logged in to the Site are displayed.

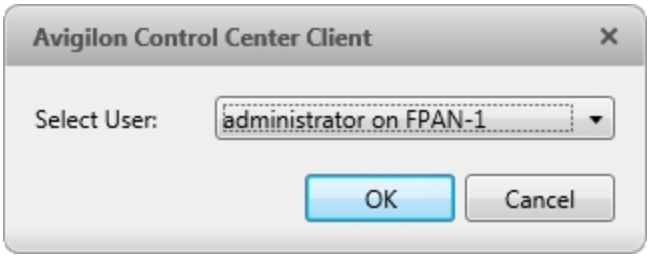


Figure 103: The Select User: dialog box

   a. The user you select will see a pop-up message with your invitation to collaborate and may choose to accept or decline.

   b. You will receive a pop-up message with the user's response to your invitation.

      If they say *Yes*, the View you are looking at is automatically opened as a new tab in your collaborator's window.

3. Repeat this procedure to collaborate with multiple users.

While you are collaborating, any changes made to the current View by a collaborator are shared with the other collaborators. Anything that you can do in a standard View can be done in a shared View.

Leaving a Shared View

- To leave a shared View, just close the View tab. The remaining users stay in collaboration mode.

Virtual Matrix

The optional Virtual Matrix feature allows you to control the View displayed on multiple monitors, or a video wall, from any instance of the application. To use this feature, the Virtual Matrix software must be installed on the system that all the displays are connected to.

A copy of the Virtual Matrix software can be downloaded from the Avigilon website.

For more information about the Virtual Matrix software, see *The Avigilon Control Center Virtual Matrix User Guide*.

Once the Virtual Matrix has been installed and loaded, the monitors connected to the system are automatically added to a Site. All monitors linked by the Virtual Matrix software are displayed in the System Explorer as  followed by the monitor name.

Adding and Removing Virtual Matrix Monitors

You can only add or remove Virtual Matrix monitors through the Virtual Matrix software.

For more information, see the *Avigilon Control Center Virtual Matrix User Guide*.

Controlling Virtual Matrix Monitors

In the System Explorer, each  represents a View that is displayed on a connected Virtual Matrix monitor.

To control what is displayed on each Virtual Matrix monitor, you need to open the monitor:

- In the System Explorer, right-click  and select **Open**.
- Double-click or drag  from the System Explorer to the current View.

The Virtual Matrix monitor is opened in a new tab and can be controlled like any View -- you can change the View layout, control video display, and use any active PTZ controls. The changes you make should automatically appear on the Virtual Matrix monitor.

When you are done, you can close the Virtual Matrix monitor tab. The monitor will continue to display the View you have configured until you make new changes or the Virtual Matrix is shut down.

Monitoring Video

Inside a View tab, you can monitor and control video from multiple cameras. Once you open a camera in a View tab, you can control the camera's live and recorded video stream. You also have access to the camera's PTZ controls, connected audio devices, digital outputs, and other playback settings.

To organize how video is displayed in the View tab, see **What are Views?**.

NOTE: Some features are not displayed if the server does not have the required license, or if you do not have the required user permissions.

Zooming and Panning in a Video

Use the zoom and pan tools to focus on specific areas in the live or recorded video stream.

Using the Zoom Tools

There are two ways to digitally zoom in and zoom out of a video image:

- Move your mouse over the video image, then rotate your mouse wheel forward and backward.
- On the toolbar, select  or  , then click the image panel until you reach the desired zoom depth.

Using the Pan Tools

There are two ways to pan through the video image:

- Right-click and drag inside an image panel
- On the toolbar, select  , then click and drag the video image in any direction inside the image panel.

Maximizing and Restoring an Image Panel

You can maximize an image panel to enlarge the video display.

Maximizing an Image Panel

Do one of the following:

- Right-click an image panel and select **Maximize**.
- Inside the image panel, click  .
- Double-click the image panel.

Restoring an Image Panel

In a maximized image panel, do one of the following:

- Right-click the maximized image panel and select **Restore Down**.
- Inside the image panel, click .
- Double-click the image panel.

Making Image Panel Display Adjustments

You can change the image panel display settings to bring out video details that are hard to see with the image panel's default settings.

1. Right-click an image panel and select **Display Adjustments...**.

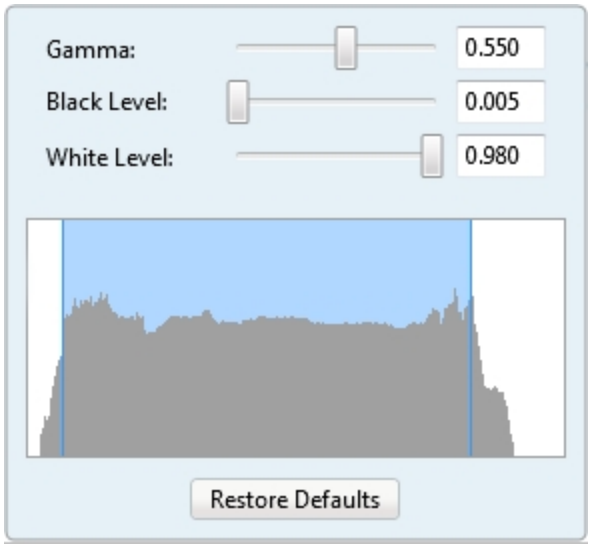


Figure 104: The Display Adjustments... panel

   The Display Adjustments... settings are displayed in a floating pane immediately beside the image panel.

2. Move the sliders to adjust the **Gamma:**, **Black Level:** and **White Level:**.

   The image panel displays a preview of your changes.

3. Click **Restore Defaults** to clear your changes.

Listening to Audio in a View

If there is an audio input device linked to a camera, the button is displayed in the image panel when you watch the camera's video. To listen to the streaming audio, make sure there are speakers connected to your computer. By default the audio is muted.

The camera's microphone must be enabled before you can listen to any audio. The button is not displayed if the microphone is disabled.

To control audio playback, do any of the following:

- In the lower-right corner of the image panel, click  to mute or activate the audio.
- Move the slider to change the volume.

To enable the camera's microphone, see **Microphone** for more information.

Triggering Custom Keyboard Commands

If your system has custom keyboard commands set up to run specific rule events, you can activate the keyboard commands by doing the following:

1. Press **Ctrl** + **K** on your keyboard.
2. Enter the custom keyboard command number to begin running the rule event.

Consult your system administrator for details about the custom keyboard commands that are available in your system. Custom keyboard commands are set up as rule events through the Rules engine. For more information about setting up rule events, see **Rules**.

Controlling Live Video

In this section are features that are only available while monitoring live video.

Broadcasting Audio in a View

If there are speakers linked to a camera, the  button is displayed in the image panel when you watch the camera's video. The  button allows you to broadcast your verbal response to what is occurring in the video, like a Public Address (P.A.) system.

The camera's speakers must be enabled before you can broadcast any audio. The  button is not displayed if the speakers are disabled.

- To broadcast audio, hold  and speak into your microphone. The red bar moves to show the microphone's audio input levels. If the level is low, speak louder or adjust the microphone volume in the Windows Control Panel.
- Release the button to stop the broadcast.

To set up two-way audio, see **General Settings**.

To enable the camera's speakers, see **Speaker** for more information.

Using Instant Replay

To review an event that just occurred, you can immediately access recently recorded video through the instant replay feature.

- Right-click the image panel and select one of the instant replay options:
  - **Replay - 30 Seconds**
  - **Replay - 60 Seconds**
  - **Replay - 90 Seconds**

The image panel immediately plays back the camera's most recently recorded video.

PTZ Cameras

PTZ cameras can be controlled through the image panel on-screen controls or by using the tools in the PTZ Controls pane.

Some tools and features may not be displayed if they are not supported by your camera.

Controlling PTZ Cameras

Pan, Tilt, Zoom (PTZ) controls allow you to control cameras with PTZ features. You can control a PTZ camera by using the on-screen controls or by using the tools in the PTZ Controls pane.

For other ways to use the PTZ Controls, see **Keyboard Commands**.

NOTE: For video analytics devices, classified object detection only works when the camera is in its Home position.

1. In the toolbar, click . PTZ controls are now enabled in image panels that are displaying PTZ video.
2. In the image panel, click .

   The PTZ Controls are displayed in a floating pane immediately beside the image panel.

   NOTE: The controls may appear differently depending on the camera. Some options are disabled or hidden if they are not supported by the camera.

Figure 105: The PTZ Controls

3. To pan or tilt, do one of the following:
   - In the image panel, drag your mouse from the center to move the camera in that direction. The farther the cursor is from the center of the image panel, the faster the camera will move.

- If the camera supports Click to Center, click anywhere on the image panel to center the camera to that point.

Figure 106: PTZ On-screen controls

4. Use the other PTZ controls to perform any of the following:

To...	Do this...
Zoom	• Click to zoom in. • Click to zoom out. • Click the image panel and use the mouse scroll wheel to zoom in and out. • If the camera supports Drag to Zoom, click and drag to create a green box to define the area you want to zoom in and see. • Right-click the image panel and select **Zoom Out Full**.
Control the iris	• Click to close the iris. • Click to open the iris.
Control the focus	• Click to focus near the camera. • Click to focus far from the camera.
Program a PTZ preset	1. Move the camera's field of view into position. 2. In the **Presets** drop down list, select a number then click . 3. In the dialog box, enter a name for the preset.

To...	Do this...
	4. Select the **Set as home preset** check box if you want this to be the camera's Home preset. 5. Click **OK**.
Activate a PTZ preset	Select a preset then click .
Return to the Home preset position	If the PTZ camera supports a Home preset position, click to return the camera to its Home position.
Program a PTZ pattern	1. In the PTZ Controls pane, select a pattern number and click . 2. Use the PTZ controls to move the camera and create the pattern. 3. Click to stop recording the pattern.
Activate a PTZ pattern	In the PTZ Controls pane, select a pattern number and click . The pattern will repeat until the pattern is stopped or another pattern is run.
Program a PTZ tour	For more information, see **Programming PTZ Tours**.
Activate a PTZ tour	In the PTZ Controls pane, select a tour number and click . The tour will repeat until stopped or until other PTZ controls are used.
Activate an auxiliary command	1. Select an aux command number and click . 2. Click to turn off the auxiliary output.
Display the PTZ camera on-screen menu	1. Click . 2. To move through the menu options, click any of the following: • Click to move down the options. • Click to move up the options. • Click to confirm your selection. • Click to cancel your selection.
Lock the PTZ controls	Click . Other users will be unable to use the PTZ controls for this camera until you unlock the controls or log out.

Programming PTZ Tours

If the PTZ camera supports guard tours, the tours can be programmed through the PTZ controls pane. Tours allow the PTZ camera to automatically move between a series of preset positions, and can be set to pause at

each preset for a specific amount of time for video monitoring.

NOTE: For video analytics devices, classified object detection only works when the camera is in its Home position.

1. Create all the PTZ presets you need for this tour.
2. In the PTZ Controls pane, select a tour number then click . The Edit PTZ Tour dialog box is displayed.

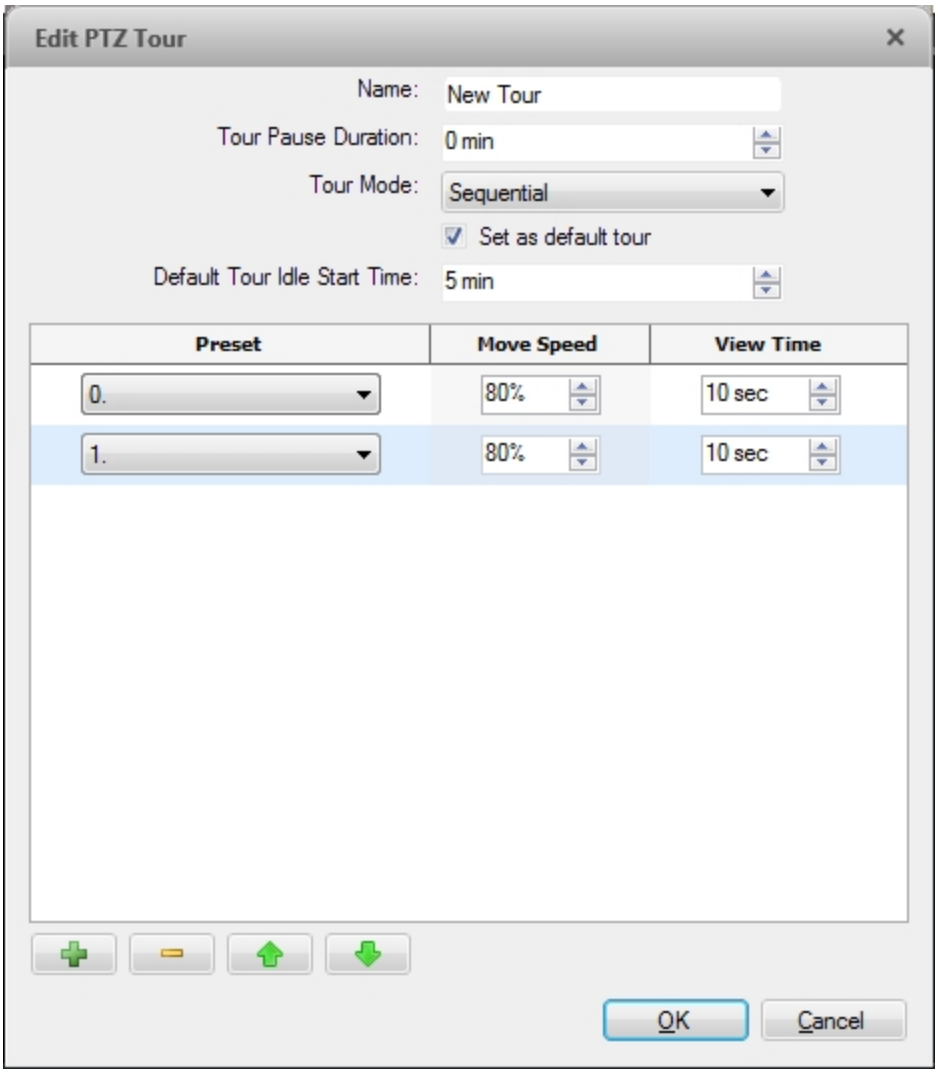


Figure 107: The Edit PTZ Tour dialog box

3. In the Edit PTZ Tour dialog box, give the tour a name.
4. In the **Tour Pause Duration:** field, enter the amount of time before a tour repeats. Tours repeat until manually stopped, or until other PTZ controls are used.
5. In the **Tour Mode:** drop down list, select one of the following:
    - **Sequential:** the PTZ camera will go to each preset in the set order.
    - **Random:** the PTZ camera will go to each preset in random order.

6. Select the **Set as default tour** check box if you want this tour to run automatically.
    - The **Default Tour Idle Start Time:** field is now enabled. Enter the amount of time the PTZ camera must be idle before this tour automatically starts.
7. To add a preset to the list, click .
    a. In the **Preset** column, select a preset from the drop down list.
    b. In the **Move Speed** column, enter how fast you want the PTZ camera to move to this preset. The higher the %, the faster the camera moves.
    c. In the **View Time** column, enter the amount of time you want the PTZ camera to stay at this preset position. The view time is 10 seconds by default.
    d. Repeat step 7 until all the presets for this tour have been added.
8. To remove a preset, select the preset then click .
9. To re-order a preset, select the preset then click or . The preset order only affects tours that use Sequential mode.
10. Click **OK** to save the tour.

Triggering Manual Recording

Cameras are set to follow a recording schedule. If an event occurs outside the camera's recording schedule, you can click the record indicator icon to force the camera to record the event.For more information about recording schedules, see **Recording Schedule**.

The Record Indicator overlay must be enabled to use manual recording. For more information, see **Video Display Settings**.

Camera Recording States

		
Recording	Recording triggered by an event	Not recording

Starting and Stopping Manual Recording

In an image panel that is displaying video, do either of the following:

- In the top-left corner of the image panel, click  to start manual recording.

  The recording indicator is highlighted in blue to show that the camera is recording. Manual recording continues until it is stopped or until the maximum manual recording time is reached.

- Click  to manually stop video recording.

The maximum manual recording time is configured in the Manual Recording dialog box. For more information, see **Manual Recording**.

Triggering Digital Outputs

While you monitor live video in an image panel, you can manually trigger any digital output that is connected to the camera.

Digital outputs are configured in the Digital Inputs and Outputs dialog box. For more information, see **Setting Up Digital Outputs**.

To trigger a digital output:

1. Open the camera's live video in an image panel.
2. In the image panel, click .
3. If there is more than one digital output linked to the camera, you will be prompted to select the digital output you want to trigger.

Monitoring Live POS Transactions

If a camera is linked to a point of sale (POS) transaction source, you can monitor live POS transactions while you monitor video from the linked camera.

1. Open the camera's video in an image panel.
2. In the image panel, click .

   NOTE: If the camera is not linked to a POS transaction source, the icon is not displayed.

   If there is more than one POS transaction source linked to the camera, you will be prompted to select one. The POS transactions are displayed in the next image panel.

   Each transaction is separated by date and time, and the most recent transaction is highlighted in blue.
3. To display cameras that are linked to the POS transaction source, click in the POS transaction image panel.

   If multiple cameras are connected to the POS transaction source, you will be prompted to select one.

Controlling Recorded Video

In this section are features that are only available while monitoring recorded video.

Playing Back Recorded Video

The Timeline displays when video was recorded and lets you control video playback.

The colored bars on the Timeline show the camera's recording history:

- A red bar shows the camera has recorded a motion event.
- A blue bar shows the camera has recorded video.
- White areas show periods of time during which the camera has not recorded any video.
- An yellow bar is a bookmark in the camera's recording history.

For more information about bookmarks, see **Bookmarking Recorded Video**.

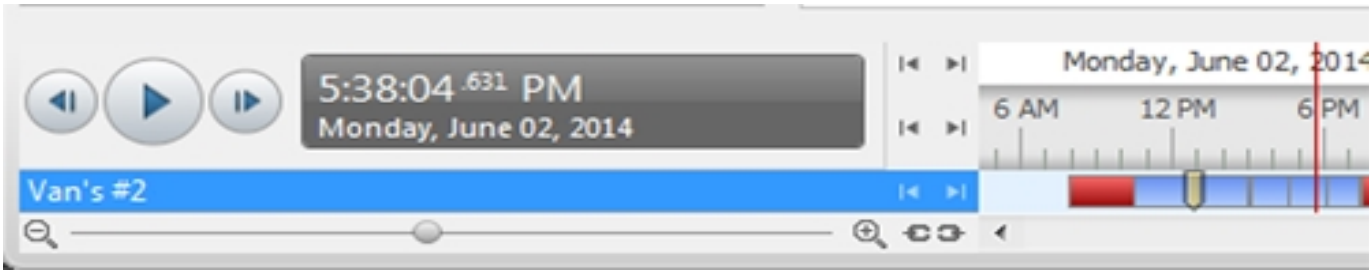
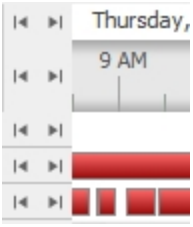
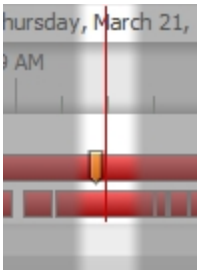


Figure 108: Playback controls on the Timeline

To...	Do this...
Select a playback time	• Click the dark gray date display and select a specific date and time. • Click a point on the Timeline.
Start playback	Click ▶. • Click ⏩ to fast forward. Tap the arrow again to increase the playback speed. • Click ⏪ to rewind. Tap the arrow again to increase the playback speed. You can play the video up to eight times the original speed.
Stop playback	Click ⏸. • Click ⏭ to step forward one frame. • Click ⏮ to step backward one frame.
Jump forward or backward on the Timeline	 On the Timeline, click ⏮ or ⏭ to move to set points on the Timeline.
Zoom in or out of the Timeline	 • Move the slider on the bottom left to zoom in or out on the Timeline. • Place your mouse over the Timeline and use the scroll wheel to zoom in or out on the Timeline. You can zoom in to a quarter of a second, and zoom out to see years if recorded video exists.
Center the Timeline on the time marker	 Right-click the Timeline, and select **Center on Marker.**
Pan the Timeline	• Click and drag the time marker through the Timeline. • Move the horizontal scroll bar under the Timeline. • Right-click and drag the Timeline.

Synchronizing Recorded Video Playback

Synchronizing recorded video playback allows you to synchronize Timelines across multiple View, Alarm, and Search tabs while they are in recorded mode.

Synchronized recorded video playback is disabled by default. Once it is enabled, it will remain enabled until it is manually disabled.

NOTE: Tabs can only be synchronized to one time. You cannot synchronize groups of tabs to separate times.

Enabling Synchronized Recorded Video Playback

- To enable synchronized recorded video playback in all new View tabs, select > **Client Settings...** > **General** > **Synchronize recorded video playback**.

  Timelines will be automatically centered on the current time.

  Enabling synchronized recorded video playback in the Client Settings... dialog box will not synchronize the Timelines of previously opened tabs. It will only synchronize new tabs that are opened after enabling synchronized recorded video playback. Previously opened tabs need to be synchronized individually.

- To synchronize playback between specific or previously opened tabs, click the gray button on the tab Timeline.

Disabling Synchronized Recorded Video Playback

- Synchronized recorded video playback can be disabled for all new tabs by clearing the **Synchronize recorded video playback** check box in the Client Settings... dialog box. Previously synchronized tabs will remain synchronized.
- Synchronized recorded video playback can also be disabled in individual tabs.

  On a synchronized Timeline, click the blue button. The button will turn gray to show that it is no longer synchronized. The Timeline will stay where it is, but will no longer be synchronized with other Timelines.

Bookmarking Recorded Video

You can add bookmarks to recorded video to help you find and review an event later. Bookmarked video can be protected against scheduled data cleanup so that the video is never deleted.

Adding a Bookmark

Tip: You can add a bookmark any time the Timeline is displayed.

1. Drag the time marker to where you want to start the bookmark, then right-click the Timeline and select **Add Bookmark**.

   The Edit Bookmark dialog box appears, and the bookmark time range is highlighted on the Timeline.

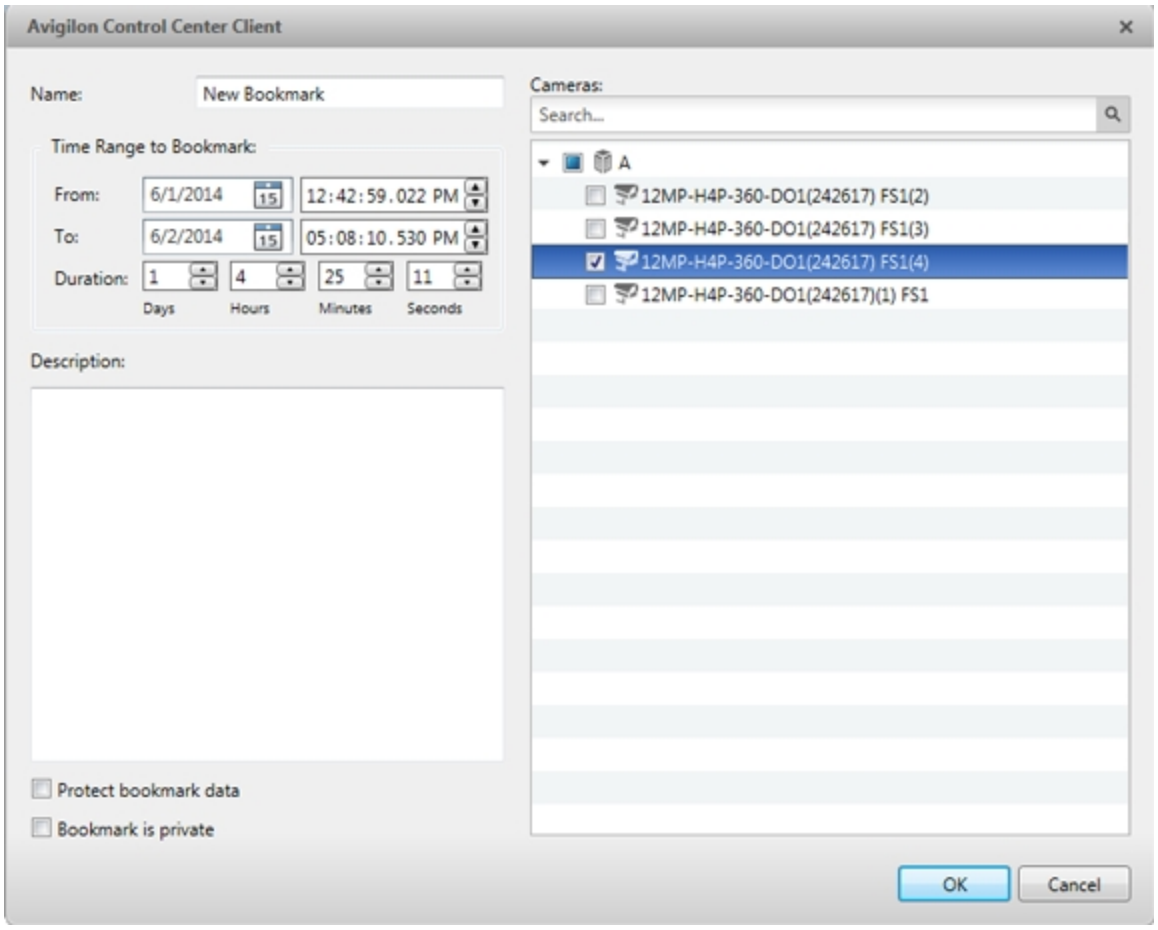


Figure 109: Edit Bookmark dialog box

2. Enter a **Name:** for the bookmark.
3. In the **Cameras:** pane, select all the cameras that need to be attached to this bookmark.

   NOTE: You can only bookmark multiple cameras from the same Site.
4. In the **Time Range to Bookmark:** area, enter the full duration of the bookmark.

   You can also move the black time range markers on the Timeline to adjust the time range.
5. In the **Description:** field, enter extra any information you want to include with the bookmark.
6. To protect the bookmark video from being deleted, select the **Protect bookmark data** check box.

   NOTE: Protected bookmarks are never deleted. Be aware that bookmarked videos take up space and can become the oldest video on the server.
7. To make the bookmark private, select the **Bookmark is private** check box. Private bookmarks are only visible to the user who marked the bookmark as private, and the system administrator. No one else will have access to the bookmark.
8. Click **OK**.

Exporting, Editing, or Deleting a Bookmark

1. Click the bookmark on the Timeline, then do one of the following:

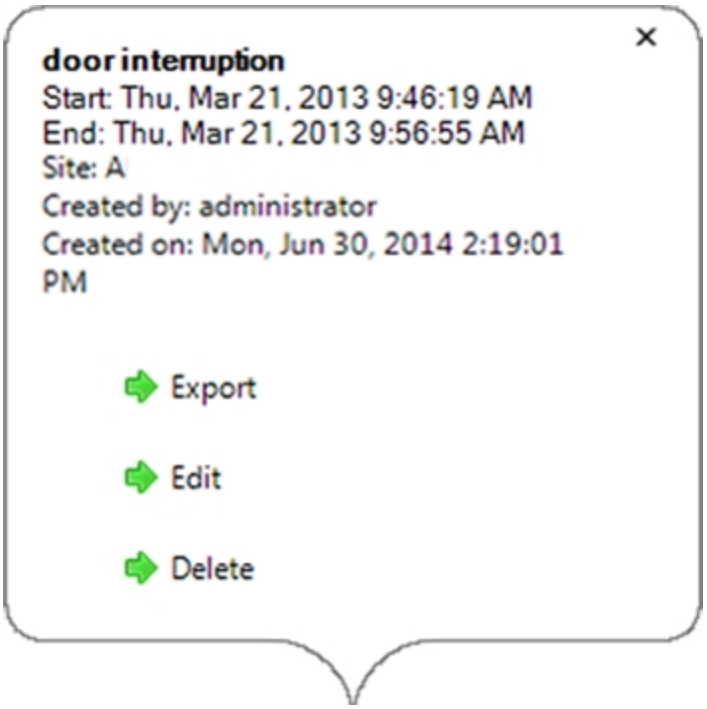


Figure 110: Pop-up Bookmark properties

To	Do this...
Export a bookmark	Click **Export**, then complete the Export tab.
Edit a bookmark	Click **Edit**, then make your changes.
Delete a bookmark	Click **Delete**. When the confirmation dialog box appears, click **Yes**.

When editing a bookmark, refer to **Adding a Bookmark** for details about the editable options.

When exporting a bookmark, refer to **Export** for information about the export options.

Reviewing Recorded POS Transactions

While you watch recorded video, you can review POS transactions that occur at the same time.

1. Select a camera that is linked to the POS transaction source and display the camera's recorded video
2. In the image panel, click  .

   If there is more than one POS transaction source linked to the camera, you will be prompted to select one. The POS transactions are displayed in the next image panel.

   - Each transaction is separated by date and time.
   - When you select a transaction, the video jumps to that event on the Timeline.
   - Scroll up or down to see other recorded POS transactions.

3. To display cameras that are linked to the POS transaction source, click  in the POS transaction image panel.

   If multiple cameras are connected to the POS transaction source, you will be prompted to select one.

4. Use the Timeline to review the video in more detail.

For more information about Timelines, see **Playing Back Recorded Video**.

If you want to find a specific POS transaction, see **Performing a POS Transaction Search**.

Working with Maps

A map is a graphical reference of your surveillance site. You can create a map out of any image of your location, then add cameras, encoders, saved Views, and other maps to the image to help you quickly navigate through your surveillance site.

Adding a Map

You can create a map from any image in JPEG, BMP, PNG, or GIF format. The image is used as the map background and cameras are added on top to show where they are located in your surveillance Site.

1. In the System Explorer, right-click a Site or Site folder and select **New Map...**.
2. In the Map Properties dialog box, click **Change Image...** and locate your map image.

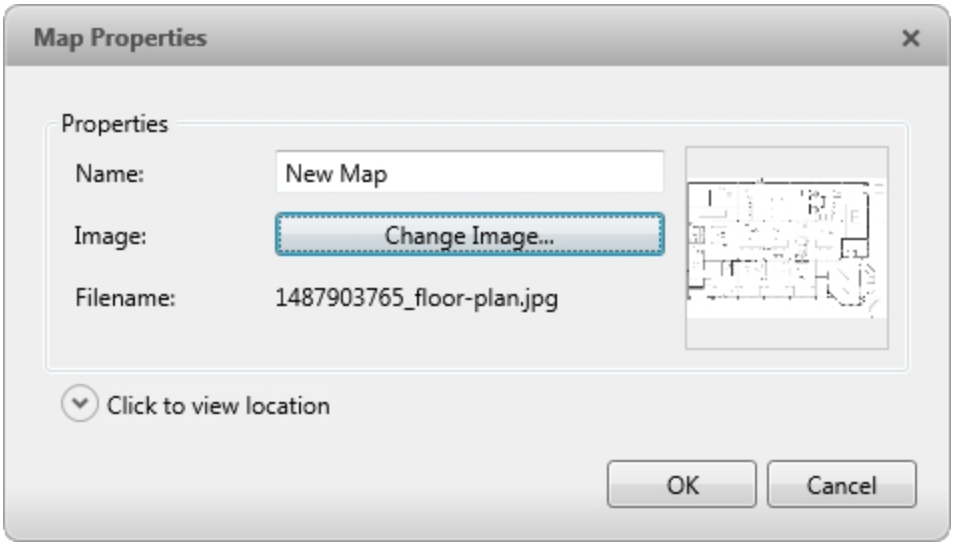


Figure 111: The Map Properties dialog box

3. In the **Name:** field, enter a name for the map.
4. Click to choose where the map appears in the System Explorer. By default, the map is added to the Site that you initially selected.
    - If your Site includes virtual sub-sites, select a location for the map. The list on the right updates to show what is stored in that directory.
    - In the Site directory, drag the map up and down to set where it is displayed.
5. Click **OK**.

    In the following Editing: Map tab, you can click **Edit Properties...** to open the Map Properties dialog box again.

6. Drag and place cameras from the System Explorer onto the map.

Figure 112: The Editing: Map tab

By default a camera is displayed as an icon with a yellow triangle to represent its field of view.

- Drag the black points at the end of the yellow field of view to re-size and position the camera angle.

7. Drag encoders, saved Views, Virtual Matrix monitors, and other maps that you need from the System Explorer onto the map.
8. In the **Map Icon Properties** options, you can change the way icons are displayed on the map. Select any icon on the map then do the following:

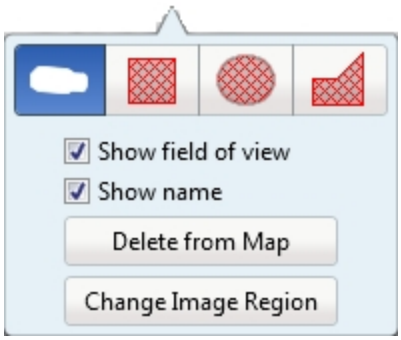


Figure 113: Map Icon Properties options

a. To replace an icon with a clickable shape region, select one of the shape buttons. You can replace the icon with a rectangle, ellipse, or polygon region.

b. Select the **Show name** check box to display the object's name on the map.

c. Click **Delete from Map** to remove the object from the map.

d. (Cameras only) Select the **Show field of view** check box to display the camera's yellow field of view. This option is only available when the camera icon is used.

   Drag the corners of the yellow triangle to expand the field of view. Drag the black circle at the end of the triangle to rotate the field of view.

9. Click  to save your new map.

Using a Map

You can open a map in any image panel, then open video or alarms from the map.

1. To open a map in an image panel, do one of the following:
   - Double-click in the System Explorer.
   - Drag from the System Explorer to an image panel.
   - In the System Explorer, right-click and select **Add To View**
2. When the map appears in an image panel, do any of the following:

Figure 114: Map in an image panel.

To...	Do this...
Review an alarm	When a camera flashes in red, an alarm linked to the camera has been triggered.

To...	Do this...
	• Click the camera to monitor the live alarm video.
Display video from a camera on the map	• Drag a camera from the map to a different image panel, or • Click the camera on the map.
Open a linked map	• Click the map icon on the map. You can use the **Forward** and **Back** buttons to move between maps.
Open a linked View	• Click the saved View on the map.

Editing and Deleting a Map

You can update a map or delete an old map anytime.

1. In the System Explorer, right-click  then select one of the following:
    - To edit the map, select **Edit...**. Refer to **Adding a Map** for details about the editable options.
    - To delete the map, select **Delete**. When the confirmation dialog box appears, click **Yes**.

Working with Web Pages

You can quickly review online content while monitoring videos by adding web pages to the System Explorer.

NOTE: Web pages will not load if you do not have internet access.

Adding a Web Page

You can add web pages to a Site for quick access to internet content that is related to your surveillance system.

1. In the System Explorer, right-click a Site or Site folder and select **New Web Page...**.

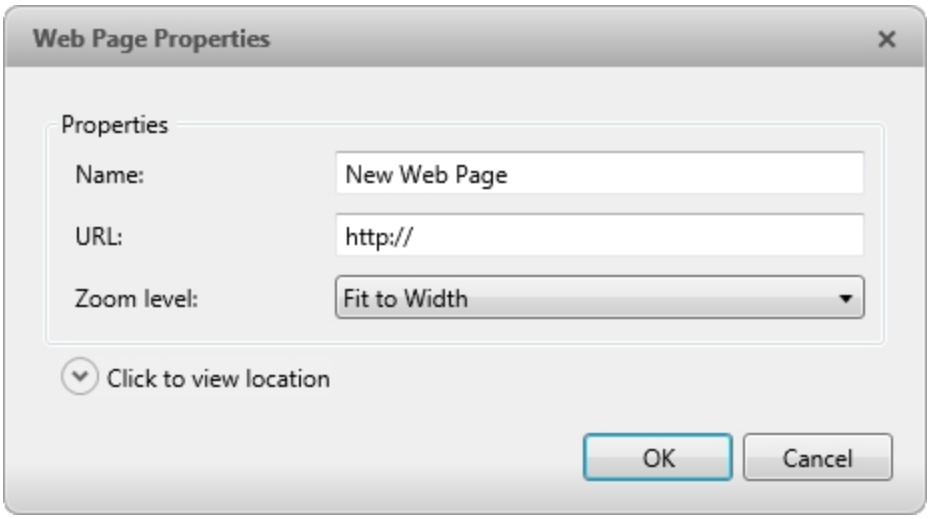


Figure 115: The Web Page Properties dialog box

2. Enter a **Name:** for the web page.
3. Enter the web page URL in the **URL:** field.
4. Select a **Zoom level:** for viewing the web page inside an image panel.
5. Click to choose where the web page appears in the System Explorer. By default, the web page is added to the Site you initially selected.
    - If your Site includes virtual sub-sites, select a location for the web page. The list on the right updates to show what is stored in that directory.
    - In the Site directory, drag the web page up and down to set where it is displayed.
6. Click **OK**.

Using a Web Page

To open a web page, do one of the following:

- Double-click in the System Explorer.
- Drag from the System Explorer to an image panel.
- In the System Explorer, right-click and select **Add To View**.

The web page is displayed in one of the image panels. Use the web browser buttons to navigate through the internet.

Figure 116: Web Page controls.

Editing and Deleting a Web Page

Whenever a web page address becomes out of date, you can choose to update the web page or delete the web page from the Site.

1. In the System Explorer, right-click then select one of the following:
    - To edit the web page, select **Edit...**. Refer to **Adding a Web Page** for information about the editable options.
    - To delete the web page, select **Delete**. When the confirmation dialog box appears, click **Yes**.

Monitoring Alarms

The Alarms tab allows you to monitor and acknowledge alarms. You can quickly review video of the event, bookmark the recorded incident, and export alarm video for further investigation.

Accessing the Alarms Tab

At the top of the application window, click > .

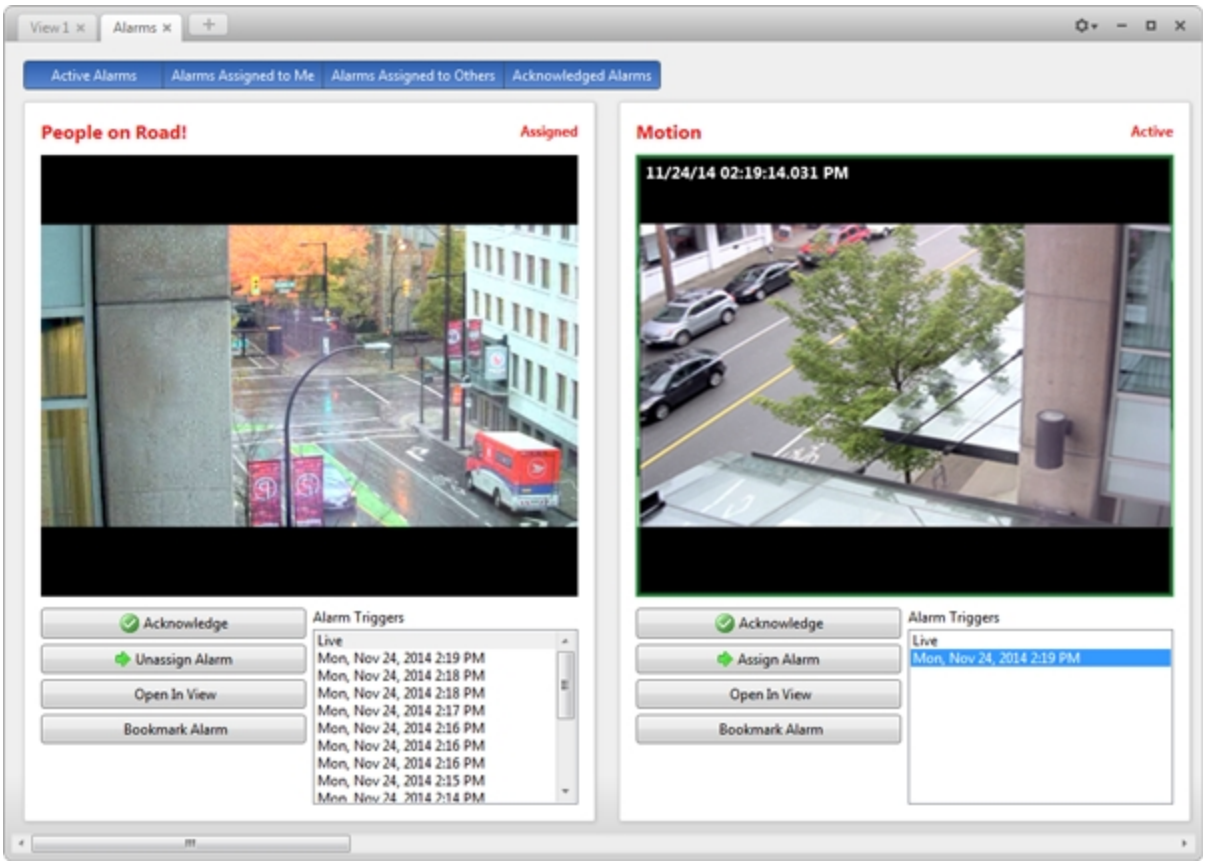


Figure 117: The Alarms tab

The Alarms tab is divided into a series of vertical alarm panels. The panels display alarms that are currently active, acknowledged, or assigned to a user.

To view more alarm panels, use the scroll bar at the bottom of the Alarms tab.

Tip: The most relevant alarm is in the leftmost panel. Alarm names that are displayed in red indicate alarms that have not been acknowledged.

Panels are sorted from left to right by:

- Alarm status: Alarms Assigned to Me, Active Alarms, Alarms Assigned to Others, Acknowledged Alarms
- Priority
- Most recent alarm trigger time

The alarm panel is divided into the following areas:

- The top of the panel lists the alarm name and status.
- The middle of the panel displays video from all of the cameras linked to the alarm.
- At the bottom of the panel, the Alarm Triggers area displays every time the alarm was triggered since you logged in.

Reviewing Alarms

In the Alarms tab, you can review and manage alarms. Active alarms can be assigned to yourself, and acknowledged alarms can be exported or purged as required.

Reviewing Alarm Video

You can review active and acknowledged alarms in detail through the alarm panel, or by opening the alarm video in a new View.

Each panel in the Alarms tab displays a different alarm.

1. At the top of the tab, click any of the **Filters** to choose what type of alarms are displayed.
   Alarms can be filtered by **Active Alarms**, **Alarms Assigned to You**, **Alarms Assigned to Others**, and **Acknowledged Alarms**.
2. In the Alarm Triggers list, select an alarm trigger to display the image for that instance of the alarm. Select **Live** to display live video in the image panels.
3. You can zoom and pan in the image panels like you would in a regular image panel. For information, see **Zooming and Panning in a Video**
4. Click **Open In View** to open the alarm video in a new View.

Acknowledging an Alarm

Acknowledging an alarm shows that an alarm has been reviewed and is no longer active. You can acknowledge any alarm that is active or assigned to you.

Tip: To hide Acknowledged alarms without purging them, disable the **Acknowledged** filter at the top of the tab.

1. If required, enter notes describing the nature of the alarm in the **Acknowledge Alarm** text box.
2. Click **Acknowledge**.
3. If there is a digital output linked to the alarm, a dialog box may appear to ask for permission to activate the digital output. Activate the digital output as required.

The Alarm is given an Acknowledged status.

Assigning an Alarm

You can assign an alarm to yourself to let others know that the alarm is being reviewed.

Although you can only assign alarms to yourself, you can unassign the alarm at any time. You can also reassign alarms assigned to others to yourself.

1. In the alarm panel, click **Assign Alarm**.
2. To unassign an alarm, in the alarm panel click **Unassign Alarm**.

Bookmarking an Alarm

You can bookmark active and acknowledged alarm video.

1. In the alarm panel, click **Bookmark Alarm**.
2. When the Edit Bookmark dialog box appears, define the details of your bookmark.

   The Edit Bookmark dialog box automatically selects all the cameras that are linked to the alarm, and sets the time range to span the first and last alarm trigger. After you make any required changes, click **OK**.

For more information about the bookmark options, see **Bookmarking Recorded Video**.

Purging an Alarm

Purging an alarm removes the alarm from the Alarms tab until the alarm is activated again. Although purged alarms are no longer visible, you can still search through the alarm's history.

- In the alarm panel, click **Purge Alarm**.

Searching Alarms

You can search through an alarm's history to review other instances of the alarm.

- In the alarm panel, click **Search Alarm**.

For more information about the alarm search options, see **Performing an Alarm Search**.

Exporting Alarms

You can export alarm video for review on other computers.

- In the alarm panel, click **Export Alarm**.

For information about the export options, see **Export**.

Arming Image Panels

Arming an image panel reserves the image panel specifically for displaying video linked to alarms or rules. Armed image panels allow you to review and acknowledge alarms while monitoring video in a View. Any image panel can be armed or disarmed as required.

If there are no armed image panels, alarm video will appear in the next empty image panel in the current View, or in a new View if all current image panels are in use.

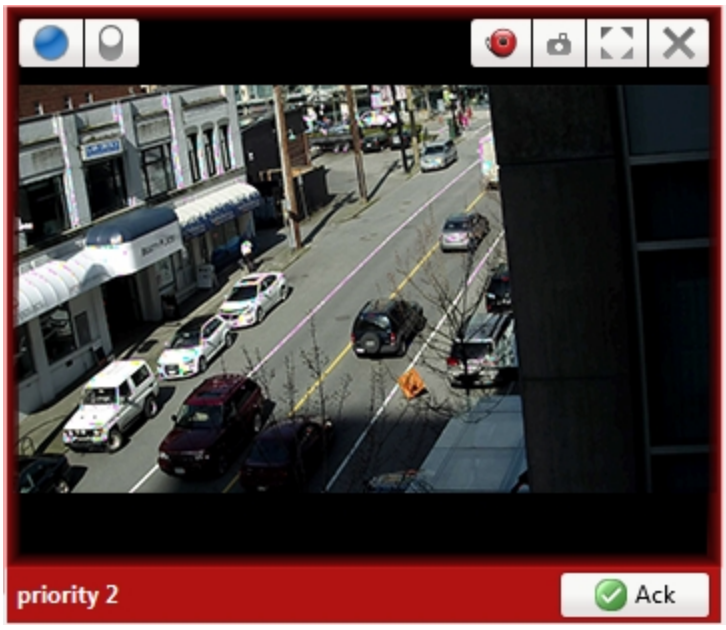


Figure 118: Armed image panel

Tip: You can still use the features that are common to all image panels in an armed panel, like taking snapshots or maximizing the image panel.

To...	Do this...
Arm an image panel	In an image panel, click . The image panel is given a **red** border and an alarm label to show that it is armed.
Acknowledge an alarm	Click .
Move between linked alarm video	If the alarm is linked to multiple cameras, use the green arrows to move between the linked cameras.
Disarm an image panel	In an armed image panel, click .

If multiple alarms are triggered at the same time, the linked videos are queued inside the armed image panel. The alarm videos are displayed by order of alarm priority, then time. Once an alarm is acknowledged or assigned to a user, the alarm video is removed from the armed image panel.

NOTE: If you choose to close a video in the armed image panel, the video is removed but the alarm continues to be active.

Videos triggered by a rule are queued in the armed image panel after alarms, with the most recent video displayed first. Rule videos are not labeled and do not need to be acknowledged.

Monitoring License Plates

License Plate Recognition (LPR) is a licensed feature that allows you to monitor vehicle license plates that are detected by the Avigilon Control Center.

You can use the license plate overlay to monitor license plates as they are detected. You can also use the License Plate Watch List feature to alert you when specific license plates are detected.

To set up License Plate Recognition, see **License Plate Recognition**.

License Plate Overlay

While you monitor video in an image panel, you can also monitor license plates as they are detected by the Avigilon Control Center.

When the license plate overlay is enabled, detected license plate numbers are displayed in the bottom right corner of the image panel.

To enable the License Plate overlay:

1. In the top-right corner of the Client window, select > **Client Settings...** > **Display**.
2. In the Image Overlays: area, select the **License Plate** check box.
3. Click **OK**.

When you display live video for a camera that is configured for license plate recognition, the detected license plates are displayed by the overlay.

Reviewing License Plate Matches

If your system is configured to track specific license plates through the Watch List, you will be notified by a pop-up dialog box when matches are detected.

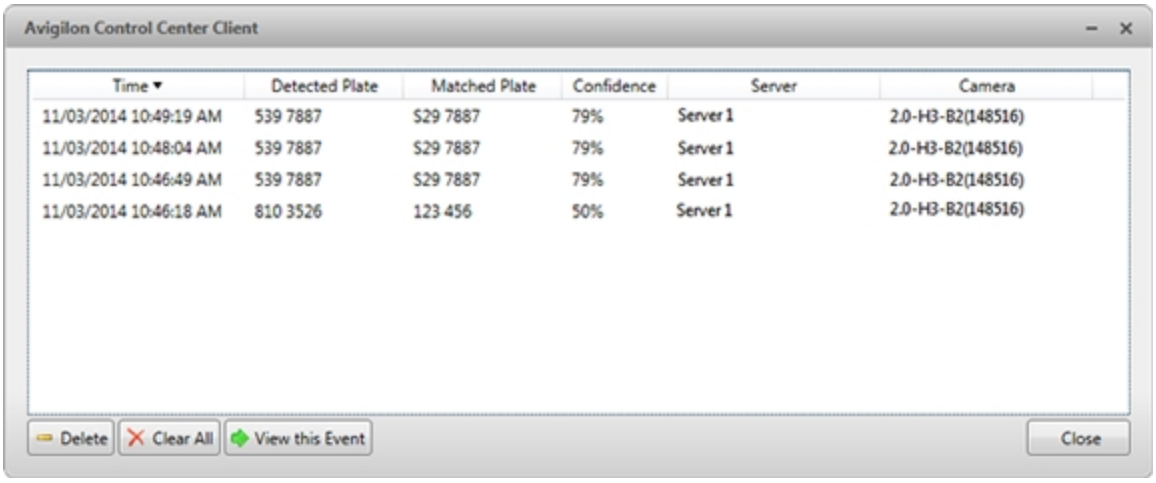


Figure 119: The License Plate Matches dialog box.

Select one of the license plate matches and do any of the following:

- Click **View this Event** or double-click the selected license plate to open a snapshot of the detected license plate in a new View.
- Click **Delete** to delete the license plate from the list.
- Click **Clear All** to empty the current match list. The list will be repopulated as new license plates are detected.

Search

You can quickly search for recorded video that is linked to an event or search through a camera's recording history.

NOTE: Some features are not displayed if the server does not have the required license, or if you do not have the required user permissions.

Performing an Alarm Search

The Alarm Search allows you to search through an alarm's history.

1. In the New Task menu, under Search, click  .

   The Search: Alarms tab is displayed.

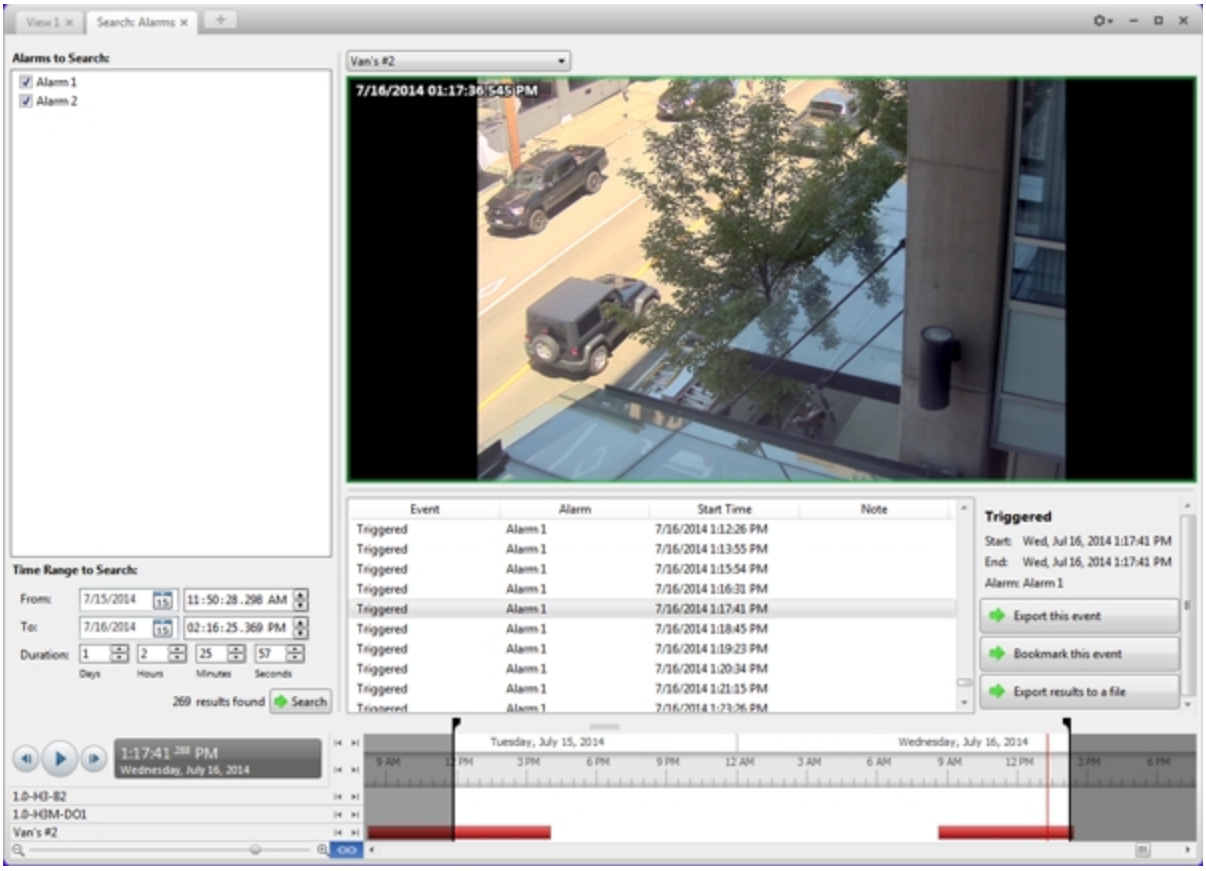


Figure 120: The Search: Alarms tab

2. In the **Alarms to Search:** list, select all the alarms you would like to include in the alarm search.
3. In the **Time Range to Search:** area, set the date and time range of your search. The time range is

highlighted on the Timeline by the black time range markers. You can also drag the time range markers to modify the time range.

4. Click **Search**.

Viewing Alarm Search Results

1. In the **Search Results** area, select a search result. The event is highlighted on the Timeline and the video is displayed in the image panel. Details about the search result are displayed to the right.
2. Use the Timeline controls to review the event.

   For more information, see **Playing Back Recorded Video**.
3. If the search result is linked to multiple cameras, select a camera from the drop down list above the image panel to change the video that is displayed.
4. Click **Export this event** to export the selected event video.

   For more information, see **Export**.
5. Click **Bookmark this event** to bookmark the selected search result.

   For more information, see **Bookmarking Recorded Video**.
6. To export all listed search results, click **Export results to a file** and save the file. The search results can be saved as either a CSV or Text file.

Performing a Bookmark Search

The Bookmark Search allows you to search for a specific bookmark.

1. In the New Task menu, click 

   The Search: Bookmark tab is displayed. All available bookmarks are listed on the left.

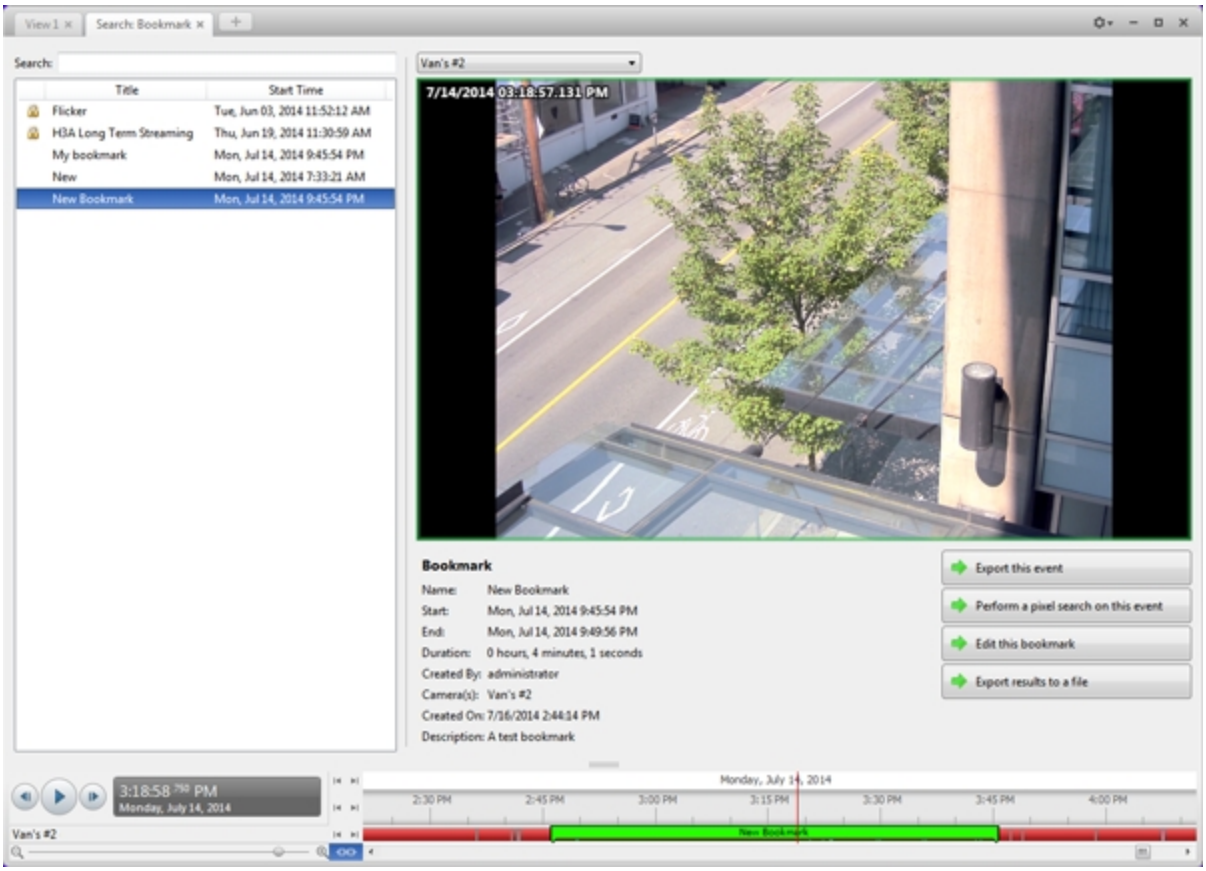


Figure 121: The Search: Bookmark tab

2. In the **Search:** field, enter any text that may appear in the bookmark's title, description, linked camera name, or the name of the user who created the bookmark.

   The search is automatically performed on all the listed bookmarks until only the matches are displayed.

Viewing Bookmark Search Results

1. In the Bookmark list, select a bookmark. The bookmark is highlighted on the Timeline and the video is displayed in the image panel. Details about the bookmark are displayed under the image panel.
2. Use the Timeline controls to review the event.

   For more information, see **Playing Back Recorded Video**.
3. If the search result is linked to multiple cameras, select a camera from the drop down list above the image panel to change the video that is displayed.
4. Click **Export this event** to export the selected bookmark.
5. If you want to further refine your search, click **Perform a pixel search on this event**. You can now search for pixel changes in the selected bookmarked video.

   For more information, see **Performing a Pixel Search**.
6. Click **Edit this bookmark** to edit the bookmark.

   For more information, see **Bookmarking Recorded Video**.

Performing an Event Search

The Event Search allows you to search for specific motion events and digital input events.

1. In the New Task menu, click 

   The Search: Event tab is displayed.

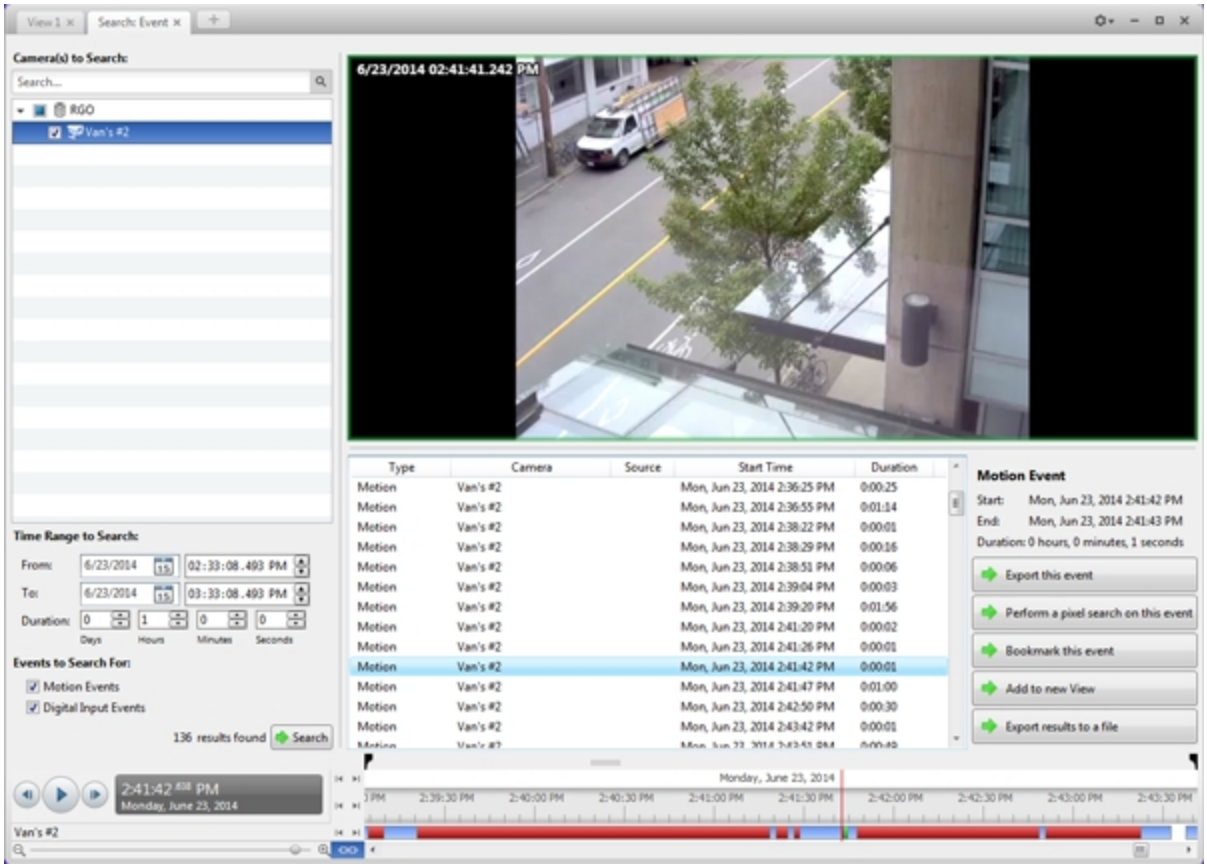


Figure 122: The Search: Event tab

2. In the **Camera(s) to Search:** area, select all the cameras you want to include in the search.
3. In the **Time Range to Search:** area, set the date and time range of your search. The time range is highlighted on the Timeline by the black time range markers. You can also drag the time range markers to modify the time range.
4. In the **Events to Search For:** area, select the types of events to include in the search.
5. Click **Search**.

Viewing Event Search Results

1. In the **Search Results** area, select a search result. The event is highlighted on the Timeline and the video is displayed in the image panel. Details about the search result are displayed to the right.
2. Use the Timeline controls to review the event.

For more information, see **Playing Back Recorded Video**.

3. Click **Export this event** to export the selected event video.

   For more information, see **Export**.

4. If you want to further refine your search, click **Perform a pixel search on this event**. You can now search for pixel changes in the selected search result.

   For more information, see **Performing a Pixel Search**.

5. Click **Bookmark this event** to bookmark the selected search result.

   For more information, see **Bookmarking Recorded Video**.

6. To export all listed search results, click **Export results to a file** and save the file. The search results can be saved as either a CSV or Text file.

Performing a License Plate Search

The License Plate Search allows you to search for detected license plates.

NOTE: The License Plate Search is only available if the License Plate Recognition feature is installed.

1. In the New Task menu, under Search, click 

   The Search: License Plates tab is displayed.

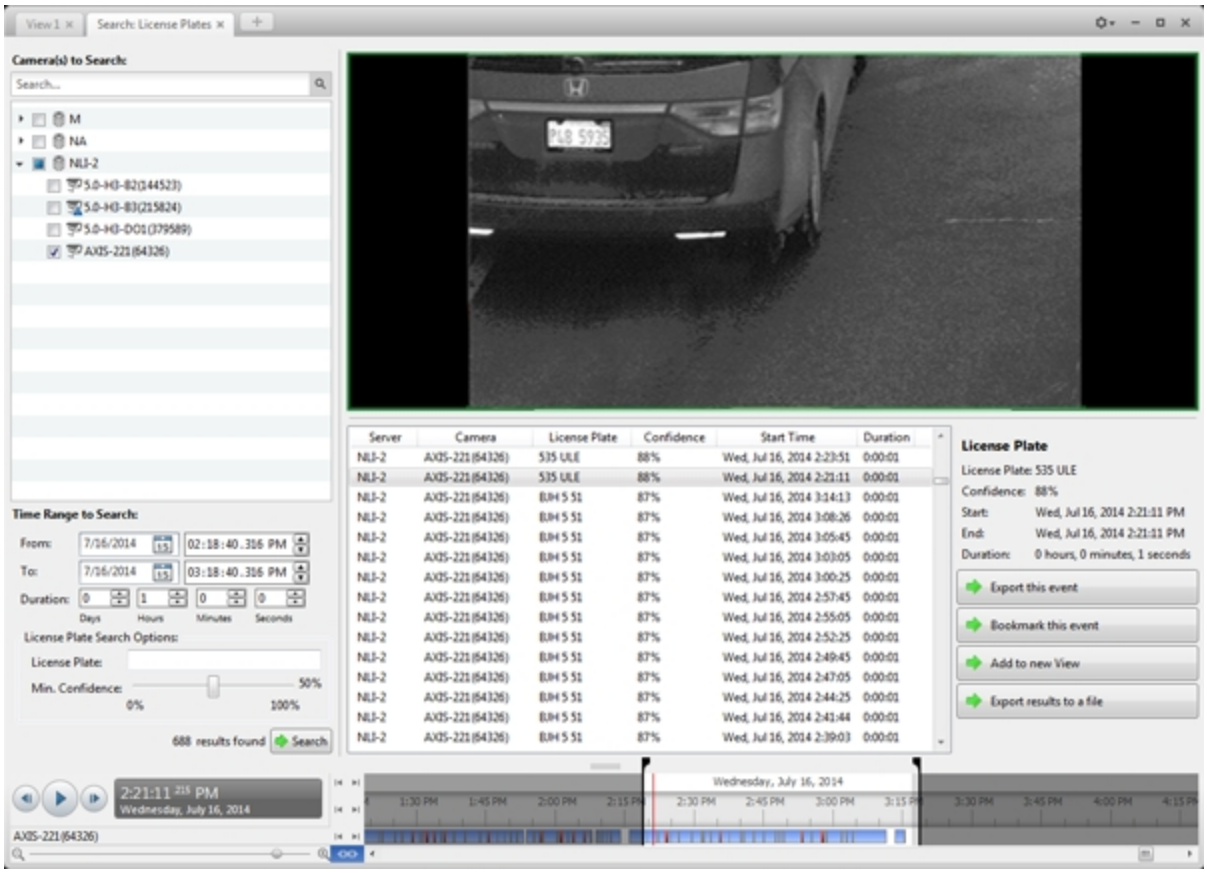


Figure 123: The Search: License Plates tab

2. In the **Camera(s) to Search:** area, select all the cameras you want to include in the search.
3. In the **Time Range to Search:** area, set the date and time range of your search. The time range is highlighted on the Timeline by the black time range markers. You can also drag the time range markers to modify the time range.
4. In the **License Plate Search Options:** area, enter the license plate you want to find and a minimum confidence of a match.
5. Click **Search**.

Viewing License Plate Search Results

1. In the **Search Results** area, select a search result. The event is highlighted on the Timeline and the video is displayed in the image panel. Details about the search result are displayed to the right.
2. Use the Timeline controls to review the event.

   For more information, see **Playing Back Recorded Video**.
3. If the search result is linked to multiple cameras, select a camera from the drop down list above the image panel to change the video that is displayed.
4. Click **Export this event** to export the selected event video.

   For more information, see **Export**.

5. Click **Bookmark this event** to bookmark the selected search result.

   For more information, see **Bookmarking Recorded Video**.

6. To export all listed search results, click **Export results to a file** and save the file. The search results can be saved as either a CSV or Text file.

Performing a Pixel Search

The Pixel Search allows you to search for tiny pixel changes in specific areas in the camera's field of view.

1. In the New Task menu, click 

   The Search: Pixel tab is displayed.

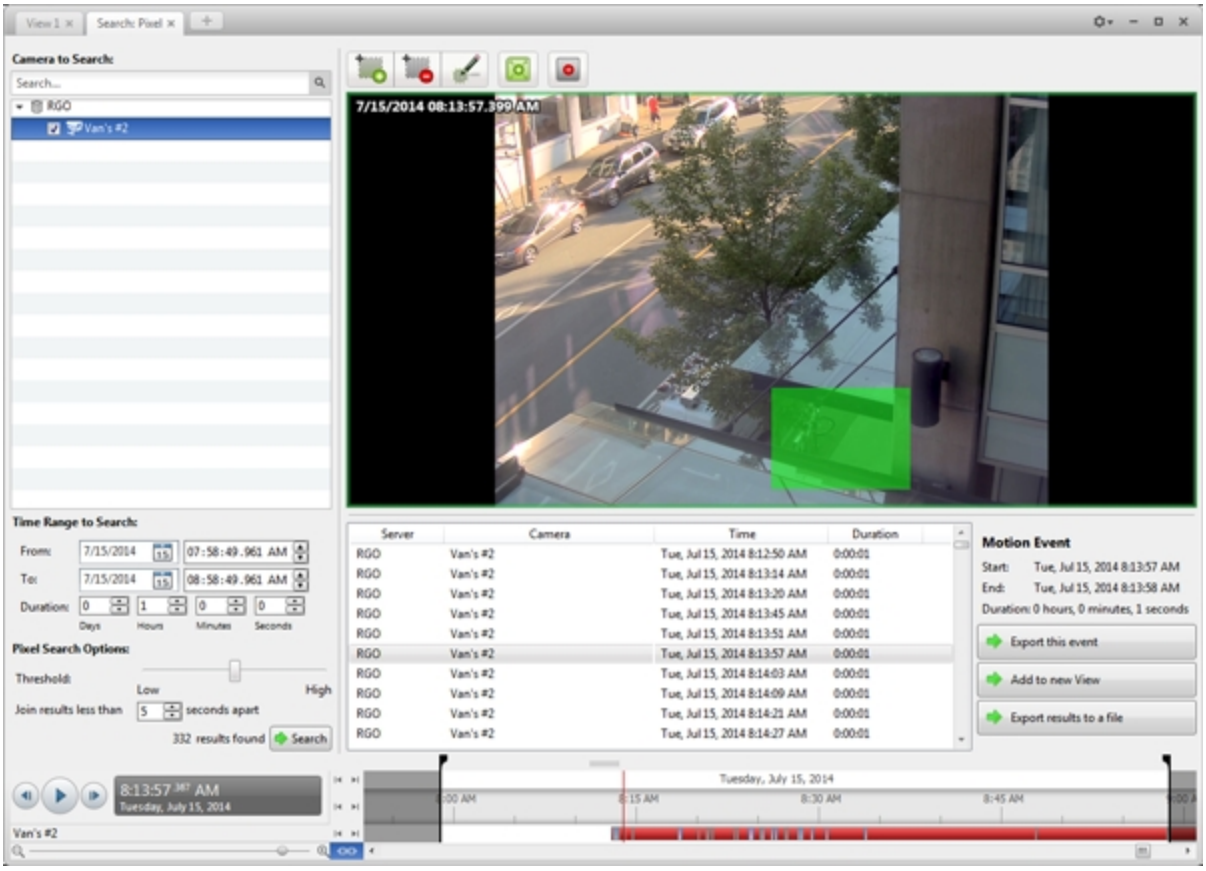


Figure 124: The Search: Pixel tab

   By default, the entire search image panel is highlighted in green.

2. In the **Camera to Search:** area, select a camera.

3. In the **Time Range to Search:** area, set the date and time range of your search. The time range is highlighted on the Timeline by the black time range markers. You can also drag the time range markers to modify the time range.

4. Define the pixel search area by using the motion detection tools above the image panel.

   Tip: If you are looking for something very specific, limit the green area to a dot to find what you're looking for more quickly.

5. In the Pixel Search Options: area, drag the **Threshold:** slider to select the amount of motion required to return a search result.

   A high threshold requires more pixels to change before results are found.

6. Enter a number in the **Join results less than** field to set the minimum number of seconds between separate search results. You can enter any number between 1-100 seconds.

7. Click **Search**.

Viewing Pixel Search Results

1. In the **Search Results** area, select a search result. The event is highlighted on the Timeline and the video is displayed in the image panel. Details about the search result are displayed to the right.

2. Use the Timeline controls to review the event.

   For more information, see **Playing Back Recorded Video**.

3. Click **Export this event** to export the selected event video.

   For more information, see **Export**.

4. To export all listed search results, click **Export results to a file** and save the file. The search results can be saved as either a CSV or Text file.

Performing a POS Transaction Search

The POS Transaction Search allows you to search for specific transactions.

1. In the New Task menu, click  .

   The Search: POS Transactions tab is displayed.

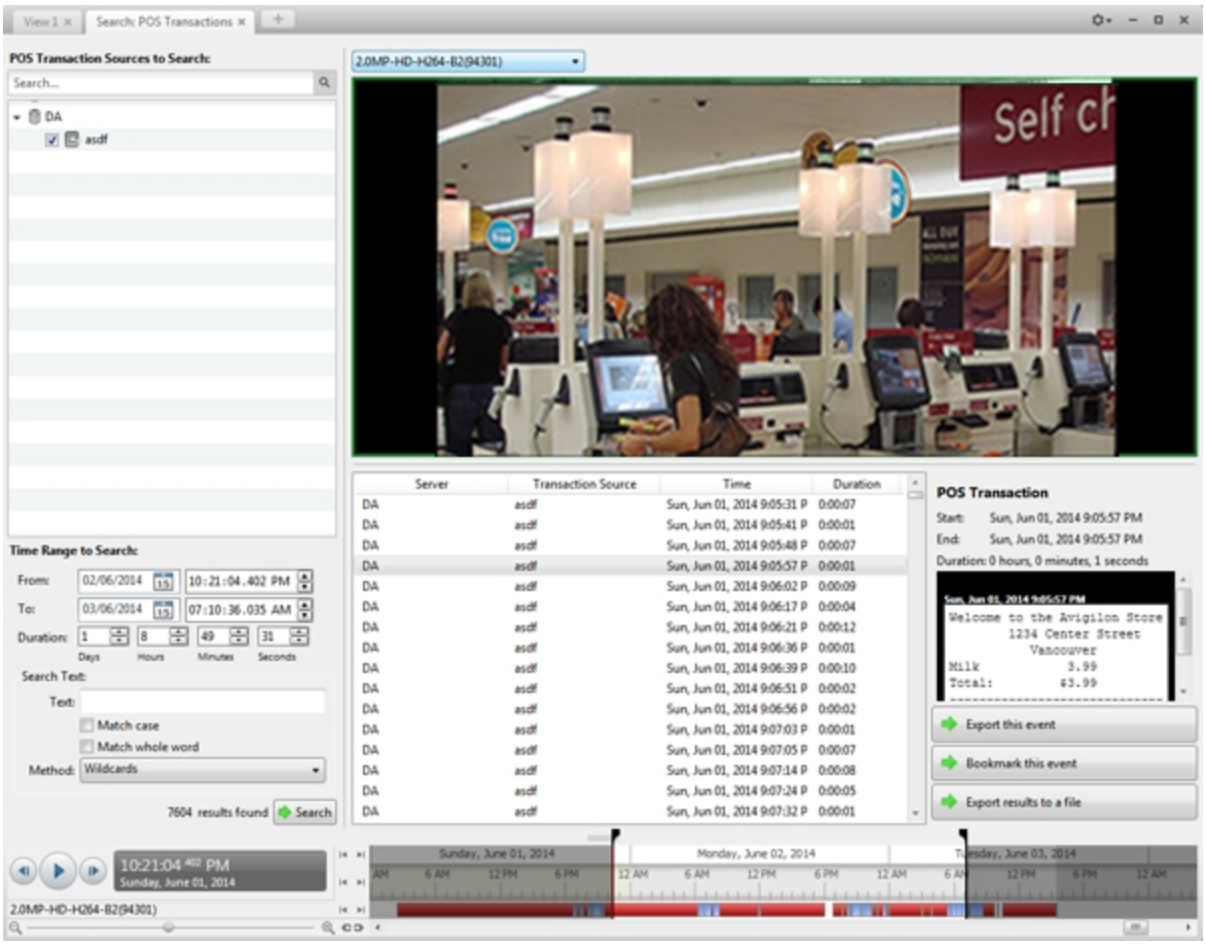


Figure 125: The Search: POS Transactions tab

2. In the **POS Transaction Sources to Search:** area, select all the POS transaction sources you would like to include in the search.
3. In the **Time Range to Search:** area, set the date and time range of your search. The time range is highlighted on the Timeline by the black time range markers. You can also drag the time range markers to modify the time range.
4. In the **Search Text:** area, enter any text that will help you filter the search results. For example, you can enter product names or transaction values.

   Use the **Wildcards** and **Regular expressions** search methods to find a range of results. Leave the **Text:** field blank to find all transactions.
5. Click **Search**.

Viewing POS Transaction Search Results

1. In the **Search Results** area, select a search result. The event is highlighted on the Timeline and the video is displayed in the image panel. Details about the search result are displayed to the right.
2. Use the Timeline controls to review the event.

   For more information, see **Playing Back Recorded Video**.

3. If the search result is linked to multiple cameras, select a camera from the drop down list above the image panel to change the video that is displayed.
4. Click **Export this event** to export the selected event video.

   For more information, see **Export**.
5. Click **Bookmark this event** to bookmark the selected search result.

   For more information, see **Bookmarking Recorded Video**.
6. To export all listed search results, click **Export results to a file** and save the file. The search results can be saved as either a CSV or Text file.

Performing a Thumbnail Search

The Thumbnail Search is a visual search that displays search results as a series of thumbnail images.

1. In the New Task menu, click  .

   The Search: Thumbnails tab is displayed.

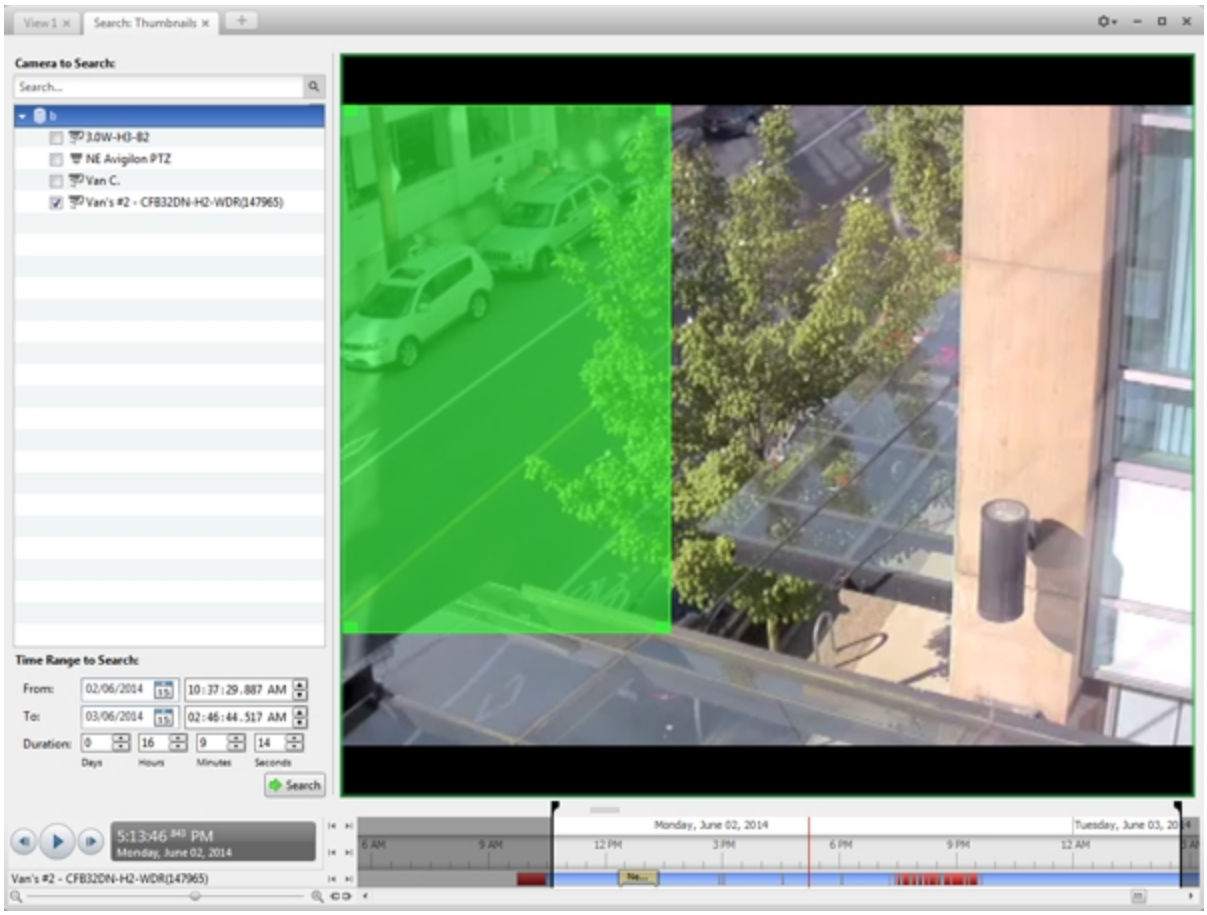


Figure 126: The Search: Thumbnails tab

2. In the **Camera to Search:** area, select a camera.
3. In the **Time Range to Search:** area, set the date and time range of your search. The time range is highlighted on the Timeline by the black time range markers. You can also drag the time range markers to modify the time range.
4. In the image panel, move or drag the edges of the green overlay to focus the search on one area in the video image. Only the area highlighted in green will be searched.
5. Click **Search**.

Viewing Thumbnail Search Results

The search results display thumbnails at equal intervals on the Timeline.

1. To change the size of the search result thumbnails, select **Large Thumbnails**, **Medium Thumbnails**, or **Small Thumbnails** from the menu above the search results.

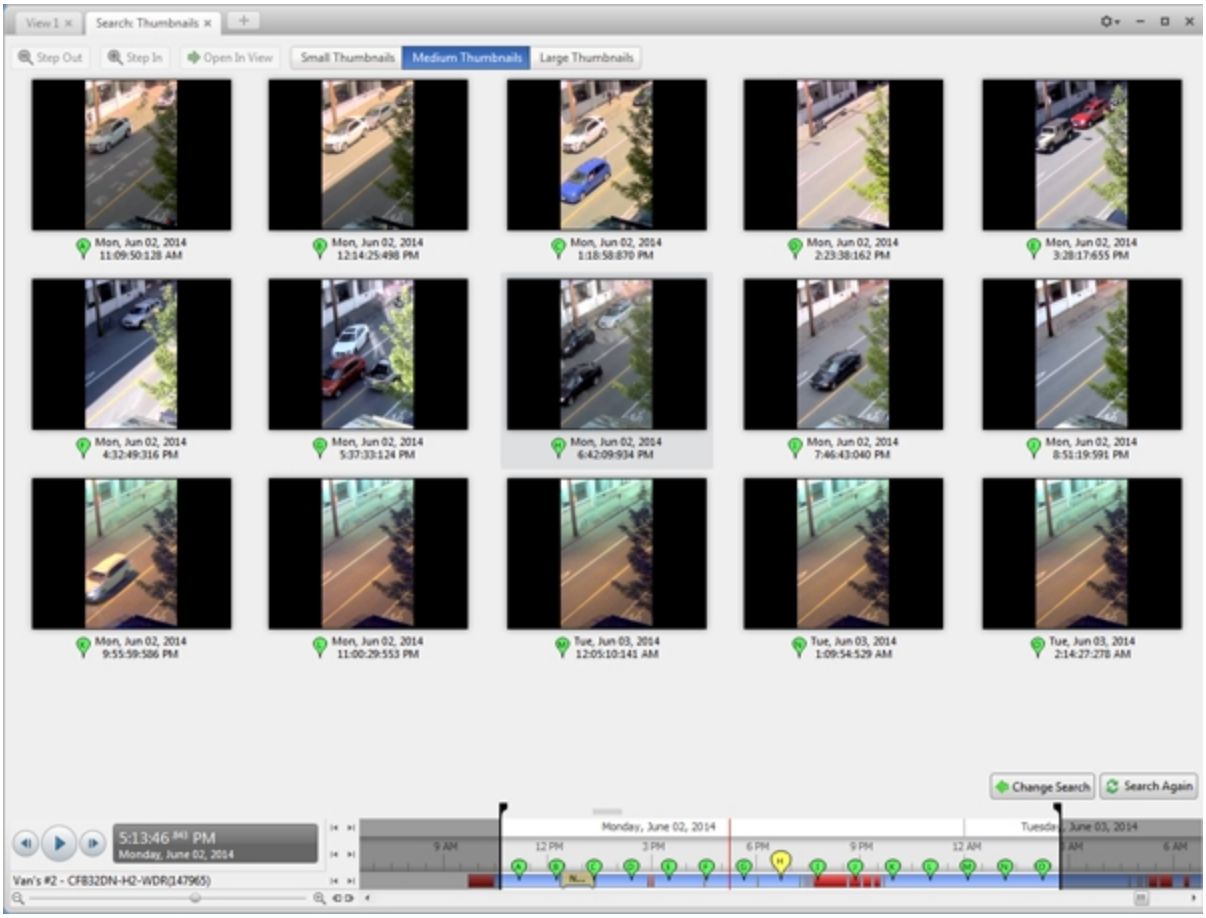


Figure 127: The Search: Thumbnails results tab

2. Select a thumbnail to highlight the video on the Timeline.
3. Click **Step In**, or double-click the thumbnail to perform another search around the thumbnail.

   Click **Step Out** to return to the previous results page.

4. Click **Open In View** (after selecting a thumbnail) to open the recorded video in a new View.
5. Click **Change Search** to change the search criteria.

Export

You can export video in multiple video and image formats. The Export tab can be accessed from bookmark options, the Alarms tab, the New Task menu, and any Search tab.

You can also export snapshots of an image panel as you monitor video.

It is recommended that you export video of individual events and back up video for your archives. For more information, see **Backup**.

Exporting Native Video

The Native (AVE) format is the recommended format for exporting video. You can export video from multiple cameras in a single file, and the video maintains its original compression. AVE video is played in the Avigilon™ Control Center Player, where the video can be authenticated against tampering and re-exported to other formats.

If there is audio linked to the video, the audio is automatically included in the export.

If you are exporting a large amount of video for your records, back up the video instead. For more information, see **Backing Up Recorded Video On Demand**.

1. In the New Task menu, click  . The Export tab opens.

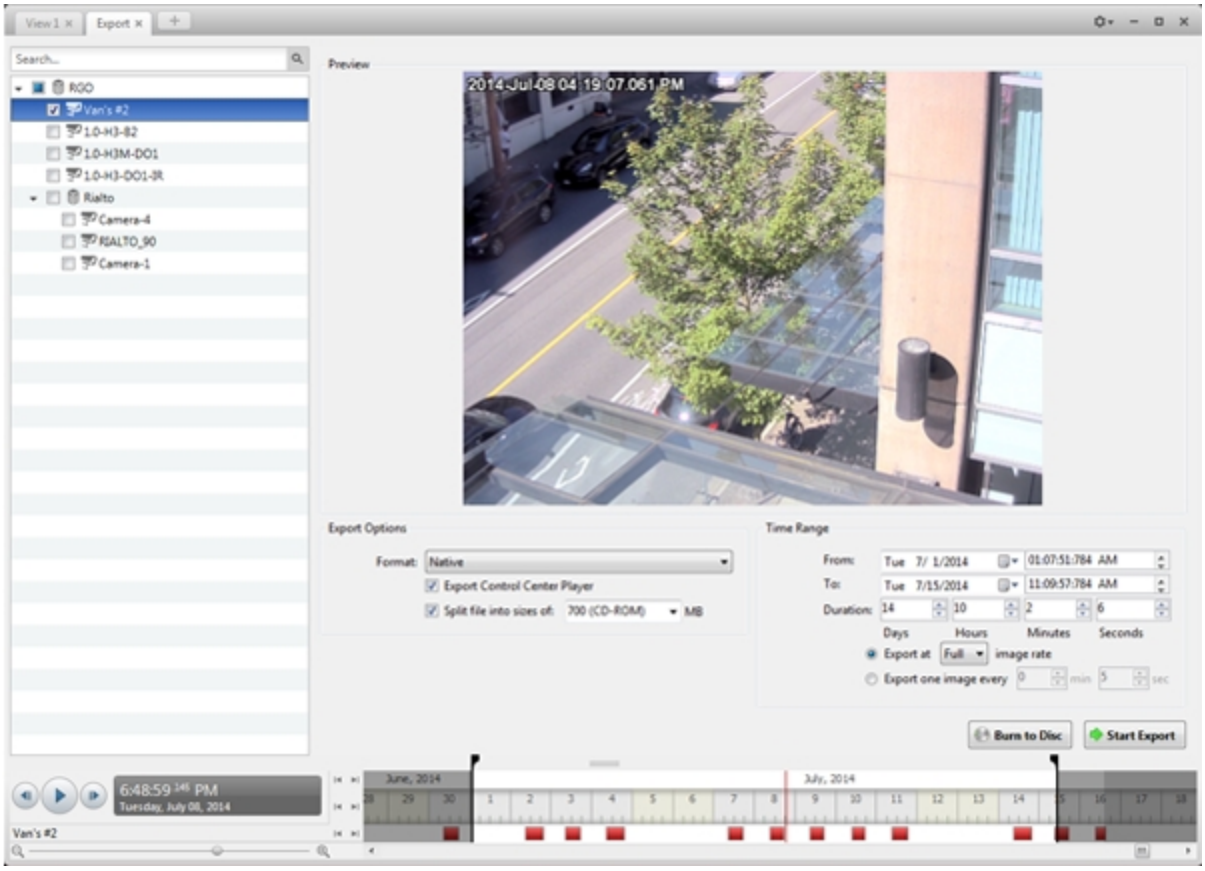


Figure 128: The Export tab for AVE export

2. In the **Format:** drop down list, select **Native**.
3. In the System Explorer, select the camera video you want to export.
4. To automatically divide the export into separate files, select the **Split file into sizes of:** check box, then select one of the options from the drop down list, or manually enter the size of each file in MB.

   This option allows you to export smaller files for storing in a flash drive or on optical media.

   This setting is automatically disabled if you choose to burn the export to disc because the system auto-detects the disc size.
5. Enter the **Time Range** you want to export. The **Time Range** is highlighted on the Timeline by black time range markers. You can also drag the time range markers to modify the time range.
6. Set the export image rate:

Option	Description
Export at _ image rate	Select this option to control how many images per second are exported. For example, the video is streaming at 30 images per second. If you select **1/2**, only

Option	Description
	15 images for that second will be exported.
Export one image every _ min _sec	Select this option to control the time between each exported video image. For example, if you enter *5* min. *0* sec., only one image will be exported for every 5 minutes of video.

7. Click one of the following:
   - **Start Export**: to save the file locally.
     - In the Save As dialog box, name the export file and click **Save**.
   - **Burn to Disc**: to burn the file directly to disc media.

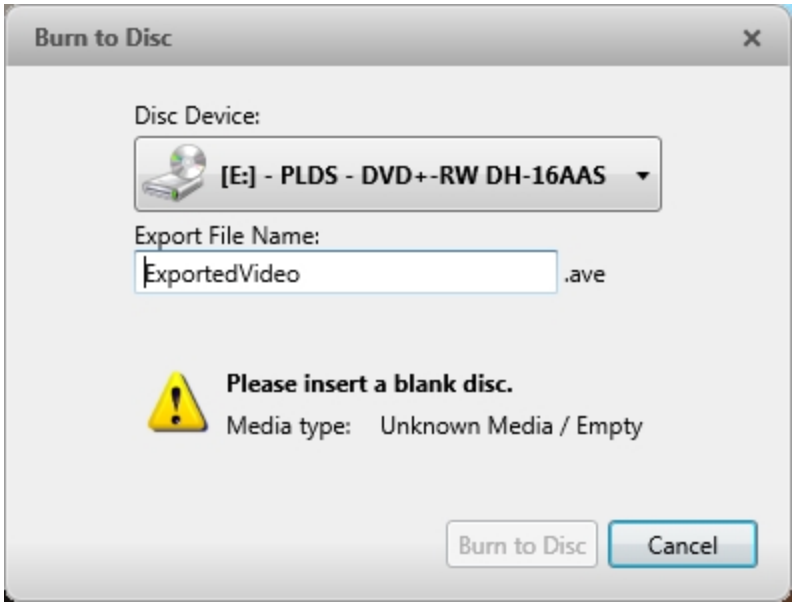


Figure 129: The Burn to Disc Dialog Box

   a. When the dialog box appears, insert a disc and select the media burning drive.
   b. Name the export file. The file name is automatically given a numbered suffix to help identify which file you are playing if the export spans multiple discs.
   c. Click **Burn to Disc** to start the export. If this button is disabled, the disc may be corrupt or full.
   d. Monitor the export progress to see if extra discs are required. When a disc is full, the export automatically pauses and you are asked to insert a new disc. After you insert a new disc, click **Resume Export**.

The number of discs required to export a video varies widely depending on the type of camera and disc used. Video is stored on the server with minimal compression to maximize the function of Avigilon's

HDSM™ technology, so the size of an export can be quite large due to the camera's high megapixel resolution and frame rate.

Generally, if you export a 2 minute video from a 2MP H.264 HD camera into AVE format, you will export a 93 MB file. To reduce the number of discs required, you can lower the frame rate or use a disc type with a larger capacity. Be aware that reducing the frame rate too much may cause the exported video to be jerky or missing data.

8. When the export is complete, click **OK**.

Exporting AVI Video

Video exported in Audio Video Interleave (AVI) format can be played in most media players. Be aware that you can only export one video at a time in this format.

If there is audio linked to the video, the audio is automatically included in the export.

1. In the New Task menu, click  . The Export tab opens.

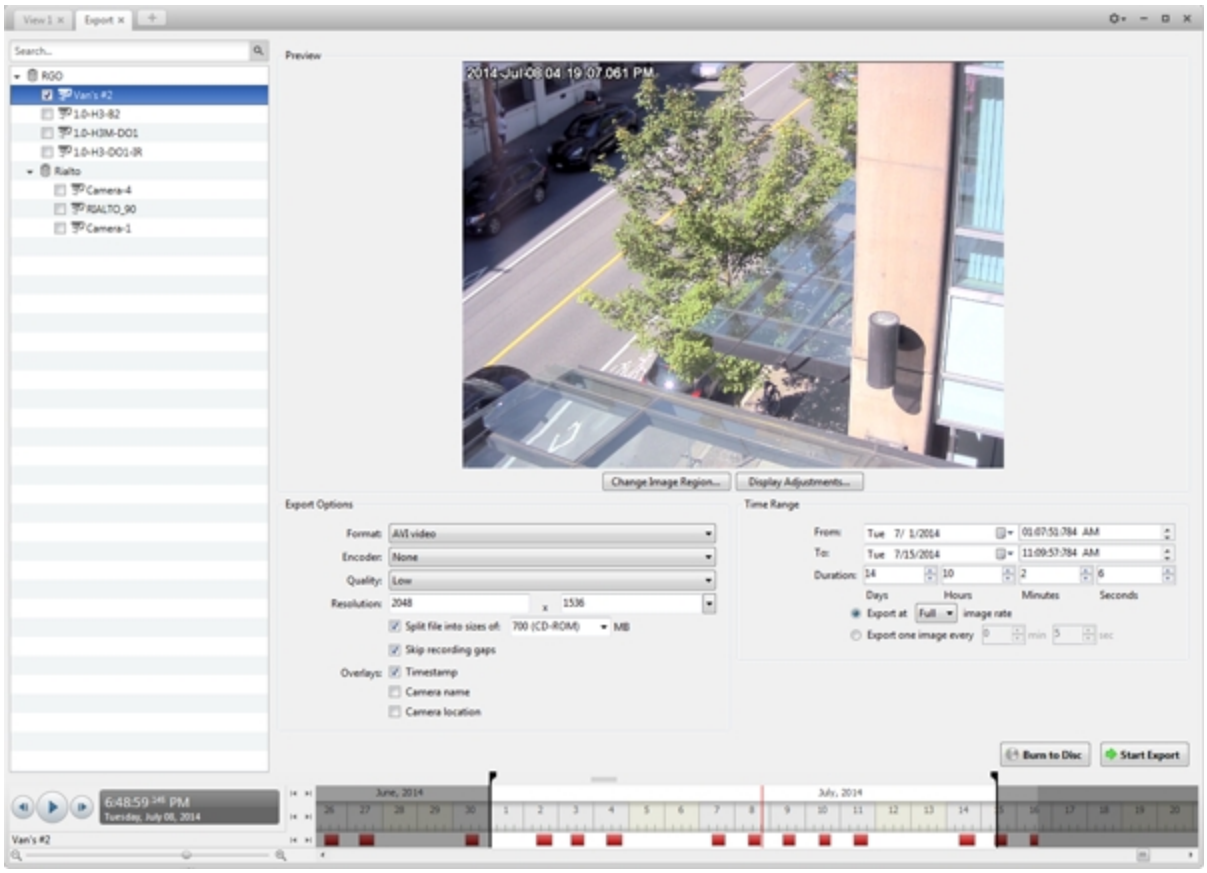


Figure 130: Export tab for AVI export

2. In the **Format:** drop down list, select **AVI video**.
3. In the System Explorer, select the camera video you want to export.
4. In the **Encoder:** field, select the compression used. The VC-1 (Windows Media Video) compression is

included by default because it is tailored for high-resolution AVI encoding.

If you are planning to burn the export to disc, it is important to select a compression method to help reduce the export size and maintain video quality.

5. In the **Quality:** drop down list, select the exported image quality level.
6. In the **Resolution:** field, select a resolution for the video image. You can manually enter the resolution or click the drop down arrow to select a standard resolution.

   NOTE: The Resolution: field automatically maintains the image aspect ratio.
7. To automatically divide the export into separate files, select the **Split file into sizes of:** check box, then select one of the options from the drop down list, or manually enter the size of each file in MB.

   This option allows you to export smaller files for storing in a flash drive or on optical media.

   This setting is automatically disabled if you choose to burn the export to disc because the system auto-detects the disc size.
8. Select the **Skip recording gaps** check box to avoid pauses in the video caused by gaps in the recording.
9. Select the image overlays you want: **Timestamp**, **Camera name**, and **Camera location**.

   Select the **Video Analytics Activity** overlay to include video analytics bounding boxes with the video. These boxes cannot be hidden or removed from the exported video.
10. Enter the **Time Range** you want to export. The **Time Range** is highlighted on the Timeline by black time range markers. You can also drag the time range markers to modify the time range.
11. Set the export image rate:

Option	Description
Export at _ image rate	Select this option to control how many images per second are exported. For example, the video is streaming at 30 images per second. If you select **1/2**, only 15 images for that second will be exported.
Export one image every _ min _sec	Select this option to control the time between each exported video image. For example, if you enter *5* min. *0* sec., only one image will be exported for every 5 minutes of video.

12. Click **Change Image Region...** to only export part of the video image. In the **Change Image Region...** dialog box, move and resize the green overlay to select the region you want to export, then click **OK**. Only areas highlighted in green will be exported.
13. Click **Display Adjustments...** to adjust the **Gamma:**, **Black Level:** and/or **White Level:**.
14. Click one of the following:

- **Start Export**: to save the file locally.
    - In the Save As dialog box, name the export file and click **Save**.
- **Burn to Disc**: to burn the file directly to disc media.

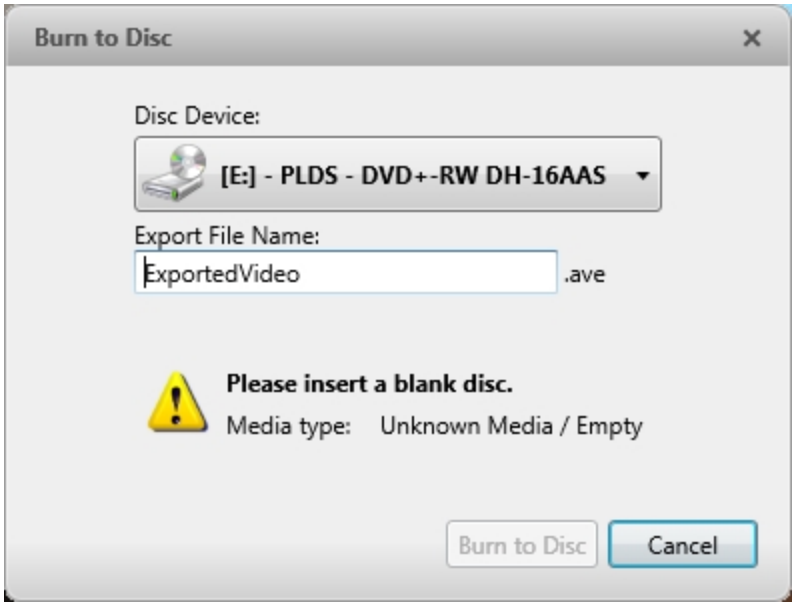


Figure 131: The Burn to Disc Dialog Box

a. When the dialog box appears, insert a disc and select the media burning drive.

b. Name the export file. The file name is automatically given a numbered suffix to help identify which file you are playing if the export spans multiple discs.

c. Click **Burn to Disc** to start the export. If this button is disabled, the disc may be corrupt or full.

d. Monitor the export progress to see if extra discs are required. When a disc is full, the export automatically pauses and you are asked to insert a new disc. After you insert a new disc, click **Resume Export**.

The number of discs required to export a video varies widely depending on the type of camera and disc used. Video is stored on the server with minimal compression to maximize the function of Avigilon's HDSM technology, so the size of an export can be quite large due to the camera's high megapixel resolution and frame rate.

Generally, if you export a 2 minute video from a 2MP H.264 HD camera into uncompressed AVI format, you will export a 2.7 GB file. If you select an **Encoder:** format and compress the video, you can export a 224 MB video at high quality. It is recommended that you always select an Encoder: format for AVI export to help significantly reduce the file size.

To further reduce the file size you can select a lower quality setting, lower the export frame rate, reduce the video resolution, or focus the export on a specific image region. Be aware that reducing each of the available settings too much may cause the export to be blurry or missing frames.

If it is important to have a high quality and full frame rate export, it is recommended that you use the AVE export format instead. AVE export intelligently compresses the video to create a smaller export file while

maintaining video data so that you can search, re-export video, and authenticate the video against tampering through the Avigilon Control Center Player software.

15. When the export is complete, click **OK**.

Exporting a Print Image

You can export a frame of video directly to your printer or as a PDF, and include notes related to the image.

To print a photo of the video you are currently watching, take a snapshot. For more information, see **Exporting a Snapshot of an Image**.

1. In the New Task menu, click  . The Export tab opens.

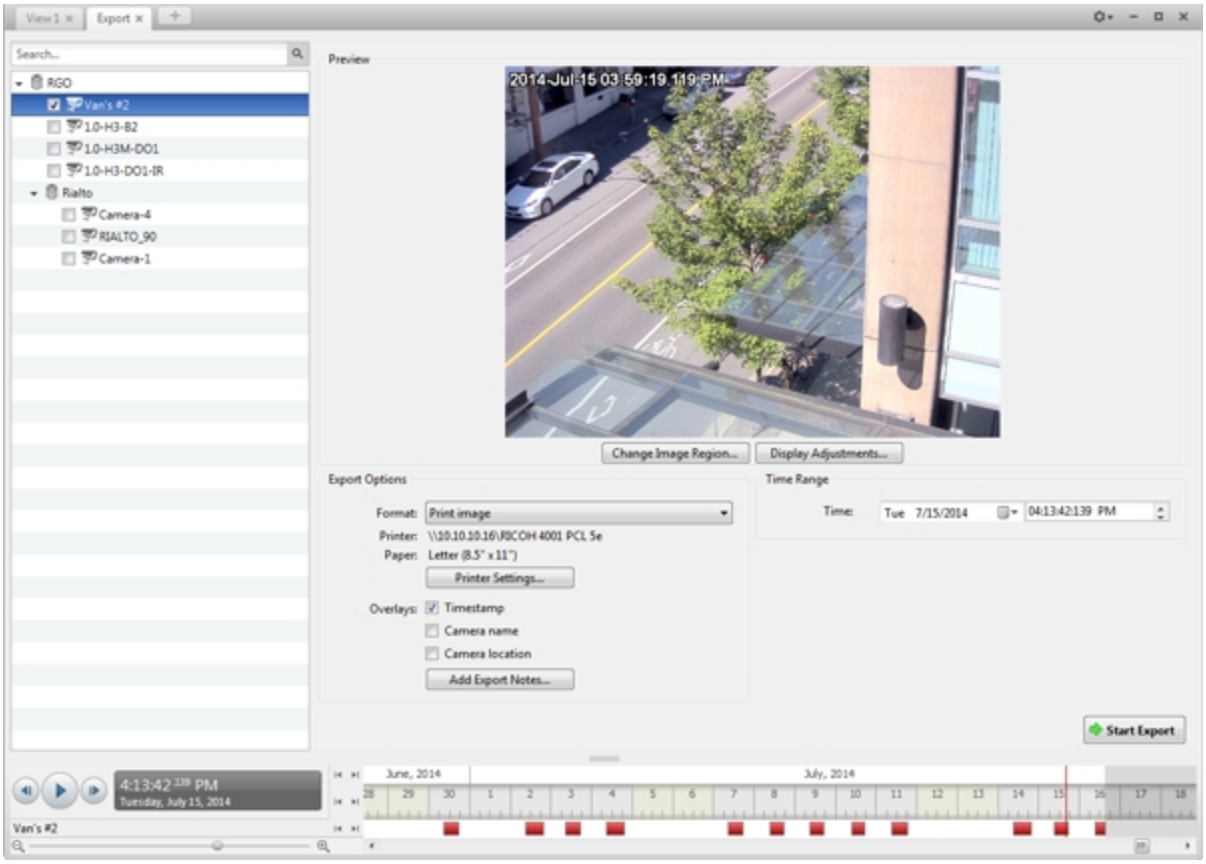


Figure 132: Export tab for print image export

2. In the **Format:** drop down list, select **Print image** or **PDF file**.
3. In the System Explorer, select the camera video you want to export.
4. (Print Image Only) Click **Printer Settings...** to change the printer and paper size that the image is printed on.
5. Select the image overlays you want: **Timestamp**, **Camera name**, and **Camera location**.

6. Click **Add Export Notes...** to add notes about the exported image. The notes are added below the image.
7. In the **Time Range** box, enter the exact date and time of the video image you want to export.
8. Click **Change Image Region...** to only export part of the video image. In the **Change Image Region...** dialog box, move and resize the green overlay to select the region you want to export, then click **OK**. Only areas highlighted in green will be exported.
9. Click **Display Adjustments...** to adjust the **Gamma:**, **Black Level:** and/or **White Level:**.
10. Click **Start Export**.
    - If you are exporting a Print image, the image is sent to the printer.
    - If you are exporting a PDF file, save the image.

    The Preview area displays the video you are exporting.
11. When the export is complete, click **OK**.

Exporting a Snapshot of an Image

You can export a snapshot of any image panel with video. When you export a snapshot, you are exporting what the image panel is currently displaying.

1. To export a snapshot, do one of the following:
    - In the image panel, click  .
    - Right-click the image panel and select **Save Snapshot**.

    The snapshot Export tab is opened, and the image you want to export is displayed.

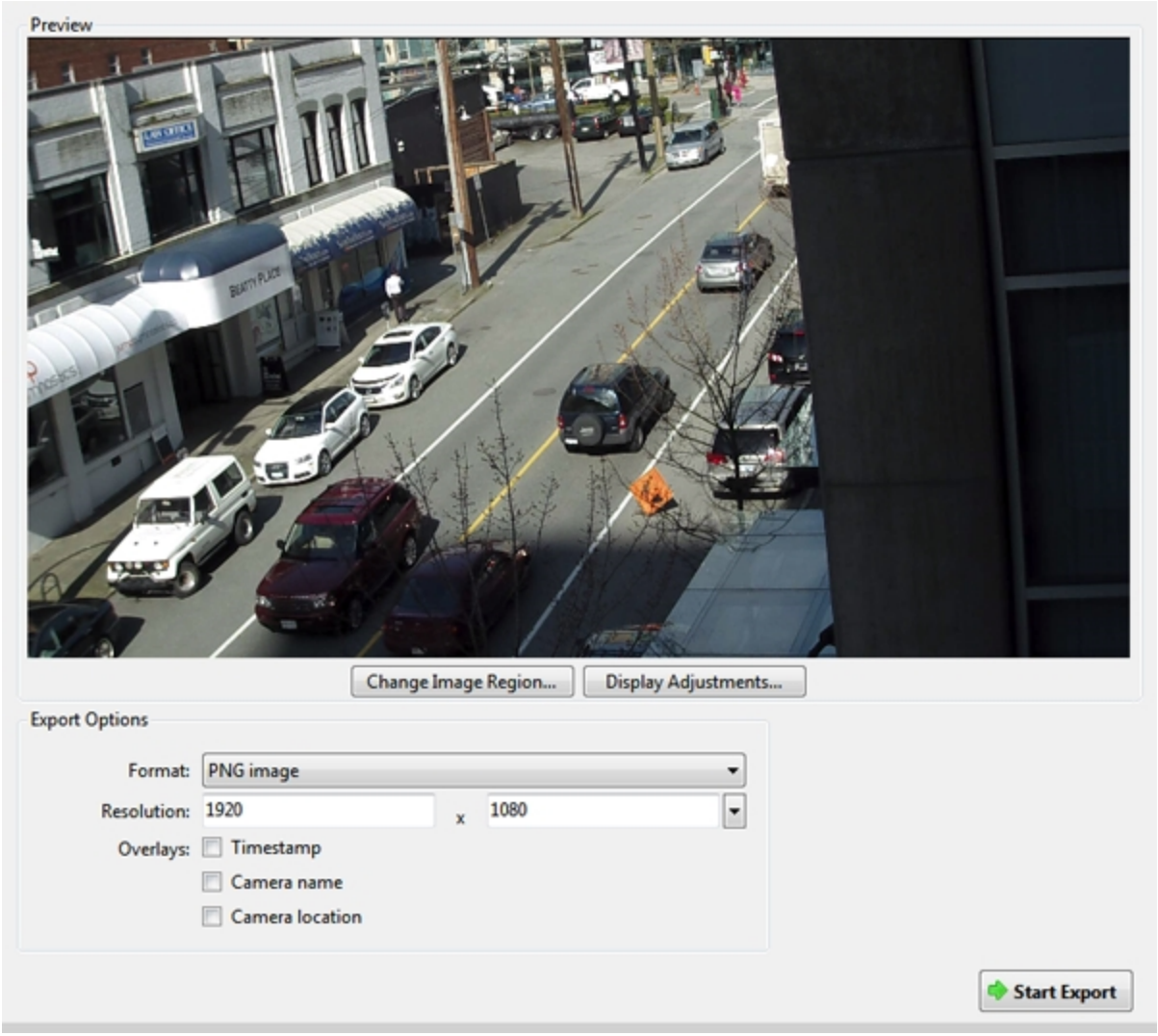


Figure 133: The Export tab for snapshot export

2. In the **Format:** drop down list, select an export format.
3. For the selected export format, define your preferences:

Format	Export options
Native **NOTE:** The Native format requires the Avigilon Control Center Player to view.	This is the recommended export format because the exported image maintains its original compression and can be authenticated against tampering in the Avigilon Control Center Player. • Select the **Export Control Center Player** check box if you want a copy of the Avigilon Control Center Player to be distributed with your Native image file.
PNG image	1. In the **Resolution:** field, select a resolution for the video image. You can manually enter the resolution or click the drop down arrow to select a standard resolution. **NOTE:** The Resolution: field automatically maintains the

Format	Export options
	image aspect ratio. 2. Select the image overlays you want: **Timestamp**, **Camera name**, and **Camera location**. 3. Click **Change Image Region...** to only export part of the video image. In the **Change Image Region** dialog box, move and resize the green overlay, then click **OK**. Only areas highlighted in green are exported. 4. Click **Display Adjustments...** to adjust the **Gamma:**, **Black Level:**, and/or **White Level:**.
JPEG image	1. In the **Quality:** drop down list, select the exported image quality level. 2. Set the image **Resolution:**. 3. Select the image overlays you want. 4. Click **Change Image Region...** to only export a part of the video image. 5. Click **Display Adjustments...** to modify the image quality.
TIFF image	1. Set the image **Resolution:**. 2. Select the image overlays you want. 3. Click **Change Image Region...** to only export a part of the video image. 4. Click **Display Adjustments...** to modify the image quality.
Print image	1. Click **Printer Settings...** to change the selected printer and paper size. 2. Select the image overlays you want. 3. Click **Add Export Notes...** to add notes about the exported image. The notes are printed below the image. 4. Click **Change Image Region...** to only export a part of the video image. 5. Click **Display Adjustments...** to modify the image quality.
PDF file	1. Select the image overlays you want. 2. Click **Add Export Notes...** to add notes about the exported image. 3. Click **Change Image Region...** to only export a part of the video image. 4. Click **Display Adjustments...** to modify the image quality.

4. Click **Start Export**.
5. In the Save As dialog box, name the export file and click **Save**. If you are printing the snapshot, the image is sent to your printer instead.

The Preview area displays the snapshot you are exporting.

6. When the export is complete, click **OK**.

Exporting Still Images

Video can be exported as a series of still PNG images, JPEG images, or TIFF images. When you export a series of still images, you are exporting each frame of video as an independent file.

If you only want one photo of the video you are watching, take a snapshot. For more information, see **Exporting a Snapshot of an Image**.

1. In the New Task menu, click  . The Export tab opens.

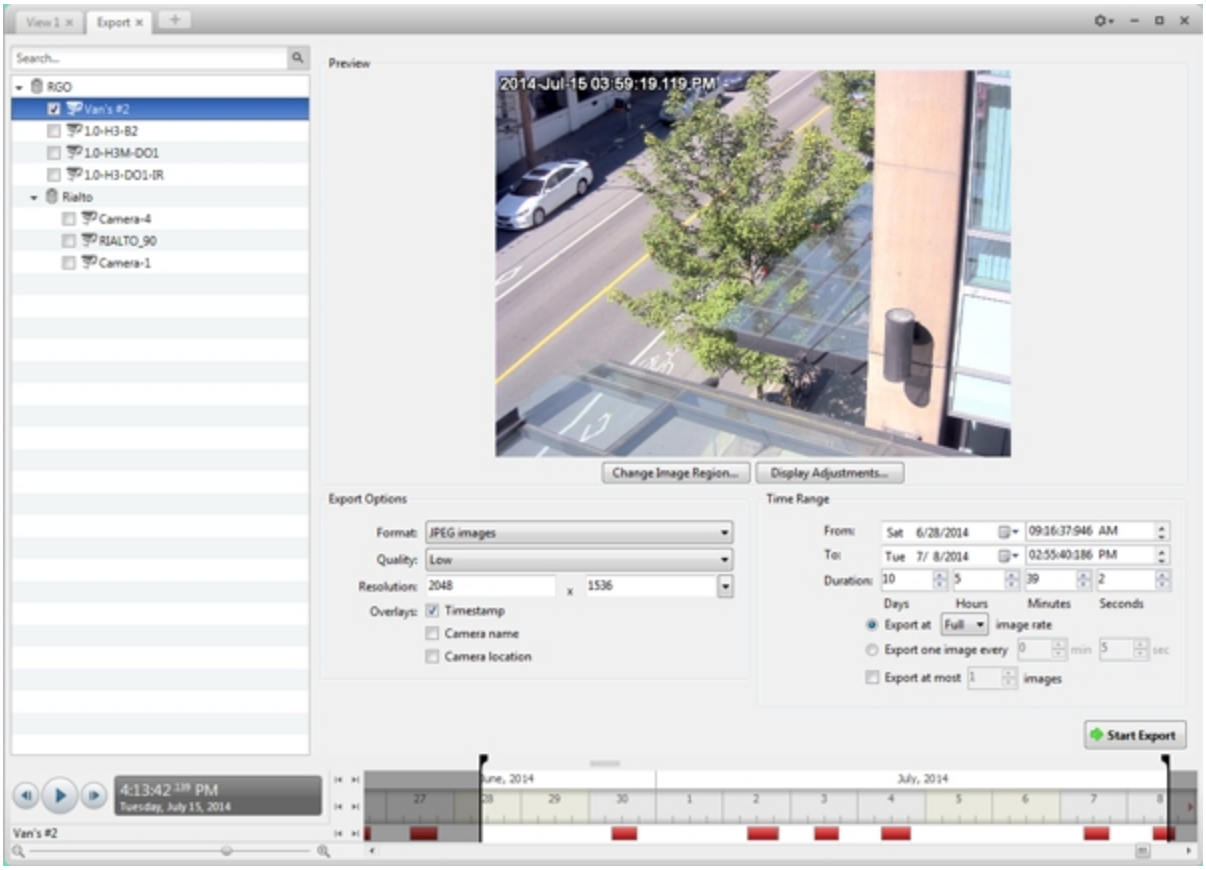


Figure 134: Export tab for still image export

2. In the **Format:** drop down list, select **PNG images**, **JPEG images**, or **TIFF images**.
3. In the System Explorer, select the camera video you want to export.
4. (JPEG only) In the **Quality:** drop down list, select the exported image quality level.
5. In the **Resolution:** field, select a resolution for the video image. You can manually enter the resolution or click the drop down arrow to select a standard resolution.

   NOTE: The Resolution: field automatically maintains the image aspect ratio.

6. Select the image overlays you want: **Timestamp**, **Camera name**, and **Camera location**.
7. Enter the **Time Range** you want to export. The **Time Range** is highlighted on the Timeline by black time range markers. You can also drag the time range markers to modify the time range.
8. Set the export image rate:

Option	Description
Export at _ image rate	Select this option to control how many images per second are exported. For example, the video is streaming at 30 images per second. If you select **1/2**, only 15 images for that second will be exported.
Export one image every _ min _sec	Select this option to control the time between each exported video image. For example, if you enter *5* min. *0* sec., only one image will be exported for every 5 minutes of video.

9. To limit the number of images that are exported, select the **Export at most _ images** check box and enter a number.
10. Click **Change Image Region...** to only export part of the video image. In the **Change Image Region...** dialog box, move and resize the green overlay to select the region you want to export, then click **OK**. Only areas highlighted in green will be exported.
11. Click **Display Adjustments...** to adjust the **Gamma:**, **Black Level:** and/or **White Level:**.
12. Click **Start Export**.
13. In the Save As dialog box, name the export file and click **Save**.

    The Preview area displays the video you are exporting.
14. When the export is complete, click **OK**.

Exporting WAV Audio

If you want to export audio with video, simply export the video in Native or AVI format. Any audio that is linked to the video is automatically included in the export file.

This procedure exports the audio alone.

1. In the New Task menu, click  . The Export tab opens.

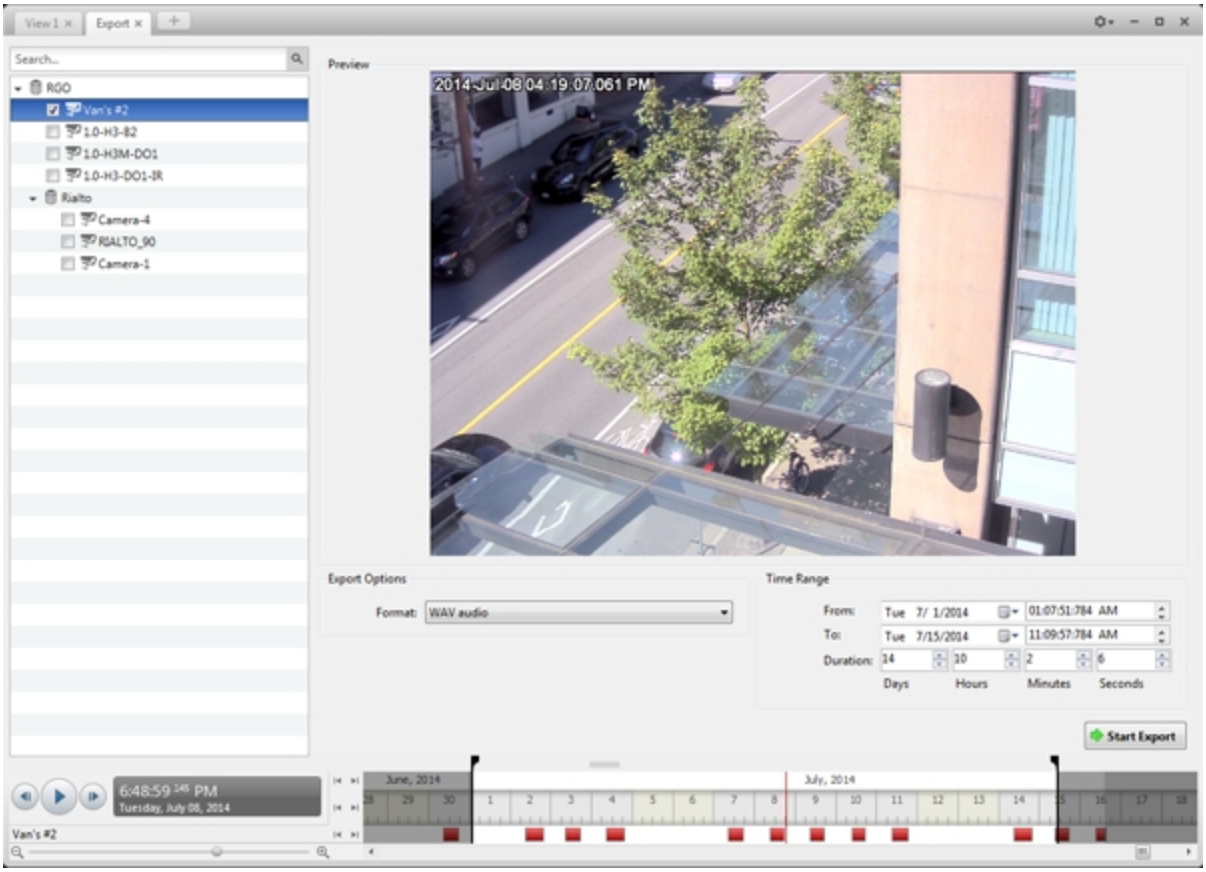


Figure 135: Export tab for audio export

2. In the **Format:** drop down list, select **WAV audio**.
3. In the System Explorer, select the camera that the audio is linked to.
4. Enter the **Time Range** you want to export. The **Time Range** is highlighted on the Timeline by black time range markers. You can also drag the time range markers to modify the time range.
5. Click **Start Export**.
6. In the Save As dialog box, name the export file and click **Save**.

   The Preview area displays the video linked to the audio you are exporting.
7. When the export is complete, click **OK**.

Backup

If you need to export a large amount of camera video, it is faster to back up the content into Avigilon Backup (AVK) format. AVK files can be opened in the Avigilon™ Control Center Player and re-exported as needed.

It is recommended that you export video of individual events and back up video for your archives. For more information, see **Export**.

In the Enterprise Edition of the software, you can set the system to back up files automatically on a schedule. For information about configuring automatic backup, see **Scheduled Backup**.

Backing Up Recorded Video On Demand

If you want a copy of the recorded video in your system, use the backup feature. Video is always backed up in Avigilon Backup (AVK) format. You can review the backed up video in the Avigilon Control Center Player.

If you want backups to occur automatically at a scheduled time, see **Scheduled Backup**. This feature is only available in the Enterprise Edition.

The backup files are stored in a backup folder set by the Avigilon™ Control Center Admin Tool. For information about changing the backup folder, see *The Avigilon Control Center Server User Guide*.

1. In the application window, click  >  .

   The Backup tab is displayed.

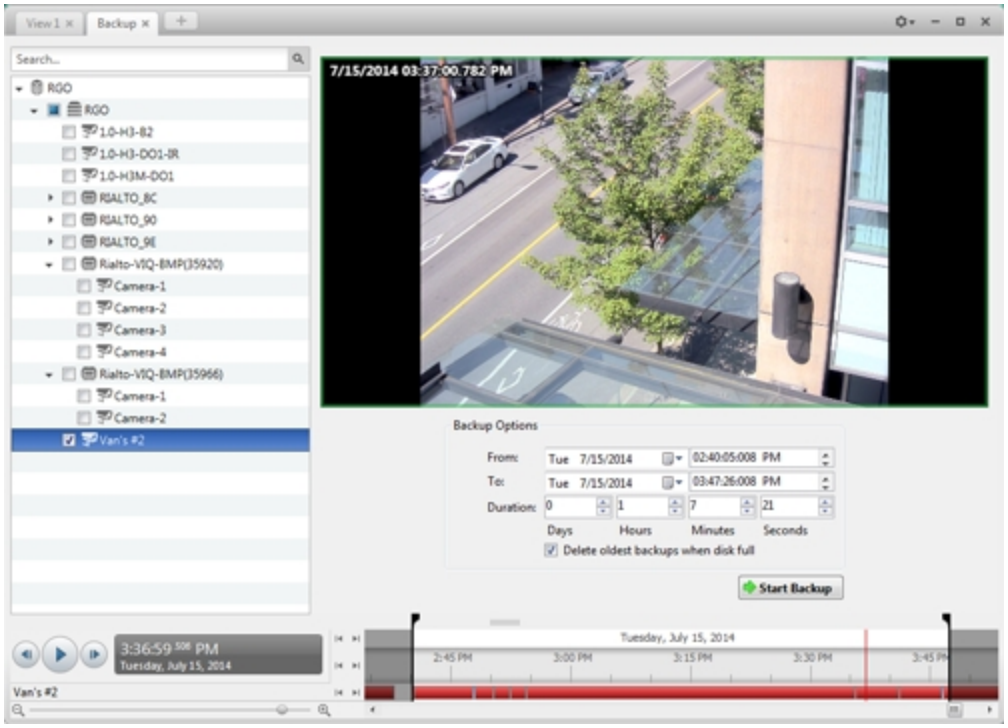


Figure 136: The Backup tab

2. In the System Explorer, select all the cameras you want to back up.
3. In the **Backup Options** area, set the time range you want to back up. The time range is highlighted on the Timeline by the black time range markers. You can also drag the time range markers to change the time range.
4. Select the **Delete oldest backups when disk full** check box to allow the application to automatically overwrite old backup files when the backup folder is full.
5. Click **Start Backup**.
6. When the backup is complete, click **OK**.

Appendix

Event and Trigger Descriptions

NOTE: Some features are not displayed if the server does not have the required license, or if you do not have the required user permissions.

In this section are descriptions of the options available in the Site setup when configuring Alarm triggers, Email Notification triggers, Group Permissions, and Rule Events and Actions.

Video Analytics Event Descriptions

The following table shows the Activity: options that can be used as triggers when configuring video analytics events. These triggers are based on the activity of detected classified objects.

NOTE: All events are reset when their duration reaches the specified Timeout: period.

For more information, see **Adding Video Analytics Events**.

Activity:	Description
Objects in area	The event is triggered when the specified Number of Objects: is detected in the region of interest. **NOTE:** Additional objects past the specified Number of Objects: that are detected in the region of interest will not trigger the event until it is reset. The event is reset when the Number of Objects: in the region of interest falls below the specified Number of Objects:.
Object loitering	The event is triggered after an object is detected in the selected region of interest for longer than the specified Threshold Time:. The event is reset when the object leaves the region of interest.
Objects crossing beam	The event is triggered when the specified Number of Objects: have crossed the beam that has been placed in the camera's field of view. The beam can be unidirectional or bidirectional. **NOTE:** Additional objects past the specified Number of Objects: that cross the beam will not trigger the event until it is reset. The event is reset when it times out.
Object appears or enters area	The event is triggered by each object that enters the region of interest. This event can be used to count objects.
Object not present in area	The event is triggered when no objects are present in the region of interest.
Objects enter area	The event is triggered when the specified Number of Objects: have entered the region of interest.
Objects leave area	The event is triggered when the specified Number of Objects: have left the region of interest.
Object stops in area	The event is triggered when an object in a region of interest stops moving for the specified Threshold Time:.

Activity:	Description
Direction violated	The event is triggered when an object moves in the direction specified by the Prohibited Direction: wheel in the Video Analytics Configuration dialog box.

Alarm Trigger Source Descriptions

The following table shows the Alarm Trigger Source: options that are available when you set up an alarm. For more information about setting up an alarm, see **Adding a New Alarm**.

Alarm Trigger Source:	Description
Motion Detection	The alarm is triggered when motion is detected by the selected cameras.
Video Analytics Event	The alarm is triggered when a video analytics event is detected by the selected cameras.
Digital Input Activation	The alarm is triggered when the selected digital inputs are activated.
License Plate Watchlist Match	The alarm is triggered when a license plate on the Watch List is detected.
POS Transaction Exception	The alarm is triggered when a POS transaction exception has occurred.
Camera Error	The alarm is triggered when a camera error occurs.
System Error	The alarm is triggered when a system error occurs.
External Software Event	The alarm is triggered by third party integration software.

Email Notification Trigger Descriptions

The following table shows the email notification trigger options that are available when you set up an email notification. For more information about setting up an email notification, see **Configuring Email Notifications**.

Email Notification Trigger	Description
System event	Email notifications are sent when one of the following rule events occurs: • Server application starting up • Server application shutting down • Server application terminated unexpectedly • Server application low on resources • Server application installation error • Server connection lost • Server hardware event • Connection created to standby server • Connection removed from standby server • Connection failure

Email Notification Trigger	Description
	• Connection restored • Network connection found • Network connection lost • Network packet loss acceptable • Network packet loss unacceptable • License expires soon • License expired • Database error • Data initialization error • Data volume size reduced • Data write error • Data upgrade started • Data upgrade completed • Data upgrade failed • Data volume failed • Data volume recovered • Data recovery started • Data recovery completed • Data recovery failed • Firmware upgrade failed • Recording interrupted • Recording resumed
Motion detected on _	An email notification is sent when camera motion detection has started. You can select the camera.
Digital input activated on _	An email notification is sent when a digital input has been activated. You can select the digital input.
POS transaction exception on _	An email notification is sent when a POS transaction exception occurs. You can select the transaction source.

Group Permission Descriptions

The following table shows the options that are available when you set up a permission group. For more information about setting up a permission group, see **Adding Groups**.

Group Permission		Description
View live images		Allows users to watch a camera's live video stream in a View.
	Use PTZ controls	Allows users to use a camera's PTZ controls.
	Lock PTZ controls	Allows users to lock a camera's PTZ controls.
	Trigger manual recording	Allows users to trigger manual recording while

Group Permission		Description
		watching video in a View.
	Trigger digital outputs	Allows users to trigger digital outputs while watching video in a View.
	Broadcast to speakers	Allows users to broadcast audio through speakers that are connected to a camera.
View recorded images		Allows users to watch a camera's recorded video in a View.
	Export images	Allows users to export recorded images.
	Backup images	Allows users to back up recorded images.
	Teach by example	Allows users to access the Teach By Example tab.
Manage saved views		Allows users to add and edit saved Views.
Manage maps		Allows users to add and edit maps.
Manage web pages		Allows users to add and edit web pages.
Manage virtual matrix monitors		Allows users to add and edit Virtual Matrix monitors.
Initiate collaboration sessions		Allows users to initiate collaboration sessions with other users on the same network.
Manage user sessions		Allows users to log other users out of the Site.
Listen to microphones		Allows users to listen to microphones that are connected to a camera.
Setup cameras		Allows users to configure cameras.
	Setup general settings	Allows users to edit a camera's General dialog box.
	Setup network settings	Allows users to edit the Network dialog box.
	Setup image and display settings	Allows users to edit the Image and Display dialog box.
	Setup compression and image rate settings	Allows users to edit the Compression and Image Rate dialog box.
	Setup image dimension settings	Allows users to edit the Image Dimensions dialog box.
	Setup motion detection settings	Allows users to edit the Motion Detection dialog box.
	Setup privacy zone settings	Allows users to edit the Privacy Zones dialog box.
	Setup manual recording settings	Allows users to edit the Manual Recording dialog box.
	Setup digital input & output settings	Allows users to edit the Digital Inputs and Outputs dialog box.

Group Permission		Description
	Setup microphone settings	Allows users to edit the Microphone dialog box.
	Setup speaker settings	Allows users to edit the Speaker dialog box.
	Setup analytics settings	Allows user to edit the Video Analytics Configuration dialog box.
Setup sites		Allows users to configure Sites.
	Setup name	Allows users to edit the Site name.
	Manage site	Allows users to add servers to the Site.
	Setup site view	Allows users to organize the order of cameras in the System Explorer.
	Setup user and group settings	Allows users to edit the Users and Groups dialog box.
	Setup Active Directory Synchronization	Allows users to set up Active Directory Synchronization.
	Setup corporate hierarchy	Allows users to edit the Edit Corporate Hierarchy dialog box.
	Setup alarm management settings	Allows users to edit the Alarms dialog box.
	Setup POS transaction settings	Allows users to edit the POS Transactions dialog box.
	Setup LPR settings	Allows users to edit the License Plate Recognition dialog box.
	Setup email settings	Allows users to edit the Email Notifications dialog box.
	Setup rule engine settings	Allows users to edit the Rules dialog box.
	View site logs	Allows users to view Site Logs.
	Connect and disconnect cameras	Allows users to connect and disconnect cameras to servers.
	Import and export settings	Allows users to import and export configuration settings.
	View Server Status	Allows users to see Server Status details.
Setup servers		Allows users to configure servers.
	Setup name	Allows users to edit the server name.
	Setup schedule settings	Allows users to edit the camera Recording Schedule .
	Setup recording and bandwidth settings	Allows users to edit the camera Recording and Bandwidth settings.
	Setup scheduled backup settings	Allows users to set up Scheduled Backup .

Rule Event and Action Descriptions

The following tables describe the trigger events and actions that are available when you set up a rule. For more information about setting up a rule, see **Adding a Rule**.

Rule Events

Rule events are the events that trigger a rule.

Rule Events		Description
Server Events		
	Server application starting up	The server software starts up.
	Server application shutting down	The server software shuts down.
	Server application terminated unexpectedly	The server software shuts down unexpectedly.
	Server application low on resources	The server software is low on memory or storage.
	Server application installation error	The server software was installed incorrectly.
	License expires soon	The server software license expires soon.
	License expired	The server software license has expired.
	Database error	The server database has generated an error.
	Data initialization error	The server database has generated an error during initialization.
	Data volume failed	The server data volume has failed.
	Data volume recovered	The server data volume was recovered.
	Data volume size reduced	The server data volume size was reduced.
	Data write error	The server generated an error while writing data.
	Data upgrade started	A server data upgrade has started.
	Data upgrade completed	A server data upgrade has completed.
	Data upgrade failed	A server data upgrade has failed.
	Data recovery started	Server data recovery has started.
	Data recovery completed	Server data recovery has completed.
	Data recovery failed	Server data recovery has failed.
	Bookmark save failed	A bookmark failed to save.
	Network connection found	The server network connection was found.
	Network connection lost	The server network connection was lost.
	Email send error	An error was generated while sending an email notification.
	Server hardware event	A server hardware error has occurred.
	Backup started	Server backup has started.
	Backup completed	Server backup has completed.
	Backup failed	Server backup has failed.

Rule Events		Description
	Server connection lost	The server connection to the Site was lost.
Device Events		
	Connection created	A camera or device has connected to a server.
	Connection removed	A camera or device has disconnected from a server.
	Connection created to standby server	A camera or device has connected to a standby server.
	Connection removed from standby server	A camera or device has disconnected from a standby server.
	Connection failure	A camera or device connection has failed.
	Connection restored	A camera or device connection has been restored.
	Network packet loss unacceptable	A camera or device network packet loss is unacceptable.
	Network packet loss acceptable	A camera or device network packet loss is acceptable.
	Motion detection started	Motion detection has started on a camera.
	Motion detection ended	Motion detection has ended on a camera.
	Video analytics event started	A video analytics event has started.
	Video analytics event ended	A video analytics event has ended.
	Tampering detected	Tampering with a camera has been detected.
	Recording started	A camera or device recording has started.
	Recording ended	A camera or device recording has ended.
	Recording interrupted	A camera or device recording was interrupted.
	Recording resumed	A camera or device recording has resumed.
	Digital input activated	A camera or device digital input was activated.
	Digital input deactivated	A camera or device digital input was deactivated.
	Firmware upgrade started	A camera or device firmware upgrade has started.
	Firmware upgrade completed	A camera or device firmware upgrade has been completed.
	Firmware upgrade failed	A camera or device firmware upgrade has failed.
User Events		
	User login	A user has logged in.
	User logout	A user has logged out.
	Server setting changed	A user has changed the server settings.
	Site setting changed	A user has changed the Site settings.
	Device setting changed	A user has changed the camera or device

Rule Events		Description
		settings.
	Device connected	A user has connected a camera or device to a server.
	Device disconnected	A user has disconnected a camera or device from a server.
	Digital output triggered	A user has manually triggered a digital output.
	Bookmark added	A user has added a bookmark.
	Bookmark updated	A user has updated a bookmark.
	Bookmark deleted	A user has deleted a bookmark.
	PTZ moved	A user has moved a PTZ camera.
	PTZ idle	A user has left a PTZ camera idle.
	Export performed	A user has performed a video export.
	Speaker activated	A user is broadcasting audio through camera or device speakers.
	Speaker deactivated	A user has stopped broadcasting audio.
	Virtual matrix monitor opened	A user has opened a Virtual Matrix monitor in the View.
	Map added	A user has added a new map.
	Map updated	A user has updated a map.
	Map deleted	A user has deleted a map.
	View added	A user has added a saved View.
	View updated	A user has updated a saved View.
	View deleted	A user has deleted a saved View.
	Web Page added	A user has added a new web page.
	Web Page updated	A user has updated a web page.
	Web Page deleted	A user has deleted a web page.
	Site View updated	A user has updated the way cameras are organized in the System Explorer.
	Custom keyboard command triggered	A user has triggered a custom keyboard command.
Alarm Events		
	Alarm acknowledged	An alarm has been acknowledged.
	Alarm auto acknowledged	An alarm has been acknowledged automatically.
	Alarm triggered	An alarm has been triggered.
	Alarm assigned	An alarm has been assigned to a user.
	Alarm unassigned	An alarm has been unassigned from a user.
	Alarm purged	An alarm has been purged.

Rule Events		Description
POS Transaction Events		
	POS transaction started	A POS transaction has started.
	POS transaction ended	A POS transaction has ended.
	POS transaction exception	A POS transaction exception has occurred.
License Plate Recognition Events		
	License plate detection started	License plate detection has started.
	License plate detection ended	License plate detection has ended.
	License plate watchlist match	A license plate on the LPR Watch List has been detected.

Rule Actions

Rule actions are the response to a rule event.

Rule Actions		Description
User Notification Actions		
	Display on-screen message	An on-screen message is displayed about the rule event.
	Send email	An email notification is sent about the rule event to the selected recipient(s).
	Play a sound	A notification sound is played within the Client when the rule event occurs.
Monitoring Actions		
	Start live streaming	The linked live video stream is displayed when the rule event occurs.
	Create Bookmark	The recorded video of the rule event is bookmarked.
	Open a saved view	The selected saved View is automatically displayed.
	Start live streaming on a virtual matrix monitor	The live stream from the selected camera is automatically displayed on the selected Virtual Matrix monitor.
	Open a map on a virtual matrix monitor	The selected map is automatically displayed on the selected Virtual Matrix monitor.
	Open a web page on a virtual matrix monitor	The selected web page is automatically displayed on the selected Virtual Matrix monitor.
Device Actions		
	Reboot camera	The camera or device reboots when the rule event occurs.
	Trigger digital output	A digital output is triggered when the rule event occurs.

Rule Actions		Description
PTZ Actions		
	Go to Preset	The selected PTZ camera(s) moves to the selected preset position when the rule event occurs.
	Run a Pattern	The selected PTZ camera(s) runs a selected pattern when the rule event occurs.
	Set Auxiliary	The selected PTZ camera(s) starts the selected auxiliary command when the rule event occurs.
	Clear Auxiliary	The selected PTZ camera(s) ends the selected auxiliary command when the rule event occurs.
Alarm Actions		
	Trigger an alarm	An alarm is triggered when the rule event occurs.
	Acknowledge an alarm	An alarm is acknowledged when the rule event occurs.

Updating the Client Software

Avigilon™ Control Center Client software updates are typically included with the Avigilon™ Control Center Server update packages. When you first open the Client software, the following dialog box will appear if a Client software update is available:

Figure 137: The Update Control Center Client dialog box

- Click **Update** to allow the Client software to update. The software update is automatically downloaded. The following dialog box will appear to show the download progress:

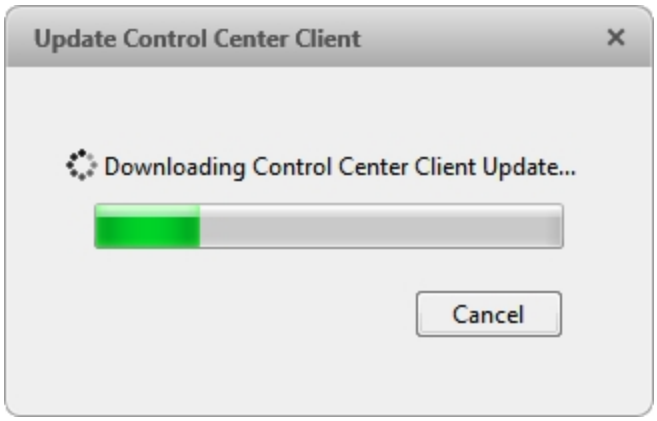


Figure 138: The Update Progress dialog box

When the update has finished downloading, click **Update Control Center Client**. When the installation wizard appears, follow the prompts to complete the update.

- Click **Do Not Update** to continue working with the Client software without updating. The Client software will not be updated, and you can continue working with the software as before.

The Client software can also be downloaded from the Software Updates & Downloads page of the Avigilon website: http://avigilon.com/support-and-downloads/for-software/software-updates-and-downloads/

Updating the Help Files

The help files for the Control Center Client software and Virtual Matrix software are all stored with the Control Center Server application.

If one of these components is ever updated before the others, the help files may become out of date or describe features that are not currently supported by your system.

- If the help files become out of date, download and install the latest help files from the Avigilon website. The help files are available in different installer packages divided by language and related software components.
- If the help files describe a feature that is not currently supported by your copy of the software, upgrade to the latest version.

Accessing the Control Center Web Client

You have the option of accessing cameras in your Site through the Web Client. The Web Client is a simplified version of the Client software. It allows you to monitor your surveillance system, search for video events and export recorded video outside the Client software.

NOTE: You cannot modify any system settings through the Control Center Web Client.

To access the Web Client, you need the IP address and port number of the server in your Site. The IP address is listed in the server's Setup tab in the Avigilon Control Center Client. The port number can be found in the Admin Tool under **Settings > Network**.

If you are running a multi-server Site, you only need to access one of the servers in your Site to have access to all the available cameras.

1. To access the Web Client, open Internet Explorer (version 6+) and enter the address of your Web Client in the following format:

   http://*<server ip address>*:*<port number>*/

   (For example, http://192.168.2.62:38880/)

   If you have not accessed the Web Client before, you may be prompted to install the required plug-in software before the Web Client will open.

2. When the login screen appears, enter your username and password for the Site.

The Web Client will open in your browser, and you can access the video and cameras that are connected to the server.

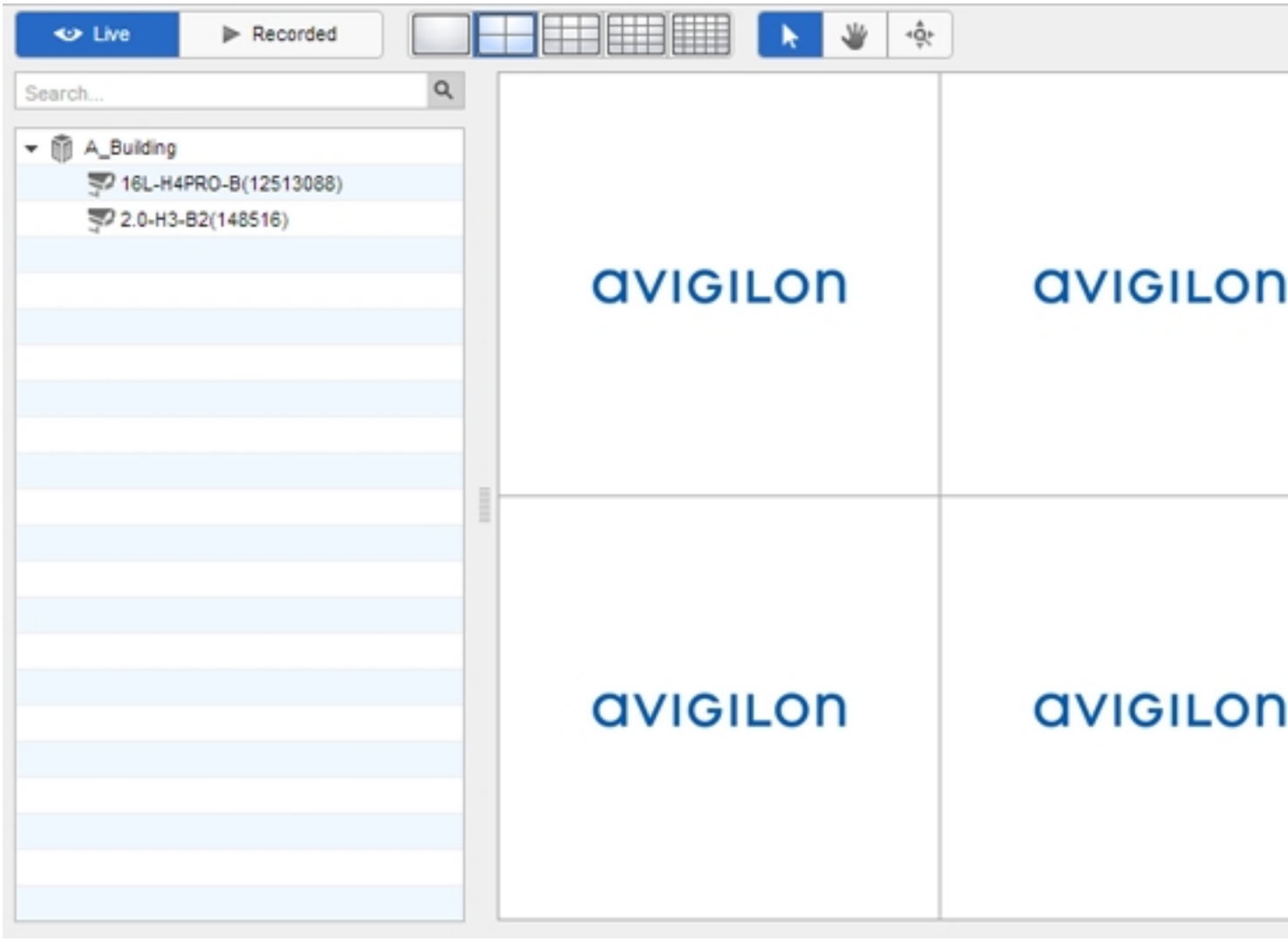


Figure 139: The Avigilon Control Center Web Client

Supported License Plates

The following license plates are currently supported by the Avigilon Control Center License Plate Recognition (LPR) feature. If the license plate format you need is not listed, you can email Avigilon Technical Support at **support@avigilon.com** and request an LPR Font Template.

To configure one of the following license plates for LPR, see **License Plate Recognition**.

- Africa
    - Morocco
    - South Africa
- Asia
    - China
    - Pakistan
    - Singapore
    - South Korea
    - Thailand
- Australia
- Europe
    - Belarus
    - Belgium
    - Bulgaria
    - Croatia
    - Estonia
    - France
    - Germany
    - Hungary
    - Ireland
    - Italy
    - Netherlands
    - Poland
    - Portugal
    - Romania
    - Spain

- Switzerland
- United Kingdom
- BE-DE-NL
- BG-DE
- BG-DE-RO
- HRV-DEU-HUN-ITA
- UK-IE
- UK-FR

- Middle East
  - Bahrain
  - Dubai
  - Israel
  - Jordan
  - Kuwait
  - Lebanon
  - Qatar
  - Saudi Arabia
- New Zealand
- North America
  - Canada
    - British Columbia
    - New Brunswick
    - Ontario
    - Quebec
  - Mexico
  - USA
    - Alaska
    - Arizona
    - California
    - Florida

- Illinois
- Indiana
- Kansas
- Louisiana
- Massachusetts
- Michigan
- Minnesota
- Missouri
- Montana
- New Hampshire
- New Jersey
- New Mexico
- New York
- North Carolina
- Ohio
- Pennsylvania
- South Carolina
- Texas
- Utah
- Virginia
- Washington
- Wisconsin
- Wyoming
- AZ-CA
- MI-IN-OH
- NY-VA-MD
- MO-KS
- MT-WY
- NC-VA-MD
- NY-NJ

- Russia

- South America
  - Argentina
  - Brazil
  - Chile

Reporting Bugs

If an error occurs in the Avigilon Control Center, you can contact Avigilon Technical Support at support@avigilon.com or +1.888.281.5182 option 1.

To help diagnose your problem, the Avigilon Technical Support team may ask you to provide a System Bug Report. The System Bug Report is a zip file generated by the Avigilon Control Center Client software that contains the system log and error reports for each of the servers that you can access.

To generate a System Bug Report:

1. Select > **System Bug Report...**.
2. When the Download System Bug Report dialog box appears, click **Download**.
3. In the Save As dialog box, name the file and click **Save**.
4. Once the System Bug Report has downloaded successfully, click **Close**.

Keyboard Commands

Use any of the keyboard commands below to help you navigate the Avigilon™ Control Center Client software.

The Key Combination column shows the commands used on a standard keyboard, while the Keypad Combination column shows the commands used on an Avigilon USB Professional Joystick Keyboard.

NOTE: Some features are not displayed if the server does not have the required license, or if you do not have the required user permissions.

Image Panel & Camera Commands

Command	Key Combination	Keypad Combination (Image Panel buttons)
Select an image panel Image panel # is displayed after pressing the first key.	* + <*image panel #*> + Enter	SELECT + <*image panel #*> + ENTER
Add a camera to the View The camera's ***logical ID*** is required.	/ + <*logical ID*> + Enter	CAMERA + <*logical ID*> + ENTER
Select the next image panel	Tab	
Select the previous image	Shift + Tab	

Command	Key Combination	Keypad Combination (Image Panel buttons)
panel		
Clear image panel selection	* + 0 + Enter	
Remove camera from the selected image panel	Backspace	
Maximize/Restore the selected image panel	Ctrl + E	
Replay 30 seconds	Ctrl + ,	
Replay 60 seconds	Ctrl + .	
Replay 90 seconds	Ctrl + /	
Add a bookmark for selected camera **NOTE:** For recorded video only.	Ctrl + B	
Start/Stop manual recording for the selected camera	R	
Activate/Mute audio for the selected camera	A	
Broadcast audio	S Hold to speak. Release to stop broadcasting.	 Hold to speak. Release to stop broadcasting.
Take a snapshot of the selected image panel	F4	
Display linked POS transaction source/camera	Ctrl + I	
Enable digital output	K	
Acknowledge the alarm currently displayed in an armed image panel	L	
Trigger custom keyboard command	Ctrl + K	

View Tab Commands

Command	Key Combination	Keypad Combination (View buttons)
Select the next View	Ctrl + Tab	NEXT 2
Select the previous View	Ctrl + Shift + Tab	PREV 1
Jump to View #_	Ctrl + 1 to 9	
Start/Stop cycle Views	Ctrl + Y	CYCLE
Open a new View	Ctrl + T	
Close current View	Ctrl + W	CLOSE 6
Open a new window	Ctrl + N	
Switch current View to display live video	Ctrl + L	LIVE
Switch current View to display recorded video	Ctrl + P	RECORDED
Remove all cameras from the current View	Ctrl + Backspace	
Full screen a View/End full screen	F11	FULLSCREEN
Open a saved View The saved View's ***logical ID*** is required.	Ctrl + G + *<logical ID>*	OPEN 3 + *<logical ID>* + ENTER
Open a Virtual Matrix monitor The Virtual Matrix monitor's ***logical ID*** is required.	Ctrl + G + *<logical ID>*	OPEN 3 + *<logical ID>* + ENTER

View Layout Commands

NOTE: Customized View layouts are linked to their position in the Layouts list. For example, if your custom layout is placed at the top of the Layouts list, you can use the keyboard command for layout 1 to select the custom layout.

Command	Key Combination	Keypad Combination (View buttons)
Change to layout 1	Alt + 1	LAYOUT 4 + PREV 1
Change to layout 2	Alt + 2	LAYOUT 4 + NEXT 2
Change to layout 3	Alt + 3	LAYOUT 4 + OPEN 3
Change to layout 4	Alt + 4	LAYOUT 4 + LAYOUT 4

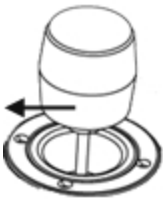
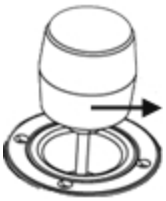
Command	Key Combination	Keypad Combination (View buttons)
Change to layout 5	Alt + 5	LAYOUT 4 + 5
Change to layout 6	Alt + 6	LAYOUT 4 + CLOSE 6
Change to layout 7	Alt + 7	LAYOUT 4 + 7
Change to layout 8	Alt + 8	LAYOUT 4 + 8
Change to layout 9	Alt + 9	LAYOUT 4 + 9
Change to layout 10	Alt + 0	LAYOUT 4 + 0
Change to next layout	Alt +]	
Change to previous layout	Alt + [	

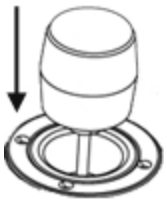
Playback Commands

Command	Key Combination	Keypad Combination (Timeline buttons)
Play/Pause video playback	Spacebar	
Increase playback speed	Page Up	
Decrease playback speed	Page Down	
Step to next frame	Shift + →	
Step to previous frame	Shift + ←	
Go to next event	Alt + →	
Go to previous event	Alt + ←	
Go forward one second	Ctrl + →	
Go forward five seconds	Ctrl + Shift + →	
Go backward one second	Ctrl + ←	
Go backward five seconds	Ctrl + Shift + ←	
Zoom in on the Timeline	Ctrl + Alt + +	
Zoom out on the Timeline	Ctrl + Alt + –	
Scroll forward on the Timeline	Ctrl + Alt + →	

Command	Key Combination	Keypad Combination (Timeline buttons)
Scroll backward on the Timeline	Ctrl + Alt + ←	
Move the Timeline marker forward		
Move the Timeline marker backward		
Go to the start of the Timeline	Ctrl + Alt + Home	
Go to the end of the Timeline	Ctrl + Alt + End	
Center the Timeline on the time marker	Ctrl + C	

PTZ Commands (Digital and Mechanical)

Command	Key Combination	Keypad Combination (PTZ buttons)
Toggle PTZ controls	Ctrl + D	
Zoom in	+	
Zoom out	–	
Pan center	←	
Pan right	→	

Command	Key Combination	Keypad Combination (PTZ buttons)
Tilt up	↑	
Tilt down	↓	
Open iris	Home	
Close iris	End	
Focus near	Insert	
Focus far	Delete	
PTZ menu left	←	
PTZ menu right	→	
PTZ menu up	↑	
PTZ menu down	↓	
Activate preset	Q + *<Preset #>*	PRESET + *<Preset #>* + ENTER
Run pattern		PATTERN + *<Pattern #>* + ENTER
Start auxiliary	W + *<Aux #>*	START + *<Aux #>* + ENTER
Stop auxiliary	E + *<Aux #>*	STOP + *<Aux #>* + ENTER

This Page Left Intentionally Blank

Avigilon™ Control Center Player User Guide

Version 5.4.2

Avigilon Corporation
http://www.avigilon.com

Revised: 2014-12-09

PDF-PLAYER5-E-Rev1

Table of Contents

What is the Avigilon Control Center Player?

The Avigilon Control Center Player is the video player for Avigilon Native Video Export (AVE) files and Avigilon Backup (AVK) files.

The Player displays video in image panels, and allows you to control their playback through the Timeline. The Player is able to authenticate video files against tampering, and can be used to re-export video into other formats. Both AVE and AVK video include event data embedded in the file, so you are also able to search for specific alarms, POS transactions, and other events that are linked to the video.

A copy of the Player can be downloaded from the Avigilon website, or exported with the AVE file from the Avigilon Control Center Client software (see *The Avigilon Control Center Client User Guide* for more information).

For More Information

Visit Avigilon at **http://www.avigilon.com/** for additional product documentation.

The Avigilon Training Center

The Avigilon Training Center provides free online training videos that demonstrate how to set up and use the Avigilon Surveillance System. Register online at the Avigilon Partner Portal site to begin: **http://avigilon.force.com/login**

Support

For additional support information, visit **http://avigilon.com/support-and-downloads/**. The Avigilon Partner Portal also provides self-directed support resources - register and login at **http://avigilon.force.com/login**.

Regular Avigilon Technical Support is available Monday to Friday from 12:00 a.m. to 6:00 p.m. Pacific Standard Time (PST):

- North America: +1.888.281.5182 option 1
- International: +800.4567.8988 or +1.604.629.5182 option 1

Emergency Technical Support is available 24/7:

- North America: +1.888.281.5182 option 1 then dial 9
- International: +800.4567.8988 or +1.604.629.5182 option 1 then dial 9

E-mails can be sent to: **support@avigilon.com**.

Upgrades

Software and firmware upgrades will be made available for download as they become available. Check **http://avigilon.com/support-and-downloads/** for available upgrades.

Feedback

We value your feedback. Please send any comments on our products and services to **feedback@avigilon.com**

Starting Up and Shutting Down the Avigilon Control Center Player

The Avigilon Control Center Player can be started up or shut down at any time.

Starting Up the Player

The Player can be opened in any of the following ways:

- Double-click the  shortcut icon on the desktop.
- In Windows, select **All Programs** or **All Apps > Avigilon > Avigilon Control Center Player > Avigilon Control Center Player**.

When the application first opens, you will be prompted to open an AVE or AVK file.

- Double-click an Avigilon Native Video Export (AVE) file or Avigilon Backup (AVK) file. The Player will open and display the video file.

Shutting Down the Player

- In the Avigilon Control Center Player software, select  > **Exit**.

Authenticating Video

All Avigilon Native Video Export (AVE) and Avigilon Backup (AVK) files contain an encrypted digital signature that is used to confirm that exported images have not been tampered with.

- To authenticate a video, select > **Authenticate Images...**.

  The Authenticate Images dialog box appears and displays the progress as the application checks all the video images for tampering.

When the process is complete, the Authenticate Images dialog box displays the number of images that are authentic and the number of images that have been corrupted.

Figure 1: The Authenticate Images dialog box

What are Views?

A View tab is where you watch camera video. Inside the View tab is a set of image panels that allows you to organize how video is displayed.

You can arrange image panels into different layouts to take advantage of different camera angles and save View layouts that you like.

Making a View Full Screen

You can maximize a View to fill an entire monitor screen.

- On the toolbar, click  .

Ending Full Screen Mode

- While the View is in full screen mode, click  .

Selecting a Layout for a View

You can organize how video is displayed by selecting a View layout. The figure below shows the default View layouts.

- On the toolbar, select  , then select one of the following layout options.

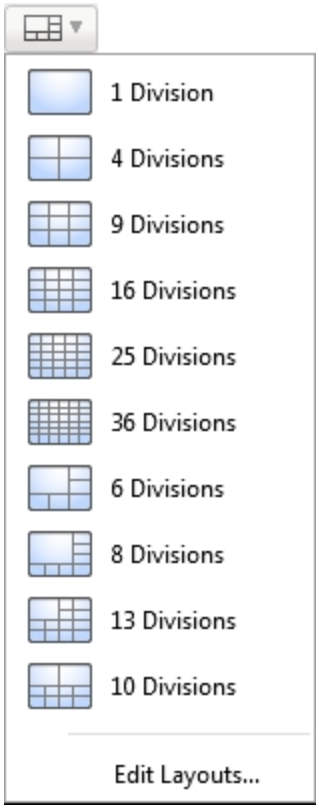


Figure 2: Layouts in the toolbar

Editing a View Layout

If the default View layouts do not fit your surveillance requirements, you can customize a View layout.

1. On the toolbar, select  > **Edit Layouts...**.

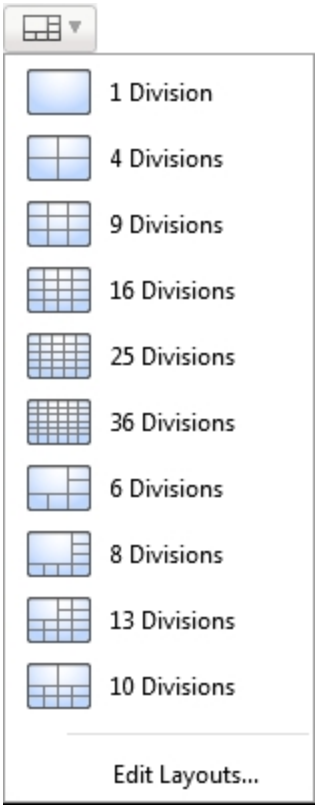


Figure 3: Layouts in the toolbar

2. In the Edit Layouts dialog box, select the layout you want to change.
3. Enter the number of **Columns:** and **Rows:** you want in your layout.

4. In the layout diagram, do any of the following to further customize the layout.

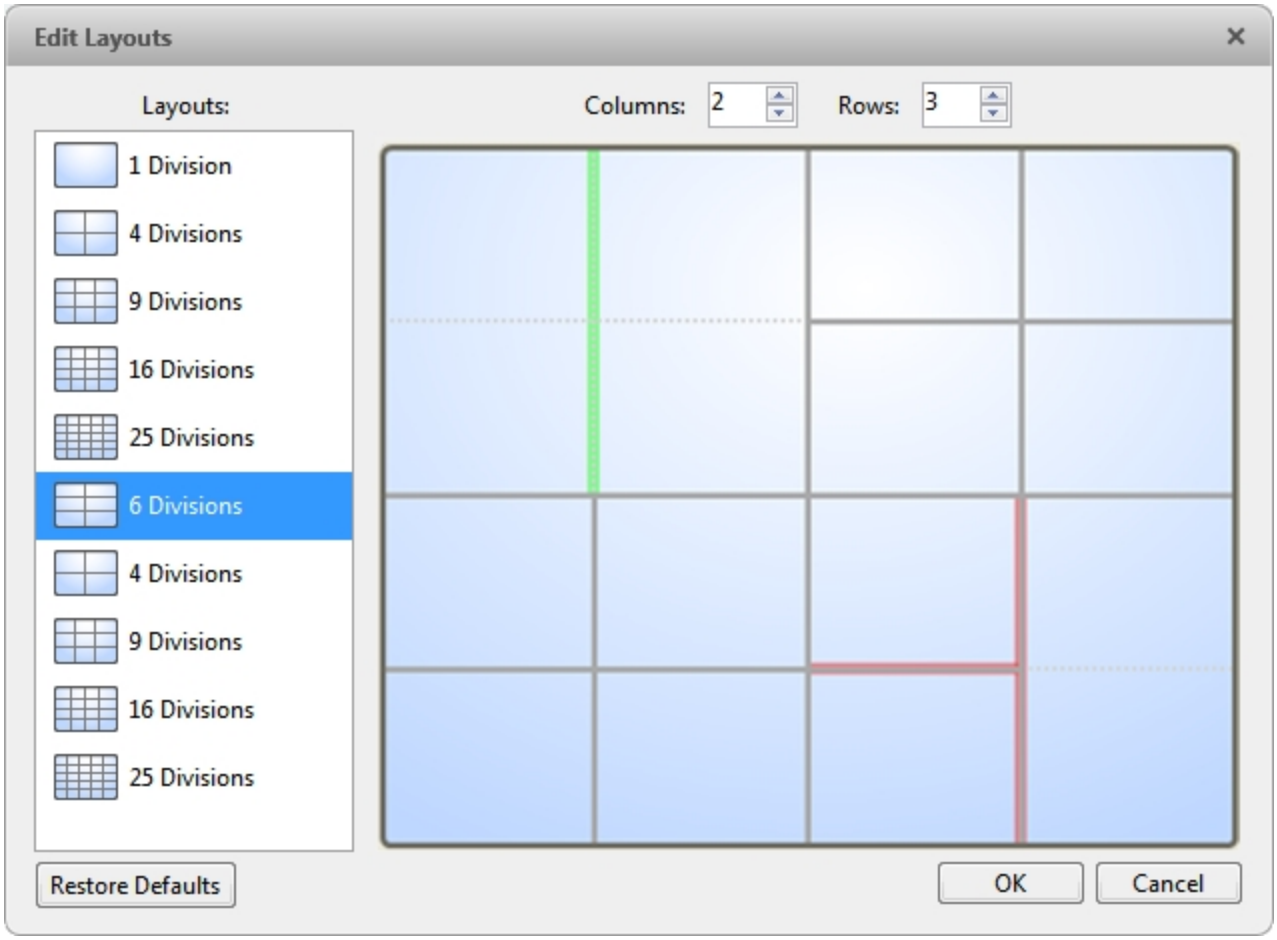


Figure 4: The Edit Layouts dialog box

- To create a larger image panel, select a gray line to delete the border between two image panels. When a line is highlighted in red, the line can be deleted.
- To restore an image panel, select a dotted line to divide a larger image panel into two. When a dotted line is highlighted in green, the line can be restored.
- To restore all default View layouts, click **Restore Defaults**. All custom layouts in the Layouts: list will be replaced.

NOTE: You can only add or subtract lines to create a rectangular shape.

5. Click **OK** to save your changes. The previous View layout has been replaced with your customized layout.

Tip: The keyboard commands used to access View layouts are linked to the layout's position in the Layouts: list. For example, if your custom layout is placed at the top of the Layouts: list (layout 1), you can press Alt + 1 to use that layout.

Video

The Avigilon Control Center Player allows you to watch exported Avigilon Native Video Export (AVE) video and Avigilon Backup (AVK) video in View tabs, similar to the Avigilon Control Center Client software.

If the video file contains video from multiple cameras, the video can be displayed in multiple image panels. You can zoom and pan the exported video images, and use the Timeline to control the playback of the recorded video.

Adding and Removing Cameras in a View

You can add and remove cameras from the View to focus on specific parts of the video file.

Adding a Camera to a View

Do one of the following:

- Drag the camera from the System Explorer to an empty image panel in the View tab.
- Double-click a camera in the System Explorer.
- In the System Explorer, right-click the camera and select **Add To View**.

  The camera is added to the next empty image panel in the View layout.

Tip: You can drag the same camera to multiple image panels to watch the video at different zoom levels.

Removing a Camera from a View

Do one of the following:

- Right-click the image panel and select **Close**.
- Inside the image panel, click  .

Playing Back Recorded Video

The Timeline displays when video was recorded and lets you control video playback.

The colored bars on the Timeline show the camera's recording history:

- A red bar shows the camera has recorded a motion event.
- A blue bar shows the camera has recorded video.
- White areas show periods of time during which the camera has not recorded any video.
- An yellow bar is a bookmark in the camera's recording history.

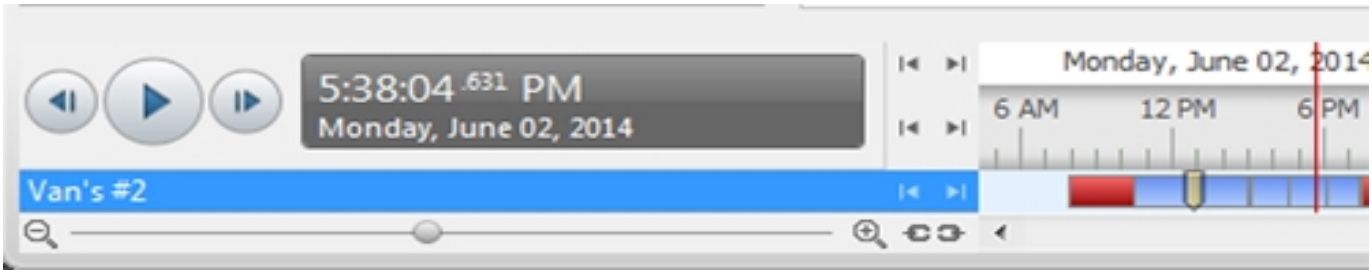
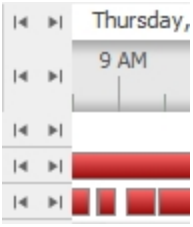
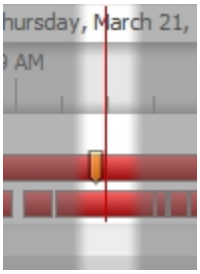


Figure 5: Playback controls on the Timeline

To...	Do this...
Select a playback time	• Click the dark gray date display and select a specific date and time. • Click a point on the Timeline.
Start playback	Click ▶. • Click ⏩ to fast forward. Tap the arrow again to increase the playback speed. • Click ⏪ to rewind. Tap the arrow again to increase the playback speed. You can play the video up to eight times the original speed.
Stop playback	Click ⏸. • Click ⏭ to step forward one frame. • Click ⏮ to step backward one frame.
Jump forward or backward on the Timeline	 On the Timeline, click ⏮ or ⏭ to move to set points on the Timeline.
Zoom in or out of the Timeline	 • Move the slider on the bottom left to zoom in or out on the Timeline. • Place your mouse over the Timeline and use the scroll wheel to zoom in or out on the Timeline. You can zoom in to a quarter of a second, and zoom out to see years if recorded video exists.
Center the Timeline on the time marker	 Right-click the Timeline, and select **Center on Marker.**
Pan the Timeline	• Click and drag the time marker through the Timeline. • Move the horizontal scroll bar under the Timeline. • Right-click and drag the Timeline.

Zooming and Panning in a Video

Use the zoom and pan tools to focus on specific areas in the recorded video stream.

Using the Zoom Tools

There are two ways to digitally zoom in and zoom out of a video image:

- Move your mouse over the video image, then rotate your mouse wheel forward and backward.
- On the toolbar, select  or  , then click the image panel until you reach the desired zoom depth.

Using the Pan Tools

There are two ways to pan through the video image:

- Right-click and drag inside an image panel
- On the toolbar, select  , then click and drag the video image in any direction inside the image panel.

Maximizing and Restoring an Image Panel

You can maximize an image panel to enlarge the video display.

Maximizing an Image Panel

Do one of the following:

- Right-click an image panel and select **Maximize**.
- Inside the image panel, click  .
- Double-click the image panel.

Restoring an Image Panel

In a maximized image panel, do one of the following:

- Right-click the maximized image panel and select **Restore Down**.
- Inside the image panel, click  .
- Double-click the image panel.

Listening to Audio

If audio was included in the video file, you can listen to it through the video image panel. The audio is muted by default.

To control audio playback, do any of the following:

- In the lower-right corner of the image panel, click  to mute or activate the audio.
- Move the slider to change the volume.

Reviewing Recorded POS Transactions

While you watch recorded video, you can review POS transactions that occur at the same time.

1. Select a camera that is linked to the POS transaction source and display the camera's recorded video
2. In the image panel, click  .

   If there is more than one POS transaction source linked to the camera, you will be prompted to select one. The POS transactions are displayed in the next image panel.

   - Each transaction is separated by date and time.
   - When you select a transaction, the video jumps to that event on the Timeline.
   - Scroll up or down to see other recorded POS transactions.
3. To display cameras that are linked to the POS transaction source, click  in the POS transaction image panel.

   If multiple cameras are connected to the POS transaction source, you will be prompted to select one.
4. Use the Timeline to review the video in more detail.

For more information about Timelines, see **Playing Back Recorded Video**.

If you want to find a specific POS transaction, see **Performing a POS Transaction Search**.

Video Display

You can adjust how video is displayed on your monitor. The settings only affect how video is displayed on your monitor and will not affect the contents of the video file.

Adjusting Video Display

You can adjust the Display settings to improve how video is displayed on your monitor.

1. In the top-right corner of the Player, select ⚙ > **Player Settings...**.

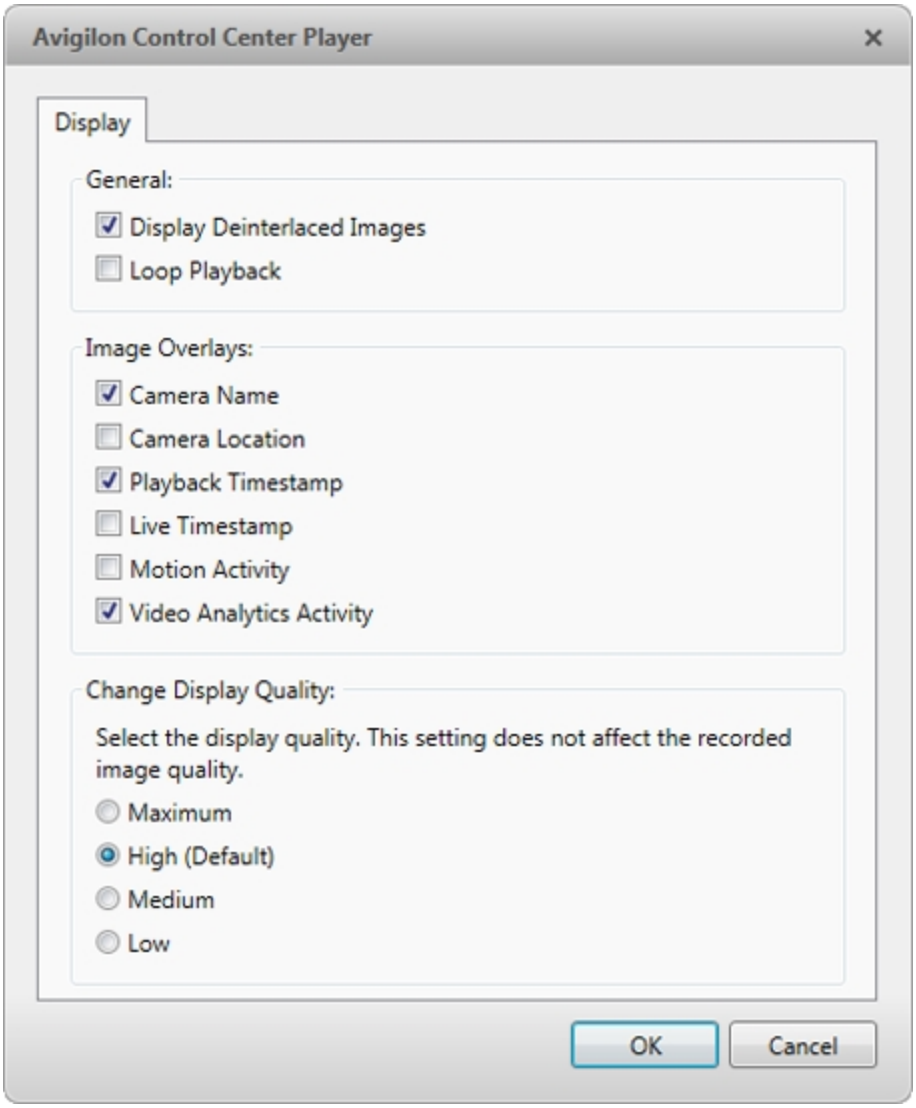


Figure 6: The Player Settings... dialog box

2. Perform any of the following procedures to adjust how video is displayed in image panels.

Displaying Analog Video in Deinterlaced Mode

Select the **Display Deinterlaced Images** check box if the analog video you are watching is showing interfacing artifacts. This setting will help improve video image and smooth out some of the artifacts.

Looping Playback

If you want the Player to automatically repeat the video it is playing, select the **Loop Playback** check box.

Displaying Image Overlays

Select any of the Image Overlays: options to set the type of information that is displayed over video.

Overlay	Description
Camera Name	Displays the name assigned to the camera.
Camera Location	Displays the location assigned to the camera.
Playback Timestamp	(Recorded video only) Displays the exposure timestamp for the video.
Live Timestamp	(Live video only) Displays the current system date and time to the millisecond.
Motion Activity	Highlights motion in red.
Video Analytics Activity	Bounding boxes outline objects detected in the video. The color of the bounding box identifies the object type: • Red - a person • Blue - a vehicle The Video Analytics Activity overlay is only activated for video from a video analytics device.

Changing Display Quality

If your computer does not have enough network bandwidth or processing power, you may not be able to watch video at its full image rate and quality. You can configure the image panels to display video in high quality and low frame rate, or low quality and high frame rate.

Select a higher display quality setting if you need to see specific details or faces in the scene. Select a lower display quality setting if it's more important to see moving events as they occur.

The Change Display Quality: settings only affect the image panel display and do not affect the actual video quality or image rate between the camera and the server. Therefore, you can review recorded footage later to confirm what you saw in the image panel.

In the Change Display Quality: area, select one of the following options:

- **Maximum:** displays video at full resolution with the lowest image rate.
- **High (Default):** displays video at 1/4 resolution.
- **Medium:** displays video at 1/16 resolution.
- **Low:** displays video at 1/64 resolution with the highest image rate.

Making Image Panel Display Adjustments

You can change the image panel display settings to bring out video details that are hard to see with the image panel's default settings.

1. Right-click an image panel and select **Display Adjustments...**.

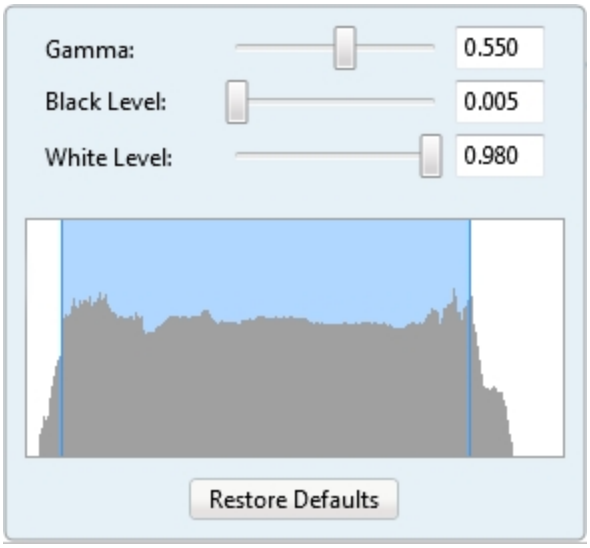


Figure 7: The Display Adjustments... panel

   The Display Adjustments... settings are displayed in a floating pane immediately beside the image panel.

2. Move the sliders to adjust the **Gamma:**, **Black Level:** and **White Level:**.

   The image panel displays a preview of your changes.

3. Click **Restore Defaults** to clear your changes.

Camera Properties

To see detailed information about any camera in the AVE file, you need to access the camera properties.

- In the System Explorer, right-click a camera and select **Properties...**.

Figure 8: The Camera Properties dialog box

The Camera Properties dialog box displays the following information about the camera:

- Camera Name
- Model number

- Firmware Version:
- Location:
- MAC Address:
- Serial Number:
- Resolution:

Search

AVE and AVK files have embedded event data, so you can quickly search for events or motion that occur within the video file.

NOTE: If your video file does not contain a specific type of data, that search option will not be available.

Performing an Alarm Search

If the video is linked to an alarm, you can search for specific alarm triggers in the video file.

1. In the New Task menu, under Search, click  .

   The Search: Alarms tab is displayed.

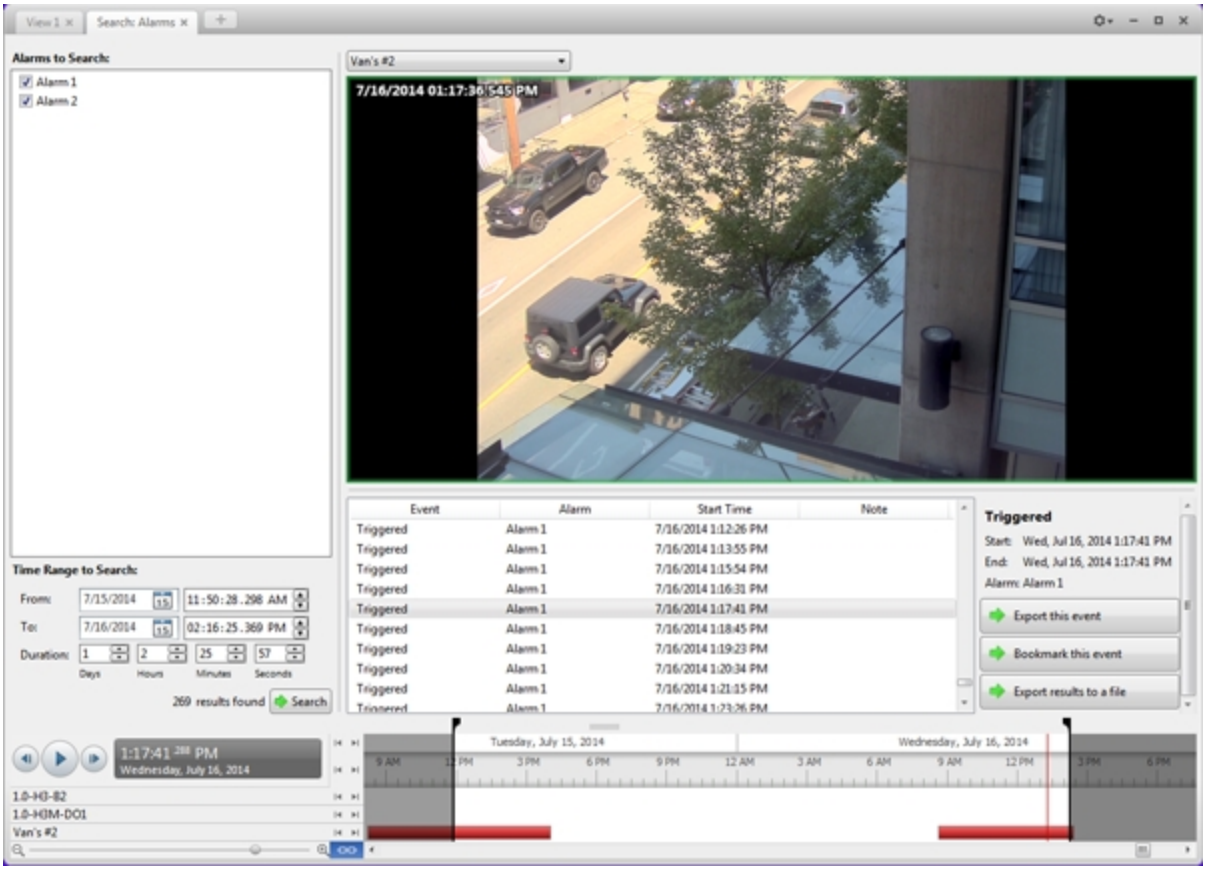


Figure 9: The Search: Alarms tab

2. In the **Alarms to Search:** list, select all the alarms you would like to include in the alarm search.
3. In the **Time Range to Search:** area, set the date and time range of your search. The time range is highlighted on the Timeline by the black time range markers. You can also drag the time range markers to

modify the time range.

4. Click **Search**.

Viewing Alarm Search Results

1. In the **Search Results** area, select a search result. The event is highlighted on the Timeline and the video is displayed in the image panel. Details about the search result are displayed to the right.
2. Use the Timeline controls to review the event.

   For more information, see **Playing Back Recorded Video**.
3. If the search result is linked to multiple cameras, select a camera from the drop down list above the image panel to change the video that is displayed.
4. Click **Export this event** to export the selected event video.

   For more information, see **Export**.
5. To export all listed search results, click **Export results to a file** and save the file. The search results can be saved as either a CSV or Text file.

Performing an Event Search

The Event Search allows you to search for specific motion events and digital input events.

1. In the New Task menu, click 

   The Search: Event tab is displayed.

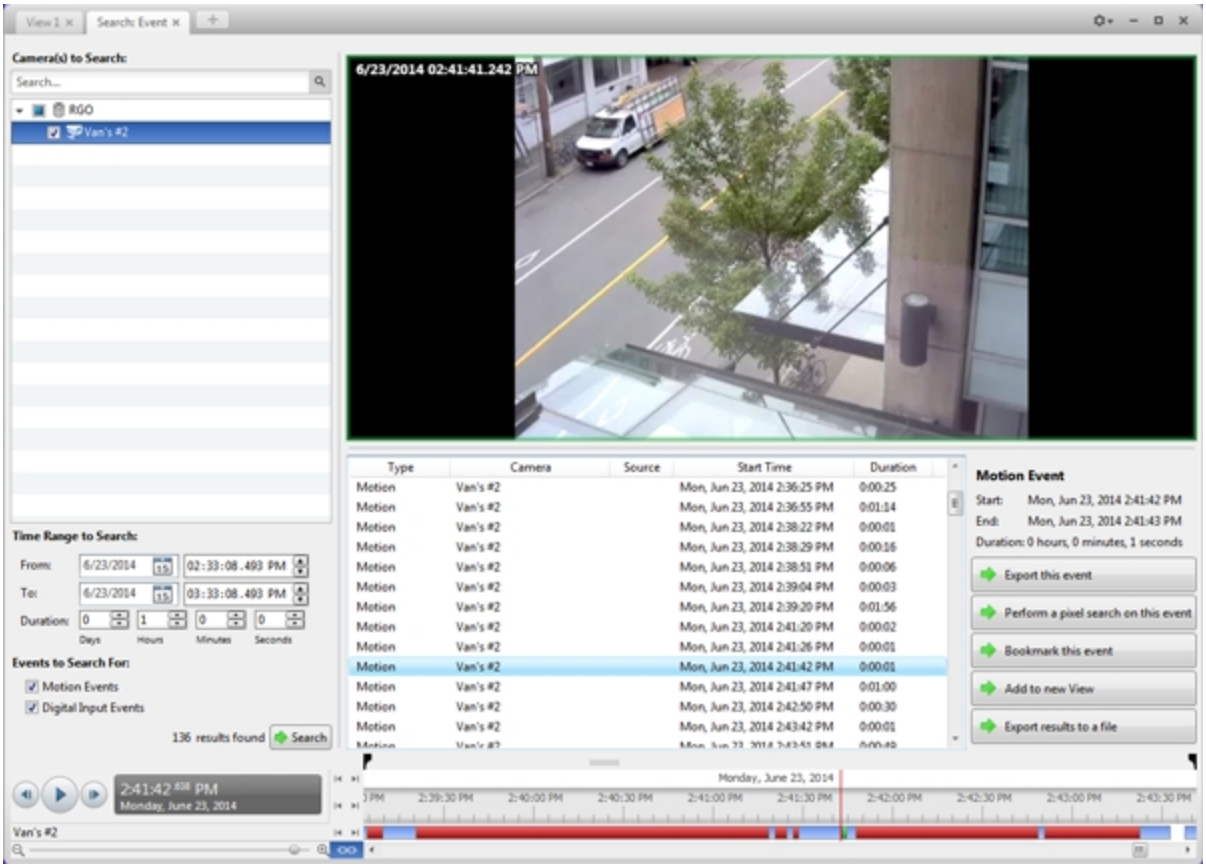


Figure 10: The Search: Event tab

2. In the **Camera(s) to Search:** area, select all the cameras you want to include in the search.
3. In the **Time Range to Search:** area, set the date and time range of your search. The time range is highlighted on the Timeline by the black time range markers. You can also drag the time range markers to modify the time range.
4. In the **Events to Search For:** area, select the types of events to include in the search.
5. Click **Search**.

Viewing Event Search Results

1. In the **Search Results** area, select a search result. The event is highlighted on the Timeline and the video is displayed in the image panel. Details about the search result are displayed to the right.
2. Use the Timeline controls to review the event.

   For more information, see **Playing Back Recorded Video**.
3. Click **Export this event** to export the selected event video.

   For more information, see **Export**.
4. If you want to further refine your search, click **Perform a pixel search on this event**. You can now search for pixel changes in the selected search result.

   For more information, see **Performing a Pixel Search**.

5. To export all listed search results, click **Export results to a file** and save the file. The search results can be saved as either a CSV or Text file.

Performing a License Plate Search

The License Plate Search allows you to search for license plates that were detected in the exported video.>

1. In the New Task menu, under Search, click 

   The Search: License Plates tab is displayed.

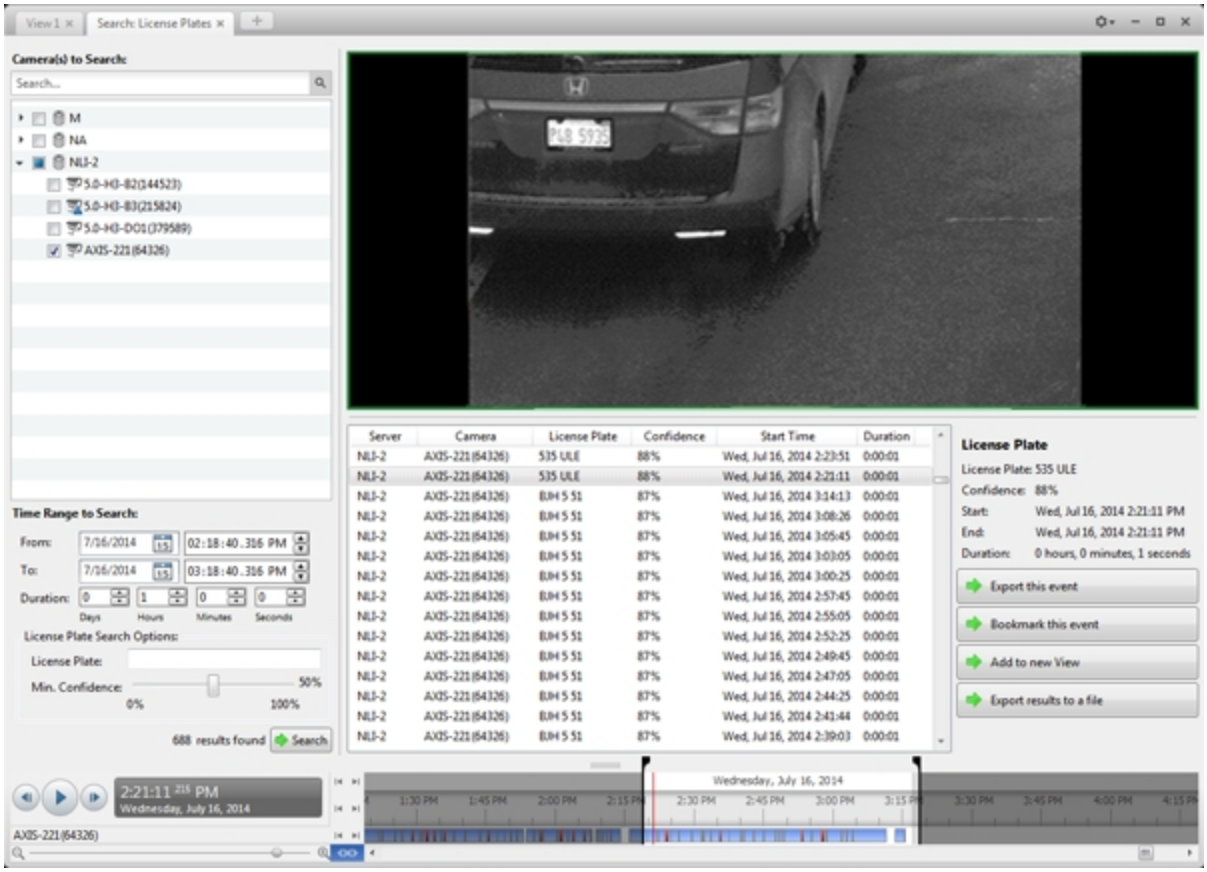


Figure 11: The Search: License Plates tab

2. In the **Camera(s) to Search:** area, select all the cameras you want to include in the search.
3. In the **Time Range to Search:** area, set the date and time range of your search. The time range is highlighted on the Timeline by the black time range markers. You can also drag the time range markers to modify the time range.
4. In the **License Plate Search Options:** area, enter the license plate you want to find and a minimum confidence of a match.
5. Click **Search**.

Viewing License Plate Search Results

1. In the **Search Results** area, select a search result. The event is highlighted on the Timeline and the video is displayed in the image panel. Details about the search result are displayed to the right.
2. Use the Timeline controls to review the event.

   For more information, see **Playing Back Recorded Video**.
3. If the search result is linked to multiple cameras, select a camera from the drop down list above the image panel to change the video that is displayed.
4. Click **Export this event** to export the selected event video.

   For more information, see **Export**.
5. To export all listed search results, click **Export results to a file** and save the file. The search results can be saved as either a CSV or Text file.

Performing a Pixel Search

The Pixel Search allows you to search for tiny pixel changes in specific areas in the camera's field of view.

1. In the New Task menu, click 

   The Search: Pixel tab is displayed.

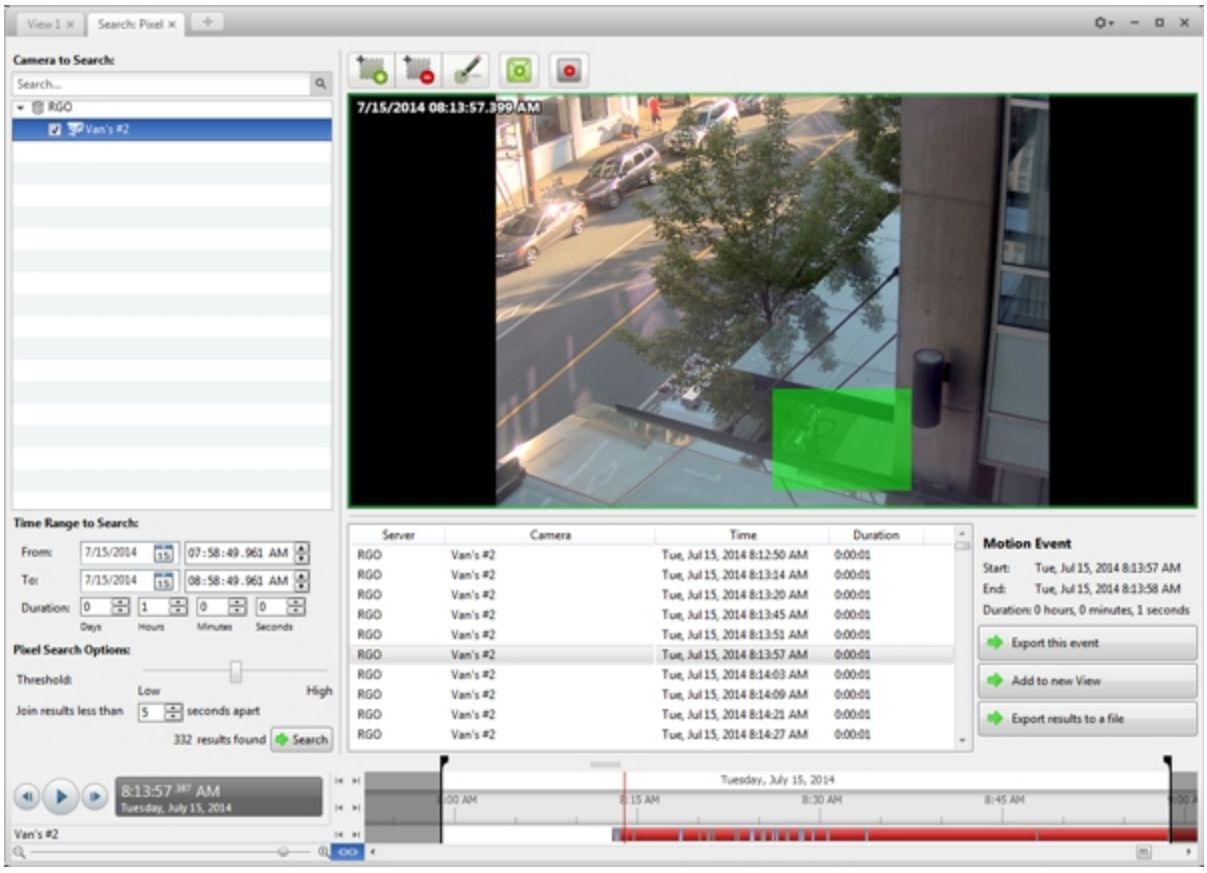


Figure 12: The Search: Pixel tab

By default, the entire search image panel is highlighted in green.

2. In the **Camera to Search:** area, select a camera.
3. In the **Time Range to Search:** area, set the date and time range of your search. The time range is highlighted on the Timeline by the black time range markers. You can also drag the time range markers to modify the time range.
4. Define the pixel search area by using the motion detection tools above the image panel.

   Tip: If you are looking for something very specific, limit the green area to a dot to find what you're looking for more quickly.
5. In the Pixel Search Options: area, drag the **Threshold:** slider to select the amount of motion required to return a search result.

   A high threshold requires more pixels to change before results are found.
6. Enter a number in the **Join results less than** field to set the minimum number of seconds between separate search results. You can enter any number between 1-100 seconds.
7. Click **Search**.

Viewing Pixel Search Results

1. In the **Search Results** area, select a search result. The event is highlighted on the Timeline and the video is displayed in the image panel. Details about the search result are displayed to the right.
2. Use the Timeline controls to review the event.

   For more information, see **Playing Back Recorded Video**.
3. Click **Export this event** to export the selected event video.

   For more information, see **Export**.
4. To export all listed search results, click **Export results to a file** and save the file. The search results can be saved as either a CSV or Text file.

Performing a POS Transaction Search

The POS Transaction Search allows you to search for specific transactions in the video file.

1. In the New Task menu, click  .

   The Search: POS Transactions tab is displayed.

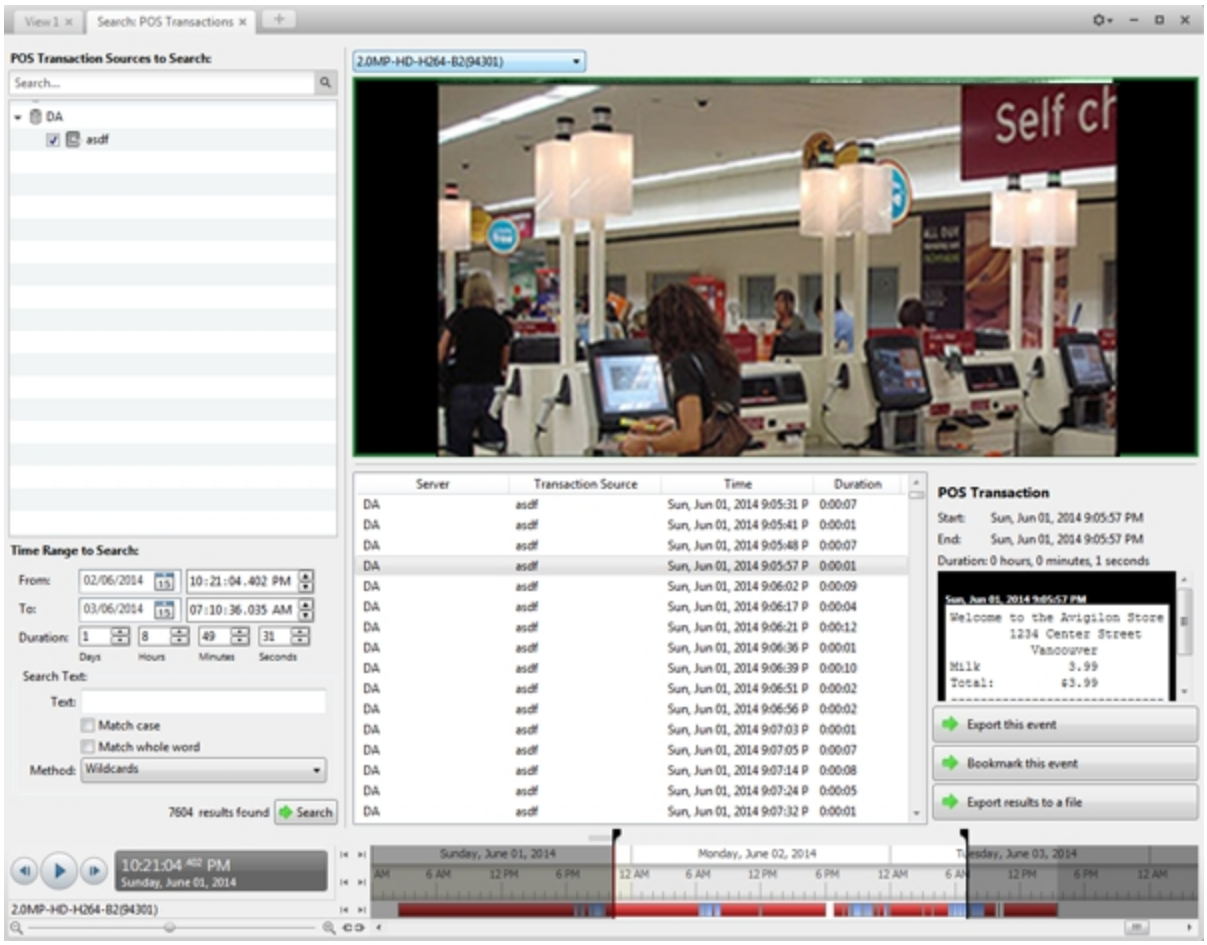


Figure 13: The Search: POS Transactions tab

2. In the **POS Transaction Sources to Search:** area, select all the POS transaction sources you would like to include in the search.
3. In the **Time Range to Search:** area, set the date and time range of your search. The time range is highlighted on the Timeline by the black time range markers. You can also drag the time range markers to modify the time range.
4. In the **Search Text:** area, enter any text that will help you filter the search results. For example, you can enter product names or transaction values.

   Use the **Wildcards** and **Regular expressions** search methods to find a range of results. Leave the **Text:** field blank to find all transactions.
5. Click **Search**.

Viewing POS Transaction Search Results

1. In the **Search Results** area, select a search result. The event is highlighted on the Timeline and the video is displayed in the image panel. Details about the search result are displayed to the right.
2. Use the Timeline controls to review the event.

   For more information, see **Playing Back Recorded Video**.

3. If the search result is linked to multiple cameras, select a camera from the drop down list above the image panel to change the video that is displayed.
4. Click **Export this event** to export the selected event video.

   For more information, see **Export**.
5. To export all listed search results, click **Export results to a file** and save the file. The search results can be saved as either a CSV or Text file.

Performing a Thumbnail Search

The Thumbnail Search is a visual search that displays search results as a series of thumbnail images.

1. In the New Task menu, click  .

   The Search: Thumbnails tab is displayed.

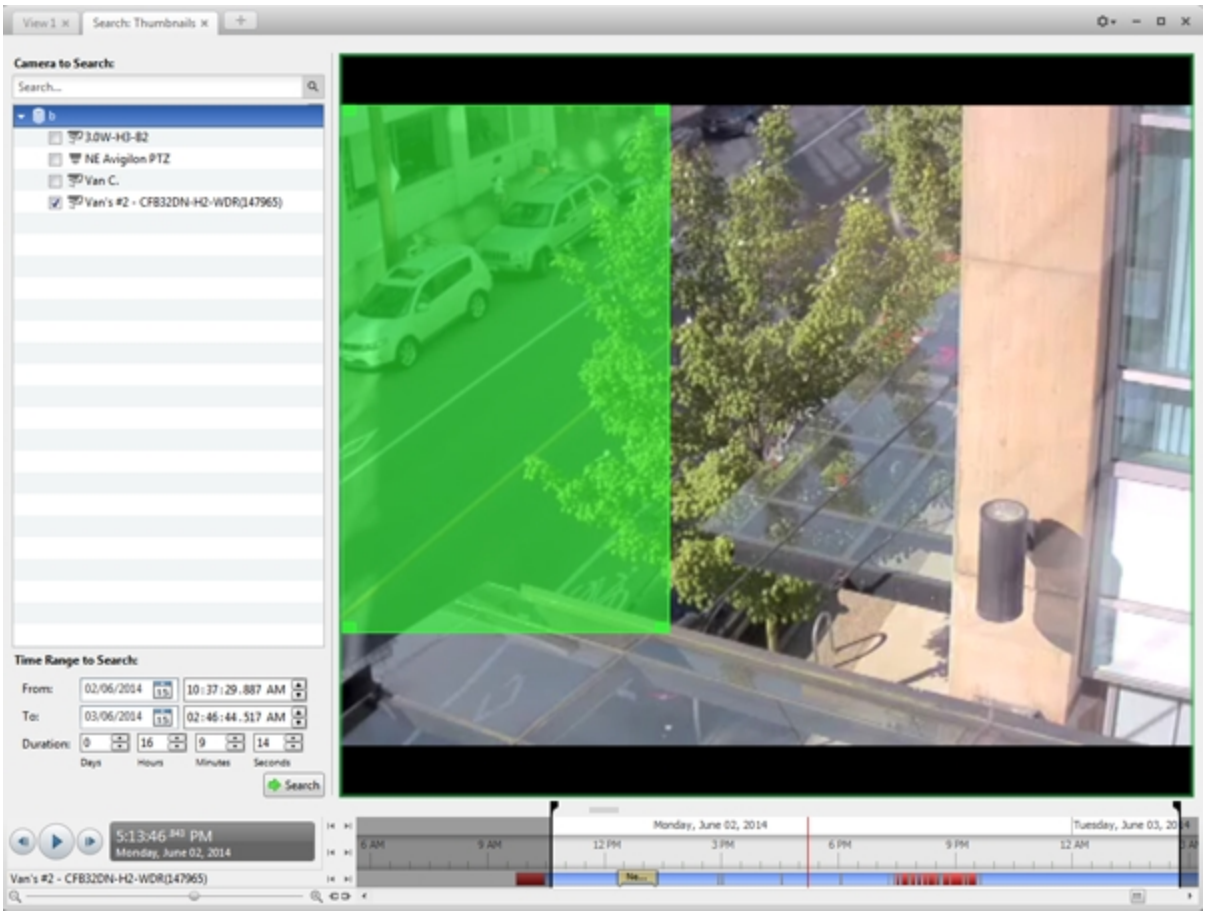


Figure 14: The Search: Thumbnails tab

2. In the **Camera to Search:** area, select a camera.
3. In the **Time Range to Search:** area, set the date and time range of your search. The time range is

highlighted on the Timeline by the black time range markers. You can also drag the time range markers to modify the time range.

4. In the image panel, move or drag the edges of the green overlay to focus the search on one area in the video image. Only the area highlighted in green will be searched.
5. Click **Search**.

Viewing Thumbnail Search Results

The search results display thumbnails at equal intervals on the Timeline.

1. To change the size of the search result thumbnails, select **Large Thumbnails**, **Medium Thumbnails**, or **Small Thumbnails** from the menu above the search results.

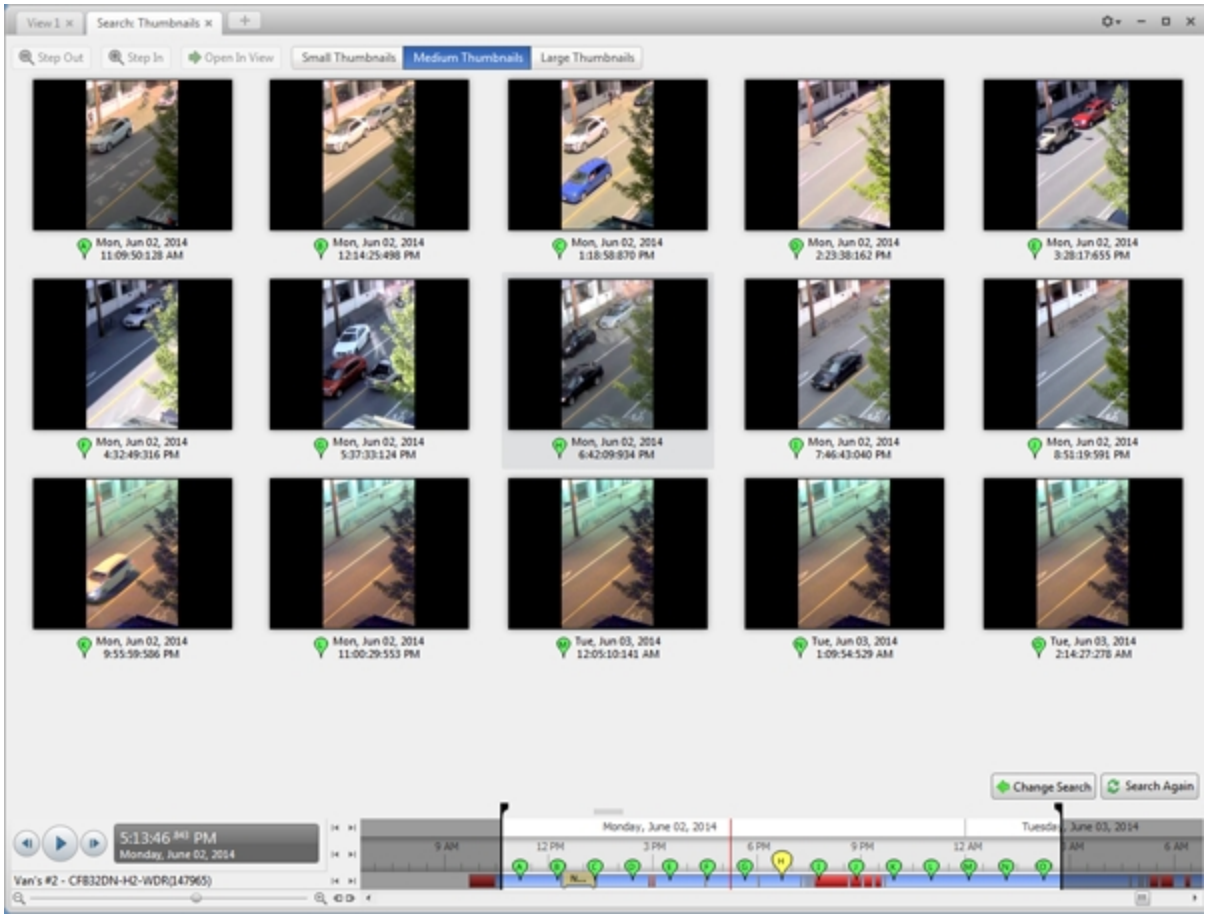


Figure 15: The Search: Thumbnails results tab

2. Select a thumbnail to highlight the video on the Timeline.
3. Click **Step In**, or double-click the thumbnail to perform another search around the thumbnail.

   Click **Step Out** to return to the previous results page.
4. Click **Open In View** (after selecting a thumbnail) to open the recorded video in a new View.
5. Click **Change Search** to change the search criteria.

Export

You can export video in multiple video and image formats. The Export tab can be accessed from bookmark options, the New Task menu, and any Search tab.

You can also export snapshots of an image panel as you monitor video.

Exporting Native Video

The Native (AVE) format is the recommended format for exporting video. You can export video from multiple cameras in a single file, and the video maintains its original compression.

If there is audio linked to the video, the audio is automatically included in the export.

1. In the New Task menu, click  . The Export tab opens.

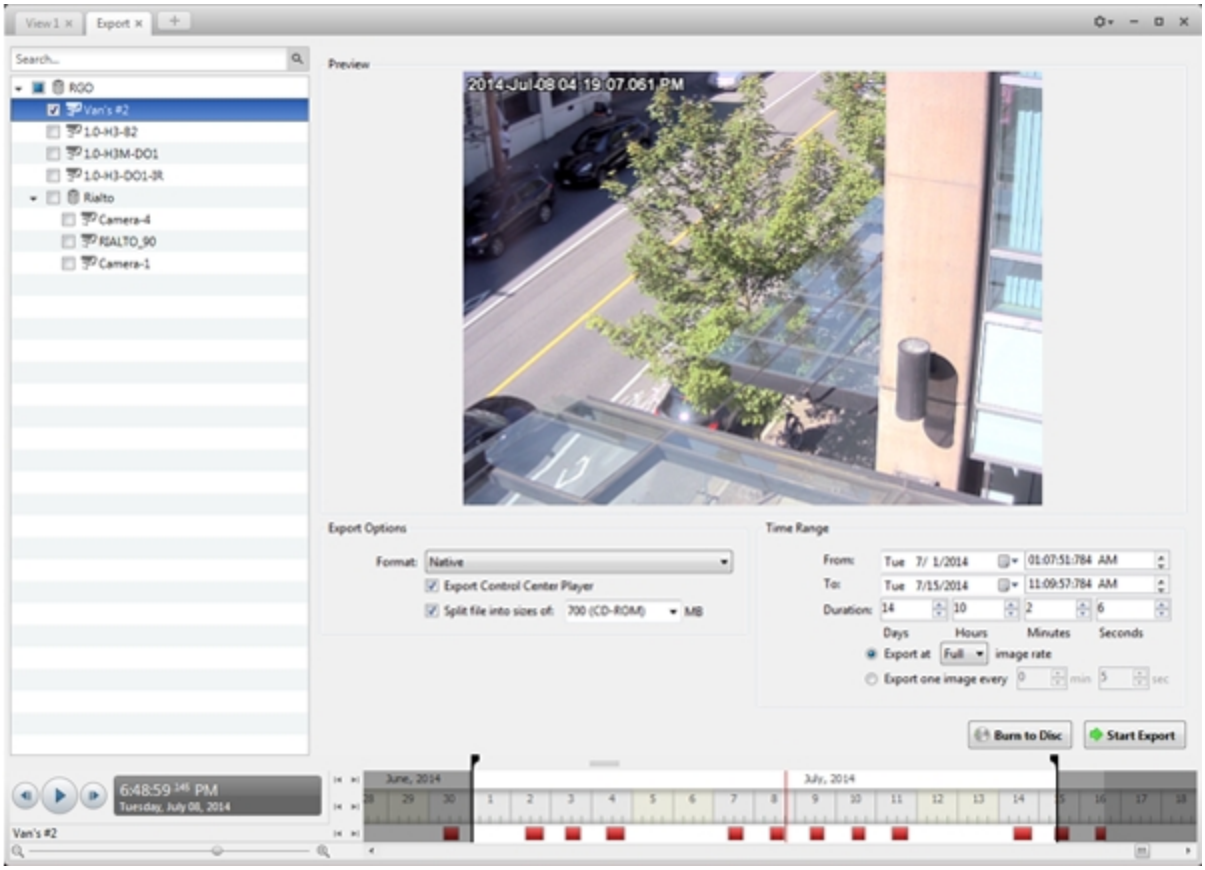


Figure 16: The Export tab for AVE export

2. In the **Format:** drop down list, select **Native**.
3. In the System Explorer, select the camera video you want to export.
4. To automatically divide the export into separate files, select the **Split file into sizes of:** check box, then

select one of the options from the drop down list, or manually enter the size of each file in MB.

This option allows you to export smaller files for storing in a flash drive or on optical media.

This setting is automatically disabled if you choose to burn the export to disc because the system auto-detects the disc size.

5. Enter the **Time Range** you want to export. The **Time Range** is highlighted on the Timeline by black time range markers. You can also drag the time range markers to modify the time range.
6. Set the export image rate:

Option	Description
Export at _ image rate	Select this option to control how many images per second are exported. For example, the video is streaming at 30 images per second. If you select **1/2**, only 15 images for that second will be exported.
Export one image every _ min _sec	Select this option to control the time between each exported video image. For example, if you enter *5* min. *0* sec., only one image will be exported for every 5 minutes of video.

7. Click one of the following:
   - **Start Export**: to save the file locally.
     - In the Save As dialog box, name the export file and click **Save**.
   - **Burn to Disc**: to burn the file directly to disc media.

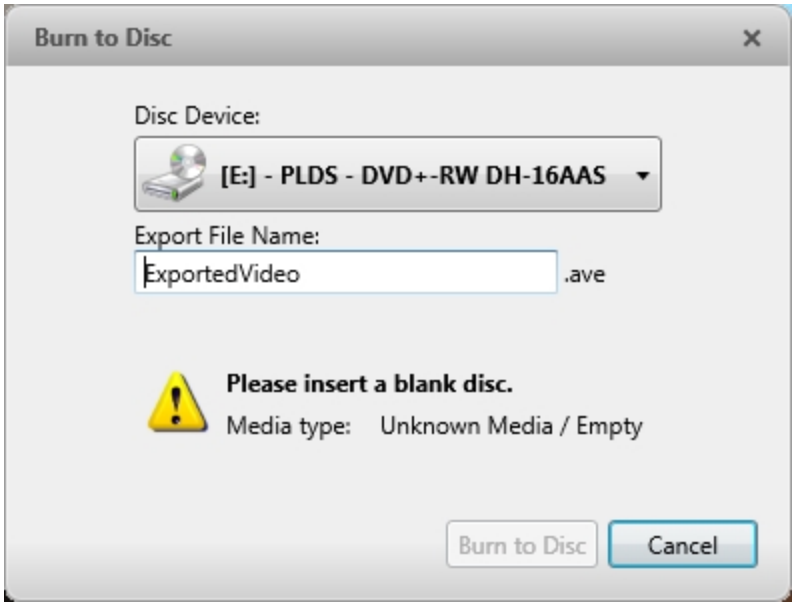


Figure 17: The Burn to Disc Dialog Box

a. When the dialog box appears, insert a disc and select the media burning drive.

b. Name the export file. The file name is automatically given a numbered suffix to help identify which file you are playing if the export spans multiple discs.

c. Click **Burn to Disc** to start the export. If this button is disabled, the disc may be corrupt or full.

d. Monitor the export progress to see if extra discs are required. When a disc is full, the export automatically pauses and you are asked to insert a new disc. After you insert a new disc, click **Resume Export**.

The number of discs required to export a video varies widely depending on the type of camera and disc used. Video is stored on the server with minimal compression to maximize the function of Avigilon's HDSM™ technology, so the size of an export can be quite large due to the camera's high megapixel resolution and frame rate.

Generally, if you export a 2 minute video from a 2MP H.264 HD camera into AVE format, you will export a 93 MB file. To reduce the number of discs required, you can lower the frame rate or use a disc type with a larger capacity. Be aware that reducing the frame rate too much may cause the exported video to be jerky or missing data.

8. When the export is complete, click **OK**.

Exporting AVI Video

Video exported in Audio Video Interleave (AVI) format can be played in most media players. Be aware that you can only export one video at a time in this format.

1. In the New Task menu, click  . The Export tab opens.

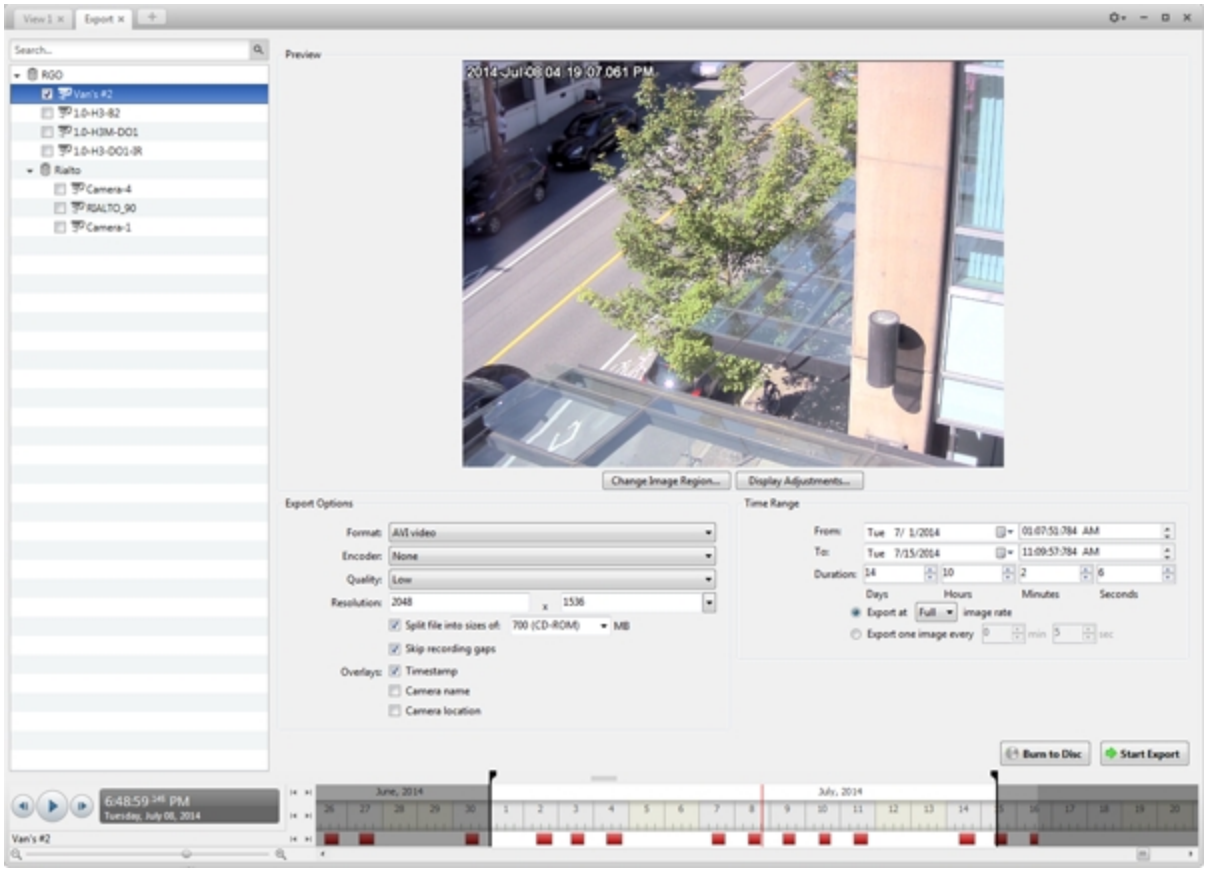


Figure 18: Export tab for AVI export

2. In the **Format:** drop down list, select **AVI video**.
3. In the System Explorer, select the camera video you want to export.
4. In the **Encoder:** field, select the compression used. The VC-1 (Windows Media Video) compression is included by default because it is tailored for high-resolution AVI encoding.

   If you are planning to burn the export to disc, it is important to select a compression method to help reduce the export size and maintain video quality.
5. In the **Quality:** drop down list, select the exported image quality level.
6. In the **Resolution:** field, select a resolution for the video image. You can manually enter the resolution or click the drop down arrow to select a standard resolution.

   NOTE: The Resolution: field automatically maintains the image aspect ratio.
7. To automatically divide the export into separate files, select the **Split file into sizes of:** check box, then select one of the options from the drop down list, or manually enter the size of each file in MB.

   This option allows you to export smaller files for storing in a flash drive or on optical media.

This setting is automatically disabled if you choose to burn the export to disc because the system auto-detects the disc size.

8. Select the **Skip recording gaps** check box to avoid pauses in the video caused by gaps in the recording.
9. Select the image overlays you want: **Timestamp**, **Camera name**, and **Camera location**.

   Select the **Video Analytics Activity** overlay to include video analytics bounding boxes with the video. These boxes cannot be hidden or removed from the exported video.
10. Enter the **Time Range** you want to export. The **Time Range** is highlighted on the Timeline by black time range markers. You can also drag the time range markers to modify the time range.
11. Set the export image rate:

Option	Description
Export at _ image rate	Select this option to control how many images per second are exported. For example, the video is streaming at 30 images per second. If you select **1/2**, only 15 images for that second will be exported.
Export one image every _ min _sec	Select this option to control the time between each exported video image. For example, if you enter *5* min. *0* sec., only one image will be exported for every 5 minutes of video.

12. Click **Change Image Region...** to only export part of the video image. In the **Change Image Region...** dialog box, move and resize the green overlay to select the region you want to export, then click **OK**. Only areas highlighted in green will be exported.
13. Click **Display Adjustments...** to adjust the **Gamma:**, **Black Level:** and/or **White Level:**.
14. Click one of the following:
    - **Start Export**: to save the file locally.
      - In the Save As dialog box, name the export file and click **Save**.
    - **Burn to Disc**: to burn the file directly to disc media.

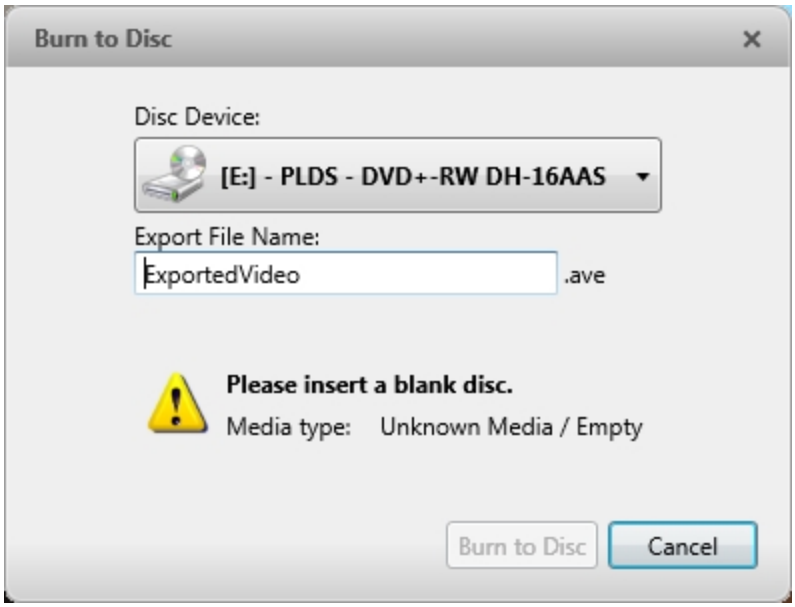


Figure 19: The Burn to Disc Dialog Box

a. When the dialog box appears, insert a disc and select the media burning drive.

b. Name the export file. The file name is automatically given a numbered suffix to help identify which file you are playing if the export spans multiple discs.

c. Click **Burn to Disc** to start the export. If this button is disabled, the disc may be corrupt or full.

d. Monitor the export progress to see if extra discs are required. When a disc is full, the export automatically pauses and you are asked to insert a new disc. After you insert a new disc, click **Resume Export**.

The number of discs required to export a video varies widely depending on the type of camera and disc used. Video is stored on the server with minimal compression to maximize the function of Avigilon's HDSM technology, so the size of an export can be quite large due to the camera's high megapixel resolution and frame rate.

Generally, if you export a 2 minute video from a 2MP H.264 HD camera into uncompressed AVI format, you will export a 2.7 GB file. If you select an **Encoder:** format and compress the video, you can export a 224 MB video at high quality. It is recommended that you always select an Encoder: format for AVI export to help significantly reduce the file size.

To further reduce the file size you can select a lower quality setting, lower the export frame rate, reduce the video resolution, or focus the export on a specific image region. Be aware that reducing each of the available settings too much may cause the export to be blurry or missing frames.

If it is important to have a high quality and full frame rate export, it is recommended that you use the AVE export format instead. AVE export intelligently compresses the video to create a smaller export file while maintaining video data so that you can search, re-export video, and authenticate the video against tampering through the Avigilon Control Center Player software.

15. When the export is complete, click **OK**.

Exporting a Print Image

You can export a frame of video directly to your printer or as a PDF, and include notes related to the image.

To print a photo of the video you are currently watching, take a snapshot. For more information, see **Exporting a Snapshot of an Image**.

1. In the New Task menu, click  . The Export tab opens.

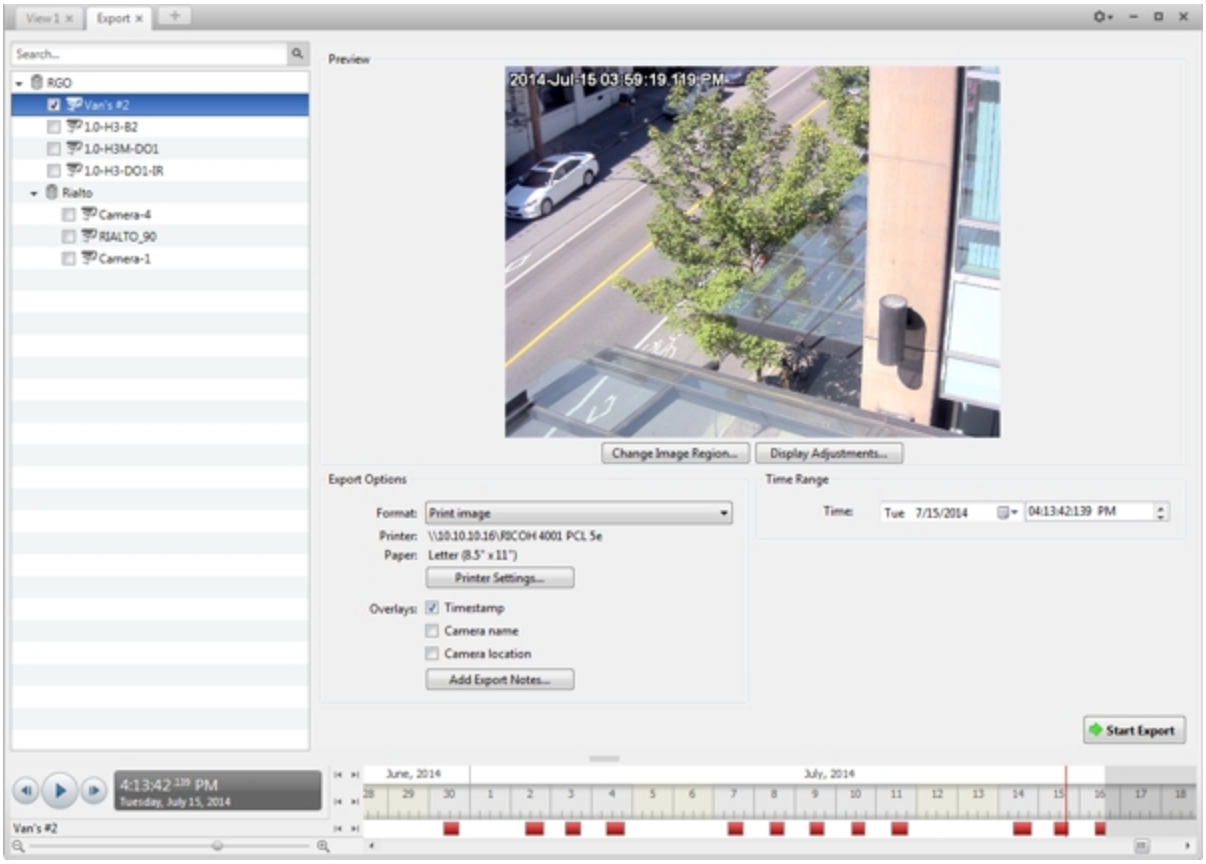


Figure 20: Export tab for print image export

2. In the **Format:** drop down list, select **Print image** or **PDF file**.
3. In the System Explorer, select the camera video you want to export.
4. (Print Image Only) Click **Printer Settings...** to change the printer and paper size that the image is printed on.
5. Select the image overlays you want: **Timestamp**, **Camera name**, and **Camera location**.
6. Click **Add Export Notes...** to add notes about the exported image. The notes are added below the image.
7. In the **Time Range** box, enter the exact date and time of the video image you want to export.
8. Click **Change Image Region...** to only export part of the video image. In the **Change Image Region...** dialog box, move and resize the green overlay to select the region you want to export, then click **OK**. Only areas highlighted in green will be exported.

9. Click **Display Adjustments...** to adjust the **Gamma:**, **Black Level:** and/or **White Level:**.
10. Click **Start Export**.
    - If you are exporting a Print image, the image is sent to the printer.
    - If you are exporting a PDF file, save the image.

    The Preview area displays the video you are exporting.
11. When the export is complete, click **OK**.

Exporting a Snapshot of an Image

You can export a snapshot of any image panel with video. When you export a snapshot, you are exporting what the image panel is currently displaying.

1. To export a snapshot, do one of the following:
    - In the image panel, click  .
    - Right-click the image panel and select **Save Snapshot**.

    The snapshot Export tab is opened, and the image you want to export is displayed.

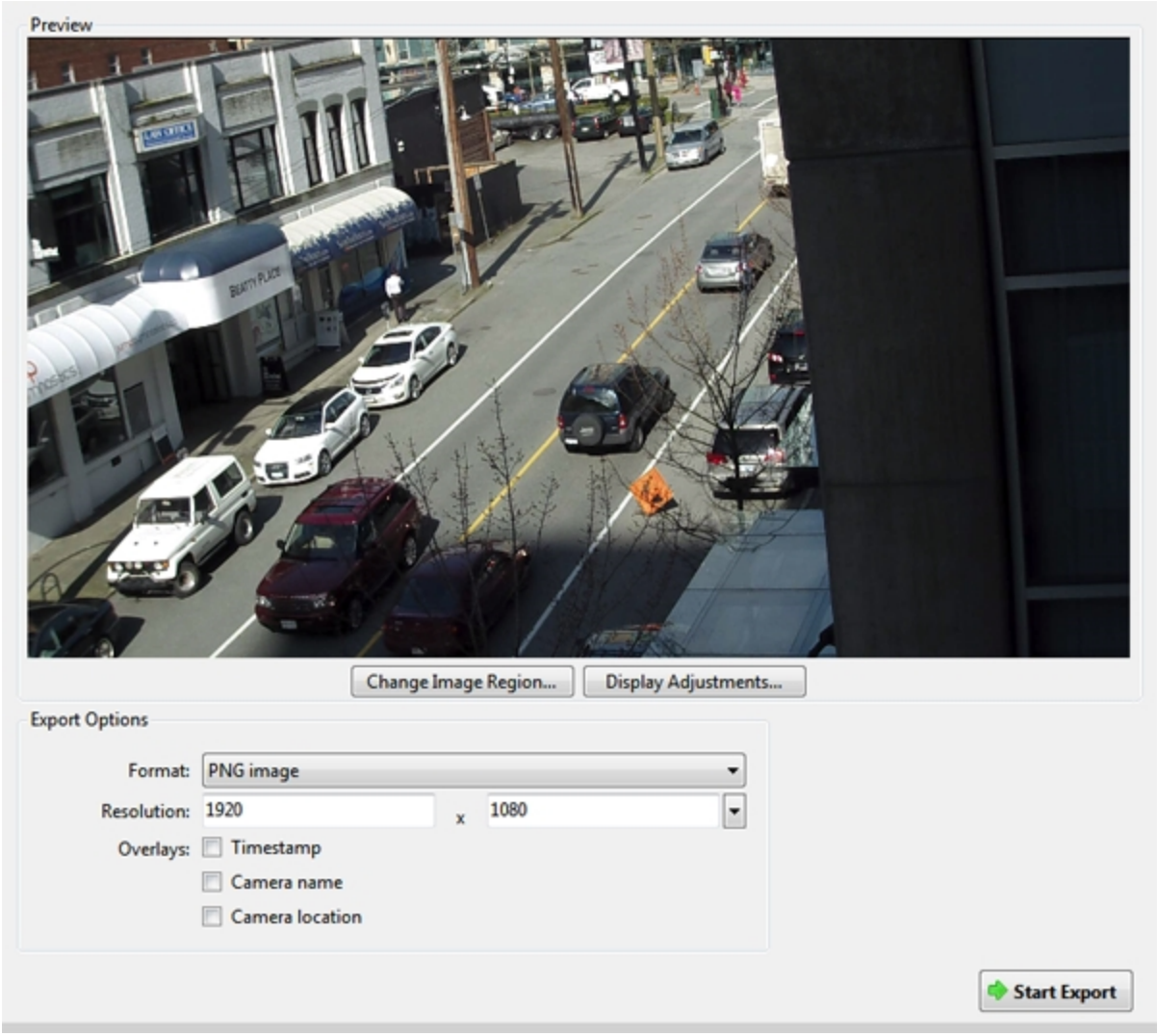


Figure 21: The Export tab for snapshot export

2. In the **Format:** drop down list, select an export format.
3. For the selected export format, define your preferences:

Format	Export options
Native **NOTE:** The Native format requires the Avigilon Control Center Player to view.	This is the recommended export format because the exported image maintains its original compression and can be authenticated against tampering in the Avigilon Control Center Player.
PNG image	1. In the **Resolution:** field, select a resolution for the video image. You can manually enter the resolution or click the drop down arrow to select a standard resolution. **NOTE:** The Resolution: field automatically maintains the image aspect ratio. 2. Select the image overlays you want: **Timestamp**, **Camera name**, and **Camera location**.

Format	Export options
	3. Click **Change Image Region...** to only export part of the video image. In the **Change Image Region** dialog box, move and resize the green overlay, then click **OK**. Only areas highlighted in green are exported. 4. Click **Display Adjustments...** to adjust the **Gamma:**, **Black Level:**, and/or **White Level:**.
JPEG image	1. In the **Quality:** drop down list, select the exported image quality level. 2. Set the image **Resolution:**. 3. Select the image overlays you want. 4. Click **Change Image Region...** to only export a part of the video image. 5. Click **Display Adjustments...** to modify the image quality.
TIFF image	1. Set the image **Resolution:**. 2. Select the image overlays you want. 3. Click **Change Image Region...** to only export a part of the video image. 4. Click **Display Adjustments...** to modify the image quality.
Print image	1. Click **Printer Settings...** to change the selected printer and paper size. 2. Select the image overlays you want. 3. Click **Add Export Notes...** to add notes about the exported image. The notes are printed below the image. 4. Click **Change Image Region...** to only export a part of the video image. 5. Click **Display Adjustments...** to modify the image quality.
PDF file	1. Select the image overlays you want. 2. Click **Add Export Notes...** to add notes about the exported image. 3. Click **Change Image Region...** to only export a part of the video image. 4. Click **Display Adjustments...** to modify the image quality.

4. Click **Start Export**.
5. In the Save As dialog box, name the export file and click **Save**. If you are printing the snapshot, the image is sent to your printer instead.

   The Preview area displays the snapshot you are exporting.
6. When the export is complete, click **OK**.

Exporting Still Images

Video can be exported as a series of still PNG images, JPEG images, or TIFF images. When you export a series of still images, you are exporting each frame of video as an independent file.

If you only want one photo of the video you are watching, take a snapshot. For more information, see **Exporting a Snapshot of an Image**.

1. In the New Task menu, click  . The Export tab opens.

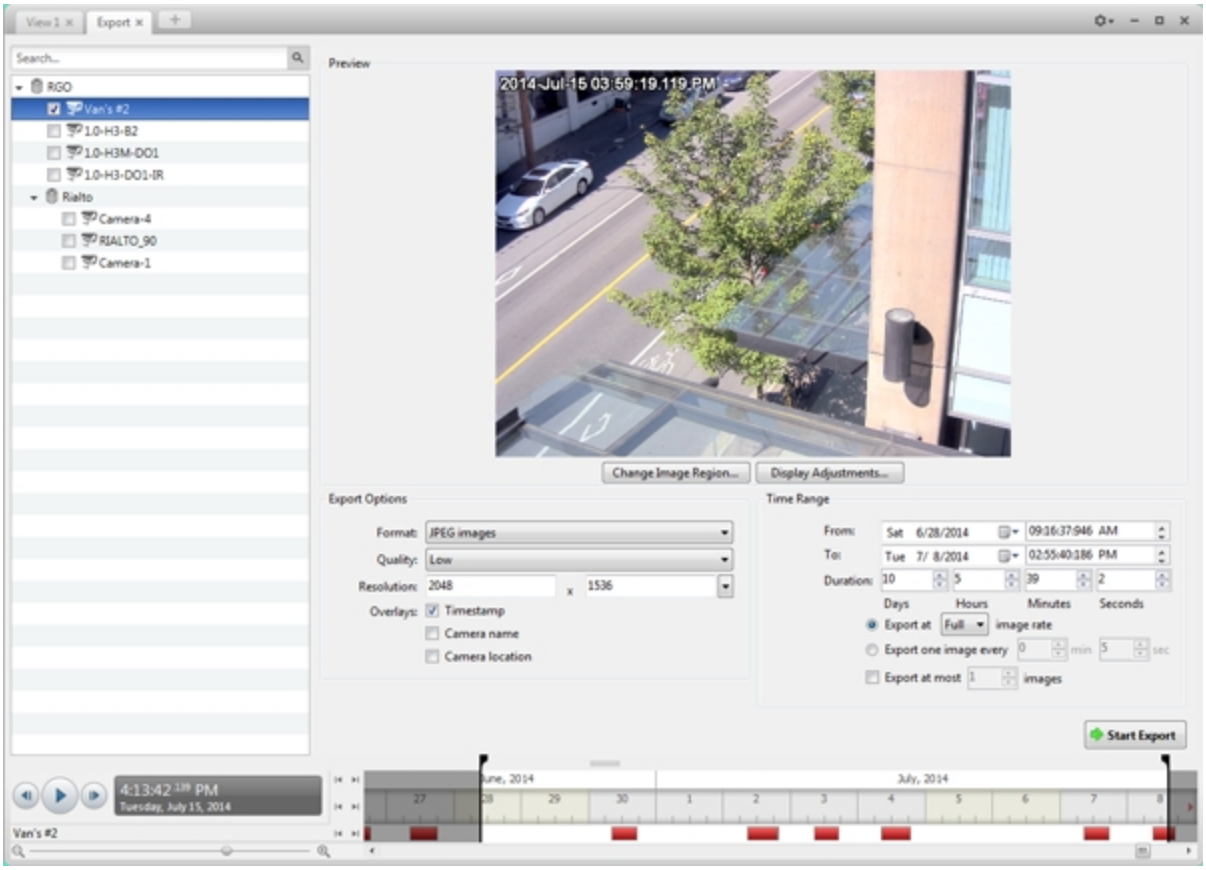


Figure 22: Export tab for still image export

2. In the **Format:** drop down list, select **PNG images**, **JPEG images**, or **TIFF images**.
3. In the System Explorer, select the camera video you want to export.
4. (JPEG only) In the **Quality:** drop down list, select the exported image quality level.
5. In the **Resolution:** field, select a resolution for the video image. You can manually enter the resolution or click the drop down arrow to select a standard resolution.

   NOTE: The Resolution: field automatically maintains the image aspect ratio.
6. Select the image overlays you want: **Timestamp**, **Camera name**, and **Camera location**.
7. Enter the **Time Range** you want to export. The **Time Range** is highlighted on the Timeline by black time range markers. You can also drag the time range markers to modify the time range.

8. Set the export image rate:

Option	Description
Export at _ image rate	Select this option to control how many images per second are exported. For example, the video is streaming at 30 images per second. If you select **1/2**, only 15 images for that second will be exported.
Export one image every _ min _sec	Select this option to control the time between each exported video image. For example, if you enter *5* min. *0* sec., only one image will be exported for every 5 minutes of video.

9. To limit the number of images that are exported, select the **Export at most _ images** check box and enter a number.
10. Click **Change Image Region...** to only export part of the video image. In the **Change Image Region...** dialog box, move and resize the green overlay to select the region you want to export, then click **OK**. Only areas highlighted in green will be exported.
11. Click **Display Adjustments...** to adjust the **Gamma:**, **Black Level:** and/or **White Level:**.
12. Click **Start Export**.
13. In the Save As dialog box, name the export file and click **Save**.

    The Preview area displays the video you are exporting.
14. When the export is complete, click **OK**.

Exporting WAV Audio

If you want to export audio with video, simply export the video in Native or AVI format. Any audio that is linked to the video is automatically included in the export file.

This procedure exports the audio alone.

1. In the New Task menu, click  . The Export tab opens.

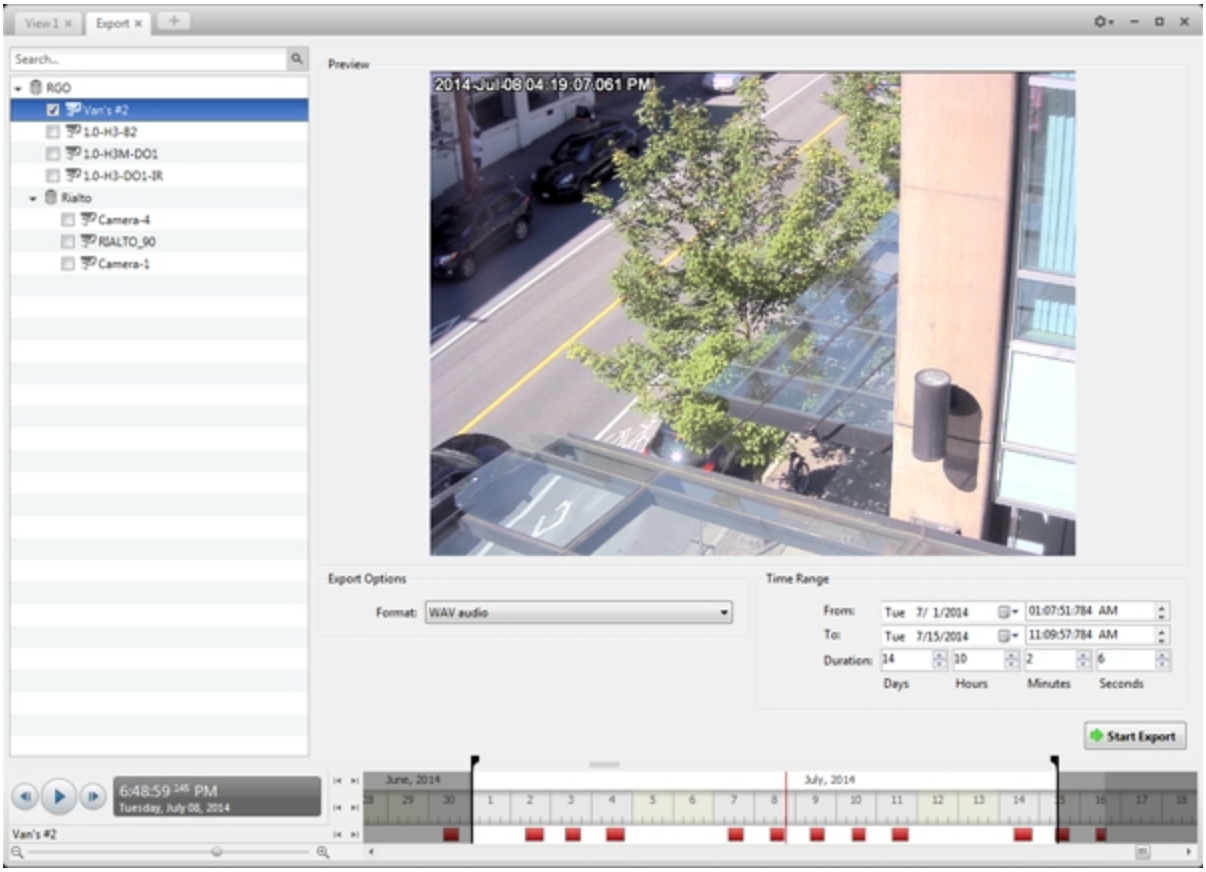


Figure 23: Export tab for audio export

2. In the **Format:** drop down list, select **WAV audio**.
3. In the System Explorer, select the camera that the audio is linked to.
4. Enter the **Time Range** you want to export. The **Time Range** is highlighted on the Timeline by black time range markers. You can also drag the time range markers to modify the time range.
5. Click **Start Export**.
6. In the Save As dialog box, name the export file and click **Save**.

   The Preview area displays the video linked to the audio you are exporting.
7. When the export is complete, click **OK**.

This Page Left Intentionally Blank

Avigilon™ Control Center Gateway User Guide

Version 5.4.2

Avigilon Corporation
http://www.avigilon.com

Revised: 2014-12-09

PDF-ACCGATEWAY5-E-Rev1

Table of Contents

Introduction

The Avigilon™ Control Center Gateway software works with the Avigilon™ Control Center Mobile (ACC Mobile) app and the Avigilon™ Control Center Gateway Web Client to give users remote access to your Avigilon™ Control Center system.

ACC Mobile is installed on a user's mobile device for remote video monitoring, and the Gateway Web Client is a simplified web browser version of the Avigilon™ Control Center Client software. The Gateway software is used to configure remote access and stream video from your Avigilon Control Center system to remote devices.

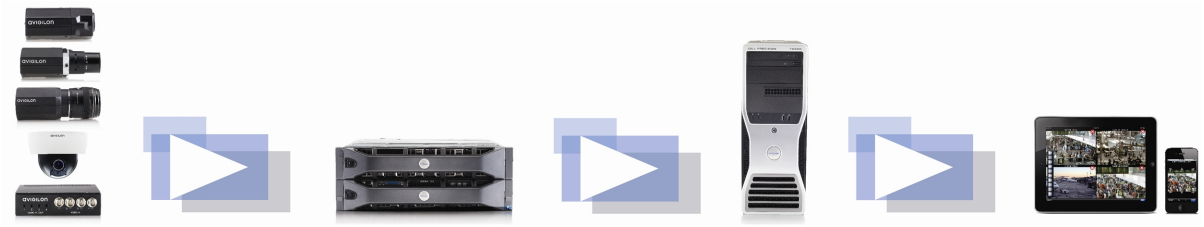


Figure 1: The Avigilon Control Center system workflow

Accessing the Gateway

On the computer running the Gateway, the Gateway configuration can be accessed in any of the following ways:

- Double-click the  **Avigilon Control Center Gateway** shortcut on the desktop.
- From the Start menu, select **All Programs > Avigilon > Avigilon Control Center Gateway > Avigilon Control Center Gateway**.
- In a web browser, enter **http://localhost/**.

NOTE: By default, the Gateway can only be configured locally, but you can enable remote configuration on the Network page.

When the Gateway opens in a web browser, enter your login information.

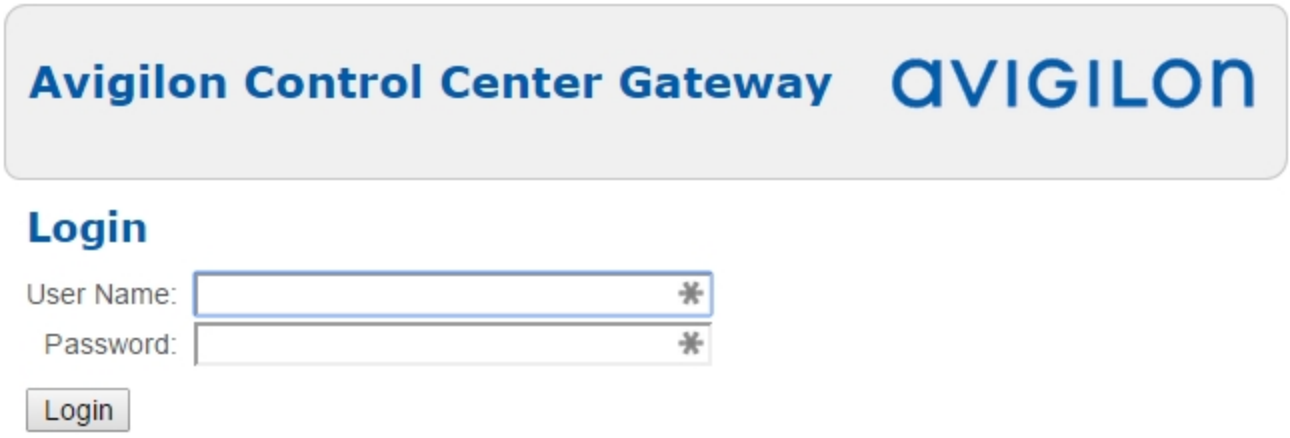


Figure 2: The Avigilon Control Center Gateway page

System Requirements

The Gateway software can be installed on the same computer as the Avigilon Control Center Server software, but it is strongly recommended that the Gateway be installed separately.

The Gateway can handle up to 36 concurrent video streams if installed on a computer with the following minimum system requirements:

System Requirement	Recommended
Operating System	Windows Server 2008, or Windows 7
Processor	Quad Core 2.0 GHz
System RAM	4 GB DDR2
Hard Drive Capacity	500 MB

NOTE: Supported browsers are: Safari - Versions 6+, Firefox - Versions 15+, Chrome - Versions 20+, Internet Explorer - Versions 9+.

For More Information

Visit Avigilon at **http://www.avigilon.com/** for additional product documentation.

The Avigilon Training Center

The Avigilon Training Center provides free online training videos that demonstrate how to set up and use the Avigilon Surveillance System. Register online at the Avigilon Partner Portal site to begin: **http://avigilon.force.com/login**

Support

For additional support information, visit **http://avigilon.com/support-and-downloads/**. The Avigilon Partner Portal also provides self-directed support resources - register and login at **http://avigilon.force.com/login**.

Regular Avigilon Technical Support is available Monday to Friday from 12:00 a.m. to 6:00 p.m. Pacific Standard Time (PST):

- North America: +1.888.281.5182 option 1
- International: +800.4567.8988 or +1.604.629.5182 option 1

Emergency Technical Support is available 24/7:

- North America: +1.888.281.5182 option 1 then dial 9
- International: +800.4567.8988 or +1.604.629.5182 option 1 then dial 9

E-mails can be sent to: **support@avigilon.com**.

Upgrades

Software and firmware upgrades will be made available for download as they become available. Check http://avigilon.com/support-and-downloads/ for available upgrades.

Feedback

We value your feedback. Please send any comments on our products and services to feedback@avigilon.com

Setup

Initial Login

When you log in for the first time, use the default **User Name:** *administrator* and no **Password:**.

Once logged in, you are automatically redirected to the Set Administrator Password page to change the Administrator password.

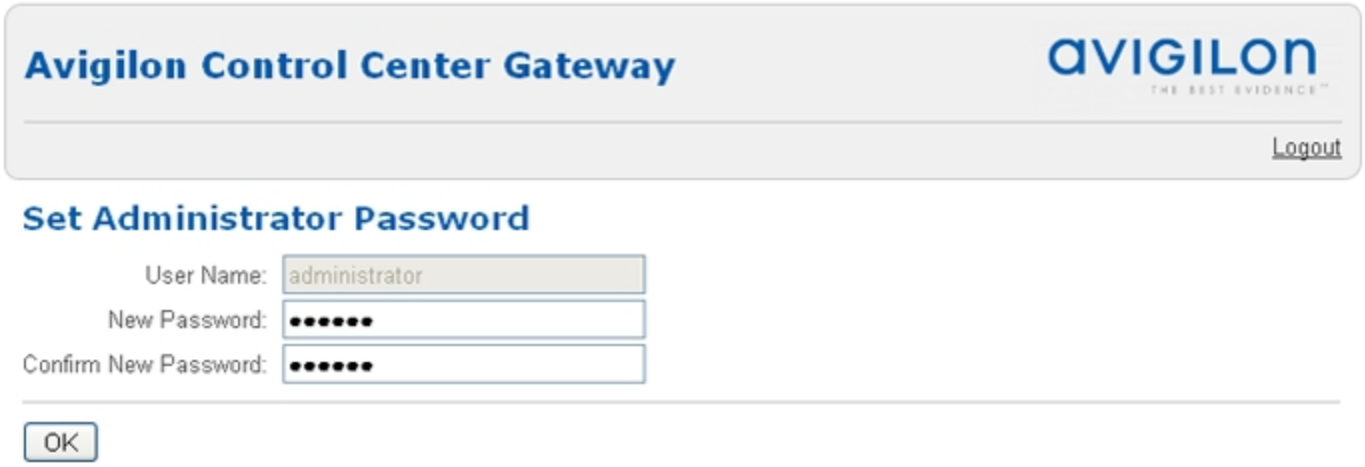


Figure 3: Gateway Set Administrator Password page

- Enter and confirm a **New Password:** for the administrator account, then click **OK**.

You are now logged in to the Gateway. You can access each of the Gateway configuration pages from the menu on the left.

Connecting Sites

After you log in, you are immediately taken to the Connect Sites page. You must connect Sites to the Gateway before they can be accessed through ACC Mobile and the Gateway Web Client.

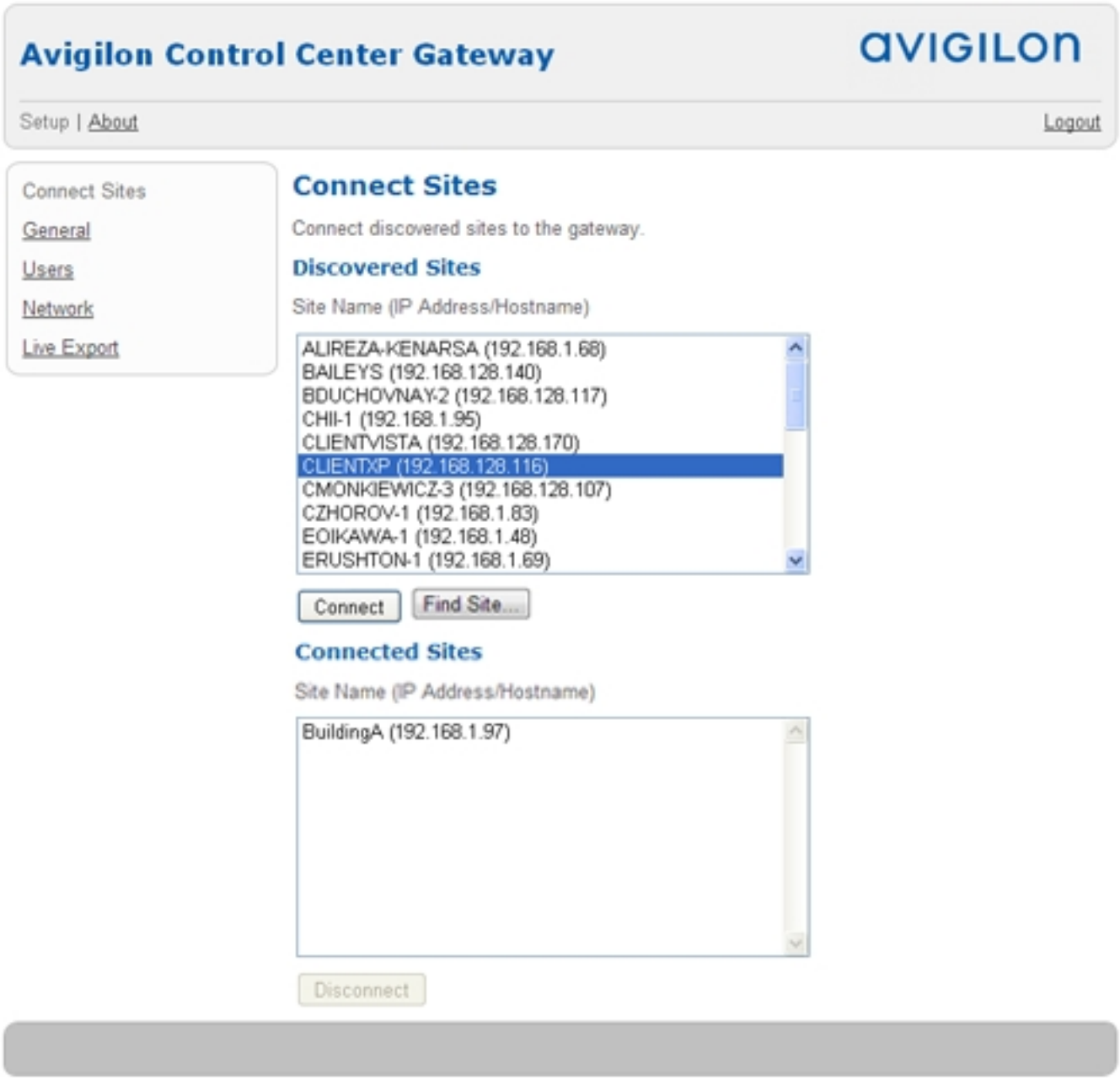


Figure 4: The Connect Sites page

1. To connect a Site to the Gateway, select a Site from the **Discovered Sites** list, then click **Connect**. The Site is added to the Connected Sites list.

   NOTE: Only Avigilon Control Center 5 Sites are listed. This version of the Gateway is incompatible with Avigilon Control Center 4.

2. To find a Site that is not listed, click **Find Site...**. On the Find Site page, enter the **IP Address/Hostname:** and **Port:** of a server in the Site you want to find, then click **OK**. The default port number is 38880.
3. To disconnect a Site from the Gateway, select the Site from the **Connected Sites** list and click **Disconnect**.

General

On the General page, you can name the Gateway.

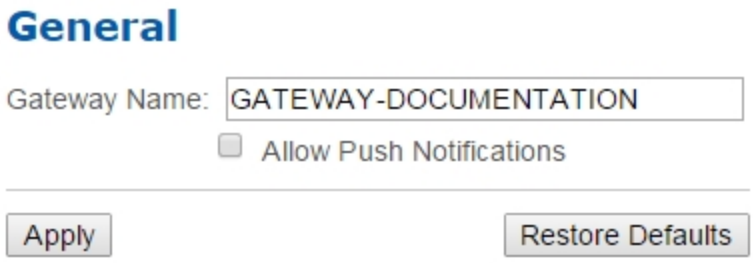


Figure 5: The General page

1. Enter a **Gateway Name:**. This is the name used to identify the Gateway in the ACC Mobile app.
2. To enable alarm push notifications to the ACC Mobile app, select the **Allow Push Notifications** check box.
3. Click **Apply**.
4. To restore the Gateway's default settings, click **Restore Defaults**. By default, the Gateway Name: is the same as the local computer.

Users

By default, the Gateway has two users: an administrator that configures the Gateway, and an operator that connects to the Gateway through ACC Mobile or the Gateway Web Client.

You can change the User Name: and Password: for the operator, but you cannot change the User Name: for the administrator.

The default operator User Name: is *operator* with no Password:.

The default administrator User Name: is *administrator* with no Password:. You are required to change this Password: after your initial login.

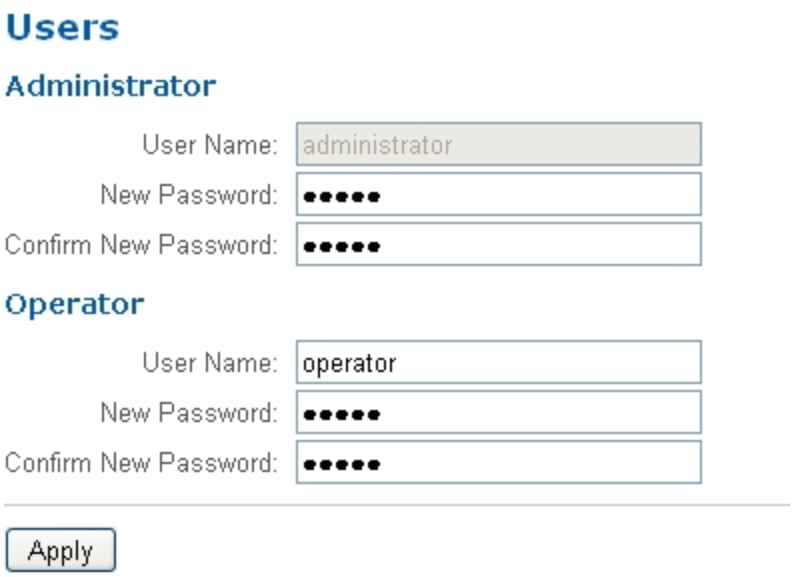


Figure 6: The Users page

1. To change the Password: for either the administrator or operator, enter and confirm a **New Password:**, then click **Apply**.
2. To change the operator User Name:, enter a new **User Name:**, then click **Apply**.

Network

On the Network page, you can set the ports used to access the Gateway.

The Streaming Ports are used to stream video from the Avigilon Control Center system to ACC Mobile or the Gateway Web Client. The Configuration Ports are used to access and configure the Gateway.

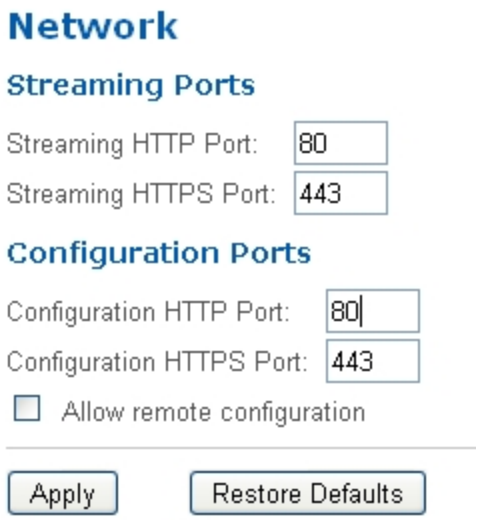


Figure 7: The Network page

1. To change the ports, enter a new port number, then click **Apply**.

   NOTE: After you change the port number, be sure to check that the Gateway still has access through your firewall. If using the Windows firewall, you must manually add an exception for the new port number.

2. If you want to configure the Gateway from a remote computer, select the **Allow remote configuration** check box and click **Apply**.

   Once the check box is selected, the Gateway can be accessed from any web browser at http://<Gateway IP Address>:<port number>

3. To restore the Gateway's default settings, click **Restore Defaults**. By default, the HTTP Port number is 80 and the HTTPS Port number is 443.

Live Export

On the Live Export page, you can set the system to export live video as a series of still images. You can choose the Image Format:, and select your export preferences.

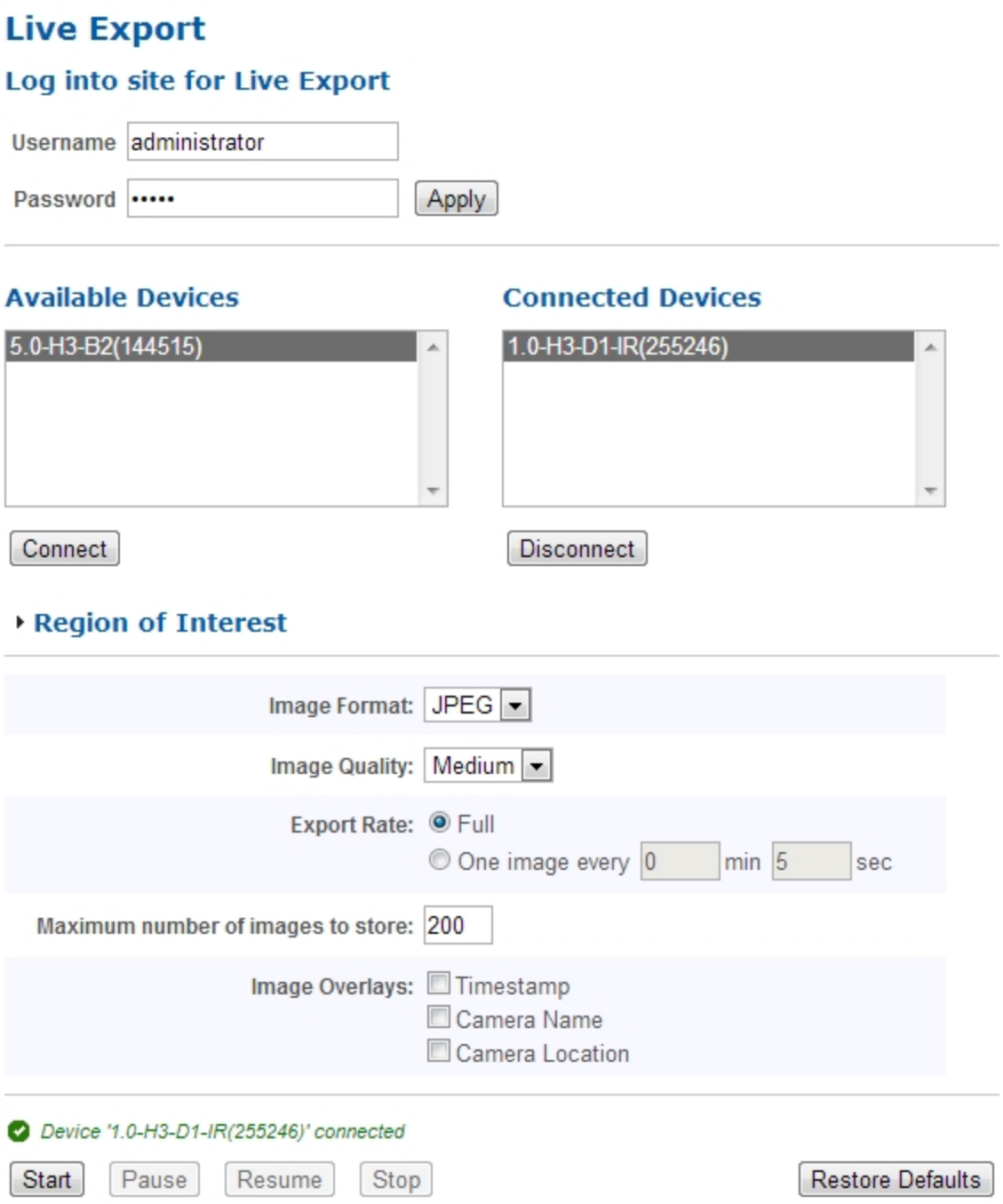


Figure 8: The Live Export page

1. Log in to the Site to which the Gateway is connected.
2. All the cameras that are connected to the servers you added to the Gateway are listed under **Available Devices**.

   Select a camera from the **Available Devices** list, then click **Connect**. You can connect multiple devices.

   NOTE: Live export will only occur on cameras that are connected to the Gateway.
3. In the **Image Format:** drop down list, select the export format: PNG, JPEG or TIFF.

4. (JPEG images only) In the **Image Quality:** drop down list, select the export quality level.
5. Set the Export Rate:
    - Select **Full** to export the live video stream at the camera's full image rate.
    - Select **One image every** to control the time between each exported image. For example, if you enter *0* min *5* sec, one image will be exported for every 5 seconds of video.
6. To limit the amount of images that are exported, enter a number into the **Maximum number of images to store:** field. The default number is 200 images.

    Be aware that if you leave the field blank, the live export will continue until there is no more available storage.
7. Select any of the listed image overlays to include that information on the exported images.
8. If you only want to export part of the camera's field of view, click **area**.

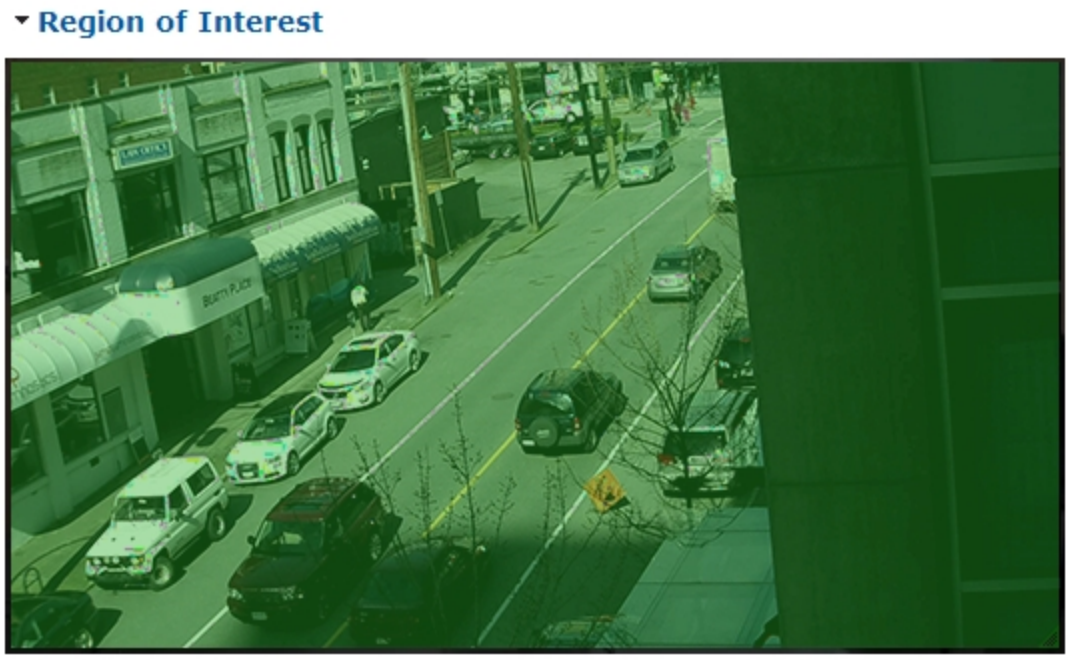


Figure 9: The area image panel

In the expanded image panel, move and resize the green overlay to highlight the area you want to export. Only the area covered by the green overlay is exported.

9. When you are ready, click **Start**.

    The export will run until the maximum number of images is reached, or you click **Stop**.

The exported images are automatically saved to the Avigilon Control Center Gateway *img* folder.

The folder is typically located here: C:\Program Files\Avigilon\Avigilon Control Center Gateway\img

Using the Gateway Web Client

The Gateway Web Client allows you to access your Avigilon Control Center system from any web browser.

To access the Gateway Web Client, you will need the IP Address/Hostname:, User Name: and Password: of the Gateway software, and a user account in the Avigilon Control Center system.

1. In a supported web browser, enter the Gateway IP address in this format: http://<Gateway IP Address>/acc

   NOTE: Supported browsers are: Safari - Versions 6+, Firefox - Versions 15+, Chrome - Versions 20+, Internet Explorer - Versions 9+.

   NOTE: If you are using Firefox, you need to manually override automatic cache management to avoid using excessive amounts of memory. Do the following:

   a. Open Firefox.

   b. Click  >  > **Network**.

   c. Select the **Override automatic cache management** check box. Make sure it is checked.

   d. In the **Limit cache to __ MB of space** field, enter a low value like **10**.

   e. Click **OK**.

2. The browser will prompt you to enter the Gateway **User Name** and **Password**.

   After you log in, the System Explorer will list all the Sites that are connected to the Gateway.

3. Right-click a Site and select **Log In...**
4. In the following dialog box, enter your **User Name:** and **Password:** for the Site then click **Log In**.

All the cameras in the Site are listed in alphabetical order. You can control video like you would in the Avigilon Control Center Client.

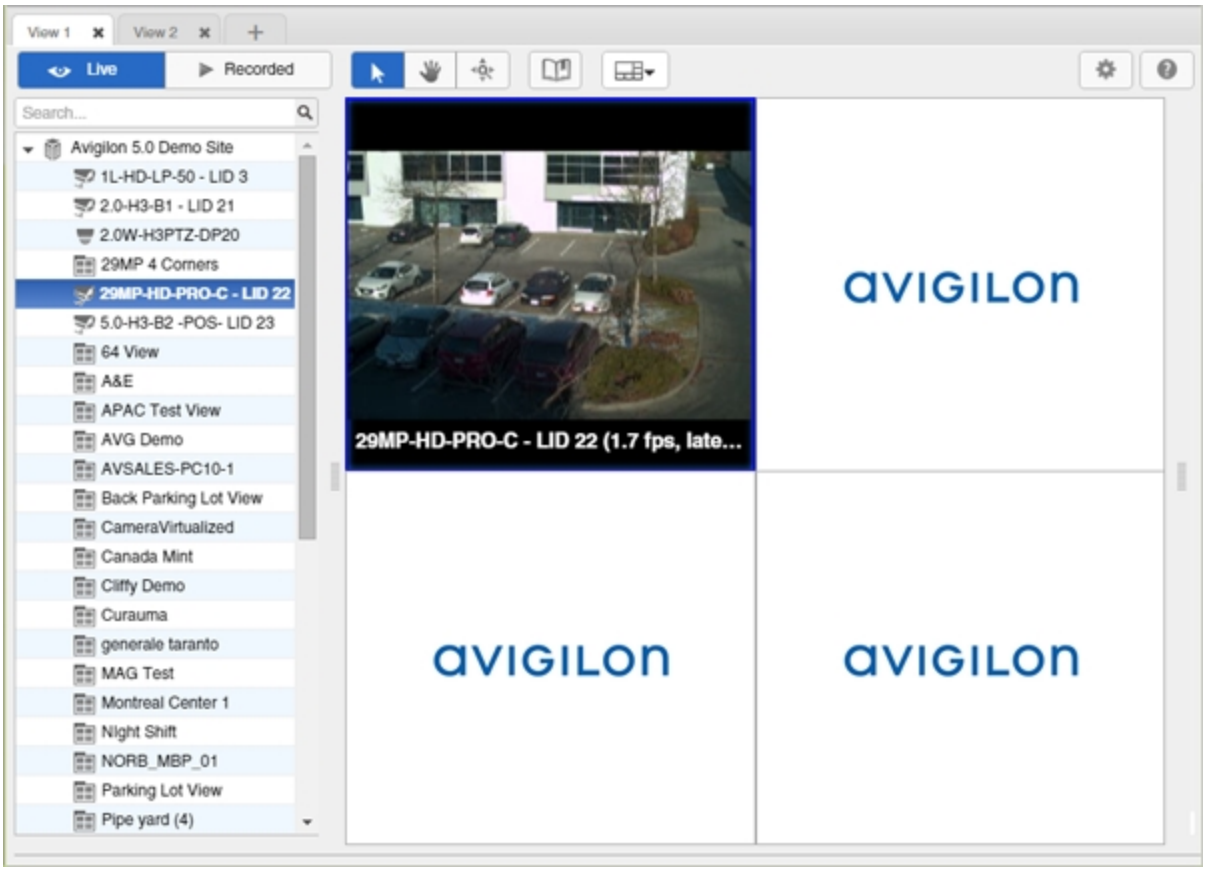


Figure 10: Gateway Web Client page

Avigilon Control Center Mobile

ACC Mobile is currently available for free from the Apple App Store and the Android Play Store.

To use the app, you will need to know the IP Address/Hostname:, Port:, User Name:, and Password: of the Gateway software, and have a user account in the Avigilon Control Center system.

Implementing an SSL Certificate for the Gateway

If your internal security settings require a specific type of SSL certificate, you can replace the certificate provided by Avigilon with your own certificate.

1. On the computer where the Gateway software is installed, use the Windows `certmgr.msc` to import your SSL certificate into Windows.
2. In Windows Explorer, navigate to `%programfiles%\Avigilon\Avigilon Control Center Gateway\cert`.
3. Back up this folder.
4. Rename your own SSL certificate `.pfx` file as `GatewayCertificate.pfx` and copy it into to the `\cert` folder.
5. Make a backup of `Gateway.cfg`.
6. Open `Gateway.cfg` in a text editor.
7. After opening `<Gateway>`, insert the following string:

   `<ConfigItem name="CertificatePassword" type="String"value="mypassword"/>`.
8. Replace the value *mypassword* in this configuration item with the SSL certificate's secret key.
9. Restart the Gateway service:
   a. In the **Start** menu, search for `services.msc`.
   b. In the Services window, select **Avigilon Control Center Gateway**.
   c. Click **Restart**.

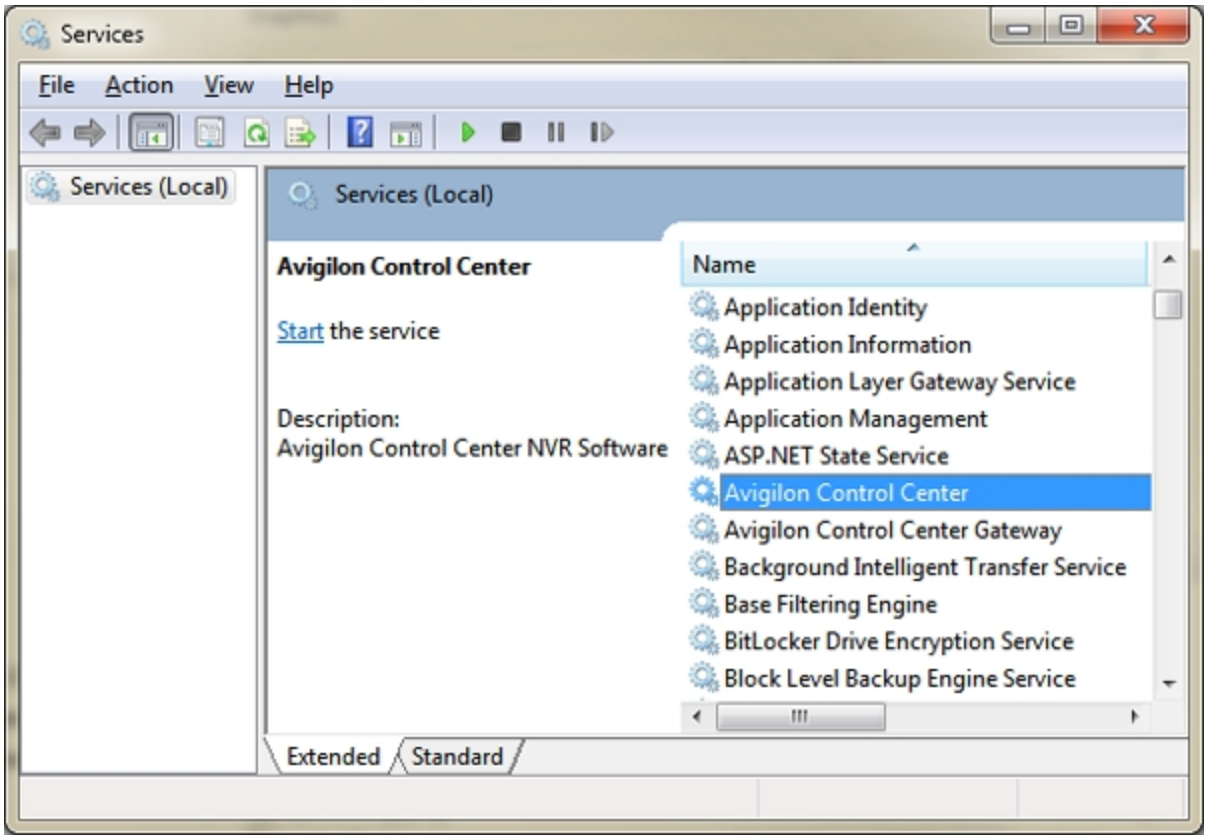


Figure 11: The Services window

NOTE: If your changes are not implemented or you notice an error while restarting the Gateway service, do the following:

a. Navigate to `%ProgramFiles%\Windows NT\Accessories\`.

b. Right click on **`Wordpad.exe`** and select **Run as administrator**.

c. Open `%ProgramFiles%\Avigilon Control Center Gateway\Gateway.cfg`.

d. Repeat steps 7 - 9.

This Page Left Intentionally Blank

Avigilon™ Control Center Virtual Matrix User Guide

Version 5.4.2

Avigilon Corporation
http://www.avigilon.com

Revised: 2014-12-23

PDF-ACCVM-E-Rev1

Table of Contents

What is the Avigilon™ Control Center Virtual Matrix?

The Avigilon Control Center Virtual Matrix software is an optional Enterprise Edition feature that allows you to control how video is monitored across multiple displays.

The Virtual Matrix software is used to connect a system with multiple monitors to the Avigilon Control Center system. Once connected, you can control what is displayed on each of the linked monitors through any instance of the Avigilon Control Center Client software. This includes choosing the cameras that are displayed, setting the View layout, and displaying maps, web pages and alarms.

A copy of the Virtual Matrix software can be downloaded from the Avigilon website.

System Requirements

	Minimum Requirements	Recommended Requirements
Monitor resolution	1280 x 1024	1280 x 1024
OS	Windows Vista, Windows 7, Windows 8 (32-bit or 64-bit) or Windows 8.1	Windows 7 (64-bit)
CPU	Intel Dual Core 2.0 GHz processor	Quad Core 2.0 GHz
System RAM	2 GB	2 GB
Video card	PCI Express, DirectX 10.0 compliant with 256 MB RAM	PCI Express, DirectX 10.0 compliant with 256 MB RAM
Network card	1 Gbps	1 Gbps
Hard disk space	500 MB	500 MB

Updating the Help Files

The help files for the Control Center Client software and Virtual Matrix software are all stored with the Control Center Server application.

If one of these components is ever updated before the others, the help files may become out of date or describe features that are not currently supported by your system.

- If the help files become out of date, download and install the latest help files from the Avigilon website. The help files are available in different installer packages divided by language and related software components.
- If the help files describe a feature that is not currently supported by your copy of the software, upgrade to the latest version.

For More Information

Visit Avigilon at **http://www.avigilon.com/** for additional product documentation.

The Avigilon Training Center

The Avigilon Training Center provides free online training videos that demonstrate how to set up and use the Avigilon Surveillance System. Register online at the Avigilon Partner Portal site to begin: http://avigilon.force.com/login

Support

For additional support information, visit http://avigilon.com/support-and-downloads/. The Avigilon Partner Portal also provides self-directed support resources - register and login at http://avigilon.force.com/login.

Regular Avigilon Technical Support is available Monday to Friday from 12:00 a.m. to 6:00 p.m. Pacific Standard Time (PST):

- North America: +1.888.281.5182 option 1
- International: +800.4567.8988 or +1.604.629.5182 option 1

Emergency Technical Support is available 24/7:

- North America: +1.888.281.5182 option 1 then dial 9
- International: +800.4567.8988 or +1.604.629.5182 option 1 then dial 9

E-mails can be sent to: support@avigilon.com.

Upgrades

Software and firmware upgrades will be made available for download as they become available. Check http://avigilon.com/support-and-downloads/ for available upgrades.

Feedback

We value your feedback. Please send any comments on our products and services to feedback@avigilon.com

Getting Started

1. After you install the Avigilon Control Center Virtual Matrix software, launch the application by doing one of the following:

   - Double-clicking the  desktop shortcut
   - In the Start menu, select **All Programs** or **All Apps > Avigilon > Avigilon Control Center Virtual Matrix > Avigilon Control Center Virtual Matrix**.

2. When you are prompted, log in to a Primary Site.

   The Primary Site is the Site you plan to use to control the Virtual Matrix. You can add other Sites later, but you will only be able to edit the Virtual Matrix monitor views from the Primary Site.

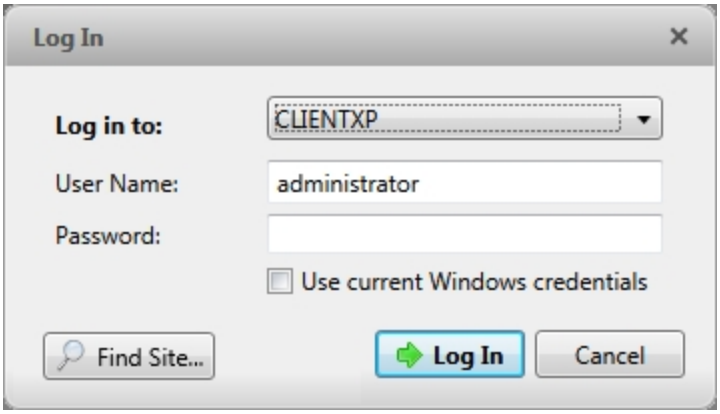


Figure 1: The Log In dialog box

   a. In the **Log in to:** drop down list, select the Site you want to connect to. If the Site you want to access is not listed, click **Find Site...**. For more information, see *Logging In To and Out Of a Site* on page 8.

   b. Enter your **User Name:** and **Password:** for the Site.

   c. Click **Log In**.

Once you are logged in, a View is automatically added to each monitor that is connected to the system. When you move your mouse, the Monitor Settings dialog box is automatically displayed on all monitors. If you leave your monitor idle, the dialog box will automatically hide itself. For more information about editing monitor settings, see *Editing Monitor Settings* on page 11.

To edit or control what is displayed in each View, you must log in to the Primary Site through the Avigilon™ Control Center Client software. Through the Client software, you can add cameras, maps and web pages to each View, and you can change the View layout of each monitor. For more information, see *The Avigilon Control Center Enterprise Client User Guide*.

Starting Up and Shutting Down the Virtual Matrix

Starting Up the Virtual Matrix

To start the Virtual Matrix software, repeat the procedure described in *Getting Started* on the previous page. By default, the application automatically logs back in to all of the Sites it was previously logged in to.

Shutting Down the Virtual Matrix

- To shut down the Virtual Matrix software, move your mouse across the screen to display the Monitor Settings dialog box, then click **Exit Application**.

This will shut down the Virtual Matrix software on the system and close all monitor Views.

While the Virtual Matrix software is shut down, the monitors remain listed in the Avigilon Control Center Client software. Any changes made to the monitor display settings are applied when the Virtual Matrix software is next launched.

Logging In To and Out Of a Site

To log in to a new Site, you will need to access the Monitor Settings dialog box.

Logging in to a Site

1. Click the screen to display the Monitor Settings dialog box.
   - If you want to change your Primary Site, click . This is the Site from which you edit the Virtual Matrix View.
   - If you want to add additional Sites, click **Add Site**. Adding extra Sites allows you include to cameras from the other Sites in the Virtual Matrix Views.
2. Click **OK**.
3. In the Log In dialog box, select the a Site from the drop down list then enter the **User Name:** and **Password:**.
4. Click **Log In**.
5. If the Site you want is not listed, click **Find Site...** to manually discover it.

   NOTE: All users with access to the Virtual Matrix are able to see the manually discovered Sites.

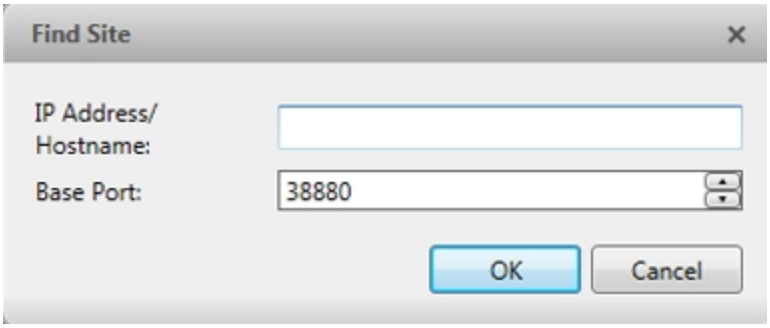


Figure 2: The Find Site dialog box

   a. Enter the **IP Address/Hostname:** of the Site you want to connect to.

   b. The Base Port: is 38880 by default. Consult your System Administrator if the Base Port: has been changed in the Admin Tool. For more information, see *The Avigilon Control Center Server User Guide*.

   c. Click **OK**

   d. Enter your Site **User Name:** and **Password:**.

Removing Additional Sites

1. Click the screen to display the Monitor Settings dialog box.
2. Under Additional Sites, select the Site you want to remove.

3. Click .

Adding and Removing a Monitor View

By default, a View from the Avigilon Control Center Client software is added to each monitor when the Virtual Matrix is launched. You can add or remove monitor Views as required.

Adding a Monitor View

- Move your mouse across the screen to display the Monitor Settings dialog box, then click **Add Monitor**.

A new View is automatically added to the same monitor. In the Client software, the new View is added to the Primary Site as a new monitor and can be controlled like the other Views displayed by the Virtual Matrix.

Removing a Monitor View

- Move your mouse across the screen to display the Monitor Settings dialog box, then click **Close Monitor**.

The Monitor Settings dialog box is closed with the View and the monitor is removed from the Primary Site.

Editing Monitor Settings

When you move your mouse across any monitor, the Monitor Settings dialog box automatically appears on every monitor. Each dialog box is specific to the monitor it is displayed on. If you leave the monitors idle, the dialog box will auto-hide on all monitors.

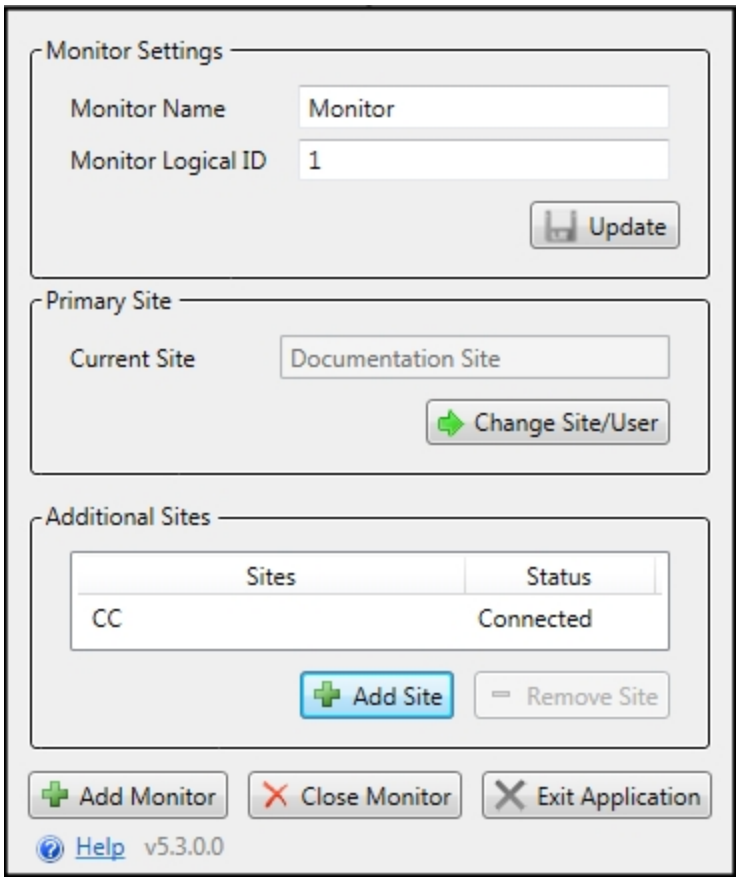


Figure 3: The Monitor Settings dialog box

1. **Monitor Settings:**
   - **Monitor Name:** Give the monitor a meaningful name to help you identify the monitor in the Avigilon Control Center Client software. By default, the monitor name is the *< Primary Site computer name>-<monitor number>*. Click **Update** to apply any changes you make.
   - **Monitor Logical ID:** Enter a unique number to access the monitor through keyboard commands in the Client software. Click **Update** to apply any changes you make.
2. **Primary Site:**
   - **Current Site:** This is the Primary Site, where you configure your Virtual Matrix View in the Avigilon Control Center Client software. To choose a different Primary Site, click . For more information, see *Logging In To and Out Of a Site* on page 8 .

3. **Additional Sites:**
    - **Sites:** The additional Sites that you are currently connected to.
    - **Status:** The statuses of the Sites the Virtual Matrix is connected to.
4. If you want to add or remove the View monitor on your screen, see *Adding and Removing a Monitor View* on page 10.

Resizing a Monitor View

When the Virtual Matrix software is initially launched, the View on each monitor is displayed in fullscreen mode, but you can restore and resize the View as needed.

- To restore down a View, move your mouse across the screen to display the title bar, then click  .

  When the View is restored down, you can resize it to fit your needs by clicking and dragging any corner of the window.

- To maximize a View, move your mouse across the View to display the title bar, then click  .

This Page Left Intentionally Blank

Avigilon Control Center Player User Guide

Version 4.6

OLH-PLAYER-A-Rev2

Avigilon
Tel +1.604.629.5182
Fax +1.604.629.5183
http://www.avigilon.com

Revised 2010-11-22

Table of Contents

Introduction

What is the Avigilon Control Center Player

The Avigilon Control Center Player is the video player for Avigilon Native Video Export (AVE) files and Avigilon Backup (AVK) files.

The Avigilon Control Center Player displays video in image panels, and allows you to control the playback through the Timeline. The Player is able to authenticate video files against tampering, and can be used to re-export video into other formats. Both AVE and AVK video include event data embedded in the file, so you are also able to search for specific alarms, POS transactions or license plate recognition events linked to the video.

A copy of the Player can be downloaded from the Avigilon website, or exported with the AVE file from the Avigilon Control Center Client software (see the *Avigilon Control Center Client User Guide* for more information).

To watch a video overview of the application, see *Module 3 - Avigilon Control Center Player* in the Avigilon University - End User Stream.

For More Information

Visit Avigilon at http://www.avigilon.com/ for additional product documentation.

Avigilon University

The Avigilon University provides free online training videos that demonstrate how to set up and use the Avigilon Surveillance System. Register online at the Avigilon Partner site to begin: http://avigilon.com/partners/

Support

For additional support information, visit http://www.avigilon.com/support/.

Regular Avigilon Customer Support Center hours of operation are from 6:00 a.m. to 6:00 p.m. Pacific Standard Time (PST) and can be reached by calling the toll-free number: +1.888.281.5182.

E-mails can be sent to: support@avigilon.com.

For emergency technical support 24 hours a day, 7 days a week, please call the Avigilon Emergency Technical Support Hotline at +1.604.506.3117.

Upgrades

Software and firmware upgrades will be made available for download as they become available. Check http://www.avigilon.com/support/software for available upgrades.

Feedback

We value your feedback. Visit our feedback page to comment on our products and services: http://avigilon.com/feedback/

Starting and Stopping the Avigilon Control Center Player

The Avigilon Control Center Player can be started or stopped at any time for viewing exported video.

Starting the Player

The Player can be opened in the following ways:

- Double-click the  **Avigilon Control Center Player** shortcut icon on the desktop.
- From the Windows Start menu, select **All Programs > Avigilon > Avigilon Control Center Player > Avigilon Control Center Player**.

When the application first opens, you will be prompted to open an AVE or AVK file.

- Double-click an Avigilon Native Video Export (AVE) file or Avigilon Backup (AVK) file. The Player opens and displays the video file.

Shutting down the Player

- In the Avigilon Control Center Client software, select **File > Exit**.

Views

What are Views?

A View is a tab composed of image panels that allow you to organize how video is monitored.

For example, you can choose to monitor video from multiple cameras simultaneously by using different layouts.

Selecting a Layout for a View

You can organize how video from multiple cameras are displayed by selecting a View layout.

- Select **View > Layouts > # Division**.
- On the toolbar, select one of the layout options.

Figure A. Layouts on the Toolbar

Making a View Full Screen

You can enlarge a View to maximize the use of the monitor.

Making a View Full Screen

- On the toolbar, click  **Full Screen**.

Ending Full Screen

- On the toolbar at the top left of the screen, click 

.

Tip: The toolbar is hidden when the application is idle. Move your mouse to display the toolbar.

Video

The Avigilon Control Center Player allows you to view exported Avigilon Native Video Export (AVE) video and Avigilon Backup (AVK) video in View tabs, similar to the Avigilon Control Center Client software.

If the video file contains video from multiple cameras, the video can be displayed in multiple image panels. You can zoom and pan the exported video images, and use the Timeline to control the playback of the recorded video.

Viewing Recorded Video

While reviewing recorded video, you can also choose to view the same camera video at different zoom depths and control the video playback.

Perform any of the following procedures to control the recorded video playback:

Adding and Removing Cameras in a View

To view a camera's video, display the camera in a View. The video can be removed from the View when it is no longer needed.

By default, when you first open an AVE or AVK file, video from all the available cameras are displayed in the View.

Adding a Camera to a View

Perform one of the following:

- Drag the camera from the System Explorer pane to an empty image panel in a View.
- In the System Explorer, right-click the camera and select **Add to View**.

  The camera is added to the next empty image panel in the View layout.

Tip: You can drag the same camera to multiple image panels to view the images at different zoom levels or with different video adjustment properties.

Removing a Camera From a View

Perform one of the following:

- Right-click the image panel, and select **Close**.
- Inside the image panel, click  **Close**.

Zooming and Panning a Video

The zoom and pan tools allow you to focus on specific regions in a camera video.

Using the Zoom Tools

You can rotate the scroll wheel on your mouse to zoom in and out of a video image. Or you can use the Zoom tools in the application:

1. Select a Zoom tool:
   - From the **Tools** menu, select **Zoom In Tool** or **Zoom Out Tool**.
   - On the toolbar, click  **Zoom In Tool** or  **Zoom Out Tool**.
2. Click the image panel until you reach the desired zoom depth.

Using the Pan Tools

You can right-click and drag inside an image panel to pan the video image, or you can perform the following:

1. Select the Pan tool:
   - From the Tools menu, select **Pan Tool**.
   - On the toolbar, click the  **Pan Tool**.
2. Drag the video image in any direction inside the image panel.

Listening to Audio in a View

If there is a microphone linked to a camera, the Audio bar is displayed in the image panel when you view the camera's video.

To control the audio settings, perform any of the following:

- In the lower-right corner of the image panel, click the **Speaker** icon to mute or activate the audio.
- Move the slider to change the volume level.

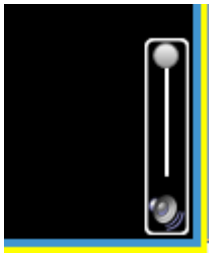


Figure A. Audio bar

Playing Back Recorded Video

The Timeline displays the time period when video were recorded and provides several controls for playing back the recordings.

The colored bars on the Timeline display a camera's recording history:

- A red bar indicates the camera recorded an event (for example, an alarm or motion event).
- A blue bar indicates the camera recorded video, but not in response to any event.
- White areas indicate that the camera did not record any video.
- An orange bar indicates a bookmark in the camera's recording history.

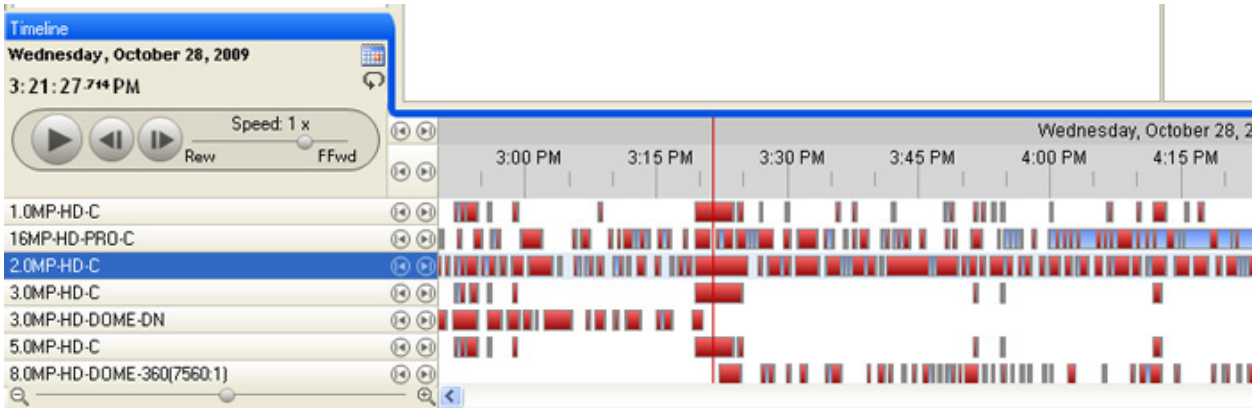
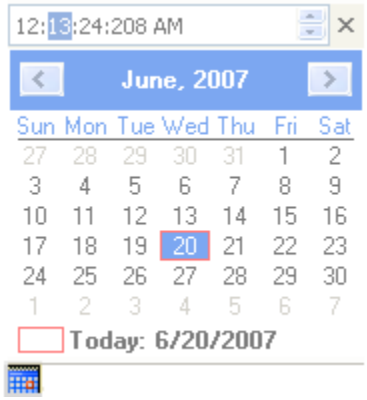
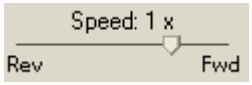
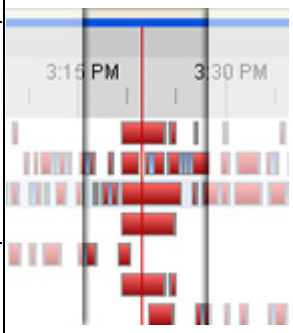


Figure A. Playback tools on the Timeline

Perform any of the following actions to control the playback of recorded video files:

Action	Tool	Procedure

To select a playback time		Perform one of the following: • Click the calendar and select a date and time. • On the Timeline, click on an area with recorded data indicated by a colored bar.
To loop playback		Click **Loop Playback** to repeat the video when the video is played.
To start playback		Click **Play**.
To stop playback		Click **Pause**.
To move forward a frame		Click **Step Forward**.
To move back a frame		Click **Step Backward**.
To control the playback direction and speed		Click and drag the slider to the right to move the video forward, or to the left to move the video in reverse. The further the slider is away from the center the faster the playback speed.
To jump forward or back on the Timeline		On the Timeline, click one of the **Go Forward** or **Go Back** buttons to move to different points on the Timeline.
To expand the Timeline to a specific moment in time		Perform one of the following: • Move the slider to zoom in or zoom out on the Timeline. • You can also use the mouse scroll wheel to zoom in or zoom out on the Timeline.

To center the Timeline on the time marker		Right-click the Timeline, and select **Center on Marker.**
To move through the Timeline quickly with the time marker		Drag the time marker through the Timeline.
To pan the Timeline		Perform one of the following: • Move the Timeline horizontal scroll bar at the bottom of the application window. • Right-click and drag the Timeline.

Adjusting Video Display in Image Panels

You can adjust the image panel display settings to enhance the video display on your monitor.

Maximizing an Image Panel

You can enlarge an image panel to help magnify the video displayed.

Maximizing an Image Panel

Perform one of the following:

- Right-click an image panel and select **Maximize**.
- Inside the image panel, click **Maximize**.
- Double-click the image panel.

Restoring an Image Panel

Perform one of the following:

- Right-click the maximized image panel, and select **Restore Down**.

- Inside the image panel, click **Restore Down**.
- Double-click the image panel.

Displaying Video Overlays

When you monitor video in a View, you can select the type of information that is displayed over the video in each image panel.

- Select **View > Image Overlays**, then select one or more of the following:

Option	Description
Camera Name	Displays the name given to the camera.
Camera Location	Displays the location given to the camera.
Timestamp	Displays the exposure timestamp of the video.
Motion Activity	Highlights detected motion events in red.

Changing the Display Quality

If you do not have sufficient network bandwidth or processing power, you may not be able to view video at the full image rate and full quality. You can bias the image panels to display video in high quality/low frame rate or low quality/high frame rate.

1. Select **Tools > Change Display Quality...** to open the Change Display Quality dialog box.
2. In the Change Display Quality dialog box, select one of the following:

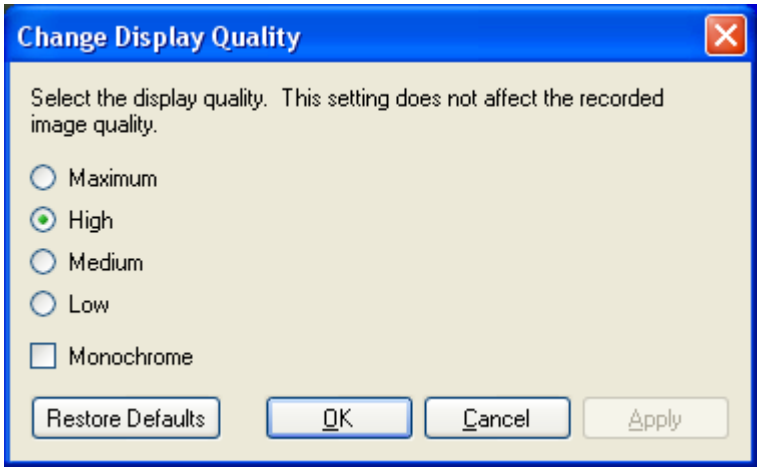


Figure A. Change Display Quality dialog box

- **Maximum:** displays the full video quality and results in lowest displayed image rate.
- **High:** displays 1/4 of the full video resolution.
- **Medium:** displays 1/16 of the full video resolution.
- **Low:** displays 1/64 of the full video resolution and results in the highest displayed image rate.

3. Select the **Monochrome** check box to display the video in black and white.
4. Click **OK**.

Changing the Image Panel Display Settings

You can change the image panel display settings to bring out video details that are hard to see with the image panel's default settings.

1. Right-click an image panel and select **Display Adjustments...**.

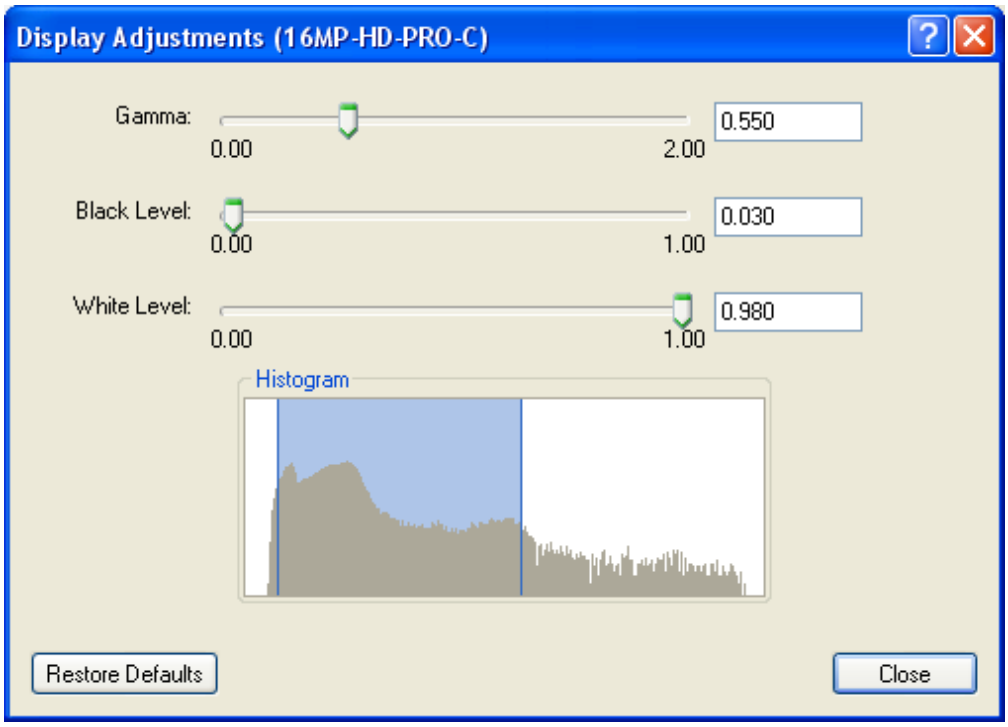


Figure A. Display Adjustments dialog box

2. Move the sliders to adjust the **Gamma**, **Black Level** and **White Level**.

   The image panel displays a preview of your adjustments.

3. Click **Restore Defaults** to clear your changes.

4. Click **Close**.

Viewing Analog Video in Deinterlaced Mode

If there are visible interlacing artifacts in the analog camera video, you can enable the deinterlacing filter to help improve the video image.

- To enable the deinterlacing filter, select **View > Display Deinterlaced Images**.

Authenticating Video

All Avigilon Native Video Export (AVE) and Avigilon Backup (AVK) files contain an encrypted digital signature that is used to ensure exported images have not been tampered with.

- To authenticate a video, select **Tools > Authenticate Images...**.

  The Authenticate Images dialog box appears and displays the application's progress as it checks all the video images for tampering.

When the process is complete, the Authenticate Images dialog box displays the number of images that are authentic and the number of images that have been corrupted.

Figure A. Authenticate Images dialog box

Search

You can search for recorded video by events, thumbnails, pixel area, POS transactions, alarms or license plates.

Note: If your video file does not contain any of the following information, that search option will not be displayed.

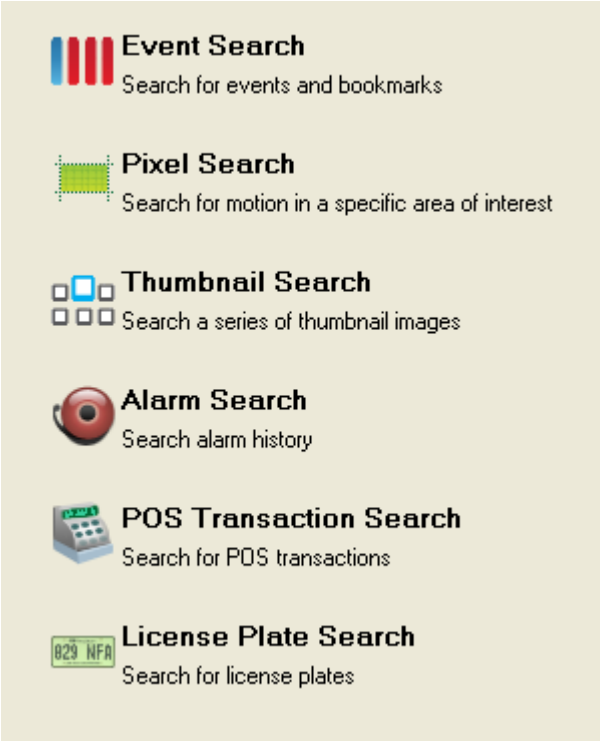


Figure A. Search options

Performing an Event Search

The Event Search allows you to search for a specific motion or digital input event by time range for the selected cameras.

1. Click 

to open the Search tab.
2. In the Search tab, select **Event Search**.

   The Search:Event tab is displayed.

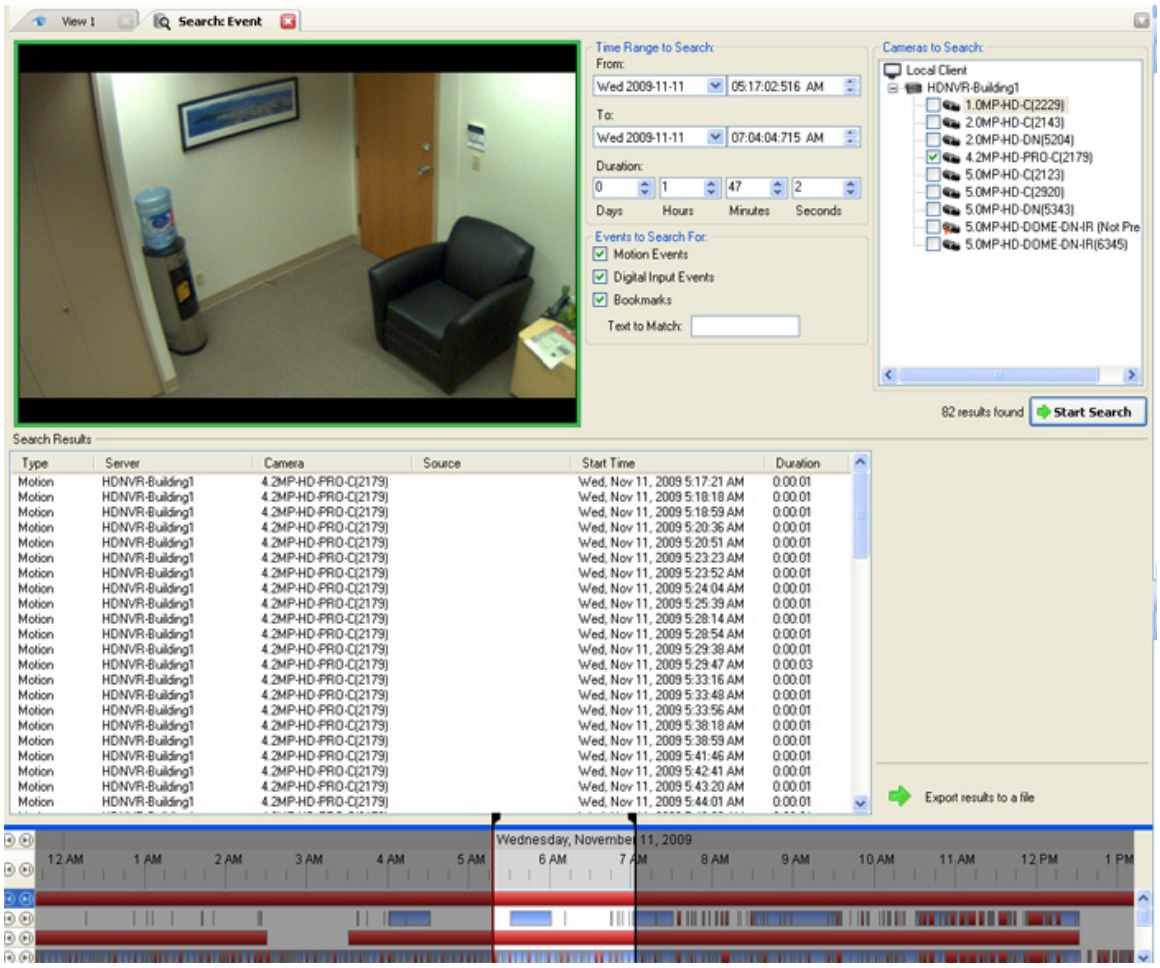


Figure A. Search: Event tab

3. In the Camera to Search area, select all the cameras you want to include in the search.
4. In the Time Range to Search area, set the date and time range of your search. The time range is highlighted on the Timeline by the black time range markers. You can also drag the time range markers to modify the time range.
5. In the Events to Search For area, select the types of events or bookmarks to include in the search.
6. In the Text to Match area, enter text to search for in the titles and descriptions of bookmarks.
7. Click **Start Search**.

Viewing Event Search Results

1. In the Search Results area, select a search result. The event timeline is highlighted and the related video is displayed in the search image panel.
2. Use the Timeline controls to review the event. See Playing Back Recorded Video for more information.
3. If you want to further refine your search, click **Perform a pixel search on this event** to perform a pixel search on the selected result. See Performing a Pixel Search for more information.
4. Click **Export this event** to export the selected event video. See Exporting Recorded Video and Images for more information about the available export settings.
5. To export all listed results, click **Export results to a file** and save the file.

Performing a Pixel Search

The Pixel Search allows you to search for motion events in specific areas of the camera's field of view.

1. Click 

to open the Search tab.
2. In the Search tab, select **Pixel Search**.

   The Search:Pixel tab displays.

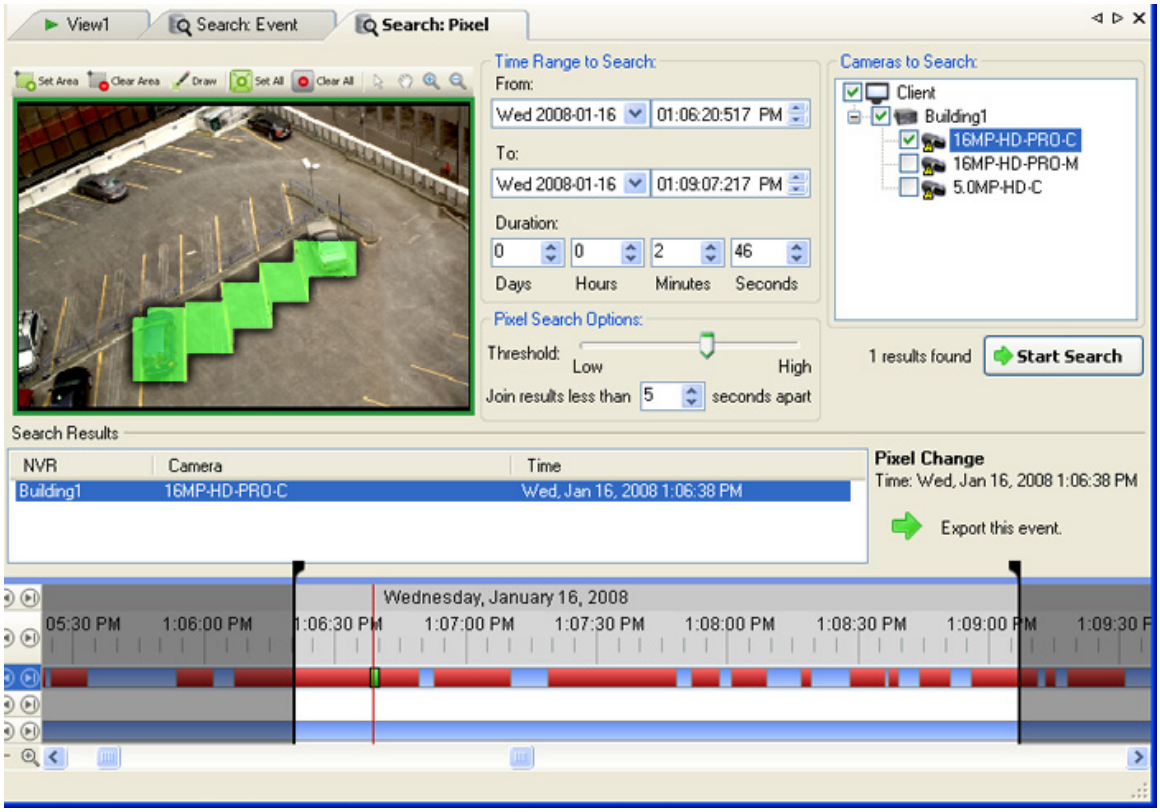


Figure A. Search:Pixel tab

By default, the entire video image is highlighted in green.

3. In the Camera to Search area, select a camera.
4. In the Time Range to Search area, set the date and time range of your search. The time range is highlighted on the Timeline by the black time range markers. You can also drag the time range markers to modify the time range.
5. Define the pixel search region by using the motion detection selection tools above the image panel. The pixel search will be performed in all areas highlighted in green.
6. In the Pixel Search Options area, drag the **Threshold** slider to select the amount of motion required to return a search result.

   The higher the threshold, the greater number of pixels must change before a result is returned.
7. Enter a number in the **Join results less than** field to define the minimum number of seconds between motion events before they are considered separate search results.
8. Click **Start Search**.

Viewing Pixel Search Results

1. In the Search Results area, select a search result. The event timeline is highlighted and the related video is displayed in the search image panel.
2. Use the Timeline controls to review the event. See Playing Back Recorded Video for more information.
3. Click **Export this event** to export the selected event video. See Exporting Recorded Video and Images for more information about the available export settings.
4. To export all listed results, click **Export results to a file** and save the file.

Performing a Thumbnail Search

The Thumbnail Search allows you to search through a specific period of time by viewing a series of thumbnail images.

1. Click 

to open the Search tab.
2. In the Search tab, select **Thumbnail Search**.

   The Search:Thumbnails tab displays.

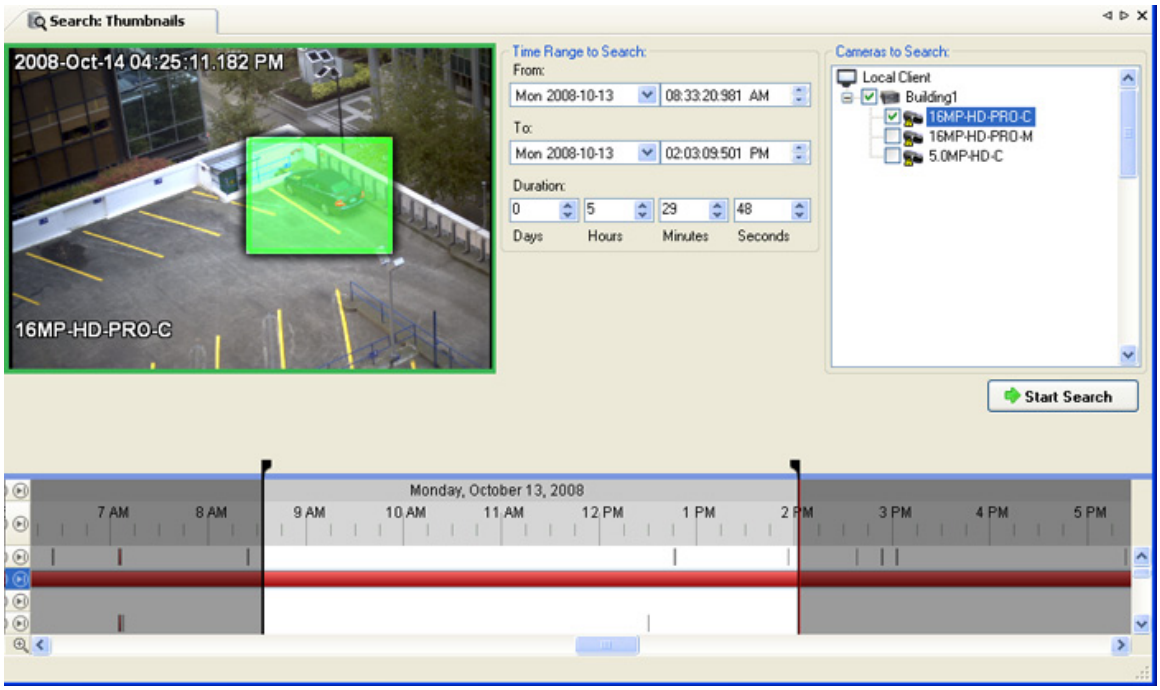


Figure A. Search:Thumbnails tab

3. In the Camera to Search area, select a camera.
4. In the Time Range to Search area, set the date and time range of your search. The time range is highlighted on the Timeline by the black time range markers. You can also drag the time range markers to modify the time range.
5. In the image panel, define the search region by moving the edges of the green overlay. Use this feature if you only want to see thumbnails for a region of the video image instead of the whole field of view.

   The thumbnail search will only be performed on the area highlighted in green.
6. Click **Start Search**.

Viewing Thumbnail Search Results

The search results display thumbnails at equal intervals on the Timeline.

1. To change the size of the search result thumbnails, select **Large Thumbnails**, **Medium Thumbnails**, or **Small Thumbnails** from the drop-down menu above the search results and click **Search Again**.

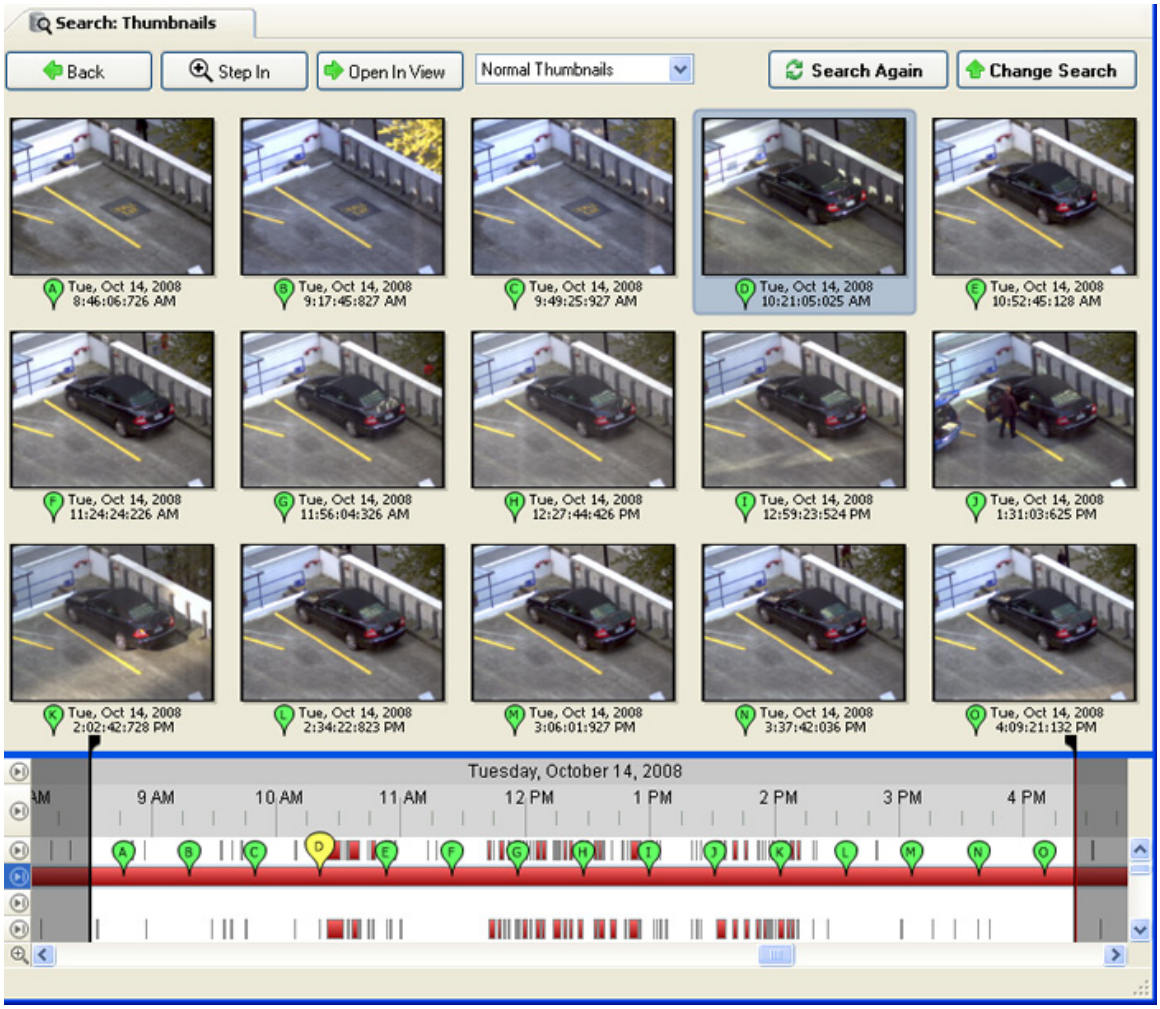


Figure B. Search:Thumbnail results tab

2. Select a thumbnail to highlight the image on the Timeline.
3. Click **Step In**, or double-click the thumbnail to perform another search around the thumbnail.

   Click **Back** to return to the previous results page.
4. Click **Open In View** to open the recorded video in a new View.

Performing an Alarm Search

Alarm search allows you to search for alarm events by time range for the selected alarms.

1. Click 

to open the Search tab.

2. In the Search tab, select **Alarm Search**.

   The Search:Alarms tab is displayed.

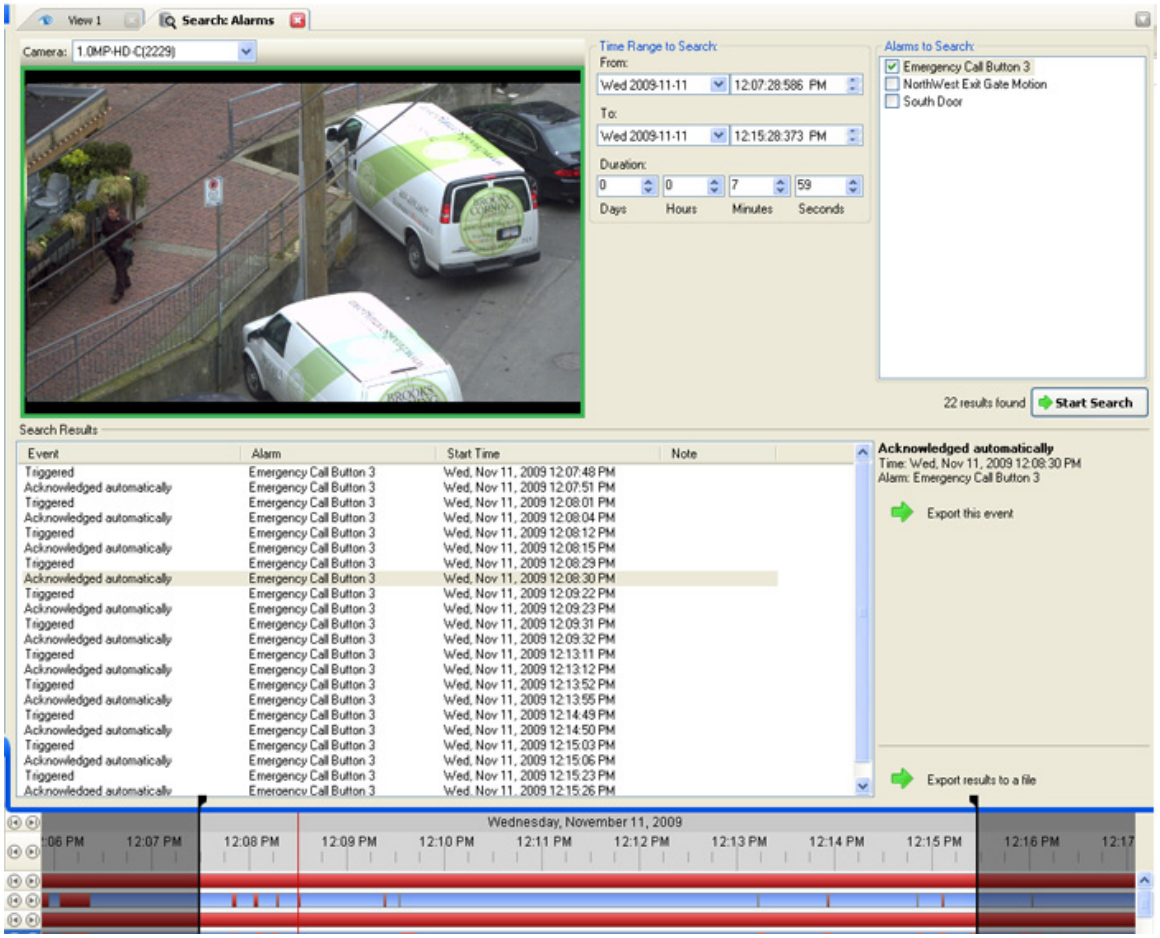


Figure A. Search:Alarms tab

3. In the Alarm to Search list, select all the alarms you would like to include in the alarm search.
4. In the Time Range to Search area, set the date and time range of your search. The time range is highlighted on the Timeline by the black time range markers. You can also drag the time range markers to modify the time range.
5. Click **Start Search**.

Viewing Alarm Search Results

1. In the Search Results area, select a search result. The event timeline is highlighted and the related video is displayed in the search image panel.
2. Use the Timeline controls to review the event. See Playing Back Recorded Video for more information.

3. If the event is linked to multiple cameras, select a camera from the **Camera** drop down list to change the video displayed in the image panel.

4. Click **Export this event** to export the selected event video. See Exporting Recorded Video and Images for more information about the available export settings.

5. To export all listed results, click **Export results to a file** and save the file.

Performing a POS Transaction Search

The POS Transaction Search allows you to search for POS transactions by transaction data source, content in the raw transaction data, and time range.

1. Click 

to open the Search tab.

2. In the Search tab, select **POS Transactions Search**.

   The Search: POS Transactions tab is displayed.

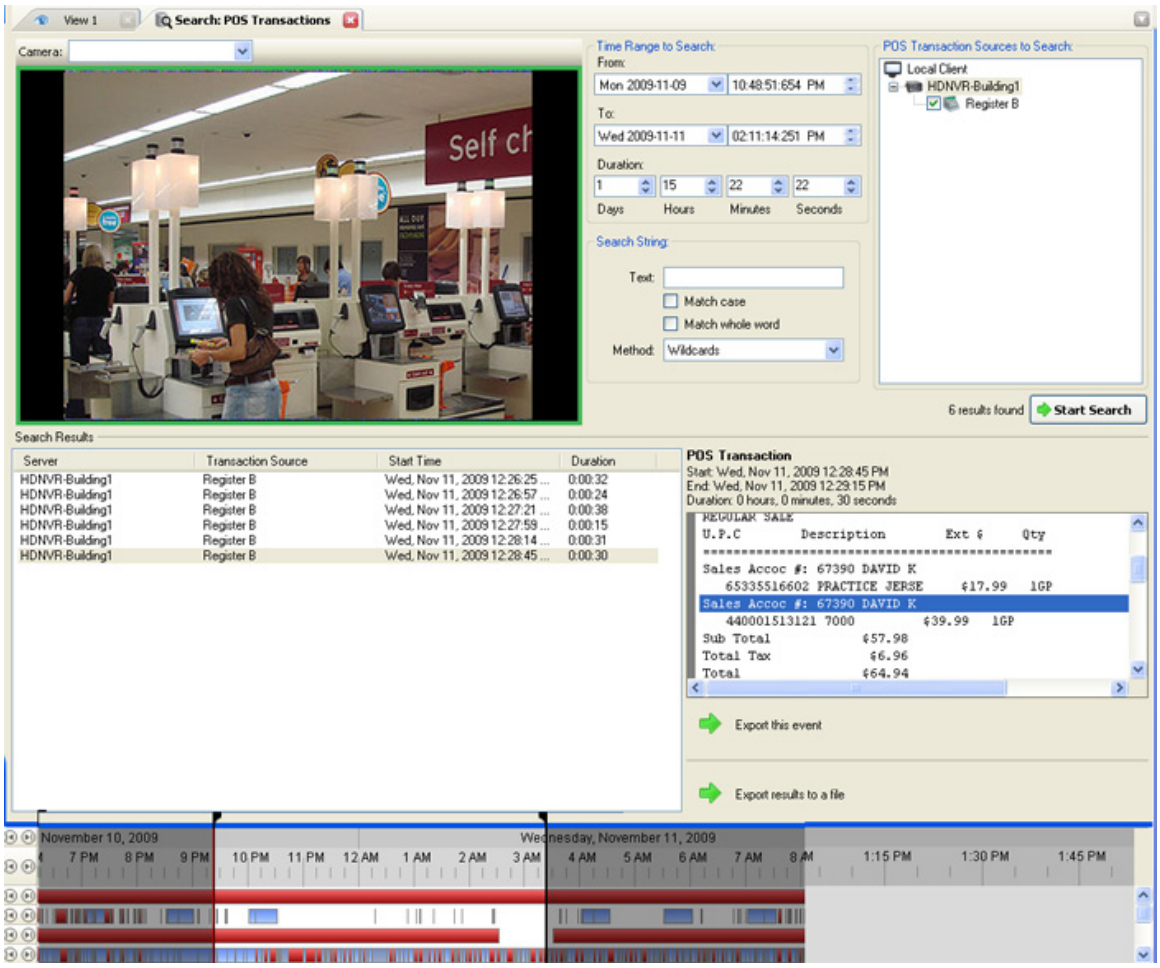


Figure A. Search:POS Transactions tab

3. In the POS Transaction Sources to Search area, select all the POS transaction sources you would like to include in the search.
4. In the Time Range to Search area, set the date and time range of your search. The time range is highlighted on the Timeline by the black time range markers. You can also drag the time range markers to modify the time range.
5. In the Search Text area, enter any text you want to search for, then select **Match case** and/or **Match whole word**, and choose a search method.

   Leave the **Text** field blank to find all transactions.
6. Click **Start Search**.

Viewing POS Transaction Search Results

1. In the Search Results area, select a search result. The event timeline is highlighted and the related video is displayed in the search image panel.
2. Use the Timeline controls to review the event. See Playing Back Recorded Video for more information.
3. If the event is linked to multiple cameras, select a camera from the **Camera** drop down list to change the video displayed in the image panel.
4. Click **Export this event** to export the selected event video. See Exporting Recorded Video and Images for more information about the available export settings.
5. To export all listed results, click **Export results to a file** and save the file.

Performing a License Plate Search

The License Plate Search allows you to search for specific license plates detected by the selected cameras.

1. Click 

to open the Search tab.
2. In the Search tab, select **License Plate Search**.

   The Search: License Plates tab is displayed.

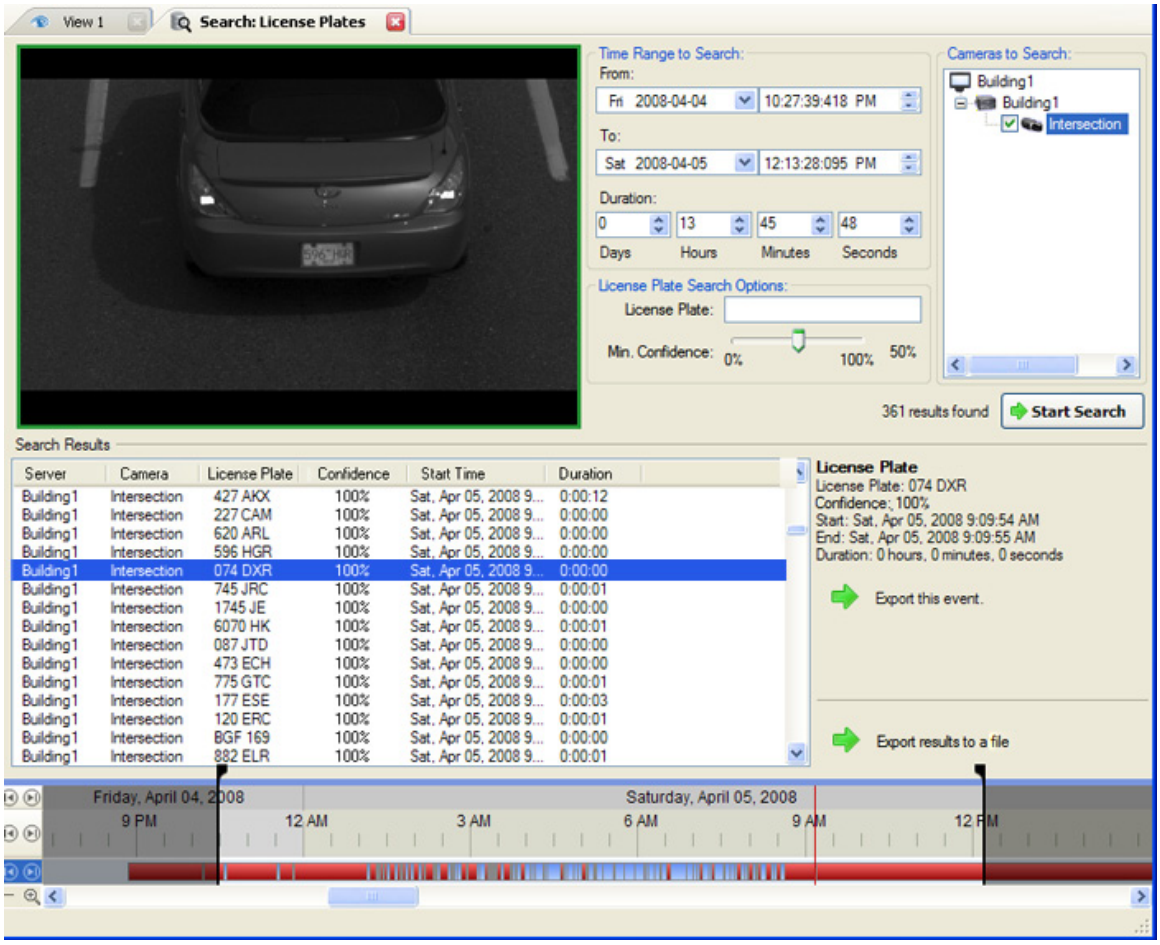


Figure A. Search: License Plates tab

3. In the Camera to Search area, select all the cameras you want to include in the search.
4. In the Time Range to Search area, set the date and time range of your search. The time range is highlighted on the Timeline by the black time range markers. You can also drag the time range markers to modify the time range.
5. In the License Plate Search Options area, enter the license plate number and minimum confidence for a match.
6. Click **Start Search**.

Viewing LPR Search Results

1. In the Search Results area, select a search result. The event timeline is highlighted and the related video is displayed in the search image panel.
2. Use the Timeline controls to review the event. See Playing Back Recorded Video for more information.

3. If the event is linked to multiple cameras, select a camera from the **Camera** drop down list to change the video displayed in the image panel.
4. Click **Export this event** to export the selected event video. See Exporting Recorded Video and Images for more information about the available export settings.
5. To export all listed results, click **Export results to a file** and save the file.

Export

You can export video and still images. You can specify a number of options to ensure the exported files are appropriate for your needs.

Saving a Snapshot of an Image

A Snapshot allows you to export a single frame in a video. You can specify the file format and various options, like overlays and resolution.

1. Open the snapshot Export tab:

   - In the image panel, click the  **Save Snapshot** icon.
   - Right-click the image panel and select **Save Snapshot**.

   The snapshot Export tab is displayed.

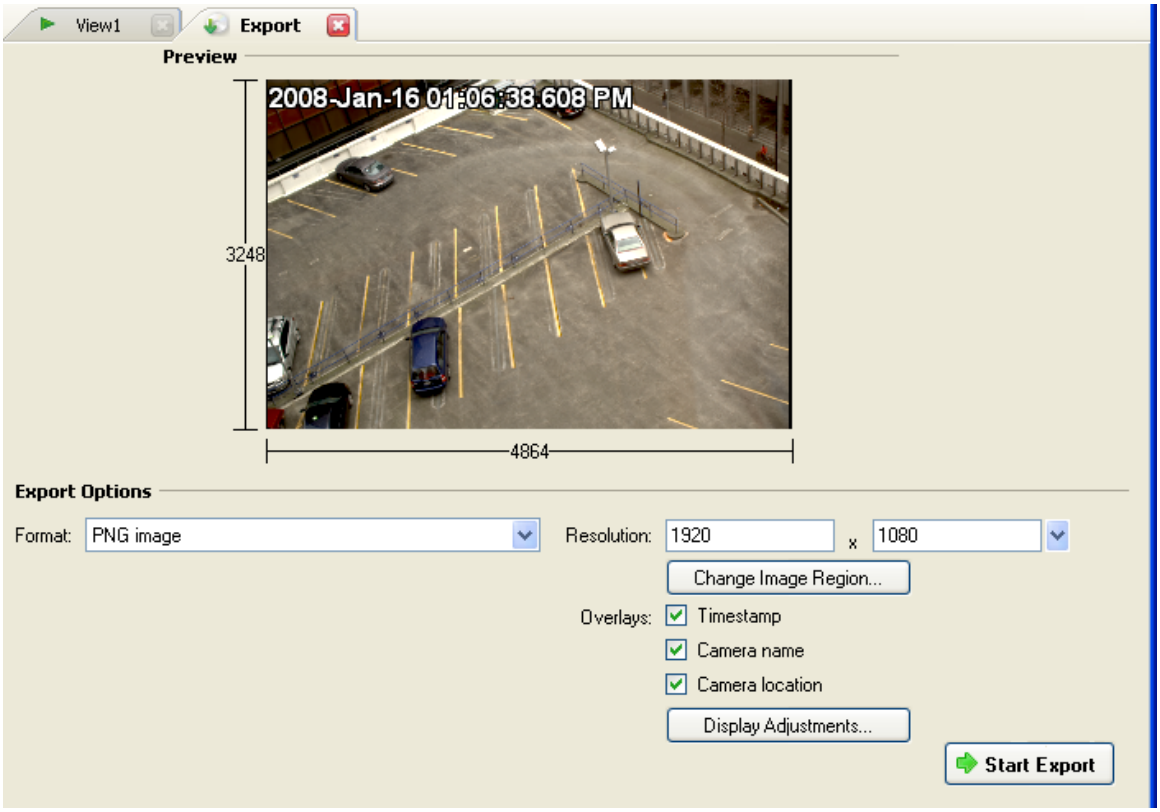


Figure A. Export tab for Snapshot export

2. In the Export Options area, select the image export format from the **Format** drop down list: **PNG**, **JPEG**, **TIFF**, **PDF**, **Print**, or **Native** format.
3. For the selected export image format, define your preferences:

Format	Image options
Native	Native (AVE) video is exported at full compression and includes data that is linked to the video image.
PNG	1. In the **Resolution** field, select a resolution for the video image. You can manually enter the resolution or click the drop down arrow to select a standard resolution. **Note:** The **Resolution** field automatically maintains the image aspect ratio. 2. Click **Change Image Region...** to change the region of the video image that is exported. In the Change Image Region dialog box, modify the size and position of the green overlay, then click **OK**. The Preview image panel will show the modified image region.

	3. Select the required image overlays: **Timestamp**, **Camera name**, and **Camera location**. 4. Click **Display Adjustments** to adjust the Gamma, Black Level and/or White Level.
JPEG	1. In the **Compression** field, select a compression level. 2. Set the image **Resolution**. 3. Click **Change Image Region** to only export a specific region of the image. 4. Select the required image overlays. 5. Click **Display Adjustments** to modify the image quality.
TIFF	1. Set the image **Resolution**. 2. Click **Change Image Region** to only export a specific region of the image. 3. Select the required image overlays. 4. Click **Display Adjustments** to modify the image quality.
Print	1. Click **Change Image Region** to only export a specific region of the image. 2. Click **Printer Settings...** to change the selected printer and paper size. 3. Select the required image overlays. 4. Click **Add Export Notes...** to add notes about the exported image. The notes are printed below the exported image. 5. Click **Display Adjustments** to modify the image quality.
PDF	1. Click **Change Image Region** to only export a specific region of the image. 2. Select the required image overlays. 3. Click **Add Export Notes...** to add notes about the exported image. 4. Click **Display Adjustments** to modify the image quality.

4. Click **Start Export**.

5. In the Save As dialog box, name the export file and click **Save**.

   The Preview area displays the video stream you are exporting.

6. When the export is complete, click **OK**.

Exporting Recorded Video and Images

You can export the video file into smaller files or into a different format for viewing in other applications.

Accessing the Export Tab

The Export tab can be accessed in any of the following ways:

- Select **File > Export**.
- On the toolbar, click 

.
- When searching for a specific video image, select a search result and click **Export this event**.

Exporting Native Video

When you export video files, you can choose to export the video in the Native (AVE) format.

1. Click 

to open the Export tab. For more information, see Accessing the Export Tab.

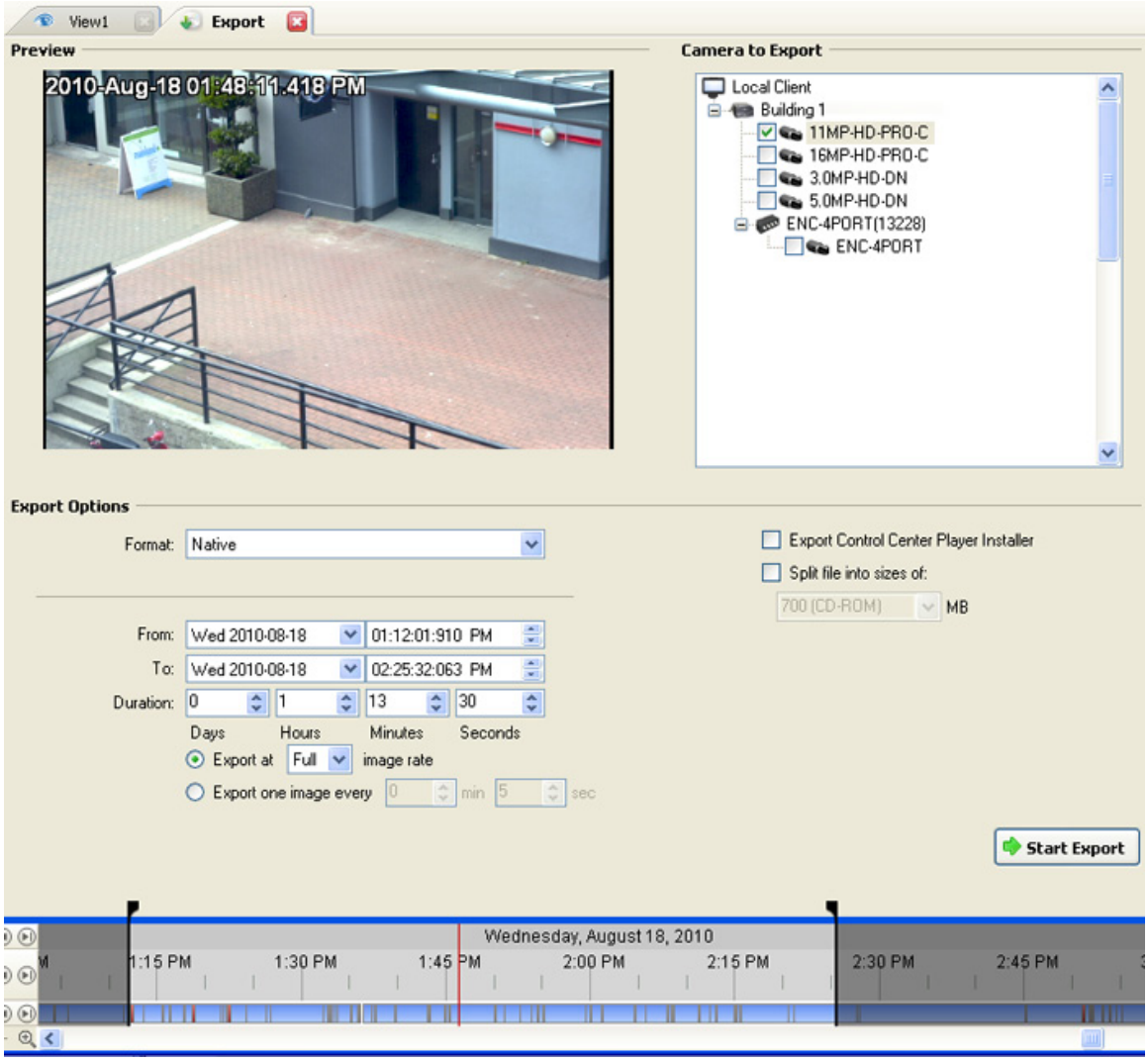


Figure A. Export tab for recorded video export

2. In the **Format** drop down list, select **Native**.
3. In the Camera to Export list, select all the camera video you want to export.
4. Enter the time range in the **From**, **To**, **Duration** fields. The time range is highlighted on the Timeline by black time range markers. You can also drag the time range markers to modify the time range.
5. Set the export image rate:

Option	Description
Export at __ image rate	Select this option to control how many images per second are exported. For example, the video is streaming at 30 images per second. If you select **1/2**, only 15 images for that second will be exported.

Export one image every __ min __sec	Select this option to control the time interval between each exported video image. For example, if you enter *5* min. *0* sec., only one image will be exported every 5 minutes.

6. Select the **Split file into sizes of:** check box to split the exported file into smaller files so the exported files can be stored on optical media, like a CD or DVD.
7. Click **Start Export**.
8. In the Save As dialog box, name the export file and click **Save**.

   The Preview area displays the video stream you are exporting.
9. When the export is complete, click **OK**.

Exporting AVI Video

When you export video files, you can choose to export the video in Audio Video Interleave (AVI) format.

1. Click 

to open the Export tab. For more information, see Accessing the Export Tab.

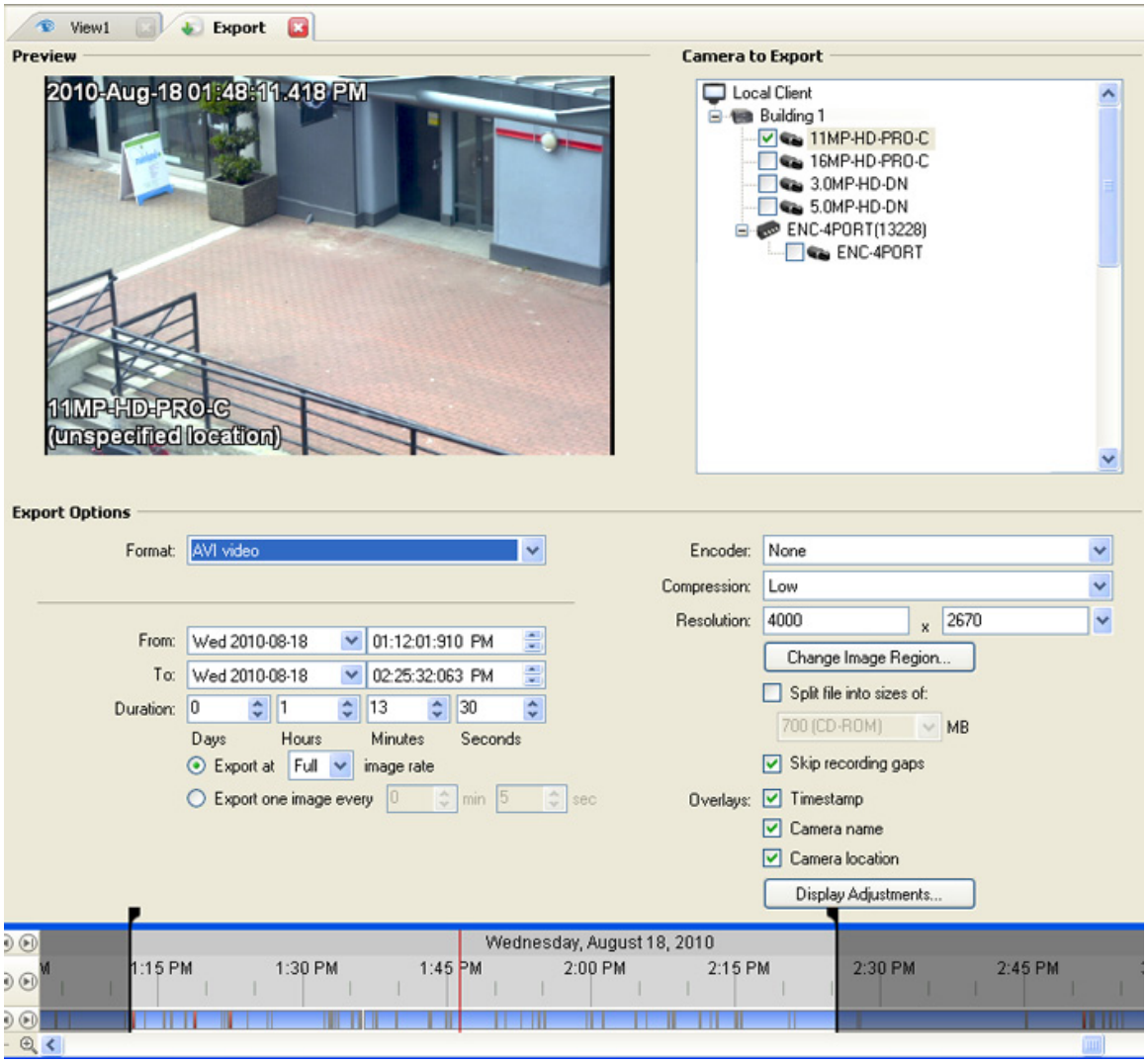


Figure A. Export tab for recorded video export

2. In the **Format** drop down list, select **AVI video**.
3. In the Camera to Export list, select all the camera video you want to export.
4. Enter the time range in the **From**, **To**, **Duration** fields. The time range is highlighted on the Timeline by black time range markers. You can also drag the time range markers to modify the time range.
5. Set the export image rate:

Option	Description
Export at __ image rate	Select this option to control how many images per second are exported. For example, the video is streaming at 30 images per second. If you select **1/2**, only 15 images for that second will be exported.

Export one image every __ min __sec	Select this option to control the time interval between each exported video image. For example, if you enter *5* min. *0* sec., only one image will be exported every 5 minutes.

6. In the **Encoder** field, select the compression used. The **VC-1 (Windows Media Video)** compression is included by default because it is tailored for high-resolution AVI encoding.
7. In the **Compression** field, select a compression level.
8. In the **Resolution** field, select a resolution for the video image. You can manually enter the resolution or click the drop down arrow to select a standard resolution.

   Note: The **Resolution** field automatically maintains the image aspect ratio.

   For high resolution video (11MP or 16MP) the greatest resolution option will be less than the camera's actual resolution because most media players cannot play high resolution AVI files.
9. Select the **Split file into sizes of:** check box to split the exported file into smaller files so the exported files can be stored on optical media, like a CD or DVD.
10. Click **Change Image Region...** to change the region of the video image that is exported.

    In the Change Image Region dialog box, modify the size and position of the green overlay, then click **OK**. The Preview image panel will show the modified image region.
11. Select the **Skips recording gaps** check box to avoid pauses in the video caused by gaps in the recorded video file.
12. Select the required image overlays: **Timestamp**, **Camera name**, and **Camera location**.
13. Click **Display Adjustments** to adjust the Gamma, Black Level and/or White Level.
14. Click **Start Export**.
15. In the Save As dialog box, name the export file and click **Save**.

    The Preview area displays the video stream you are exporting.
16. When the export is complete, click **OK**.

Exporting PNG, JPEG or TIFF Images

When you export recorded video, you can choose to export the video as still images in PNG, JPEG, or TIFF format.

1. Click 

to open the Export tab. For more information, see Accessing the Export Tab.

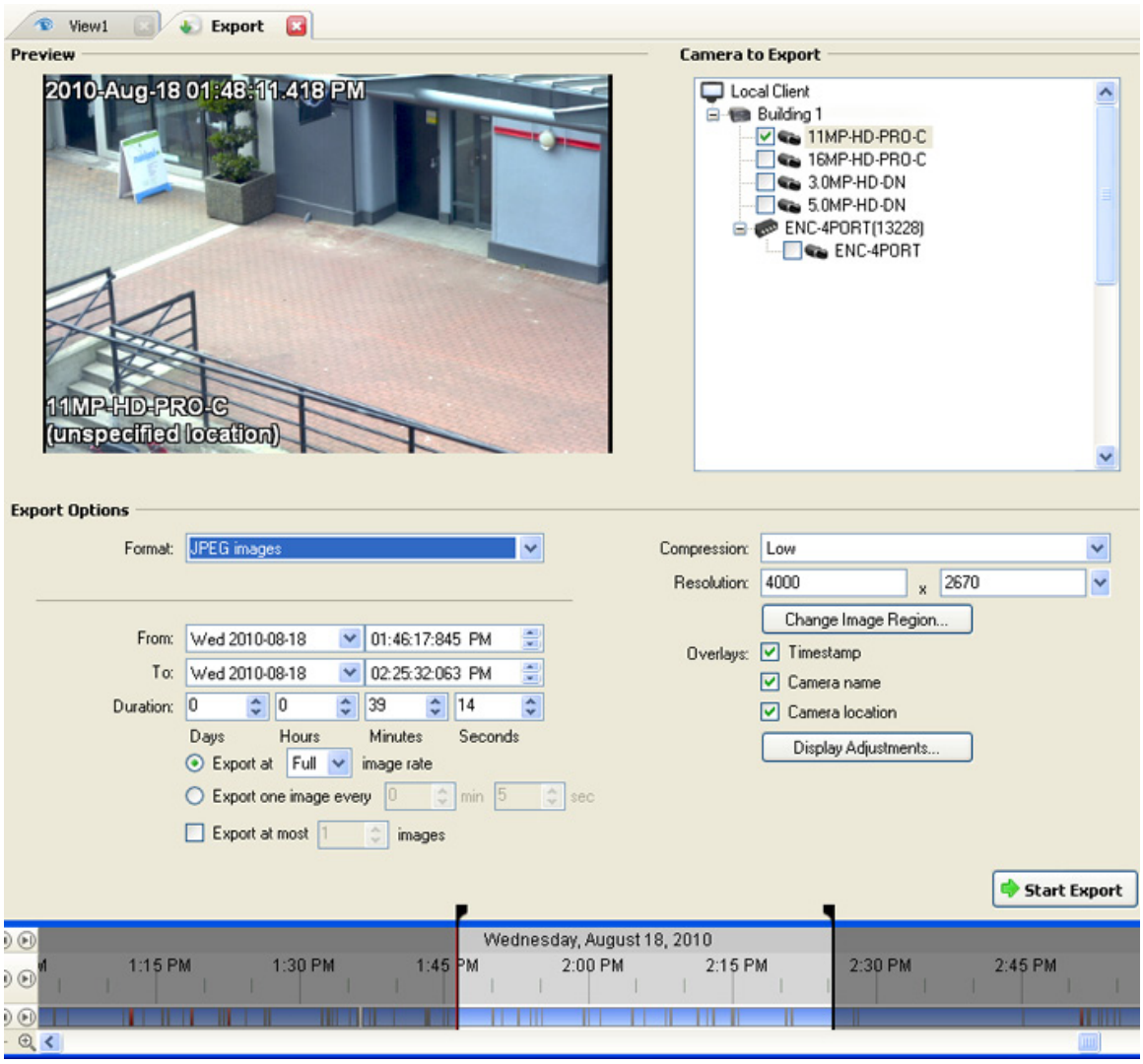


Figure A. Export tab for still image export

2. In the **Format** drop down list, select one of the following export formats: **PNG Images**, **JPEG Images**, or **TIFF Images**.
3. In the Camera to Export list, select all the camera video you want to export.
4. Enter the time range in the **From**, **To**, **Duration** fields. The time range is highlighted on the Timeline by black time range markers. You can also drag the time range markers to modify the time range.
5. Set the export image rate:

Option	Description
Export at __ image rate	Select this option to control how many images per second are exported. For example, the video is streaming at 30 images per second. If you select **1/2**, only 15

	images for that second will be exported.
Export one image every __ min __sec	Select this option to control the time interval between each exported video image. For example, if you enter *5* min. *0* sec., only one image will be exported every 5 minutes.

6. Select the **Export at most __ images** check box to limit the number of images that is exported. Enter the number of images you want exported.

   If this option is selected, the export will stop either when the number of specified images has been exported or when the specified time range has been reached.

7. (JPEG only)

   In the **Compression** field, select a compression level.

8. In the **Resolution** field, select a resolution for the video image. You can manually enter the resolution or click the drop down arrow to select a standard resolution.

   Note: The **Resolution** field automatically maintains the image aspect ratio.

9. Click **Change Image Region...** to change the region of the video image that is exported.

   In the Change Image Region dialog box, modify the size and position of the green overlay, then click **OK**. The Preview image panel will show the modified image region.

10. Select the required image overlays: **Timestamp**, **Camera name**, and **Camera location**.

11. Click **Display Adjustments** to adjust the Gamma, Black Level and/or White Level.

12. Click **Start Export**.

13. In the Save As dialog box, name the export file and click **Save**.

    The Preview area displays the video stream you are exporting.

14. When the export is complete, click **OK**.

Exporting PDF and Print Images

When you export recorded video, you can choose to export the video as still images for printing or in PDF format.

1. Click 

to open the Export tab. For more information, see Accessing the Export Tab.

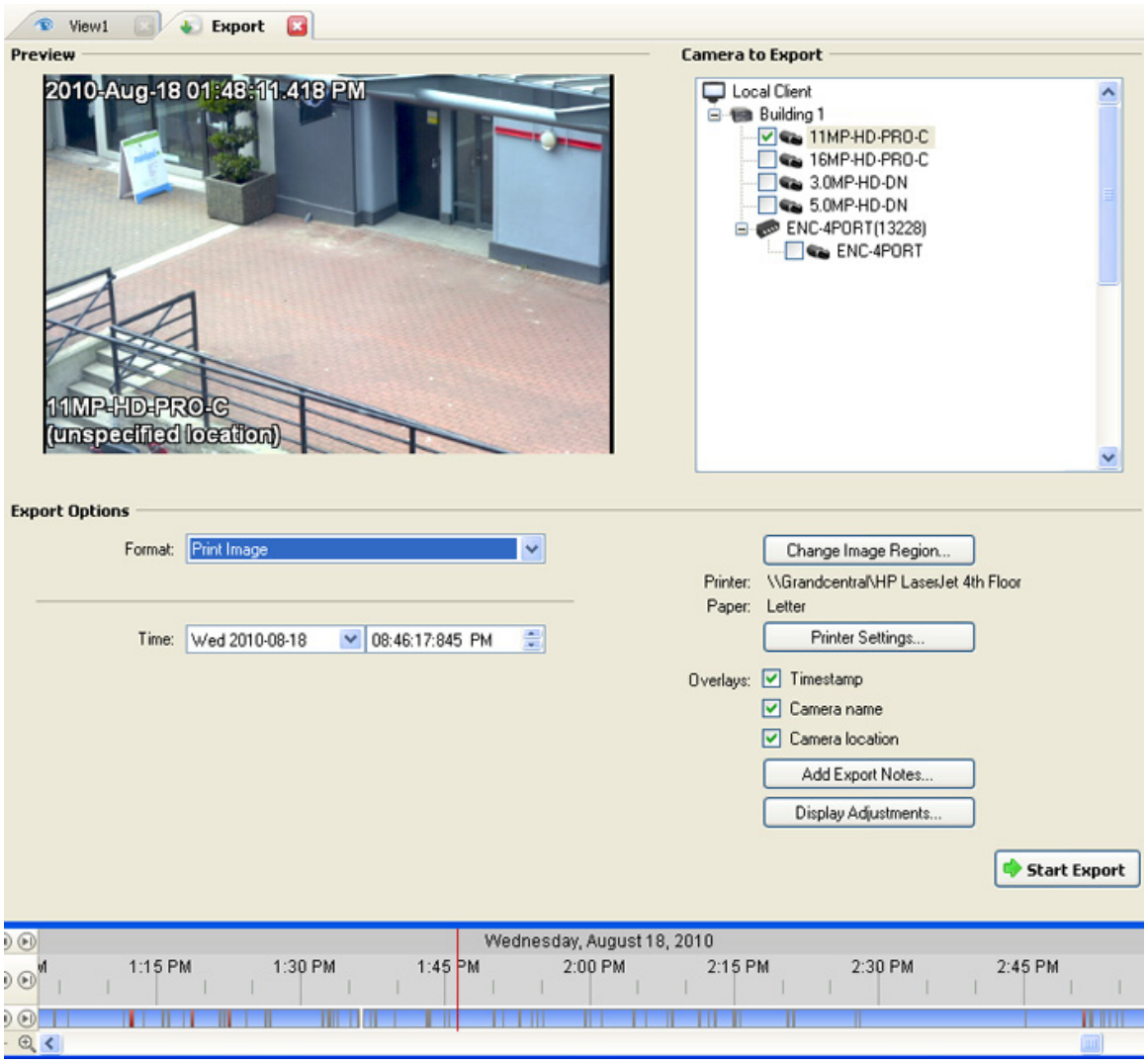


Figure A. Export tab for still image export

2. In the **Format** drop down list, select one of the following export formats: **Print Image** or **PDF File**.
3. In the Camera to Export list, select all the camera video you want to export.
4. In the **Time** field, enter the exact date and time of the video image you want to export.
5. Click **Change Image Region...** to change the region of the video image that is exported.

   In the Change Image Region dialog box, modify the size and position of the green overlay, then click **OK**. The Preview image panel will show the modified image region.
6. (Print Image only) Click **Print Settings** to change the printer and paper size that the image is printed on.
7. Select the required image overlays: **Timestamp**, **Camera name**, and **Camera location**.
8. Click **Add Export Notes** to add notes about the exported image. The notes are added below the image.

9. Click **Display Adjustments** to adjust the Gamma, Black Level and/or White Level.
10. Click **Start Export**.
11. In the Save As dialog box, name the export file and click **Save**.

    The Preview area displays the video stream you are exporting.
12. When the export is complete, click **OK**.

Exporting WAV Audio

If a video contains audio, the audio is exported with the video. If required, you can choose to only export the audio file.

1. Click 

to open the Export tab. For more information, see Accessing the Export Tab.

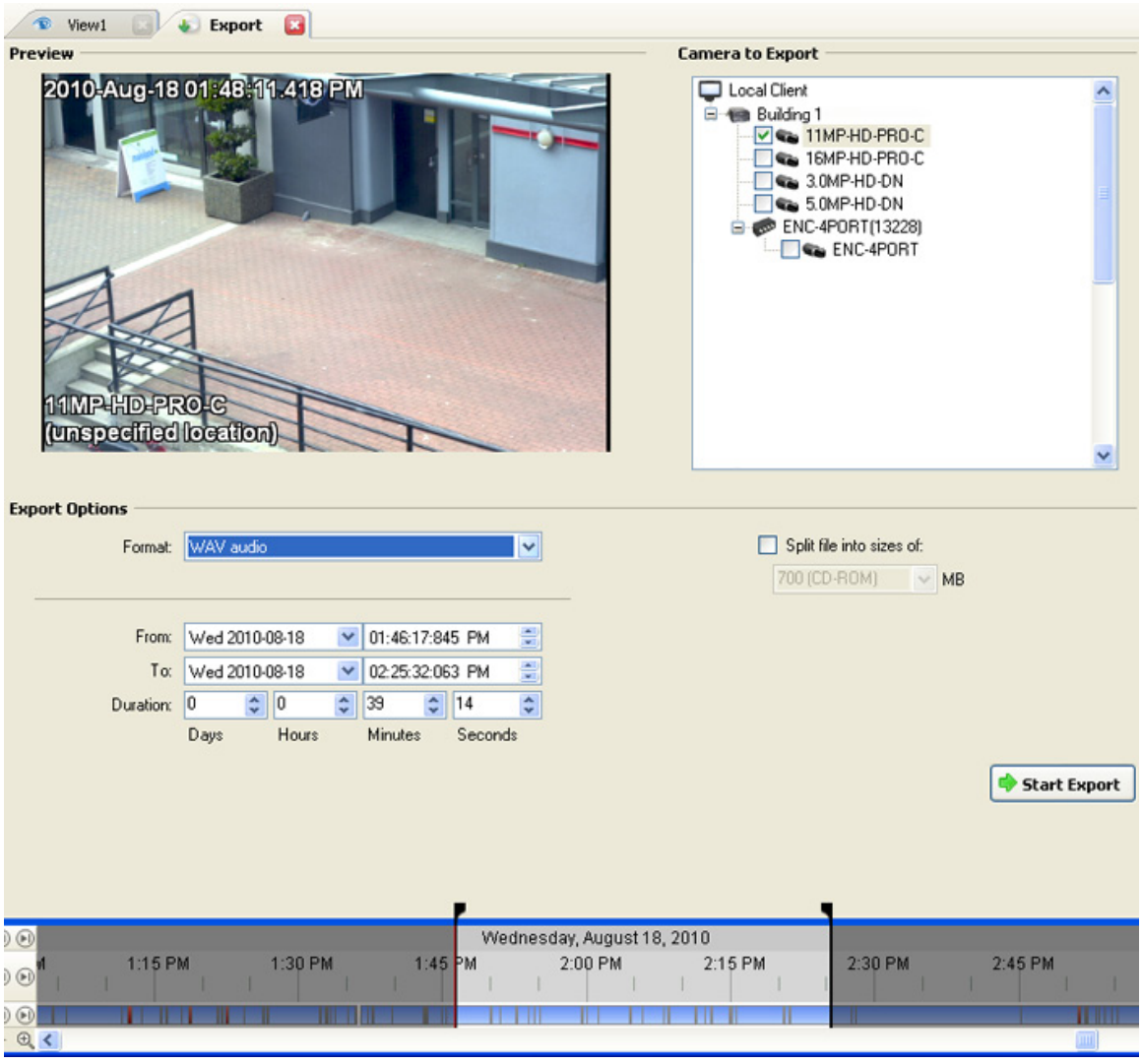


Figure A. Export tab for audio export

2. In the **Format** drop down list, select **WAV**.
3. In the Camera to Export list, select all the camera video you want to export.
4. Enter the time range in the **From**, **To**, **Duration** fields. The time range is highlighted on the Timeline by black time range markers. You can also drag the time range markers to modify the time range.
5. Click **Start Export**.
6. In the Save As dialog box, name the export file and click **Save**.

   The Preview area displays the video linked with the audio you are exporting.
7. When the export is complete, click **OK**.

This Page Left Intentionally Blank

User Guide

Avigilon™ Control Center Mobile

Version 2.0 for iOS

Avigilon Corporation
http://www.avigilon.com

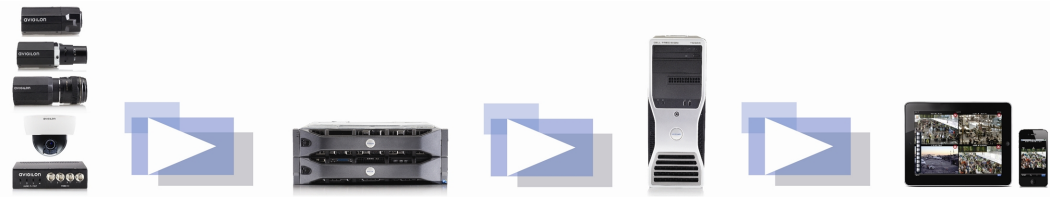
Revised: 2015-01-14

UG-ACCMOBILE-iOS-E_Rev1

Table of Contents

Introduction

The Avigilon™ Control Center Mobile app gives you access to live and recorded video from the Avigilon™ Control Center sytem on your mobile devices.



Device Requirements

- iPad® with iOS™ 7 or 8
- iPhone® with iOS 7 or 8
- iPod touch® with iOS 7 or 8

NOTE: Depending on your iOS version and type of mobile device, the screenshots in this document may look different from what is displayed on your device.

System Requirements

You must have access to the following software in your Avigilon Control Center system.

- Control Center Gateway
- Control Center Server

To make sure you have a secure connection, it is recommended that you only connect to the Gateway via HTTPS.

Consult with your System Administrator for more information.

- If you are running Avigilon Control Center 5.4 or later, you will have access to all of the features described in this document.
- If you are running Avigilon Control Center 5.2, you will not have access to Alarms.
- If you are running Avigilon Control Center 4 or 5.0, you will not have access to Saved Views or Alarms.

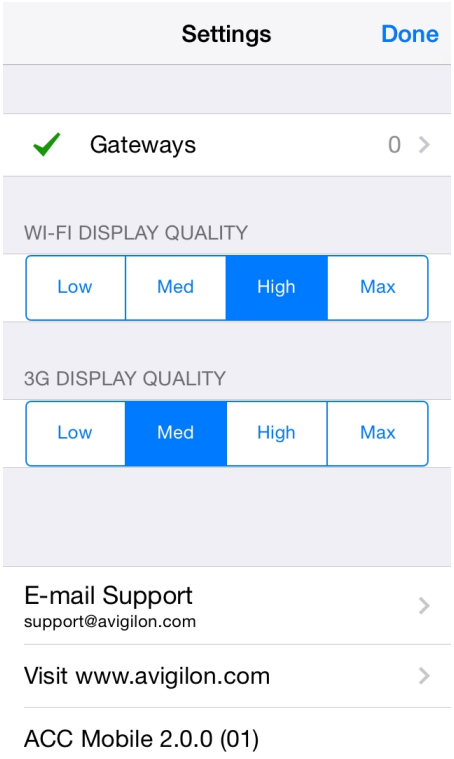
Getting Started

Once you've downloaded and installed the Control Center Mobile app, you can access the software by tapping the app icon on your Home screen.

Before you can watch video in the app, you need to set up the Control Center Mobile app to communicate with your Avigilon Control Center system.

Adding a Gateway

When you open the app for the first time, you are automatically taken to the Settings screen.



Notice that beside Gateways is the number 0. You must add at least one Control Center Gateway. The Gateway is required to link your mobile device to your Avigilon Control Center system.

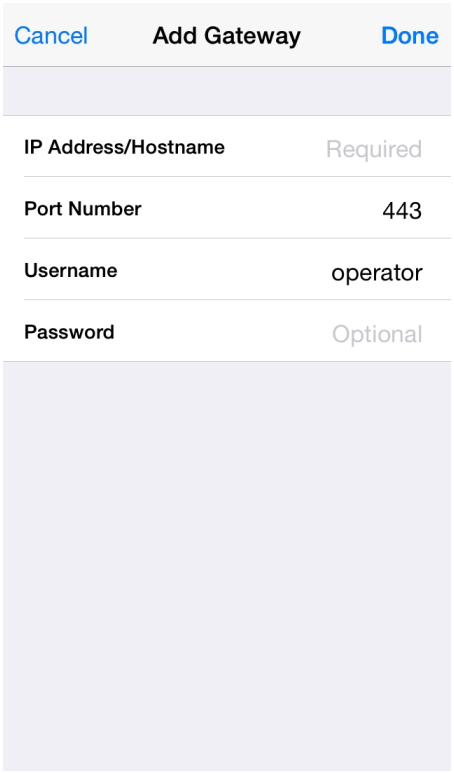
Ask your System Administrator for the Gateway's IP address and port number.

A username and password is required to access the Gateway and will be provided by your System Administrator. This may be different from the username and password used to access Sites in the Avigilon Control Center system.

NOTE: The default Gateway username is `operator` with no password.

1. Tap **Gateways**. Since there are currently no Gateways, you are automatically taken to the Add Gateway screen.

   If a Gateway has already been added, you will be taken to the Gateways screen where all the configured Gateways are listed. Tap **Add Gateway** to add a Gateway.



2. Enter the Gateway **IP Address/Hostname**.
3. Enter the Gateway's **Port Number**. The port number is 443 by default.

   NOTE: The app always tries to make a secure connection to the Gateway via HTTPS. If that fails, it will attempt an HTTP connection. If the app is able to connect via HTTP, you will see an error message advising you that you are making an unsecured connection.

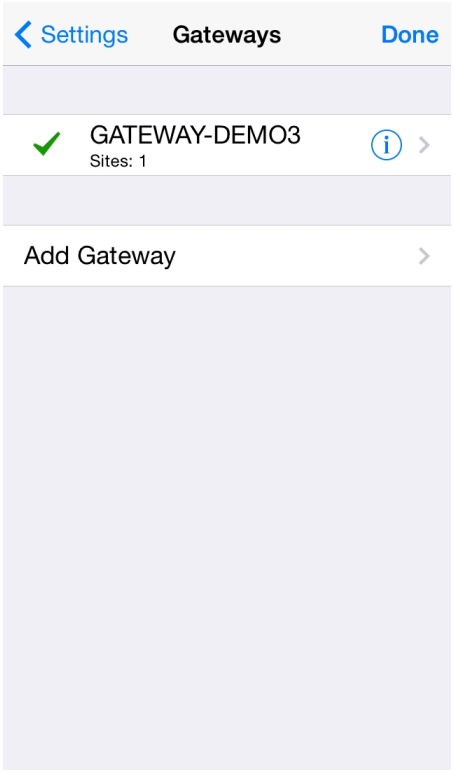
   By default, the Gateway uses port 443 for all HTTPS connections, and port 80 for all HTTP connections.
4. Enter your **Username** and **Password** for the Gateway.
5. Tap **Done**.

Logging in to a Site

On the Gateways screen, you have access to the Sites that are connected to the Gateway.

NOTE: If you are running Control Center 4, enter your server details when the app refers to a Site.

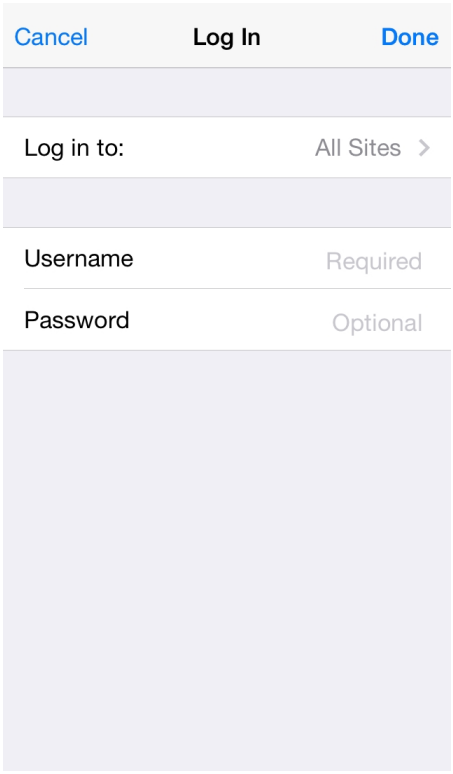
1. Tap a Gateway on the list.



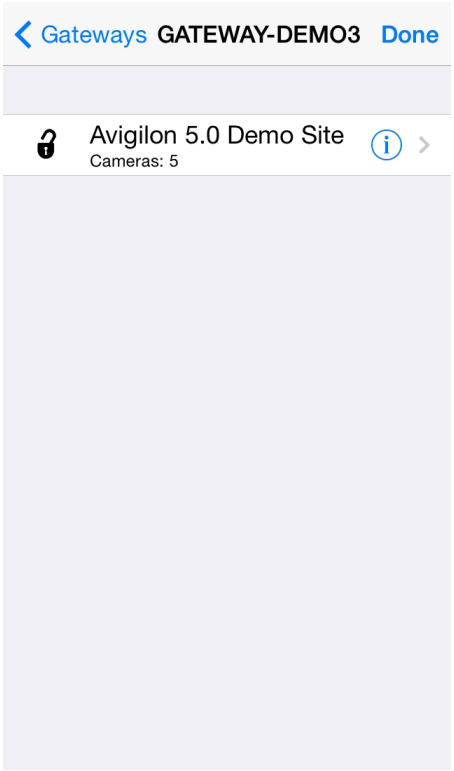
NOTE: If you tap  you will be taken to the Edit Gateway screen.

2. Tap the Site you want to log in to. If you have not provided a username and password to any Sites, the Log In screen is automatically displayed.

   Tip: Select Log in to: **All Sites** to log in to all Sites simultaneously.



3. Enter your **Username** and **Password**.
4. Tap **Done**. The app logs into the selected Site(s).



The icon shows that you are logged into that Site. Under the Site name is the number of cameras connected to that Site.

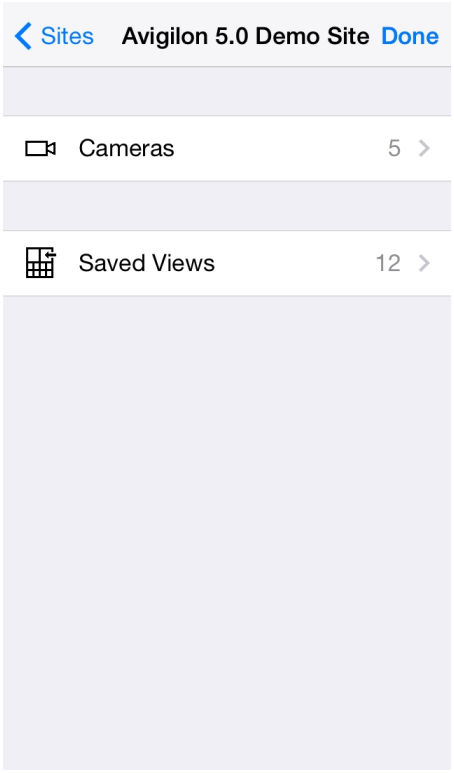
If you tap , you will be taken to the Site Log In screen again. Your Site log in information is remembered.

Accessing Cameras and Saved Views

Once you've logged in to a Site, you can access the cameras and Saved Views from the Site.

NOTE: If you are running Control Center 4 or 5.0, the Saved Views option may be displayed, but the list will be empty.

1. On the Sites screen, tap a Site.
2. On the following screen, select either **Cameras** or **Saved Views**.



3. Tap a listed camera or Saved View to open it in the View screen.

Video

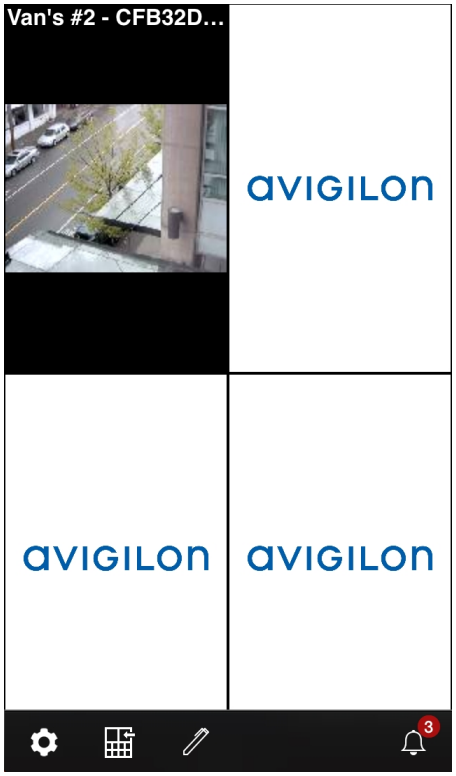
After you've set up the Gateway and Site access, you will automatically be taken to the View screen each time you open the Control Center Mobile app.

Like the Control Center Client software, video is displayed in a View and is organized by image panels.

Adding and Removing Cameras

In *Accessing Cameras and Saved Views* on page 6, you learned how to add cameras to a View through the Settings screen. For easy access, you can also add and remove cameras directly from a View.

1. On the View screen, tap the screen once to display the menu bar.



2. Tap . The Edit View screen is displayed.

3. To add a camera, tap then select the camera you want to add from the camera list.

   If you want to add a camera from a different Site, tap **Sites** and tap on a Site.

   If you then want to choose a Site that is connected to a different Gateway, tap **Gateways** and tap on a Gateway.

4. To remove a camera, tap .
5. Tap **Done** when you are finished.
6. Tap the View screen once to hide the menu bar, otherwise the menu bar auto-hides after a few seconds.

Opening a Saved View

If your Site has Saved Views set up, you can open any Saved View through the app.

NOTE: If you are running Control Center 4 or 5.0, the Saved View option may be displayed but you will not have access to the Saved Views in your system.

1. On the View screen, tap the screen once to display the menu bar.
2. Tap . This will open the Saved Views list.
3. Select a Saved View and it will open in the View screen.

NOTE: If you change the Saved View in the app, you cannot save your changes. Next time you open the Saved View from the Saved Views list, it will display the version that is stored on the Site.

Changing View Layouts

You can change the View layout to customize how video is displayed.

1. On the View screen, tap the screen once to display the menu bar.
2. Tap  .
3. Tap  to display the available View layout options.
4. Tap the View layout that you want to use. The View changes to the selected layout.
5. To move image panels, drag an image panel to a different position in the View layout.
6. When you have completed your View layout changes, tap **Done**.

Switching Views

The number of dots at the bottom of the screen show the number of Views that are open. This is the Page Views bar.

- To switch Views, flick left or right.
- To switch to a new View, flick left until you reach the last View.

  Each time you add a camera to an empty View, a new View is automatically added to the right of all available Views.

NOTE: There can be no more than eight Views.

Maximizing an Image Panel

- To maximize an image panel, double-tap an image panel.
- To restore an image panel, double-tap a maximized image panel.

Zooming and Panning

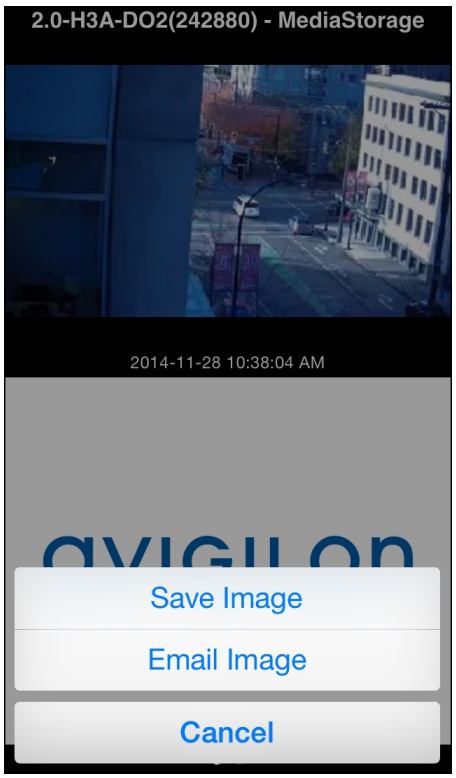
You can digitally zoom and pan video from any camera.

1. Double-tap to maximize the video image panel.
2. Place two fingers on the image panel and pull apart to zoom in.
3. While zoomed in, drag the screen to pan across the video image.
4. Place two fingers on the image panel and push together to zoom out.

Taking Snapshots

A snapshot allows you to save or email any image that is displayed in an image panel.

1. Touch and hold the image panel that currently displays your snapshot.
2. When the snapshot menu appears, select one of the following:



   - Tap **Save Image** to save a copy of the snapshot on your mobile device. The image is saved in JPEG format and is stored in your photo gallery.
   - Tap **Email Image** to email a copy of the snapshot. The image is automatically attached to an email message. This option is only available if you have email set up on your mobile device.

Using PTZ

If you are watching live video from a pan, tilt and zoom (PTZ) camera, you can control the camera's PTZ features from the app.

1. Double-tap to maximize the video image panel.
2. Tap once to display the menu bar if it is hidden.
3. Tap  .

   The camera's PTZ controls are displayed.

- To move the camera, perform one of the following:
  - If the camera supports Click to Center, tap anywhere on the video image to center the camera to that point
  - Otherwise, tap and hold an arrow that is displayed on the screen to move the camera in that direction. Release the arrow when you want the camera to stop.
- To zoom in and out, tap and hold or at the bottom of the screen.
- If the camera supports Drag to Zoom, drag your finger in any direction to create a box. When you release your finger from the screen, the camera zoom and centers on the selected area. Tap **1x** to zoom out in full.
- To have the camera perform preset movements, tap then select the preset you want to use.

  The presets are configured in the Control Center Client software.

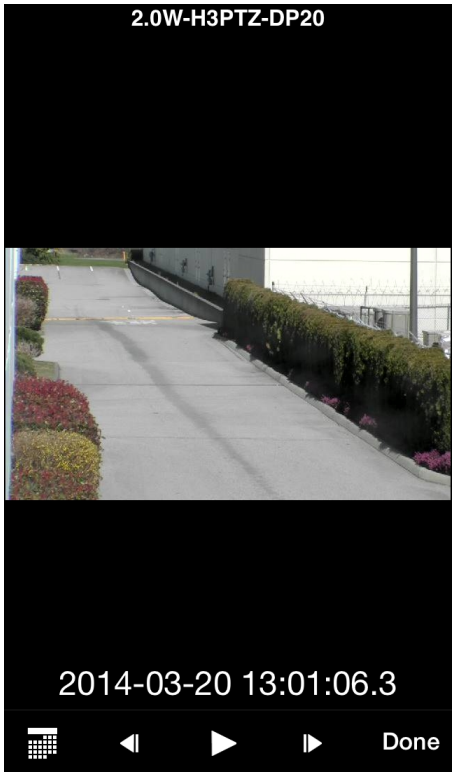
4. Tap **Done** to hide the PTZ controls.

Playing Back Recorded Video

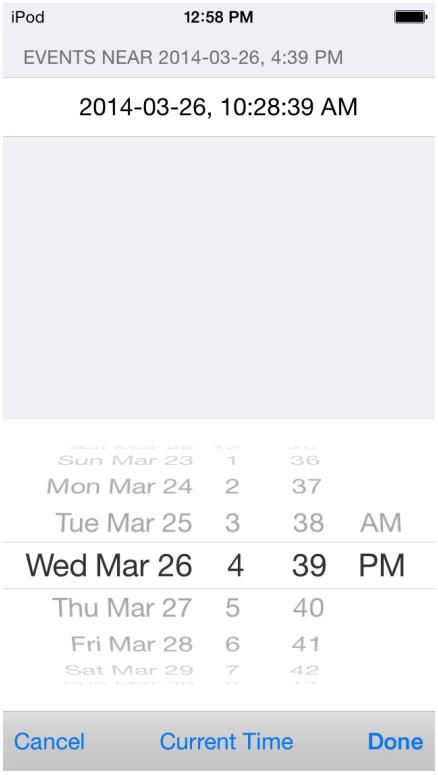
You can watch recorded events from any camera that you have access to on the app.

1. Double-tap to maximize the video image panel.
2. Tap once to display the menu bar if it is hidden.

3. Tap **Recorded** to display the Playback screen.



4. To watch video from the specific time, tap .
    a. Scroll the calendar to select the date, hour and minute of the video you want to find. Tap **Current Time** to reset the calendar to the current time.



Events that occur within 15 minutes of (or overlap) the selected time are displayed at the top of the screen.

b. Select an event from the list, or tap **Done**. The video is displayed on the Playback screen.

5. To play the recorded video, tap ▶.
   - To fast forward, tap ⏩. Tap the icon again to increase the playback speed. You can play the video up to eight times the original speed.
   - To rewind, tap ⏪. Tap the icon again to increase the playback speed. You can play the video up to eight times the original speed.
6. To stop the recorded video, tap ⏸.
   - To step forward one frame in the video, tap ⏭.
   - To step backward one frame in the video, tap ⏮.
7. When you have finished reviewing the recorded video, tap **Done** to return to the camera's live video stream.

Alarms

Alarms can be set up in the Avigilon™ Control Center Client to notify you of important trigger sources, such as a video analytics event. Alarms can be viewed and acknowledged in ACC Mobile.

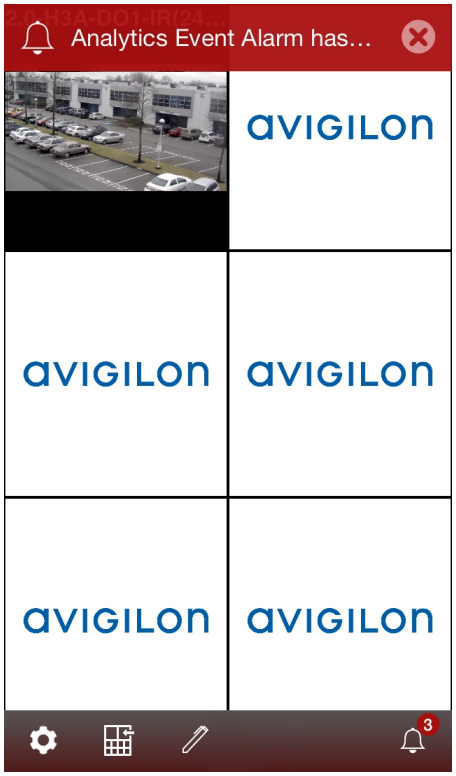
To receive alarm alerts, enable push notifications in the Avigilon Control Center Gateway. For more information, see *The Avigilon Control Center Gateway User Guide*.

Viewing Alarm Notifications

Inside the App

- When an alarm is triggered, a red banner appears at the top of the View screen. The banner displays the name of the alarm that has been triggered most recently.

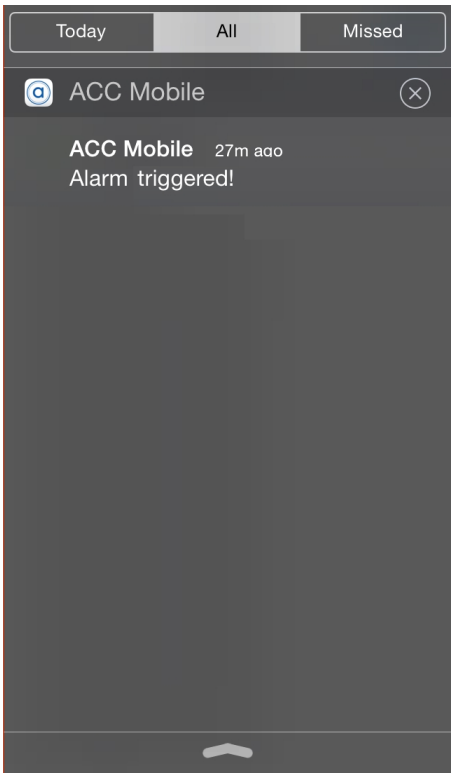
  Tapping on the banner will open the Alarm Details screen.



- If the Page Views bar is flashing red, there is an Active alarm on one of the Sites you are logged in to. For instructions on how to access these alarms, see *Accessing the Alarm List* on page 18.

Outside the App

- Tapping on an alarm alert in the Notification Center will open the app and display the Alarm Details screen.



Hiding Alarm Notifications

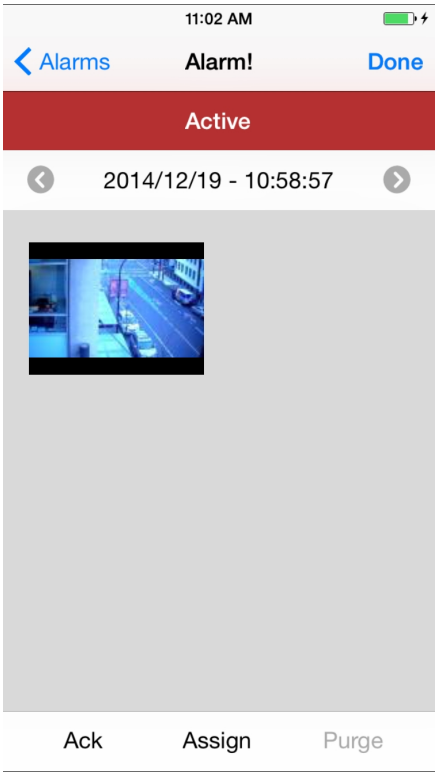
Alarm notifications can be hidden from the View screen in the app.

- To hide all current alarm notifications, swipe up on the red banner.
- To hide the most recent alarm notification, tap .

Viewing Alarm Details

Tap the alarm's name when it appears in the red banner at the top of the View screen.

Alternatively, tap the alarm's name in the Alarm List. For more information, see *Accessing the Alarm List* on page 18



The Alarm Details screen is divided into the following sections from top to bottom:

- Alarm name
- Alarm status: a red background indicates that the alarm is Active. An orange background indicates that the alarm is Active and is Assigned to Another User. A green background indicates that the alarm has been Acknowledged.
- Alarm trigger bar: tap or to view different triggers.
- Video thumbnails: tap on a thumbnail to view the camera's live video.
- The following alarm actions are available at the bottom of the Alarm Details screen.
    - **Ack:** tap to acknowledge an Active alarm.

      If the alarm is linked to a digital output, you will be asked to **Grant** or **Deny** access. If you tap **Cancel**, the alarm will not be acknowledged.
    - **Assign:** tap to assign an alarm to yourself. This tells other users that you are reviewing this alarm.
    - **Unassign:** tap to unassign an alarm that you had previously assigned to yourself.
    - **Purge:** tap to purge an Acknowledged alarm. This alarm will be removed from the Alarm List until it is triggered again.

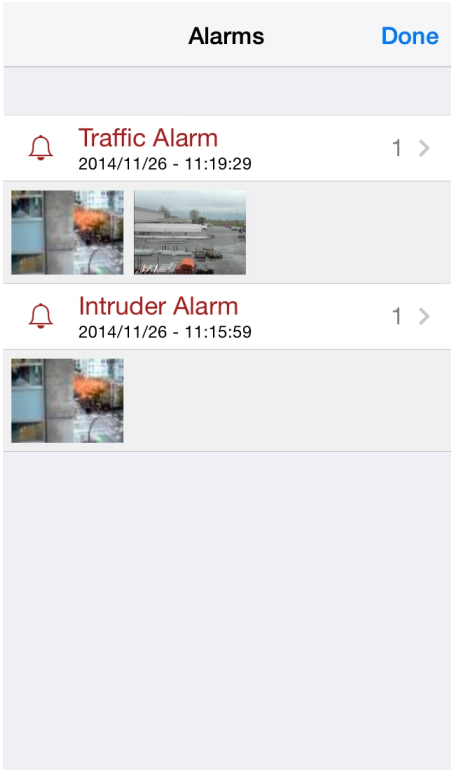
Accessing the Alarm List

The Alarm List displays all alarms that are currently Active or Acknowledged. The Alarm List can be accessed from the View screen.

1. Tap once to display the menu bar if it is hidden.
2. Tap . The Alarm List opens.

   The number on the icon indicates how many alarms are currently Active.

   The most relevant alarm is at the top of the list. Swipe up or down to view more alarms.



Alarms are sorted from top to bottom by:

- Alarm status:
  a. Active (assigned to you)
  b. Active (unassigned)
  c. Assigned to Another User
  d. Acknowledged

  Alarm names that are displayed in red indicate alarms that have not been acknowledged.
- Priority: alarm priority is set in the Avigilon Control Center Client.
- Most recent alarm trigger time

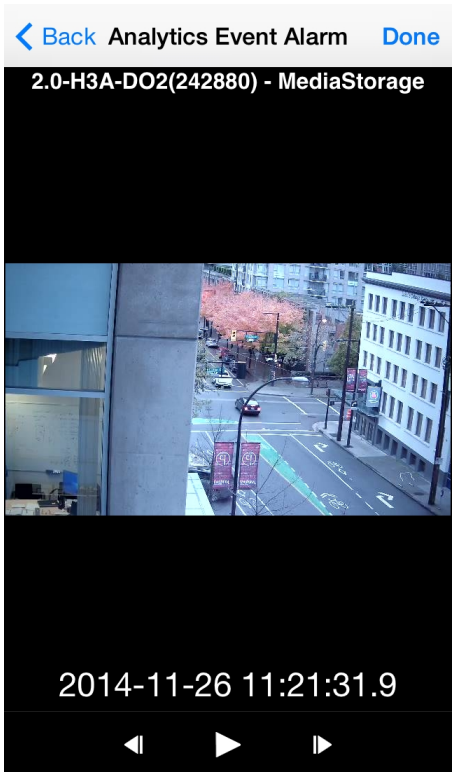
The number of current alarm triggers is displayed to the right of each alarm's name.

Tap on thumbnail to view that camera's live video.

Playing Back Recorded Alarm Video

Playing back recorded alarm video allows you to review video for each alarm trigger. You can also view live video from cameras linked to an alarm. For more information, see *Accessing the Alarm List* on the previous page.

1. In the Alarm Details screen, tap or to choose an alarm trigger to view.
2. Tap on a camera thumbnail. The Alarm Playback screen will open.



3. To play the recorded video, tap .
    - To fast forward, tap . Tap the icon again to increase the playback speed. You can play the video up to eight times the original speed.
    - To rewind, tap . Tap the icon again to increase the playback speed. You can play the video up to eight times the original speed.
4. To stop the recorded video, tap .
    - To step forward one frame in the video, tap .
    - To step backward one frame in the video, tap .

5. When you have finished reviewing the recorded video, tap **Back** to return to the Alarm Details screen. Tap **Done** to return the View screen.

Settings

Editing Gateways

You may need multiple Gateways to connect to all the Sites and cameras in your surveillance system. You can add, edit or delete Gateways as needed.

1. On the View screen, tap the screen once to display the menu bar.
2. Tap  .
3. On the Settings screen, tap **Gateways**.
4. On the Gateways screen, perform any of the following:
    - To add a Gateway, tap **Add Gateway** then enter the new Gateway information.
    - To edit a Gateway, tap  beside the Gateway you want to edit then make the required changes.

      NOTE: If you are editing the Gateway Port Number, it is recommended that you only use ports assigned to a secure HTTPS connection. If you choose to use an HTTP port number, you will receive an warning message advising you that you are making an unsecured connection.
    - To delete a Gateway, perform one of the following:
        - Tap  beside the Gateway then tap **Delete Gateway**.
        - Swipe left over the Gateway then tap **Delete**.
5. When you've completed your changes, tap **Done**.

Editing Site Login

If your password changes, you will need to update your Site password in the app.

NOTE: If you are running Control Center 4, you will use this procedure to edit your server details.

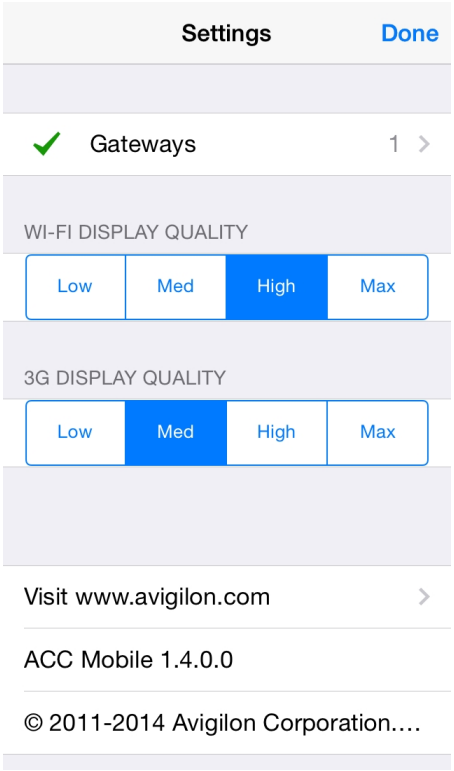
1. On the View screen, tap the screen once to display the menu bar.
2. Tap  .
3. On the Settings screen, tap **Gateways**.
4. Tap the Gateway the Site is linked to.
5. Tap  beside the Site you want to edit.
6. Enter your updated **Password** or **Username**.
7. Tap **Done**.

Changing Display Settings

To control the bandwidth used by the app, you can set the display quality according to the type of wireless network you are connected to.

The higher the display quality, the less compression is used on the video stream. This produces a better image but uses more bandwidth.

1. On the View screen, tap the screen once to display the menu bar.
2. Tap  .
3. On the Settings screen, select a display quality option.



   - **Wi-Fi Display Quality** is the setting used when you are connected to a local wi-fi network. **High** is selected by default.
   - **3G Display Quality** is the setting used when you are connected to a mobile network. **Med** is selected by default.
4. Tap **Done**.

Troubleshooting & Support

Notification Icons

Gateways and Sites have a set of notification icons to tell you their connection status.

Gateway Notification Icons

-  — You are connected to the Gateway and all Sites are accessible.
- — You are connected to the Gateway but the connection requires your attention. Some Sites may be disconnected.
-  — You are disconnected from the Gateway.

Site Notification Icons

-  — You are connected and logged in to the Site.
- — You are connected and logged in to the Site, but there may be a license issue. Contact your System Administrator.
-  — You are disconnected from the Site.
-  — You are not logged in to the Site.
-  — You provided an incorrect username or password.

Contacting Avigilon Support

If you encounter an issue while using the app, you have the option of sending Avigilon Technical Support an email directly from your mobile device.

NOTE: You must have email set up on your mobile device or this option is not displayed. You can choose to go to www.avigilon.com instead.

1. On the View screen, tap the screen once to display the menu bar.
2. Tap  .
3. On the Settings screen, tap **E-mail Support**.
4. You will automatically be taken to the new email screen. Support@avigilon.com is automatically entered as the recipient and *ACC Mobile <version #>* is entered in the subject line.
5. Enter details about your issue then tap **Send**.

This Page Left Intentionally Blank

User Guide

Avigilon™ Control Center Mobile

Version 2.0 for Android

Avigilon Corporation
http://www.avigilon.com

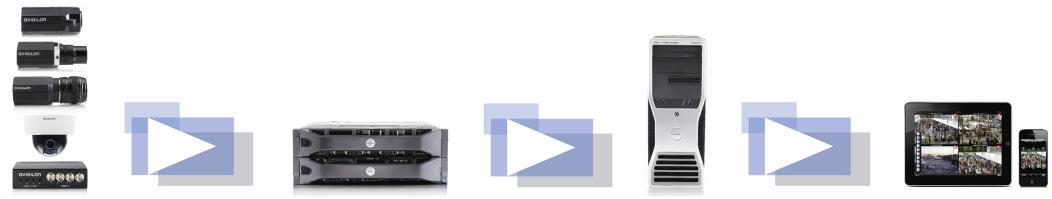
Revised: 2015-01-14

UG-ACCMOBILE-ANDROID-E_Rev1

Table of Contents

Introduction

The Avigilon™ Control Center Mobile app gives you access to live and recorded video from the Avigilon™ Control Center sytem on your mobile devices.



Device Requirements

- Android™ smartphone or tablet (version 4.0.0. or later)

NOTE: Depending on your Android version and type of mobile device, the screenshots in this document may look different from what is displayed on your device.

System Requirements

You must have access to the following software in your Avigilon Control Center system.

- Control Center Gateway
- Control Center Server

To make sure you have a secure connection, it is recommended that you only connect to the Gateway via HTTPS.

Consult with your System Administrator for more information.

- If you are running Avigilon Control Center 5.4 or later, you will have access to all of the features described in this document.
- If you are running Avigilon Control Center 5.2, you will not have access to Alarms.
- If you are running Avigilon Control Center 4 or 5.0, you will not have access to Saved Views or Alarms.

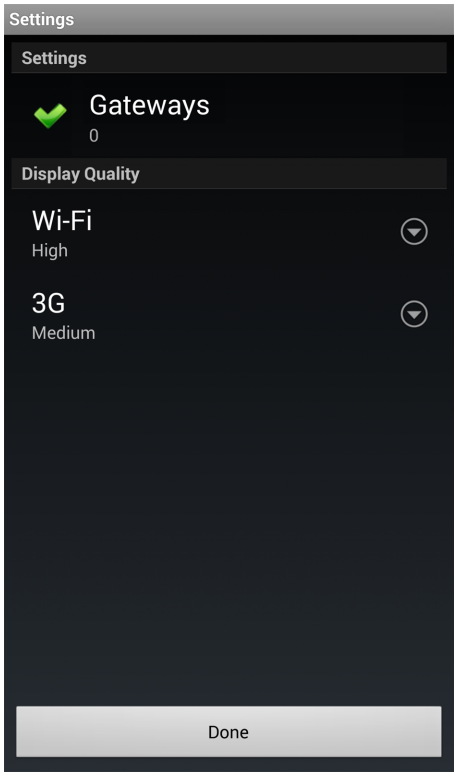
Getting Started

Once you've downloaded and installed the Control Center Mobile app, you can access the software by tapping the app icon on your Home screen.

Before you can watch video in the app, you need to set up the Control Center Mobile app to communicate with your Avigilon Control Center system.

Adding a Gateway

When you open the app for the first time, you are automatically taken to the Settings screen.



Notice that under Gateways is the number 0. You must add at least one Control Center Gateway. The Gateway is required to link your mobile device to your Avigilon Control Center system.

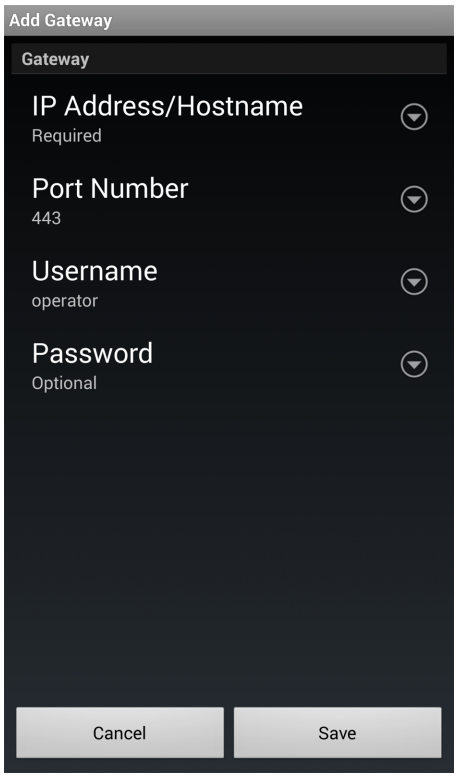
Ask your System Administrator for the Gateway's IP address and port number.

A username and password is required to access the Gateway and will be provided by your System Administrator. This may be different from the username and password used to access Sites in the Avigilon Control Center system.

NOTE: The default Gateway username is `operator` with no password.

1. Tap **Gateways**. Since there are currently no Gateways, you are automatically taken to the Add Gateway screen.

   If a Gateway has already been added, you will be taken to the Gateways screen where all the configured Gateways are listed. Tap **Add Gateway** to add a Gateway.



2. Enter the Gateway **IP Address/Hostname**.
3. Enter the Gateway's **Port Number**. The port number is 443 by default.

   NOTE: The app always tries to make a secure connection to the Gateway via HTTPS. If that fails, it will attempt an HTTP connection. If the app is able to connect via HTTP, you will see an error message advising you that you are making an unsecured connection.

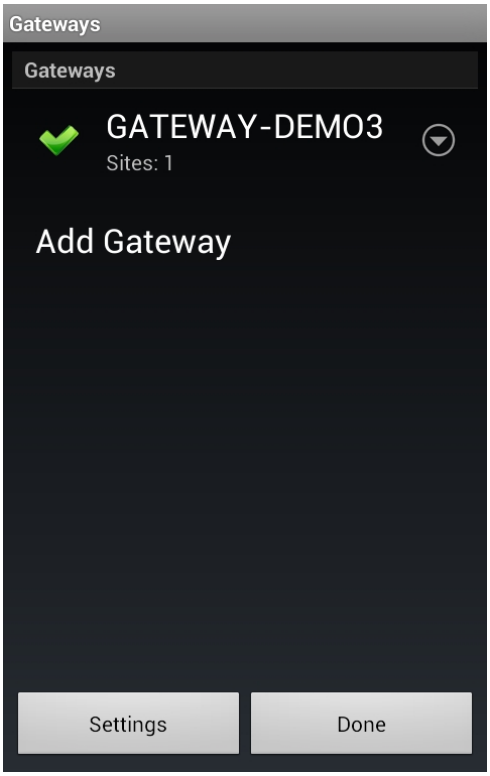
   By default, the Gateway uses port 443 for all HTTPS connections, and port 80 for all HTTP connections.
4. Enter your **Username** and **Password** for the Gateway.
5. Tap **Save**.

Logging in to a Site

On the Gateways screen, you have access to the Sites that are connected to the Gateway.

NOTE: If you are running Control Center 4, enter your server details when the app refers to a Site.

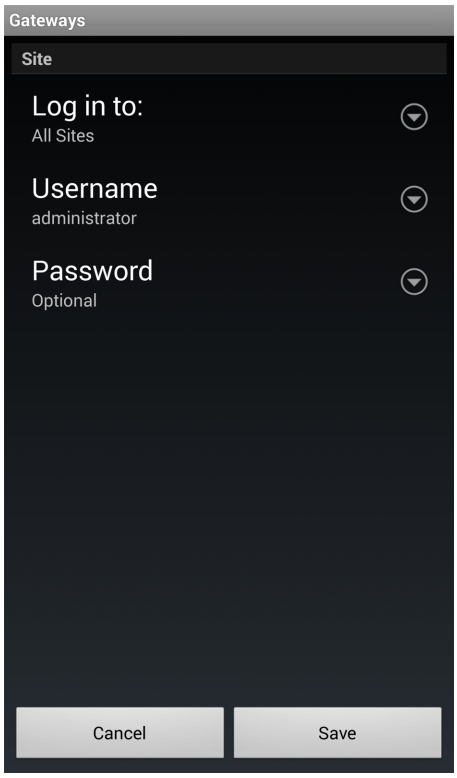
1. Tap a Gateway on the list.



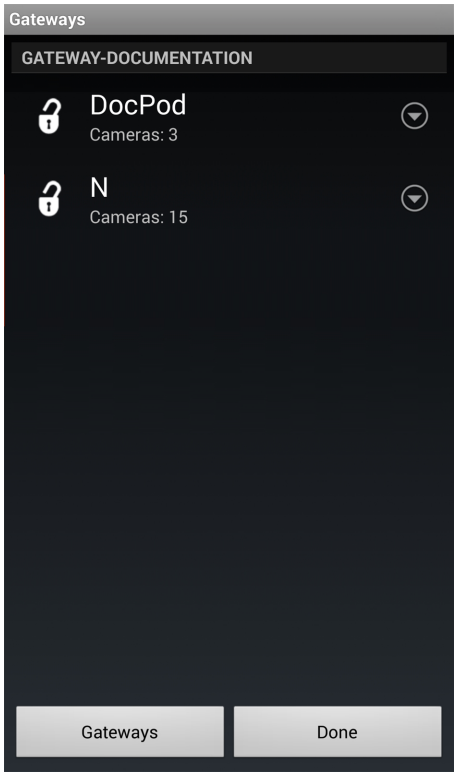
NOTE: If you tap you will be taken to the Edit Gateway screen.

2. Tap the Site you want to log in to. If you have not provided a username and password to any Sites, the Log In screen is automatically displayed.

   Tip: Select Log in to: **All Sites** to log in to all Sites simultaneously.



3. Enter your **Username** and **Password**.
4. Tap **Save**. The app logs into the selected Site(s).



The icon shows that you are logged into that Site. Under the Site name is the number of cameras connected to that Site.

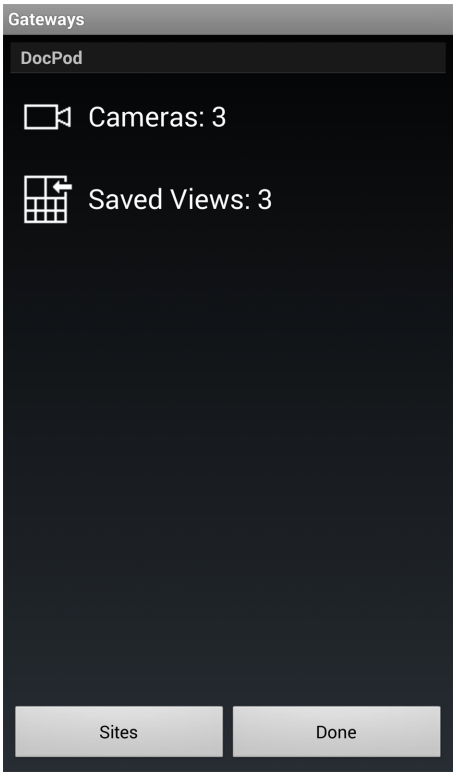
If you tap , you will be taken to the Site Log In screen again. Your Site log in information is remembered.

Accessing Cameras and Saved Views

Once you've logged in to a Site, you can access the cameras and Saved Views from the Site.

NOTE: If you are running Control Center 4 or 5.0, the Saved Views option may be displayed, but the list will be empty.

1. On the Sites screen, tap a Site.
2. On the following screen, select either **Cameras** or **Saved Views**.



3. Tap a listed camera or Saved View to open it in the View screen.

Video

After you've set up the Gateway and Site access, you will automatically be taken to the View screen each time you open the Control Center Mobile app.

Like the Control Center Client software, video is displayed in a View and is organized by image panels.

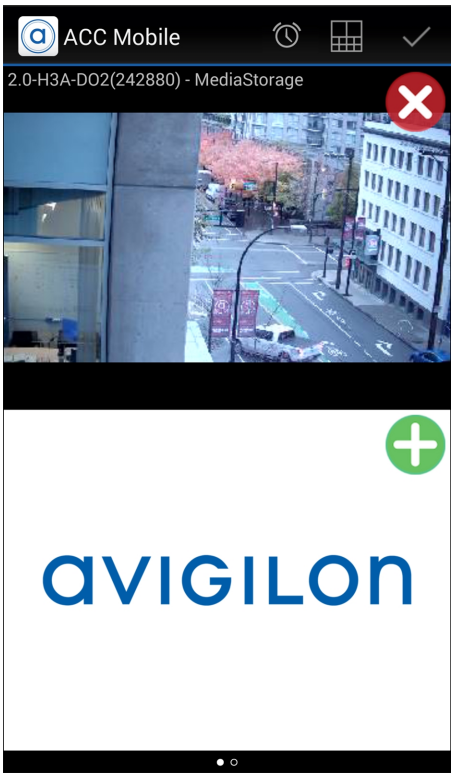
Adding and Removing Cameras

In *Accessing Cameras and Saved Views* on page 6, you learned how to add cameras to a View through the Settings screen. For easy access, you can also add and remove cameras directly from a View.

1. On the View screen, tap the screen once to display the menu bar.

To see additional options, tap the **Action Overflow** icon on the far right of the menu bar.

2. Tap **Edit**. The Edit View screen is displayed.



3. To add a camera, tap then select the camera you want to add from the camera list.

   If you want to add a camera from a different Site, tap **Resources** and tap on a Site.

   If you then want to choose a Site that is connected to a different Gateway, tap **Gateways** and tap on a Gateway.

4. To remove a camera, tap .
5. Tap when you are finished.
6. Tap the View screen once to hide the menu bar, otherwise the menu bar auto-hides after a few seconds.

Opening a Saved View

If your Site has Saved Views set up, you can open any Saved View through the app.

NOTE: If you are running Control Center 4 or 5.0, the Saved View option may be displayed but you will not have access to the Saved Views in your system.

1. On the View screen, tap the screen once to display the menu bar.
2. Tap **Edit**.
3. Tap then select the Saved View you want to open from the Saved View list.

NOTE: If you change the Saved View in the app, you cannot save your changes. Next time you open the Saved View from the Saved Views list, it will display the version that is stored on the Site.

Changing View Layouts

You can change the View layout to customize how video is displayed.

1. On the View screen, tap the screen once to display the menu bar.
2. Tap **Edit**.
3. Tap  to display the available View layout options.
4. Tap the View layout that you want to use. The View changes to the selected layout.
5. To move image panels, drag an image panel to a different position in the View layout.
6. When you have completed your View layout changes, tap  .

Switching Views

The number of dots at the bottom of the screen show the number of Views that are open. This is the Page Views bar.

- To switch Views, flick left or right.
- To switch to a new View, flick left until you reach the last View.

  Each time you add a camera to an empty View, a new View is automatically added to the right of all available Views.

NOTE: There can be no more than eight Views.

Maximizing an Image Panel

- To maximize an image panel, double-tap an image panel.
- To restore an image panel, double-tap a maximized image panel.

Zooming and Panning

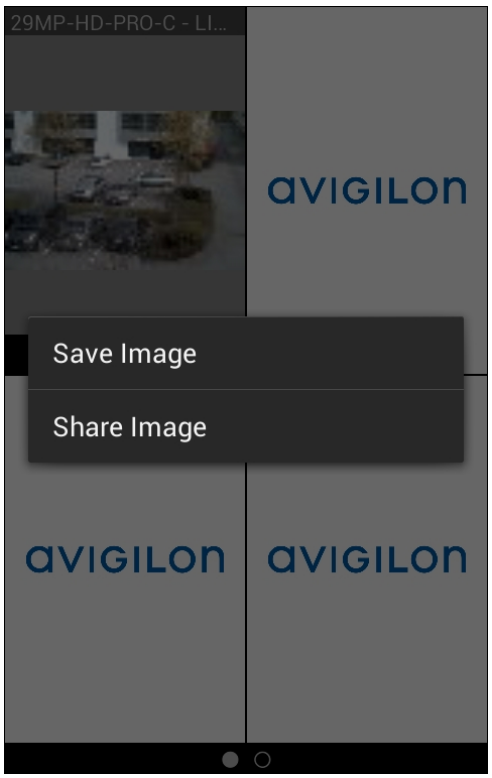
You can digitally zoom and pan video from any camera.

1. Double-tap to maximize the video image panel.
2. Place two fingers on the image panel and pull apart to zoom in.
3. While zoomed in, drag the screen to pan across the video image.
4. Place two fingers on the image panel and push together to zoom out.

Taking Snapshots

A snapshot allows you to save or email any image that is displayed in an image panel.

1. Touch and hold the image panel that currently displays your snapshot.
2. When the snapshot menu appears, select one of the following:



   - Tap **Save Image** to save a copy of the snapshot on your mobile device. The image is saved in JPEG format and is stored in your photo gallery.
   - Tap **Share Image** to send or post the image through another app that is installed on your device. Select this option if you want to email the image.

Using PTZ

If you are watching live video from a pan, tilt and zoom (PTZ) camera, you can control the camera's PTZ features from the app.

1. Double-tap to maximize the video image panel.
2. Tap once to display the menu bar if it is hidden.
3. Tap **PTZ**.

   If the PTZ button is hidden, press the **Menu** button on your device then tap **PTZ**.

   The camera's PTZ controls are displayed.

- To move the camera, perform one of the following:
  - If the camera supports Click to Center, tap anywhere on the video image to center the camera to that point
  - Otherwise, tap and hold an arrow that is displayed on the screen to move the camera in that direction. Release the arrow when you want the camera to stop.
- To zoom in and out, tap and hold or at the bottom of the screen.
- If the camera supports Drag to Zoom, drag your finger in any direction to create a box. When you release your finger from the screen, the camera zoom and centers on the selected area. Tap **1x** to zoom out in full.
- To have the camera perform preset movements, tap **Presets** then select the preset you want to use.

  The presets are configured in the Control Center Client software.

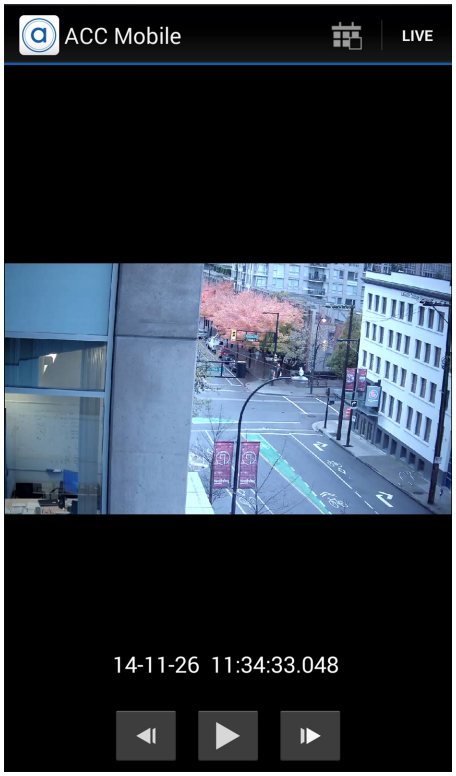
4. Tap **Live** to hide the PTZ controls.

Playing Back Recorded Video

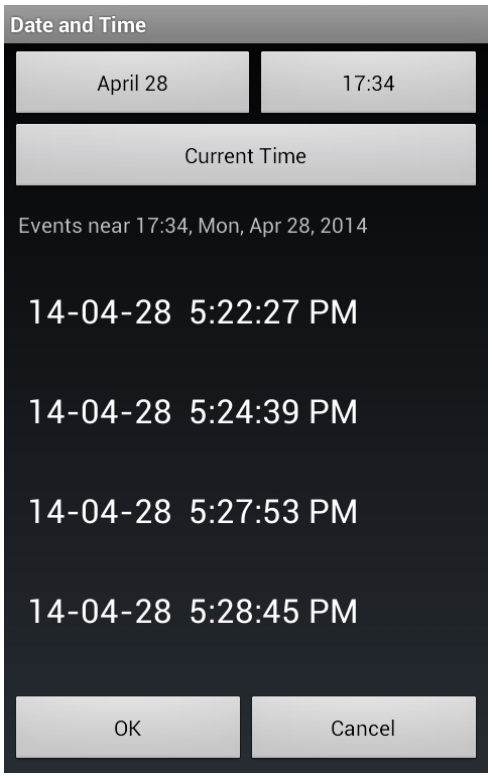
You can watch recorded events from any camera that you have access to on the app.

1. Double-tap to maximize the video image panel.
2. Tap once to display the menu bar if it is hidden.

3. Tap **Recorded** to display the Playback screen.



4. To watch video from the specific time, tap  .



a. To change the date, tap the button displaying the current date then select the date of the event you want to view.

b. To change the time, tap the button on the top right and select the time of the event you want to view.

c. Tap **Current Time** to reset the calendar to the current date and time.

d. A list of events that occured most closely around the selected date and time is displayed. Select an event to display the recorded video, or tap **OK** to close the screen.

5. To play the recorded video, tap  .

   - To fast forward, tap  . Tap the icon again to increase the playback speed. You can play the video up to eight times the original speed.

   - To rewind, tap  . Tap the icon again to increase the playback speed. You can play the video up to eight times the original speed.

6. To stop the recorded video, tap  .

   - To step forward one frame in the video, tap  .

   - To step backward one frame in the video, tap  .

7. When you have finished reviewing the recorded video, tap **Live** to return to the camera's live video stream.

   NOTE: A single tap will show/hide the playback controls.

Alarms

Alarms can be set up in the Avigilon™ Control Center Client to notify you of important trigger sources, such as a video analytics event. Alarms can be viewed and acknowledged in ACC Mobile.

To receive alarm notifications, enable push notifications in the Avigilon Control Center Gateway. For more information, see *The Avigilon Control Center Gateway User Guide*.

Viewing Alarm Notifications

Inside the App

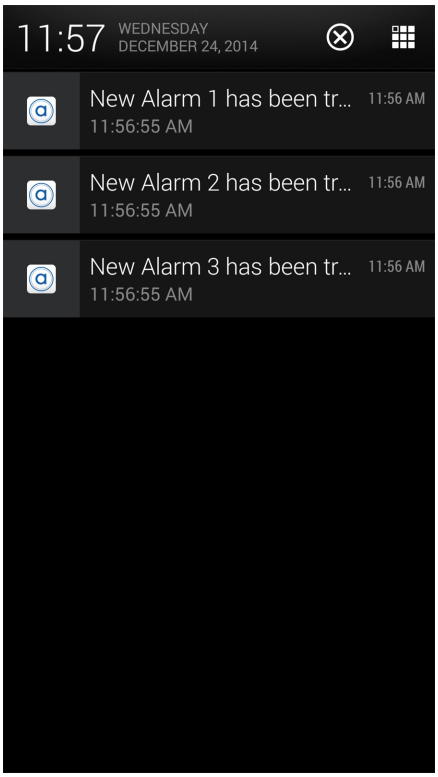
- When an alarm is triggered, a red banner appears at the bottom of the View screen. The banner displays the name of the alarm that has been triggered most recently.

  Tapping on the banner will open the Alarm Details screen.

- If the Page Views bar is flashing red, there is an Active alarm on one of the Sites you are logged in to. For instructions on how to access these alarms, see *Accessing the Alarm List* on page 18.

Outside the App

- Tapping on an alarm notification will open the app and display the Alarm Details screen.



Hiding Alarm Notifications

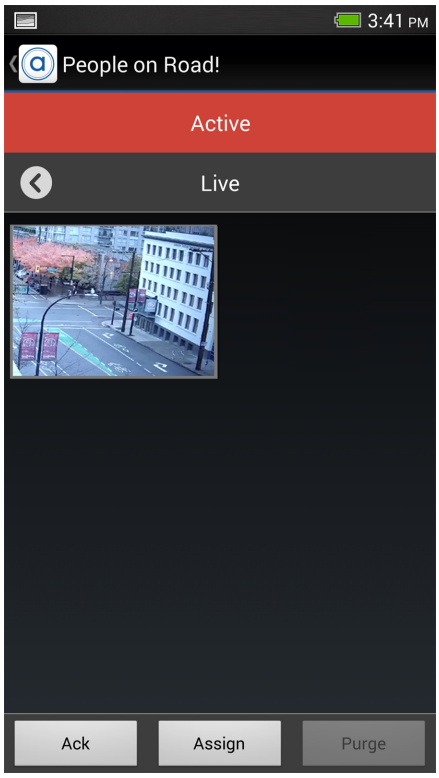
Alarm notifications can be hidden from the View screen in the app.

- To hide all current alarm notifications, swipe the red banner left or right.
- To hide the most recent alarm notification, tap .

Viewing Alarm Details

Tap the alarm's name when it appears in the red banner at the bottom of the View screen.

Alternatively, tap the alarm's name in the Alarm List. For more information, see *Accessing the Alarm List* on page 18



The Alarm Details screen is divided into the following sections from top to bottom:

- Alarm name
- Alarm status: a red background indicates that the alarm is Active. An orange background indicates that the alarm is Active and is Assigned to Another User. A green background indicates that the alarm has been Acknowledged.
- Alarm trigger bar: tap or to view different triggers.
- Video thumbnails: tap on a thumbnail to view the camera's live video.
- The following alarm actions are available at the bottom of the Alarm Details screen.
    - **Ack:** tap to acknowledge an Active alarm.

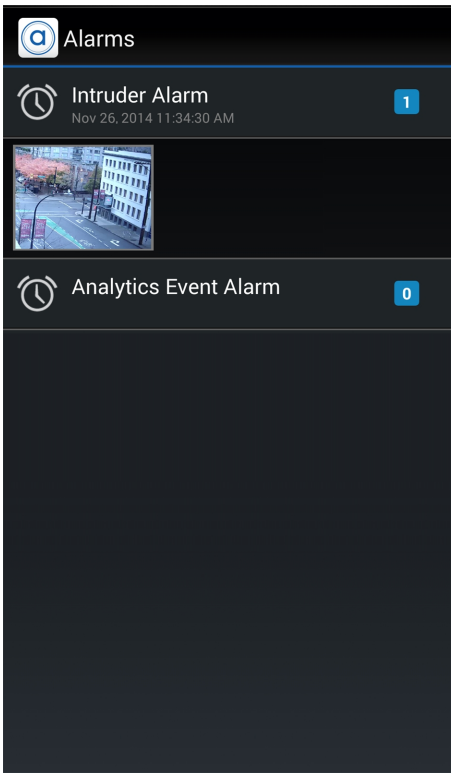
      If the alarm is linked to a digital output, you will be asked to **Grant** or **Deny** access. If you tap **Cancel**, the alarm will not be acknowledged.
    - **Assign:** tap to assign an alarm to yourself. This tells other users that you are reviewing this alarm.
    - **Unassign:** tap to unassign an alarm that you had previously assigned to yourself.
    - **Purge:** tap to purge an Acknowledged alarm. This alarm will be removed from the Alarm List until it is triggered again.

Accessing the Alarm List

The Alarm List displays all alarms that are currently Active or Acknowledged. The Alarm List can be accessed from the View screen.

1. Tap once to display the menu bar if it is hidden.
2. Tap . The Alarm List opens.

   The most relevant alarm is at the top of the list. Swipe up or down to view more alarms.



Alarms are sorted from top to bottom by:

- Alarm status:
  a. Active (assigned to you)
  b. Active (unassigned)
  c. Assigned to Another User
  d. Acknowledged
- Priority: alarm priority is set in the Avigilon Control Center Client.
- Most recent alarm trigger time

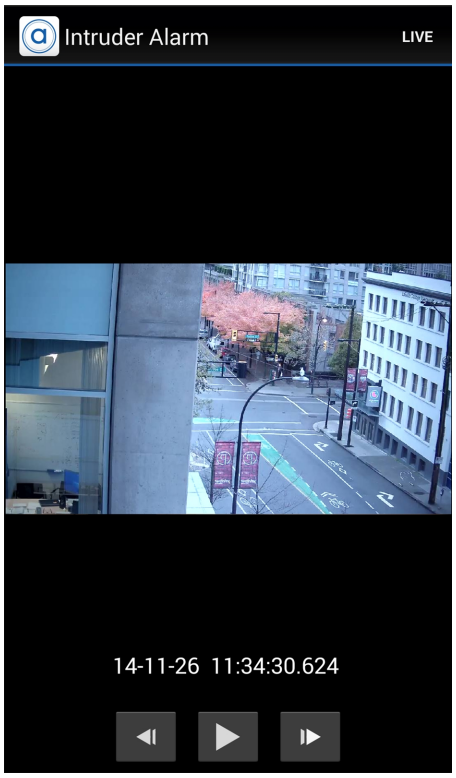
The number of current alarm triggers is displayed to the right of each alarm's name.

Tap on thumbnail to view that camera's live video.

Playing Back Recorded Alarm Video

Playing back recorded alarm video allows you to review video for each alarm trigger. You can also view live video from cameras linked to an alarm. For more information, see *Accessing the Alarm List* on the previous page.

1. In the Alarm Details screen, tap  or  to choose an alarm trigger to view.
2. Tap on a camera thumbnail. The Alarm Playback screen will open.



3. To play the recorded video, tap  .
    - To fast forward, tap  . Tap the icon again to increase the playback speed. You can play the video up to eight times the original speed.
    - To rewind, tap  . Tap the icon again to increase the playback speed. You can play the video up to eight times the original speed.
4. To stop the recorded video, tap  .
    - To step forward one frame in the video, tap  .
    - To step backward one frame in the video, tap  .
5. When you have finished reviewing the recorded video, click your device's back button to return to the Alarm Details screen.

Settings

Editing Gateways

You may need multiple Gateways to connect to all the Sites and cameras in your surveillance system. You can add, edit or delete Gateways as needed.

1. On the View screen, tap the screen once to display the menu bar.
2. Tap  .
3. On the Settings screen, tap **Gateways**.
4. On the Gateways screen, perform any of the following:
    - To add a Gateway, tap **Add Gateway** then enter the new Gateway information.
    - To edit a Gateway, tap  beside the Gateway you want to edit then make the required changes.

      NOTE: If you are editing the Gateway Port Number, it is recommended that you only use ports assigned to a secure HTTPS connection. If you choose to use an HTTP port number, you will receive an warning message advising you that you are making an unsecured connection.
    - To delete a Gateway, tap  beside the Gateway then tap **Delete Gateway**.
5. When you've completed your changes, tap **OK**.

Editing Site Login

If your password changes, you will need to update your Site password in the app.

NOTE: If you are running Control Center 4, you will use this procedure to edit your server details.

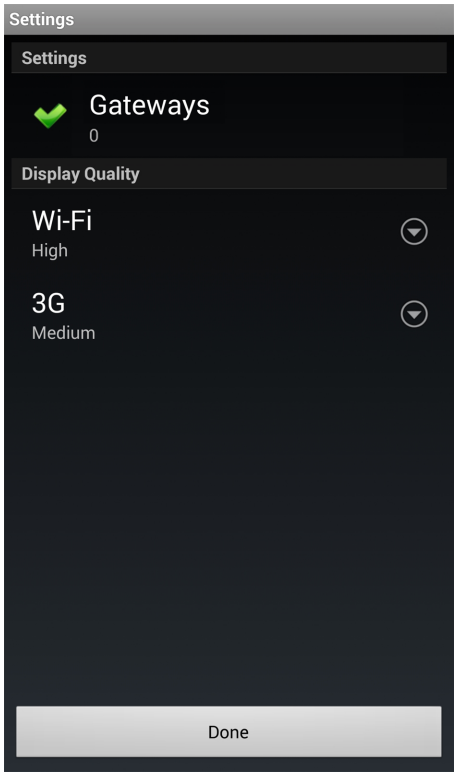
1. On the View screen, tap the screen once to display the menu bar.
2. Tap  .
3. On the Settings screen, tap **Gateways**.
4. Tap the Gateway the Site is linked to.
5. Tap  beside the Site you want to edit.
6. Enter your updated **Password** or **Username**.
7. Tap **OK**.

Changing Display Settings

To control the bandwidth used by the app, you can set the display quality according to the type of wireless network you are connected to.

The higher the display quality, the less compression is used on the video stream. This produces a better image but uses more bandwidth.

1. On the View screen, tap the screen once to display the menu bar.
2. Tap  .
3. On the Settings screen, select a display quality option.



   - **Wi-Fi** is the setting used when you are connected to a local wi-fi network. **High** is selected by default.
   - **3G** is the setting used when you are connected to a mobile network. **Medium** is selected by default.
4. Tap **Done**.

Troubleshooting & Support

Notification Icons

Gateways and Sites have a set of notification icons to tell you their connection status.

Gateway Notification Icons

-  — You are connected to the Gateway and all Sites are accessible.
-  — You are connected to the Gateway but the connection requires your attention. Some Sites may be disconnected.
-  — You are disconnected from the Gateway.

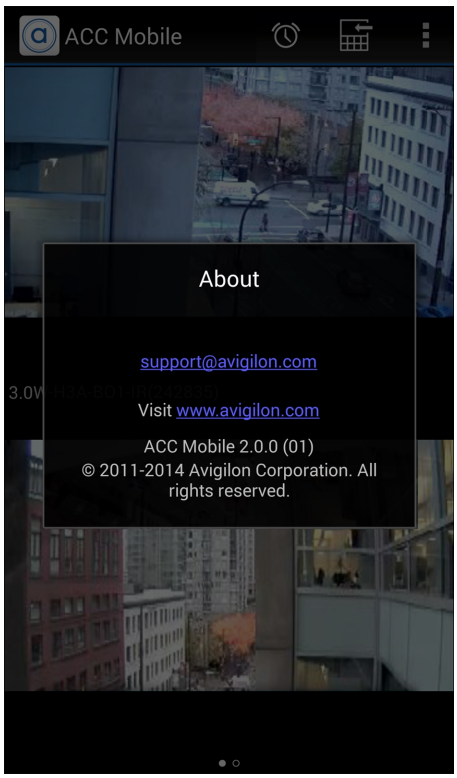
Site Notification Icons

-  — You are connected and logged in to the Site.
-  — You are connected and logged in to the Site, but there may be a license issue. Contact your System Administrator.
-  — You are disconnected from the Site.
-  — You are not logged in to the Site.
-  — You provided an incorrect username or password.

Contacting Avigilon Support

If you encounter an issue while using the app, you have the option of sending Avigilon Technical Support an email directly from your mobile device.

1. Tap once to display the menu bar if it is hidden.
2. Tap **About**.



3. Tap the email link to Avigilon Technical Support: **support@avigilon.com**.

   If you have more than one email application, you will be asked to choose one to send the email.

4. In the new email screen, support@avigilon.com is automatically entered as the recipient. Enter the details of your issue then tap **Send**.

   NOTE: Include the app version number so that Avigilon Technical Support knows which version of the Control Center Mobile app you are having issues with.

This Page Left Intentionally Blank

AVIGILON REMOTE MONITORING WORKSTATION

Operations & Maintenance Manual
December 2015

4 Monitor Professional High Performance Remote Monitoring Workstation

Avigilon's end-to-end surveillance solutions deliver image detail no other system can match. Avigilon™ Control Center software, featuring High Definition Stream Management (HDSM)™ technology combined with our broad range of megapixel cameras (from 1 MP to 29 MP) provide unprecedented clarity—while effectively managing storage and bandwidth requirements. Our components are scalable and can work together in an end-to-end system, or can be customized to create your own powerful and cost-effective solution.

The innovative remote monitoring workstation is just one way Avigilon can help provide the very best monitoring and protection.

The Avigilon Control Center professional high performance remote monitoring workstations are designed to achieve the highest performance for a client PC within an Avigilon HD Surveillance System. Pre-loaded with Avigilon Control Center, the remote monitoring workstation is easily installed to add an additional monitoring station to any existing system, with support for four high resolution monitors and up to a total of 144 channels of video.

KEY FEATURES

- Preloaded with Avigilon Control Center High Definition Network Video Management Client Software
- Supports up to four high resolution monitors
- Supports viewing up to 144 camera channels simultaneously
- Desktop form factor
- Keyboard and mouse included

*Monitors sold separately.

Specifications

SYSTEM	Control Center Edition	Enterprise, Standard or Core compatible			
	Viewing Streams	Up to 144			
	Viewing Rate	Up to 10 MB/s			
	Operating System	Microsoft® Windows Embedded Standard 7			
	Processor	Dual Intel® Xeon® Processor E5-2609			
	Memory	4 GB RAM			
	Network Interface	1 Gigabit Ethernet RJ-45 port (1000Base-T)			
	Video Outputs	4 active (2 DisplayPort and 2 DVI)			
	Optical Drive	1 DVD-RW			
MECHANICAL	Form Factor	Desktop			
	Dimensions (LxWxH)	172.6 x 414 x 471; 6.79” x 16.3” x 18.54”			
	Weight	14kg (30.86lb)			
ELECTRICAL	Power Input	100 to 240 VAC, 50/60 Hz, auto-switching			
	Power Supply	Single non-redundant			
	Power Consumption	635 W			
ENVIRONMENTAL	Operating Temperature	10° C to 35° C (50° F to 95° F)			
	Storage Temperature	-40° C to 65° C (-40° F to 149° F)			
	Humidity	20 - 80% Relative humidity (non-condensing)			
	Operating Vibration	5 Hz to 350 Hz at 0.0002 G/Hz			
	Storage Vibration	5 Hz to 500 Hz at 0.001 to 0.01 G/Hz			
	Operating Shock	Shock pulse of 40G for up to 2 ms			
	Storage Shock	Shock pulse of 105G for up to 2 ms			
	Operating Altitude	-15.2 m to 3048 m (-50 ft to 10,000 ft)			
	Storage Altitude	-15.2 m to 10,668 m (-50 ft to 35,000 ft)			
SUPPLIED ACCESSORIES		USB keyboard			
		USB mouse			
		Power cord			
		2 DisplayPort to DVI adapter			
		2 DVI to VGA adapter			
CERTIFICATIONS		FCC, Class B	VCCI, Class B	SABS, Class B	NEMKO, Class B
		ICES, Class B	BSMI, Class B	CCC, Class B	GOST, Class B
		CE, Class B	C-Tick, Class B	BCC, Class B	BELLIS, Class B
ORDERING INFORMATION	4MN-HD-RMWS	4 monitor professional high performance remote monitoring workstation			

HD Network Video Recorder Server

Avigilon's end-to-end surveillance solutions deliver image detail no other system can match. Avigilon™ Control Center software, featuring High Definition Stream Management (HDSM)™ technology combined with our broad range of megapixel cameras (from 1 MP to 29 MP) provide unprecedented clarity—while effectively managing storage and bandwidth requirements. Our components are scalable and can work together in an end-to-end system, or can be customized to create your own powerful and cost-effective solution.

The innovative HD network video recorder is just one way Avigilon can help provide the very best monitoring and protection.

Our Network Video Recorders (NVRs) have Avigilon Control Center preloaded and configured for maximum performance and reliability, making them easy to integrate into any Avigilon surveillance system. NVR servers can record up to 32 MB/s of image data from up to 128 cameras.

KEY FEATURES

- Preloaded and configured with Avigilon Control Center High Definition Network Video Management Software
- Records up to 32 MB/s of image data
- Supports up to 128 camera channels
- Supports up to 30 images per second per camera channel
- RAID 5 hard drive configuration
- Up to 21 TB effective recording capacity (after RAID 5 applied) that is expandable using HD-NVR-EXP2
- Hot-swappable hard drives and power supplies
- 2 gigabit Ethernet ports
- 2U rack mount chassis

Specifications

SYSTEM	Control Center Edition	Enterprise, Standard and Core compatible	
	Recording Rate	Up to 32 MB/s	
	Camera Channels	Up to 128	
	Recording Image Rate	Up to 30 images per second per channel, total of 3840 for 128 channels	
	Local Viewing	No	
	Operating System	Microsoft® Windows Embedded Standard 7	
	Hard Disk Drive Configuration	Hot-swappable, RAID 5	
	Recording Storage Capacity	Up to 21 TB effective (after RAID 5), expandable using HD-NVR-EXP2	
	Processor	Intel® Xeon® Processor E5-2407	
	Memory	6 GB RAM (3 x 2GB)	
	Network Interface	2 Gigabit Ethernet RJ-45 ports (1000Base-T)	
	Video Outputs	1 VGA	
	Optical Drive	1 DVD-RW	
MECHANICAL	Form Factor	2U rack mount chassis	
	Dimensions (LxWxH)	611.1 mm x 434 mm x 86.8 mm; 24.06” x 17.09” x 3.42”	
	Weight	28.2 kg (62.17 lbs)	
ELECTRICAL	Power Input	100 to 240 VAC, 50/60 Hz, auto-switching	
	Power Supply	Single hot-swappable, dual-redundant optional with HD-NVR2-2ND-PS	
	Power Consumption	495 W	
ENVIRONMENTAL	Operating Temperature	10° C to 35° C (50° F to 95° F)	
	Storage Temperature	-40° C to 65° C (-40° F to 149° F)	
	Humidity	20 - 80% Relative humidity (non-condensing)	
	Operating Vibration	0.26G at 5 Hz to 350 Hz for 2 minutes	
	Storage Vibration	1.87Grms at 10 Hz to 500 Hz for 15 minutes	
	Operating Shock	1 shock pulse of 31G for up to 2.6 ms	
	Storage Shock	6 shock pulses of 71G for up to 2 ms	
	Operating Altitude	-15.2 m to 3048 m (-50 ft to 10,000 ft)	
	Storage Altitude	-15.2 m to 10,668 m (-50 ft to 35,000 ft)	
REMOTE PC CLIENT REQUIREMENTS	Operating System	Microsoft® Windows® XP with Service Pack (SP) 2 or later, Windows® Vista, or Windows® 7	
	Processor	Intel® Single Core 2.4 GHz (minimum); Intel® Dual Core 2.0 GHz (recommended)	
	Memory	1 GB RAM (minimum); 2 GB RAM (recommended)	
	Video Card	PCI Express, DirectX 9.0c compliant with 128 MB RAM (Intel® GMA 900 or better, NVIDIA® 6600 or better, ATI X1300 or better)	
	Network Interface	100 Mbps (minimum); 1 Gbps (recommended)	
	Hard Disk Space	500 MB	
SUPPLIED ACCESSORIES		Rack mount kit (brackets, rails, and hardware)	
		Cable management arm	
		Rack bezel	
		USB keyboard	
		USB mouse	
		Power cord	
CERTIFICATIONS	Safety	EN 60950-1:2006 + A11:2009 IEC 60950-1:2005 Ed2	EN 62311:2008
	Electromagnetic Emissions	EN 55022:2006 + A1:2007 CISPR 22:2005 + A1:2005 EN 61000-3-2:2006	IEC 61000-3-2:2005 (Class D) EN 61000-3-3:1995 + A1:2001 + A2:2005 IEC 61000-3-3:1994 + A1:2001 + A2:2005
	Electromagnetic Immunity	EN 55024:1998 + A1:2001 + A2:2003	CISPR 24:1997 (modified)+A1:2001 + A2:2002
ORDERING INFORMATION	3.0TB-HD-NVR2	3.0 TB storage, Network Video Recorder Server	
	5.0TB-HD-NVR2	5.0 TB storage, Network Video Recorder Server	
	10.0TB-HD-NVR2	10.0 TB storage, Network Video Recorder Server	
	15.0TB-HD-NVR2	15.0 TB storage, Network Video Recorder Server	
	21.0TB-HD-NVR2	21.0 TB storage, Network Video Recorder Server	
	HD-NVR2-2ND-PS	Secondary redundant power supply	
	HD-NVR2-LPRPROC	LPR processor	
	HD-NVR2-EXP2-CARD	Expansion card for connecting storage expansion to an HD-NVR2	
	HD-NVR-EXP2-10TB	10 TB RAID 6 expansion, 2U rack mount	
	HD-NVR-EXP2-20TB	20 TB RAID 6 expansion, 2U rack mount	
	HD-NVR-EXP2-30TB	30 TB RAID 6 expansion, 2U rack mount	
	* Control Center licenses must be purchased separately		

HD NETWORK VIDEO RECORDER SERVER, 5.0 TB STORAGE

Operations & Maintenance Manual
December 2015

NS3550-2T-8S
NS3550-8T-2S
NS3552-8P-2S

Industrial Gigabit Managed Switches

NS3550-2T-8S
8+2 Industrial Gigabit Fiber Managed Switch

NS3550-8T-2S
8+2 Industrial Gigabit Managed Switch

NS3552-8P-2S
8+2 Industrial Gigabit PoE+ Managed Switch

OVERVIEW

The IFS® NS3552-8P-2S is an Industrial Gigabit PoE+ Managed Switch equipped with eight 10/100/1000Mbps RJ45 ports with PoE+ (30w) capabilities and two 100/1000Mbps SFP (fiber) uplink ports.

The IFS NS3550-8T-2S is an Industrial Gigabit Managed Switch equipped with eight 10/100/1000Mbps RJ45 ports and two 100/1000Mbps SFP (fiber) uplink ports.

The IFS NS3550-2T-8S is an Industrial Gigabit Fiber Managed Switch equipped with eight 100/1000Mbps SFP (fiber) ports and two 10/100/1000Mbps RJ45 ports.

These are fully managed Layer 2 switches providing a robust industrial hardened design that provides for rapid operational recovery in the event of a network or power system failure.

Layer 2 Managed Switch

The IFS Industrial Gigabit Managed Switch Series supports advanced features including IEEE 802.1Q VLAN, GVRP, port link aggregation, QoS, broadcast storm control and MAC address filtering. The series also includes IGMP snooping and querying multicasting for media operations and bandwidth utilization to fit a variety of applications. Via aggregation of supporting ports, the series allows the operation of high-speed trunk operation combining multiple ports. A maximum of four ports can be assigned for four trunk groups and support fail-over as well. Additionally, its standards-compliant implementation ensures interoperability with equipment from other vendors.

Industrial-grade Network Redundancy and Recovery

These switches not only incorporate the industry standard Rapid Spanning Tree Protocol (IEEE 802.1w RSTP), but also an advanced Industrial Fail-Safe (IFS) technology accommodating multiple redundant ring topologies and improved network recovery time of less than 20ms. The switches incorporate a redundant power supply system to further enhance network reliability and uptime. Ideal for use in implementing highly fault-tolerant ring and mesh network architectures, these switches are well suited for harsh environments such as industrial security, factory automation and intelligent transportation systems (ITS).

Robust Hardened Design

With an IP-30 rated enclosure, IFS Industrial Gigabit Managed Switches provide a high level of immunity against electromagnetic (EMI) and radio-frequency (RFI) interference typically found in industrial environments. This series of switches comply with IEC60068-2-xx standards for free-fall, shock, and vibration and operate in -40°C~75°C temperatures found in difficult environments such as plant floors or in curbside traffic control cabinets.

STANDARD FEATURES

Physical Ports
- Auto MDI/MDI-X
- Auto-negotiation
- 1 RJ-45 console port

NS3550-2T-8S
- 8-ports SFP (fiber) 100/1000Base-X and 2-ports 10/100/1000Base-T

NS3550-8T-2S
- 8-port 10/100/1000Base-T and 2-ports SFP (fiber) 100/1000Base-X

NS3552-8P-2S
- 8-port 10/100/1000Base-T with PoE+ and 2-ports SFP (fiber) 100/1000Base-X

Power over Ethernet (NS3552-8P-2S Only)
- Complies with IEEE 802.3af / IEEE 802.3at Power over Ethernet / End-Span PSE
- Up to 8 IEEE 802.3af / 802.3at devices powered
- Supports PoE Power up to 30.8 Watts for each PoE ports
- Auto detect powered device (PD)
- Circuit protection prevent power interference between ports
- Remote power feeding up to 100m
- PoE Management features
- IEEE 802.3af and IEEE 802.3at mode switch control
- Total PoE power budget control
- Per port PoE function enable/disable
- PoE Admin-mode control
- PoE Port Power feeding priority
- Per PoE port power limit
- PD classification detection
- Temperature Threshold Control
- PoE Usage Threshold Control
- PD Alive check/reboot
- PoE schedule

Robust Hardened Design
- IP30 Aluminum metal case protection
- DIN-rail and Wall Mount Design
- 48V DC, redundant power with polarity reverse protect function
- Supports EFT protection 6000VDC for power line
- Supports 6000VDC Ethernet ESD protection
- -40°C~75°C operating temperature

Digital Input/Digital Output (NS3552-8P-2S and NS3550-8T-2S Only)
- 2 Digital Input (DI)
- 2 Digital Output (DO)
- Integrate sensors into auto alarm system
- Transfer alarm to IP network via email and SNNP trap

Layer 2 Features
- Prevents packet loss with back pressure (Half-Duplex) and IEEE 802.3x PAUSE frame flow control (Full-Duplex)
- High performance of Store-and-Forward architecture and runt/CRC filtering eliminate erroneous packets to optimize the network bandwidth
- Storm Control support
- Broadcast / Multicast / Unicast
- Supports **VLAN**
- IEEE 802.1Q Tagged VLAN
- Up to 255 VLANs groups, out of 4094 VLAN IDs
- Provider Bridging (VLAN Q-in-Q) support (IEEE 802.1ad)
- Private VLAN Edge (PVE)
- Protocol-Based VLAN
- MAC-Based VLAN
- Voice VLAN
- Supports **Spanning Tree Protocol**
- STP, IEEE 802.1D Spanning Tree Protocol
- RSTP, IEEE 802.1w Rapid Spanning Tree Protocol
- MSTP, IEEE 802.1s Multiple Spanning Tree Protocol, spanning tree by VLAN
- BPDU Guard
- Supports **Link Aggregation**
- 802.3ad Link Aggregation Control Protocol (LACP)
- Cisco ether-channel (Static Trunk)
- Maximum 5 trunk groups, up to 8 ports per trunk group
- Up to 16Gbps bandwidth (Duplex Mode)
- Provides Port Mirror (1-to-1)
- Port Mirroring to monitor the incoming or outgoing traffic on a particular port
- Loop protection to avoid broadcast loops

Quality of Service
- Ingress Shaper and Egress Rate Limit per port bandwidth control
- 8 priority queues on all switch ports
- Traffic classification
- IEEE 802.1p CoS
- IP TOS / DSCP / IP Precedence
- IP TCP/UDP port number
- Typical network application
- Strict priority and Weighted Round Robin (WRR) CoS policies
- Supports QoS and In/Out bandwidth control on each port
- Traffic-policing policies on the switch port
- DSCP remarking

Multicast
- Supports IGMP Snooping v1, v2 and v3
- Supports MLD Snooping v1 and v2
- Querier mode support
- IGMP Snooping port filtering
- MLD Snooping port filtering
- MVR (Multicast VLAN Registration)

Security
- IEEE 802.1x Port-Based / MAC-Based network access authentication
- Built-in RADIUS client to co-operate with the RADIUS servers
- TACACS+ login users access authentication
- RADIUS / TACACS+ users access authentication
- IP-Based Access Control List (ACL)
- MAC-Based Access Control List
- Source MAC / IP address binding
- DHCP Snooping to filter untrusted DHCP messages
- Dynamic ARP Inspection discards ARP packets with invalid MAC address to IP address binding
- IP Source Guard prevents IP spoofing attacks
- Auto DoS rule to defend DoS attack
- IP address access management to prevent unauthorized intruder

Management
- Switch Management Interfaces
- Console / Telnet Command Line Interface
- Web switch management
- SNMP v1 and v2c switch management
- SSH / SSL and SNMP v3 secure access
- Four RMON groups (history, statistics, alarms, and events)
- **IPv6** IP Address / NTP / DNS management
- Built-in Trivial File Transfer Protocol (TFTP) client
- BOOTP and DHCP for IP address assignment
- Firmware upload / download via HTTP / TFTP
- DHCP Relay
- DHCP Option 82
- User Privilege levels control
- NTP (Network Time Protocol)
- Link Layer Discovery Protocol (LLDP) Protocol
- Cable Diagnostic technology provides the mechanism to detect and report potential cabling issues (NS3552-8P-2S Only)
- Reset button for system reboot or reset to factory default

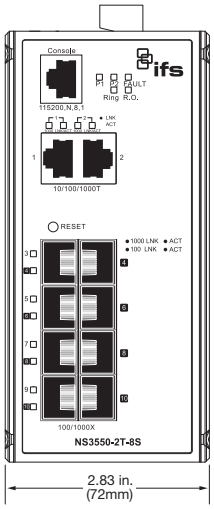
Industrial Gigabit Managed Switch Specifications

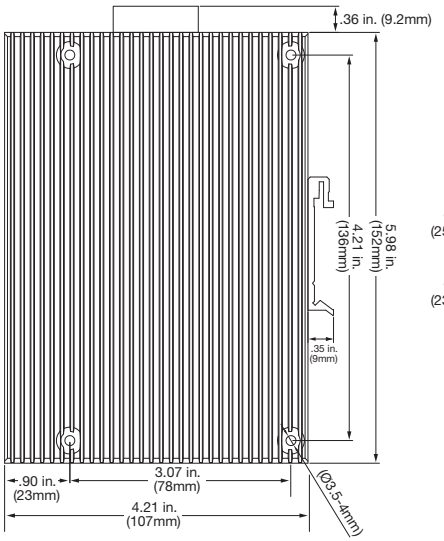
	PART NO.	NS3550-2T-8S	NS3550-8T-2S	NS3552-8P-2S
				
Physical Ports	10/100/1000Base-T Ports	RJ-45 (2)	RJ-45 (8)	RJ-45 (8)
	100/1000Base-X SFP Ports	SFP Ports (8)	SFP Ports (2)	SFP Ports (2)
	Port Configuration	Auto MDI/MDI-X		
	Port Speed	Auto-negotiate		
	Electro Static Discharge (ESD) Protection	6K VDC		
	Console Port	RJ-45 (1)		
Switch Performance	Switch Architecture	Store-and-Forward		
	Switch Fabric	20Gbps/non-blocking		
	Throughput (Packet per second)	14.8Mpps @64Bytes		
	Address Table	8K entries		
	Share Data Buffer	4Mbit		
	Maximum Frame Size	9K Bytes (Jumbo Frames)		
	Flow Control	Back pressure for Half-Duplex IEEE 802.3x Pause Frame for Full-Duplex		
Layer 2	Port Configuration	Port disable/enable, Auto-negotiation 10/1000/1000Mbps full and half-duplex mode selection, Flow control disable/enable and bandwidth control on each port		
	Port Status	Display each port's speed Auto negotiation status, duplex mode, link status, Flow control status		
	Bandwidth Control	Bandwidth control per port: Ingress: 500Kb~1000Mbps, Egress: 500Kb~1000Mbps		
	Spanning Tree	IEEE 802.1d Spanning Tree, IEEE 802.1w Rapid Spanning Tree, IEEE 802.1s Multiple spanning tree protocol		
	VLAN	802.1Q Tagged Based VLAN, up to 255 VLAN groups Q-in-Q tunneling Private VLAN Edge (PVE) MAC-Based VLAN Protocol-Based VLAN Voice VLAN MVR (Multicast VLAN Registration) Up to 255 VLAN groups, out of 4094 VLAN IDs		
	Multicast	IGMP (v1/v2/v3) Snooping, up to 255 multicast Groups IGMP Querier mode support MLD (v1/v2) Snooping, up to 255 multicast Groups MLD Querier mode support		
	QoS	Traffic classification based, Strict priority and WRR 8-Level priority for switching - Port Number - 802.1p priority - 802.1Q VLAN tag - DSCP/TOS field in IP Packet		
	Port Mirroring	RX / TX / Both		
	Security	IEEE 802.1x Port-Based / MAC-Based network access authentication. RADIUS / TACACS+ users access authentication. IP-Based Access Control List (ACL). MAC-Based Access Control List. Source MAC / IP address binding. DHCP Snooping. Dynamic ARP Inspection. IP Source Guard prevents IP spoofing attacks. Auto DoS rule to defend DoS attack. IP address access management		
	SMNP MIBs	RFC-1213 MIB-II, IF-MIB, RFC-1493 Bridge MIB, RFC-1643 Ethernet MIB, RFC-2863 Interface MIB, RFC-2665 Ether-Like MIB, RFC-2819 RMON MIB (Group 1, 2, 3 and 9), RFC-2737 Entity MIB, RFC-2618 RADIUS Client MIB, RFC-2933 IGMP-STD-MIB, RFC3411 SNMP-Frameworks-MIB, IEEE 802.1X PAE, LLDP, MAU-MIB		
	Link Aggregation	IEEE 802.3ad LACP / Static Trunk, Supports 5 groups of 8-Port trunk support		
	Management Interface	Console, Telenet, Web Browser, SNMP v1, v2c and v3		

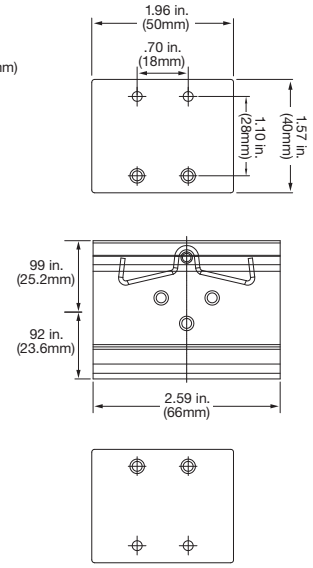
	PART NO.	NS3550-2T-8S	NS3500-8T-2S	NS3552-8P-2S
				
Power over Ethernet PoE)	IEEE PoE Standard			IEEE 802.3af/IEEE 802.3at Power over Ethernet/PSE
	Maximum Devices			8
	Output Power (per-port)			Per Port 56VDC, 350mA max. 15.4 watts (IEEE 802.3af) Per Port 56VDC, 590mA max. 30 watts (IEEE 802.3at)
	PoE Pin Assignment			1/2(+), 3/6(-)
LED Status Indicators	System	Power 1 (Green), Power 2 (Green), Fault Alarm (Green), Ring (Green), Ring Owner (Green)		
	10/100/1000Mbps Ports	LNK/ACT (Green)		PoE In-Use (Orange), LNK/ACT (Green)
	SFP GigE Uplink Ports	1000 (Orange), LNK/ACT (Green)		
Electrical & Mechanical	Power Input 1 (Primary Power)	12-48VDC or 24VAC		48VDC
	Power Input 2 (Primary Power)	12-48VDC or 24VAC		48VDC
	Electrical Fast Transient (EFT) Protection	6KV DC		
	Power and Alarm Fault Connector	6-pin removable screw terminal		
	Alarm Fault Relay	1A @ 24VDC		
	Enclosure	IP-30 Metal Case		
	Mounting	DIN-rail or wall-mount		
	Dimensions (in/cm) (W x D x H)	6 x 4.21 x 2.83 in. (152 x 107 x 72mm)	3.5 x 5.31 x 2.2 in. (88 x 135 x 56mm)	6 x 4.21 x 2.83 in. (152 x 107 x 72mm)
	Weight (lbs/g)	2.28 lbs., 1036g	1.59 lbs., 720g	3.71 lbs., 1684g
Environ-mental	Operating Temperature	-40ºC~-75ºC		
	Storage Temperature	-40ºC~-85ºC		
	Relative Humidity	5%~95% (non-condensing)		
Standards Compliance	Regulatory Standards	FCC Part 15 Class A, CE		
	IEEE/RFC Standards	IEEE 802.3 10Base-T IEEE 802.3u 100Base-TX/100Base-FX IEEE 802.3z Gigabit SX/LX IEEE 802.3ab Gigabit 1000T IEEE 802.3x Flow Control and Back Pressure IEEE 802.1d Spanning Tree Protocol IEEE 802.1w Rapid Spanning Tree Protocol IEEE 802.1p Class of Service IEEE 802.1Q VLAN Tagging IEEE 802.1x Port Authentication Network Control IEEE 802.3af Power over Ethernet (NS3552-8P-2S) RFC 768 UDP RFC 793 TFTP RFC 791 IP RFC 792 ICMP RFC 2068 HTTP RFC 1112 IGMP Version 1 RFC 2236 IGMP Version 2		
	IEC Standards	IEC60068-2-32 (Free fall) IEC60068-2-27 (Shock) IEC60068-2-6 (Vibration)		

Dimensional Diagrams

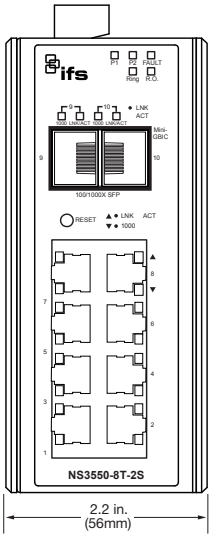
NS3550-2T-8S

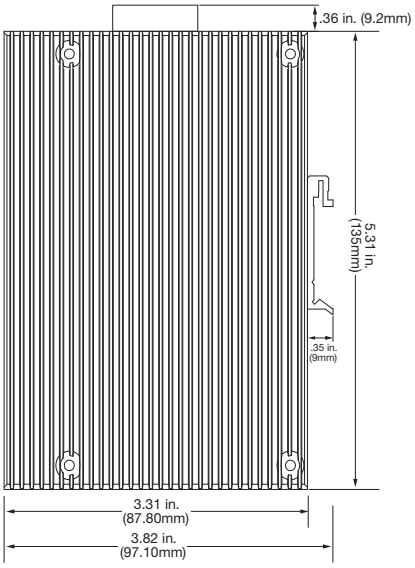


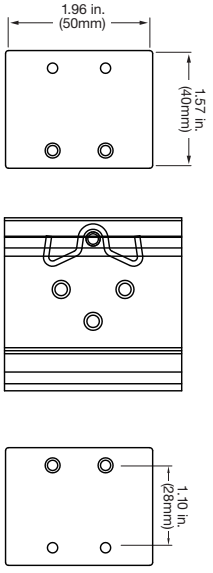




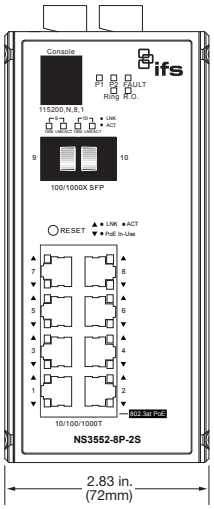
NS3550-8T-2S

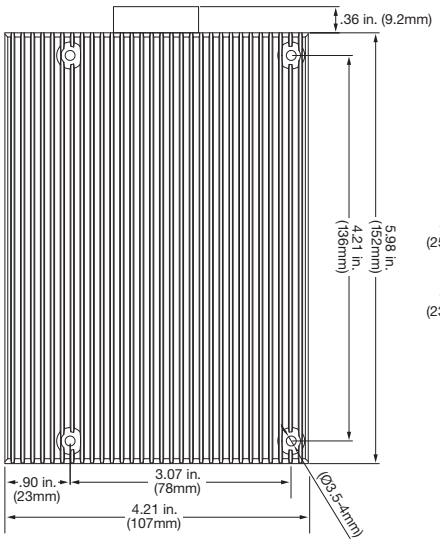


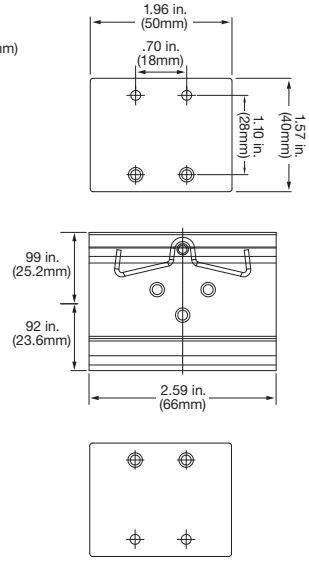




NS3552-8P-2S







This Page Left Intentionally Blank

avigilon
THE BEST EVIDENCE™

Installation Guide

Avigilon High Definition Network Video Recorder Server:

3.0TB-HD-NVR2, 5.0TB-HD-NVR2, 10.0TB-HD-NVR2,
15.0TB-HD-NVR2 and 21.0TB-HD-NVR2

920-0047B-Rev2

Avigilon
Tel +1.604.629.5182
Fax +1.604.629.5183

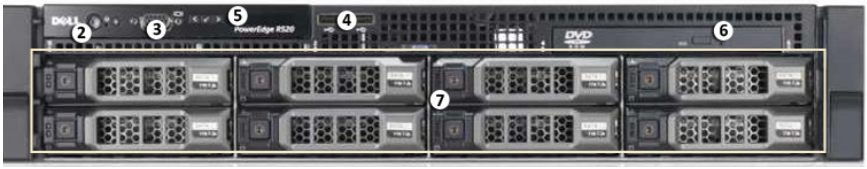
http://www.avigilon.com

Revised 07/11/2012

Table of Contents

Overview

Front



	Feature	Description
0	Bezel	The bezel protects the server from unauthorized physical access. The bezel must be removed to access the front of the server.
1	Bezel lock	Locks the bezel into place.
2	Power button	Controls the power supply to the server.
3	Video connector	Accepts a VGA monitor connection.
4	USB connectors	Accepts USB connections to external devices.
5	LCD message display	Displays server status information and error messages.
6	DVD drive	Provides access to DVD media.
7	Hard drives	Provides access to six hot-swappable hard drives. There are LED indicators on each hard drive. See *LED Indicators* on page 13 for more information.

Back

	Feature	Description
1	Power supply	Accepts power input. In the image, the secondary redundant power supply (HD-NVR2-2ND-PS) is installed.
2	Serial connector	Accepts connections to serial devices.
3	Video connector	Accepts a VGA monitor connection.
4	Expansion slots	There are 3 empty expansion slots. This is where you would install the expansion card (HD-NVR2-EXP2-CARD) for connecting to storage expansions.
5	Ethernet port	Accepts an Ethernet connection to a network.
6	USB connectors	Accepts USB connections to external devices.

Installation

Required Tools and Materials

- #1 Phillips screwdriver

Package Contents

Ensure the package contains the following:

- Avigilon High Definition Network Video Recorder (NVR) Server
- Avigilon Control Center Software Installation DVD
- Avigilon Control Center Recovery DVD
- Power Cable
- USB Keyboard
- USB Mouse
- Bezel and Key
- Rack Sliding Rail Assembly Kit
- Cable Management Arm Assembly Kit

Installation Steps

Consult the *Product Information Guide* provided with the server for relevant safety information before you begin installation.

- *Installing the Rack Rails and Cable Management Arm* on page 4
- *Connecting Cables* on page 4
- *Installing the Bezel* on page 4
- *Licensing the Avigilon Control Center* on page 5
- *Assigning an IP Address* on page 7

Installing the Rack Rails and Cable Management Arm

If the server will be kept in a server rack, install the Rack Sliding Rails and the Cable Management Arm provided in the server package. Follow the procedures outlined in the *Rack Installation Instructions* and the *CMA Installation Instructions* provided in the assembly kits.

NOTE: The supplied Rack Sliding Rails are compatible with square and round hole racks.

Connecting Cables

Refer to the server diagrams in the Overview section for the location of the different connectors.

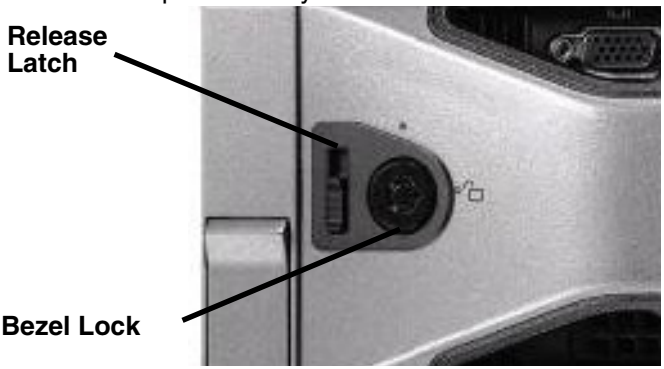
1. Connect the keyboard and mouse to an available USB connector on either the front or the back of the server.
2. Connect a monitor to the video connector on the server.
3. Connect the server to your network using an Ethernet network cable.
4. Connect the power cable to the power supply at the back of the server.
5. If you are also installing an Avigilon HD NVR Storage Expansion with your server, connect the server to the storage expansion. See *Connecting Storage Expansions* on page 9 for more information.
6. Press the power button on the front of the server. Check that the server LED indicators display the correct status. See *LED Indicators* on page 13 for more information.

Installing the Bezel

The bezel can be installed on the front of the server to help protect the power button and hard drives against unauthorized access.

1. Slide the right end of the bezel against the right hinge of the server.
2. Push the left end of the bezel against the server until it clicks into place.

3. Use the provided key to lock the bezel.



Removing the Front Bezel

The bezel must be removed before you can access the power button, hard drives, and DVD drive.

1. Unlock the bezel.
2. Pull the release latch beside the bezel lock, then carefully pull the bezel away from the server.

Licensing the Avigilon Control Center

Once the server has been installed, you need to activate the license for the Avigilon Control Center Server software before it can be used to coordinate your high definition surveillance system.

NOTE: If the Control Center Server software was not preinstalled, insert the installation DVD and install the software.

1. Log in to Windows.

   The default username is `Administrator` with no password. It is recommended that you add a password to the Administrator account after your first login. For more information, see the *Windows Help and Support*.

2. Open the Admin Tool:
   - From the Windows Start menu, select **Programs > Avigilon > Avigilon Control Center Server > Avigilon Control Center Server Admin Tool**.
   - Or, double-click the  icon on your desktop.

3. When the Avigilon Control Center Admin Tool opens, select the **Settings** tab and click **Licensing**.
4. In the License Activation dialog box, click **Add License**. The Add License wizard is displayed.

   You have two license activation options: Internet Activation or Manual Activation. Complete one of the following procedures.

Internet Activation

If you have internet access on your server, the Admin Tool connects to the internet and activates your license.

1. In the Add License wizard, click **Internet Activation**.
2. On the Enter Product Key page, enter your license key.

   A green check mark will appear beside your license key when it is correct.

3. Click **Next**.
4. On the Product Registration page, enter your contact information to receive product updates. Then click **Next**.
5. The Admin Tool connects to the Avigilon licensing server and activates the license.

   When the *Activation Succeeded* message appears, click **Finish**.

Manual Activation

If your server does not have internet access, you can activate your license by generating an activation file from the Admin Tool and uploading the file to the Avigilon License Activation web page from a computer with internet access.

1. In the Add License wizard, click **Manual Activation**.
2. On the following page, click **Step 1: Generate Activation File**.
3. On the Enter Product Key page, enter your license key.

   A green check mark will appear beside your license key when it is correct.

4. Click **Next**.
5. On the Select Activation File page, confirm where the activation file will be saved. Click **[...]** to navigate to a different file location.

   You can rename the activation file, but you must keep the *.key* extension.

6. Click **Next**.

   On the following page, you will see the *Activation File Saved* message.
7. Find the saved activation file and copy the file to a computer with internet access.
8. Open a web browser and go to http://activate.avigilon.com.
9. At the Avigilon License Activation web page, click **Browse** to locate your activation file then click **Upload Activation File**.
10. When you see the *You have successfully activated your product!* message, click **Download License File** and save the license file.
11. Complete the product registration section to receive product updates from Avigilon, then click **Register**.
12. Find the downloaded license file and copy the file to the server you are activating.
13. If the *Activation File Saved* message is still displayed in the Add License wizard, click **Next**.
14. On the following page, click **Step 2: Add License File**.
15. On the Import License File page, click **[...]** to locate the license file then click **Next**.
16. When the *Activation Succeeded* message appears, click **Finish**.

Assigning an IP Address

Once the Avigilon Control Center Server has been licensed, you can assign an IP address to the server. The server obtains an IP address automatically by default, but you can configure the server to use a static IP address.

1. In Windows, select **Start > Control Panel > Network Connections**.
2. Right-click a network connection and select **Properties**.
3. In the Local Area Connection Properties dialog box, select **Internet Protocol (TCP/IP)** then click **Properties**.
4. In the Internet Protocol (TCP/IP) Properties dialog box, you can allow the server to obtain an IP address automatically, or you can choose to assign a static IP address:
   a. Select **Use the following IP address:** then assign an **IP address**, a **Subnet mask**, and a **Default gateway**.
   b. Enter the **Preferred DNS server** address and an **Alternate DNS server** address.
   c. Click **OK**.

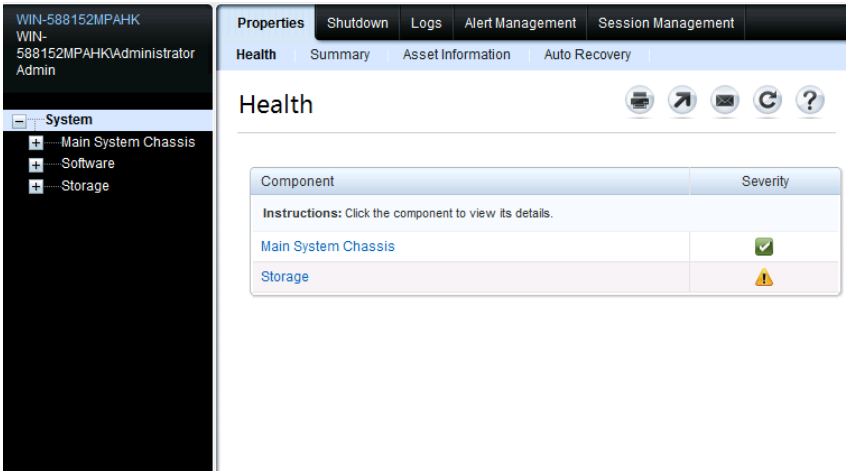
Advanced Features

Server Administrator

The Server Administrator software is preinstalled on the server. The software provides information about the server's system operation status, and gives you remote access to the server for recovery operations.

If one of the LED indicators on the server is flashing an error warning, the Server Administrator will display details about the problem. For more information about the LED indicators, see *LED Indicators* on page 13.

1. Open the Server Administrator.
   - To open the Server Administrator locally, double-click the  **Server Administrator** shortcut icon on the desktop.
   - To open the Server Administrator remotely, open a web browser and enter this address: `https://<server IP Address>:1311/` (for example, `https://192.168.1.32:1311/` or `https://localhost:1311/`)
2. Enter your Windows username and password for the server. Make sure there is a password for the Administrator account because the Server Administrator does not allow an empty password field.
3. On the Server Administrative home page, the health of the system components are displayed in the workspace on the right.



- To see the health of other system components, expand and select a different component from the System Tree on the left.
- The table displayed in the workspace lists system components and their status.

	The system component is running normally.
	The system component has an error.
	The system component has a critical failure.
	The system component status is unknown.

- To see the details of a system component, select the system component from the workspace.

4. Select **System** on the System Tree to return to the home page.

For more information about the features in the Server Administrator, see the Help system provided in the software.

Connecting Storage Expansions

To increase the recording capacity of your Avigilon HD Surveillance System, you can connect an Avigilon HD NVR Storage Expansion (HD-NVR-EXP2-x.xTB) to the server.

NOTE: The Avigilon HD NVR server must have an Avigilon NVR Expansion Card (HD-NVR2-EXP2-CARD) installed before the storage expansion can be connected.

1. Turn off the server.
2. Install the NVR Expansion Card.
   a. Open the NVR server by unlocking the latch release lock then lifting the black latch to remove the cover.
   b. On the back of the server, lift the expansion card latch
   c. Remove one of the filler brackets guarding the expansion slots.
   d. Align the NVR Expansion Card edge with the row where the filler bracket has been removed.

e. Gently press the NVR Expansion Card into the riser card slot until it is firmly in place and the card connectors extend through the expansion slot.

f. Close the expansion card latch and reinstall the server cover.

3. Connect power to the storage expansion.
4. Connect the storage expansion to the server.
   a. Connect one end of the supplied Serial Attached SCSI (SAS) cable to the storage expansion's primary **In** port.
   b. Connect the other end of the SAS cable to an available port on the expansion card installed on the back of the server.
5. Turn on the storage expansion and the server.
6. In the Admin Tool, set up the Avigilon Control Center storage configuration to include the storage expansion.

For more information, see *Connecting the NVR Expansion* that is provided with the storage expansion.

Replacing Hard Drives

The hard drives on the server are set up in a Redundant Array of Independent Disks (RAID) configuration. This allows information to be recorded across several hard drives. If one hard drive fails, there is enough information on the other hard drives for the server to continue functioning. Only one hard drive can be replaced at a time while the server is running.

If your server is still under warranty, contact Avigilon Technical Support to replace a failed hard drive: http://avigilon.com/#/support-and-downloads/

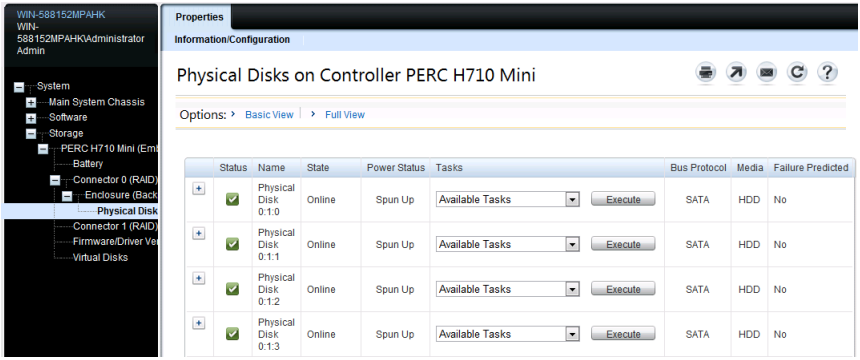
If two or more hard drives fail at the same time, contact Avigilon Support immediately for recovery instructions.

Important: Only replace a hard drive if the hard drive LED indicator and the Server Administrator displays an error. See *LED Indicators* on page 13 and *Server Administrator* on page 8 for more information.

1. Open the Server Administrator using an Administrator login.
2. In the System Tree on the left pane, select **System > Storage > Perc H710 Mini (Embedded) > Virtual Disks**.
   a. For the redundant virtual disk, select **Check Consistency** from the drop down list and click **Execute**. Wait until the task is done before continuing this procedure.

3. Select **Connector 0 (RAID)** or **Connector 1 (RAID) > Enclosure (Backplane) > Physical Disks**

   Connector 0 and Connector 1 give you access to different hard drives.



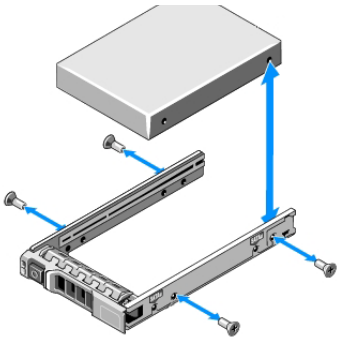
4. In the workspace, locate the hard drive you want to replace.

   To help you locate the hard drive, select **Blink** in the Available Tasks drop down list then click **Execute**. The LED indicators on the selected hard drive will start blinking. Select **Unblink** and click **Execute** to have it stop.

5. For the hard drive you want to replace, select **Offline** from the Available Tasks drop down list and click **Execute**. The hard drive will be disconnected from the server for removal.

   The hard drive is listed as Offline in the Server Administrator.

6. Press the release button on the front left of the hard drive. When the handle is released, pull the hard drive out of the server.
7. Remove the screws from the side of the hard drive carrier to remove the hard drive.



8. Install a new hard drive into the carrier then re-attach the screws. The hard drive connectors should face the back.

9. When the hard drive is secured in the carrier, insert the hard drive back into the server.
10. Once the hard drive is inserted all the way in, push the handle against the hard drive to lock it into place.

    The server immediately starts rebuilding the hard drive. The progress is displayed in the Server Administrator. This may take several hours.

When the hard drive comes online, normal operations can be resumed.

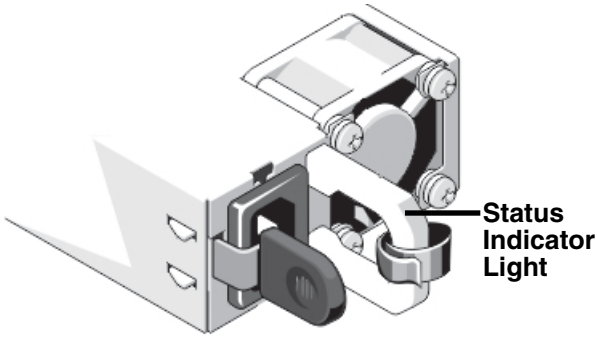
LED Indicators

The following tables describe what the LEDs on the server indicate.

Power Status Indicators

The power button on the front of the server lights up when power is on.

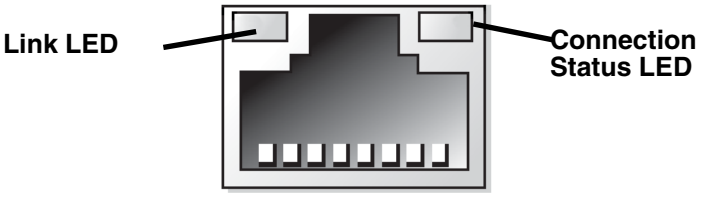
Additional information about the power supply is provided by the power status indicator on the back of the server. The following table describes what the LEDs indicate:



LED Indicator	Description
Off	Power is not connected.
Green	Power is supplied to the server.
Flashing orange	There is a problem with the power supply
Flashing green	The redundant power supply is mismatched. This only occurs if you have a secondary redundant power supply installed.

Network Link Status Indicator

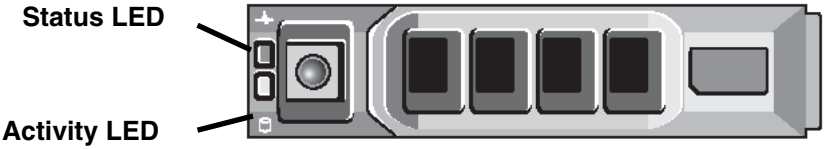
When the server is connected to the network, the server's connection status LEDs above the Ethernet port display the server's connection status to the network. The following table describes what the LEDs indicate:



LED Indicators	Description
Off	The server is not connected to the network.
Link LED is green	The server is connected to the network at its maximum port speed.
Link LED is orange	The server is connected to the network at less than its maximum port speed.
Connection Status LED is blinking green	The server is working with other parts of the Avigilon Control Center.

Hard Drive RAID Status Indicators

Each hard drive has its own set of LED indicators to show its activity and status.



The Activity LED flashes green when the hard drives are working. The following table describes what the Status LEDs indicate:

LED Indicators	Description
Green	The hard drive is online.
Off	The hard drive is disconnected from the server.
Two short green flashes every second	Identifying a new hard drive, or preparing a hard drive for removal.
Flashes green, orange then off	Hard drive is predicted to fail.
Four short orange flashes per second	Hard drive has failed.
Flashes green slowly	Hard drive is rebuilding.
Blinks green for three seconds, orange for three seconds and off for six seconds	Hard drive rebuild has been aborted

Specifications

System	
Avigilon Control Center Server software	Enterprise, Standard and Core edition compatible
Operating System	Windows Embedded Standard 7
Hard Disk Drive Configuration	Near-line SAS, hot swappable, RAID 5
Mechanical	
Dimensions (L x W x H)	611 mm x 434 mm x 86 mm (24” x 17” x 3.4”)
Weight	28.2 kg (62.2 lbs)
Form Factor	2U rack
Electrical	
Power Input	100 to 240 VAC, 50/60 Hz, auto-switching
Power Consumption	495 W
Power Supply	Single hot-swappable, dual redundant option (HD-NVR2-2ND-PS)
Environmental	
Operating Temperature	10°C to 35°C (50°F to 95°F)
Storage Temperature	-40° C to 65° C (-40° F to 149° F)
Humidity	20 - 80% Relative humidity (non-condensing)
Operating Vibration	0.26 Grms at 5 Hz to 350 Hz for 2 minutes
Storage Vibration	1.87 Grms Random Vibration at 10 Hz to 500 Hz for 15 minutes
Operating Shock	1 shock pulse of 31 G for up to 2 ms
Storage Shock	6 shock pulses of 71 G for up to 2 ms
Operating Altitude	-15.2 m to 3048 m (-50 ft to 10,000 ft)
Storage Altitude	-15.2 m to 10,668 m (-50ft to 35,000ft)
Certifications	
	EN 60950-1:2006 + A11:2009 IEC 60950-1:2005 Ed2 EN 62311:2008
Electromagnetic Emissions	EN 55022:2006 + A1:2007 CISPR 22:2005 + A1:2005 EN 61000-3-2:2006 IEC 61000-3-2:2005 (Class D) EN 61000-3-3:1995 + A1:2001 + A2:2005 IEC 61000-3-3:1994 + A1:2001 + A2:2005
Electromagnetic Immunity	EN 55024:1998 + A1:2001 + A2:2003 CISPR 24:1997 (modified)+A1:2001 + A2:2002

Limited Warranty & Technical Support

Avigilon warrants to the original consumer purchaser, that this product will be free of defects in material and workmanship for a period of 3 years from date of purchase.

The manufacturer's liability hereunder is limited to replacement of the product, repair of the product or replacement of the product with repaired product at the discretion of the manufacturer. This warranty is void if the product has been damaged by accident, unreasonable use, neglect, tampering or other causes not arising from defects in material or workmanship. This warranty extends to the original consumer purchaser of the product only.

AVIGILON DISCLAIMS ALL OTHER WARRANTIES EXPRESSED OR IMPLIED INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, EXCEPT TO THE EXTENT THAT ANY WARRANTIES IMPLIED BY LAW CANNOT BE VALIDLY WAIVED.

No oral or written information, advice or representation provided by Avigilon, its distributors, dealers, agents or employees shall create another warranty or modify this warranty. This warranty states Avigilon's entire liability and your exclusive remedy against Avigilon for any failure of this product to operate properly.

In no event shall Avigilon be liable for any indirect, incidental, special, consequential, exemplary, or punitive damages whatsoever (including but not limited to, damages for loss of profits or confidential or other information, for business interruption, for personal injury, for loss of privacy, for failure to meet any duty including of good faith or of reasonable care, for negligence, and for any other pecuniary or other loss whatsoever) arising from the use of or inability to use the product, even if advised of the possibility of such damages. Since some jurisdictions do not allow the above limitation of liability, such limitation may not apply to you.

This Limited Warranty gives you specific legal rights and you may also have other rights which vary from jurisdiction to jurisdiction.

Warranty service and technical support can be obtained by contacting Avigilon Technical Support by phone at 1.888.281.5182 or via email at support@Avigilon.com.

avigilon

THE BEST EVIDENCE™

This Page Left Intentionally Blank

IFS GIGABIT MANAGED SWITCH

Operations & Maintenance Manual
December 2015

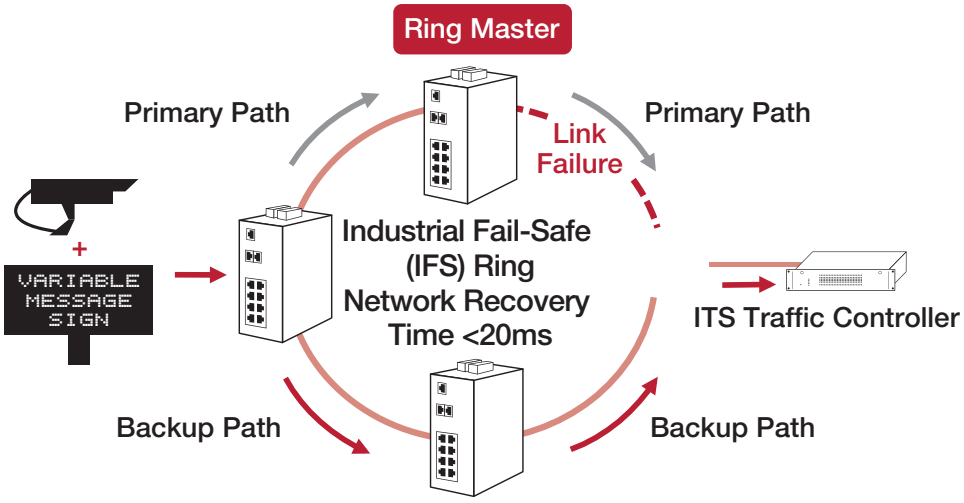
North America
T 855-286-8889

Latin America
T 561-998-6114

NS3550-2T-8S
NS3550-8T-2S
NS3552-8P-2S

Industrial Gigabit Managed Switches

Typical Application



Ordering Information

NS3550-2T-8S	8-Port Industrial Gigabit Fiber Managed Switch (SFP) (Wide Operating Temp. -40°C~75°C)
NS3550-8T-2S	8-Port Industrial Gigabit Managed Switch (Wide Operating Temp. -40°C~75°C)
NS3552-8P-2S	8-Port Industrial Gigabit PoE+ Managed Switch (Wide Operating Temp. -40°C~75°C)
Included Accessories	User's Manual, DIN-rail Kit, Wall Mount Kit

Note: These switches require a Small Form-factor Pluggable (SFP) for optical uplink use. IFS SFPs are available for multi-mode, single mode, and 1 or 2 fibers for various transmission distances over optical fiber. Please refer to the IFS SFP data sheet to select the appropriate SFP for your particular application needs. IFS S25 or S35 Series SFPs are recommended.

Note: External power supply must be purchased separately.

Accessories

SFP	S30 Series
SFP	S35 Series (wide-temp)
SFP	S20 Series
SFP	S25 Series (wide-temp)
PS48VDC100W-DIN	48VDC Industrial 100W DIN-rail Power Supply (for NS3550-2T-8S or NS3550-8T-2S)
PS48VDC480W-DIN	48VDC Industrial 480W DIN-rail Power Supply (for NS3552-8P-2S)

interlogix
United Technologies

interlogix.com

Specifications subject to change without notice.

404-3817 2014/04 (78266)

This Page Left Intentionally Blank

IFS NS3550-8T-2S User Manual

P/N 1072687 • REV B • ISS 24JUN14

Trademarks and patents

The IFS NS3550-8T-2S name and logo are trademarks of United Technologies.

Other trade names used in this document may be trademarks or registered trademarks of the manufacturers or vendors of the respective products.

Manufacturer

UTC Building & Industrial Systems, Inc.
2955 Red Hill Avenue
Costa Mesa, CA 92626-5923, USA

Authorized EU manufacturing representative:
UTC Climate Controls & Security B.V.,
Kelvinstraat 7, 6003 DH Weert, Netherlands

Intended use

Use this product only for the purpose it was designed for; refer to the data sheet and user documentation for details. For the latest product information, contact your local supplier or visit us online at www.interlogix.com.

Certification

CE

TABLE OF CONTENTS

1. INTRODUCTION

IFS NS3550-8T-2S Industrial 8-Port 10/100/1000T + 2-Port 100/1000X SFP Managed Switch (-40~75 Degree C) is a managed switch with multiple Gigabit copper ports plus two Gigabit SFP mini-GBIC slots with fiber optical connective ability and robust layer 2 features. "**Industrial Managed Switch**" mentationed in the User's Manual represnts the **NS3550-8T-2S**.

1.1 Packet Contents

Open the box of the Industrial Managed Switch and carefully unpack it. The box should contain the following items:

- ☑ **The Industrial Managed Switch** x1
- ☑ **Quick Installation Guide** x1
- ☑ **User's Manual CD** x1
- ☑ **DIN Rail Kit** x1
- ☑ **Wall Mounting Kit** X1
- ☑ **Dust Cap** X10

If any of these are missing or damaged, please contact your dealer immediately; if possible, retain the carton including the original packing material, and use them again to repack the product in case there is a need to return it to us for repair.

1.2 Product Description

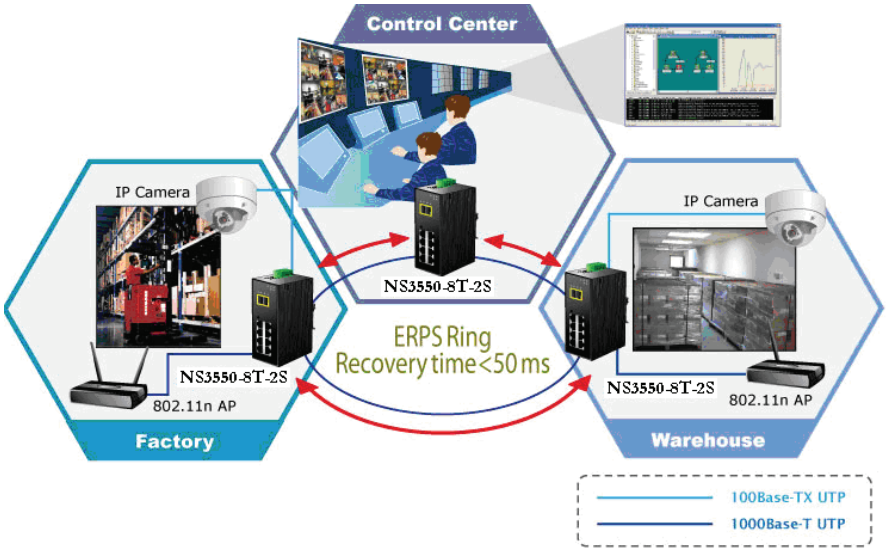
IFS NS3550-8T-2S is an **Industrial 10-Port Full Gigabit Managed Ethernet Switch** specially designed to build a full Gigabit backbone to transmit reliable but high speed data in heavy industrial demanding environments and forward data to remote network through fiber optic. It provides **8-Port 10/100/1000Base-T copper** and **2 extra 100/1000Base-X SFP fiber optic interfaces** delivered in an IP30 rugged strong case with redundant power system. Besides support for 20Gbps switch fabric to handle extremely large amounts of video, voice and important data in a secure topology, the **NS3550-8T-2S** provides user-friendly but advanced **IPv6 / IPv4 management** interfaces and abundant L2 / L4 switching functions. It is the best investment for industrial business expanding or upgrading its network infrastructure.

IPv6 / IPv4 Full-functioned Secure Switch for Building Automation Networking

The **NS3550-8T-2S** is the ideal solution to fulfilling the demand of IPv6 management Gigabit Ethernet Switch, especially in the Industrial hardened environment. It supports both IPv4 and IPv6 management functions and can work with original network structure. It provides advanced Layer 2 to Layer 4 data switching and redundancy, Quality of Service traffic control, network access control and authentication, and Secure Management features to protect customer's industrial and building automation network connectivity with reliable switching recovery capability that is suitable for implementing fault tolerant and mesh network architectures.

Redundant Ring, Fast Recovery for Surveillance System

The **NS3550-8T-2S** supports redundant ring technology and features strong rapid self-recovery capability to prevent interruptions and external intrusions. It incorporates advanced **ITU-T G.8032 ERPS (Ethernet Ring Protection Switching)** technology, Spanning Tree Protocol (802.1s MSTP), and **redundant power** input system into customer's industrial automation network to enhance system reliability and uptime in harsh factory environments. In certain simple Ring network, the recovery time of data link can be as fast as 20 ms.

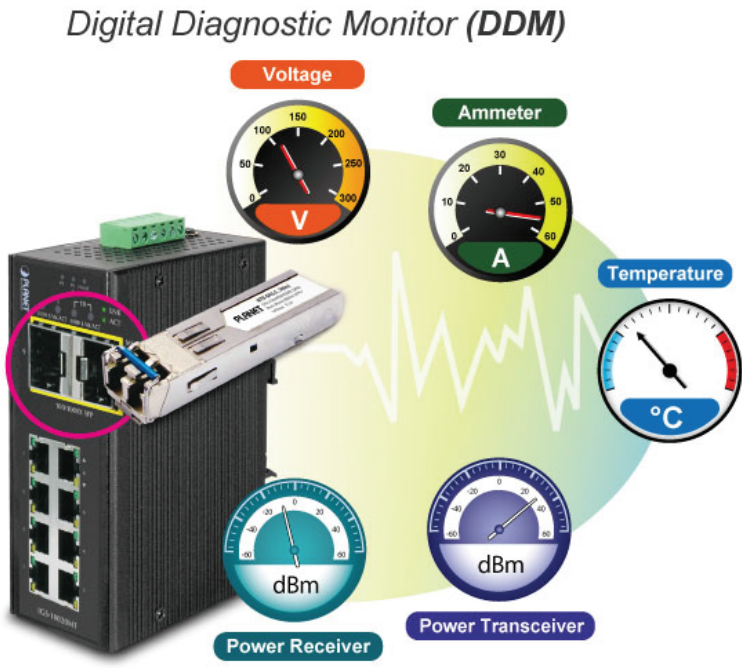


Environmentally Hardened Design

With IP30 aluminum industrial case protection, the **NS3550-8T-2S** provides a high level of immunity against electromagnetic interference and heavy electrical surges which are usually found on plant floors or in curb side traffic control cabinets. It also possesses an integrated power supply source with wide range of voltages (**12 to 48V DC** or **24V AC**) for worldwide high availability applications requiring dual or backup power inputs. Being able to operate under the temperature range from -40 to 75 degrees C, the **NS3550-8T-2S** can be placed in almost any difficult environment.

Flexible and Extendable Solution

The 2 mini-GBIC slots built in the **NS3550-8T-2S** support Dual-Speed, **100Base-FX** and **1000Base-SX/LX SFP** (Small Form-factor Pluggable) fiber-optic modules, meaning the administrator now can flexibly choose the suitable SFP transceiver according to the transmission distance or the transmission speed required to extend the network efficiently. The **NS3550-8T-2S** supports SFP-**DDM** (**Digital Diagnostic Monitor**) function that can easily monitor real-time parameters of the SFP for network administrator, such as optical output power, optical input power, temperature, laser bias current, and transceiver supply voltage.



Flexibility and Extension Solution

The two mini-GBIC slots built in the **NS3550-8T-2S** support Dual-Speed, **100Base-FX** and **1000Base-SX/LX** SFP (Small Form-factor Pluggable) fiber-optic modules, meaning the administrator now can flexibly choose the suitable SFP transceiver according to the transmission distance or the transmission speed required.

1.3 How to Use This Manual

This User Manual is structured as follows:

Section 2 INSTALLATION
The section explains the functions of the **Industrial Managed Switch** and how to physically install the **Industrial Managed Switch**.

Section 3 SWITCH MANAGEMENT
The section contains the information about the software function of the **Industrial Managed Switch**.

Section 4 WEB CONFIGURATION
The section explains how to manage the **Industrial Managed Switch** by Web interface.

Section 5 COMMAND LINE INTERFACE
The section describes how to use the Command Line interface (CLI).

Section 6 CLI MODE
The section explains how to manage the **Industrial Managed Switch** by Command Line interface.

Section 7 SWITCH OPERATION
The chapter explains how to do the switch operation of the **Industrial Managed Switch**.

Section 8 TROUBLESHOOTING
The chapter explains how to troubleshoot the **Industrial Managed Switch**.

Appendix A
The section contains cable information of the **Industrial Managed Switch**.

Appendix B
The section contains Glossary information of the **Industrial Managed Switch**.

1.4 Product Features

- **Physical Port**
  - **8-Port 10/100/1000Base-T** RJ-45 copper
  - **2 100/1000Base-X mini-GBIC/SFP** slots, SFP type auto detection
- **Industrial Case / Installation**
  - IP30 Aluminum case protection
  - DIN-Rail and Wall Mount Design
  - Redundant Power Design
    - 12 to 48V DC, redundant power with polarity reverse protect function
    - AC 24V power adapter acceptable
  - Supports EFT protection 6000 VDC for power line
  - Supports 6000 VDC Ethernet ESD protection
  - -40 to 75 degrees C operating temperature
- **Layer 2 Features**
  - Prevents packet loss with back pressure (Half-Duplex) and IEEE 802.3x PAUSE frame flow control (Full-Duplex)
  - High performance of Store-and-Forward architecture and runt/CRC filtering eliminates erroneous packets to optimize the network bandwidth
  - Storm Control support:
    - Multicast / Unknown-Unicast
  - Supports **VLAN**
    - IEEE 802.1Q Tagged VLAN
    - Up to 255 VLANs groups, out of 4095 VLAN IDs
    - Provider Bridging (VLAN Q-in-Q) support (IEEE 802.1ad)
    - Private VLAN Edge (PVE)
    - Protocol-based VLAN
    - MAC-based VLAN
    - Voice VLAN
  - Supports **Spanning Tree Protocol**
    - STP, IEEE 802.1D Spanning Tree Protocol
    - RSTP, IEEE 802.1w Rapid Spanning Tree Protocol
    - MSTP, IEEE 802.1s Multiple Spanning Tree Protocol, spanning tree by VLAN
    - BPDU Guard
  - Supports **Link Aggregation**
    - 802.3ad Link Aggregation Control Protocol (LACP)
    - Cisco ether-channel (Static Trunk)
    - Maximum 5 trunk groups, up to 10 ports per trunk group
    - Up to 20Gbps bandwidth(Duplex Mode)
  - Provides Port Mirror (many-to-1)
  - Port Mirroring to monitor the incoming or outgoing traffic on a particular port
  - Supports E.R.P.S. **(Ethernet Ring Protection Switching)**
- **Quality of Service**
  - Ingress Shaper and Egress Rate Limit per port bandwidth control
  - 8 priority queues on all switch ports

- Traffic classification:
  - IEEE 802.1p CoS
  - IP TOS / DSCP / IP Precedence
  - IP TCP/UDP port number
  - Typical network application
- Strict priority and Weighted Round Robin (WRR) CoS policies
- Supports QoS and In/Out bandwidth control on each port
- Traffic-policing policies on the switch port
- DSCP remarking

➢ **Multicast**

- Supports IGMP Snooping v1, v2 and v3
- Supports MLD Snooping v1 and v2
- Querier mode support
- IGMP Snooping port filtering
- MLD Snooping port filtering
- MVR (Multicast VLAN Registration)

➢ **Security**

- IEEE 802.1x Port-Based / MAC-Based network access authentication
- Build-in RADIUS client to co-operate with the RADIUS servers
- TACACS+ login users access authentication
- RADIUS / TACACS+ users access authentication
- IP-Based Access Control List (ACL)
- MAC-Based Access Control List
- Source MAC / IP address binding
- **DHCP Snooping** to filter untrusted DHCP messages
- **Dynamic ARP Inspection** discards ARP packets with invalid MAC address to IP address binding
- **IP Source Guard** prevents IP spoofing attacks
- Auto DoS rule to defend DoS attack
- IP address access management to prevent unauthorized intruder

➢ **Management**

- Switch Management Interfaces
  - Web switch management
  - Remote Telnet management
  - SNMP v1, v2c, and v3 switch management
  - SSH / SSL secure access
- Four RMON groups (history, statistics, alarms, and events)
- **IPv6** IP Address / NTP / DNS management
- Built-in Trivial File Transfer Protocol (TFTP) client
- BOOTP and DHCP for IP address assignment
- Firmware upload/download via HTTP / TFTP
- DHCP Relay
- DHCP Option82
- User Privilege levels control

- NTP (Network Time Protocol)
- Link Layer Discovery Protocol (LLDP) Protocol
- Cable Diagnostic technology provides the mechanism to detect and report potential cabling issues
- Reset button for system reboot or reset to factory default

1.5 Product Specifications

Model Name	**NS3550-8T-2S**	
Hardware Specification		
Copper Ports	8 10/ 100/1000Base-T RJ-45 Auto-MDI/MDI-X ports	
SFP/mini-GBIC Slots	2 1000Base-SX/LX/BX SFP interfaces (Port-9 and Port-10) Compatible with 100Base-FX SFP	
Switch Architecture	Store-and-Forward	
Switch Fabric	20Gbps / non-blocking	
Throughput (packet per second)	14.8Mpps	
Address Table	8K entries, automatic source address learning and ageing	
Share data Buffer	512 kilobytes	
Flow Control	IEEE 802.3x Pause Frame for Full-Duplex. Back pressure for Half-Duplex	
Jumbo Frame	9Kbytes	
Reset Button	< 5 sec: System reboot > 10 sec: Factory Default	
ESD Protection	6KV DC	
EFT Protection	6KV DC	
Enclosure	IP30 Aluminum Metal Case	
Installation	DIN Rail Kit and Wall Mount Kit	
Alarm	One relay output for power failure. Alarm Relay current carry ability: 1A @ DC 24V	
LED Indicator	System: Power 1 (Green) Power 2 (Green) Fault Alarm (Green) Ring (Green) R.O. (Green)	Per 10/100/1000T RJ-45 Ports: LNK/ACT (Green) 1000 (Orange) Per SFP Interface: LNK/ACT (Green) 1000 (Orange)
Dimensions (W x D x H)	87.8 x 135 x 56mm	
Weight	720g	
Power Requirements	DC 12 to 48V. AC 24V Power Adapter	
Power Consumption	10 Watts / 34BTU (Full loading)	
Layer 2 function		
Basic Management Interfaces	Web Browser, Remote Telnet, SNMPv1, v2c	
Secure Management Interface	SSH, SSL, SNMP v3	
Port configuration	Port disable/enable Auto-negotiation 10/100/1000Mbps full and half duplex mode selection Flow Control disable / enable Power saving mode control	
Port Status	Display each port's speed duplex mode, link status, Flow control status. Auto negotiation status, trunk status.	
Port Mirroring	TX / RX / Both Many to 1 monitor	
VLAN	802.1Q Tagged Based VLAN ,up to 255 VLAN groups Q-in-Q tunneling Private VLAN Edge (PVE) MAC-based VLAN Protocol-based VLAN Voice VLAN MVR (Multicast VLAN Registration) Up to 255 VLAN groups, out of 4095 VLAN IDs	
Link Aggregation	IEEE 802.3ad LACP / Static Trunk Support 5 groups of 10-Port trunk support	
QoS	Traffic classification based, Strict priority and WRR 8-level priority for switching - Port Number - 802.1p priority	

	- 802.1Q VLAN tag - DSCP/TOS field in IP Packet
IGMP Snooping	IGMP (v1/v2/V3) Snooping, up to 255 multicast Groups IGMP Querier mode support
MLD Snooping	MLD (v1/v2) Snooping, up to 255 multicast Groups MLD Querier mode support
Access Control List	IP-Based ACL / MAC-Based ACL Up to 123 entries
Bandwidth Control	Per port bandwidth control Ingress: 500Kb~80Mbps Egress: 64Kb~80Mbps
SNMP MIBs	RFC-1213 MIB-II IF-MIB RFC-1493 Bridge MIB RFC-1643 Ethernet MIB RFC-2863 Interface MIB RFC-2665 Ether-Like MIB RFC-2819 RMON MIB (Group 1, 2, 3 and 9) RFC-2737 Entity MIB RFC-2618 RADIUS Client MIB RFC-2933 IGMP-STD-MIB RFC3411 SNMP-Frameworks-MIB IEEE 802.1X PAE LLDP MAU-MIB
Standards Conformance	
Regulation Compliance	FCC Part 15 Class A, CE
Stability Testing	IEC60068-2-32 (Free fall) IEC60068-2-27 (Shock) IEC60068-2-6 (Vibration)
Standards Compliance	IEEE 802.3 10Base-T IEEE 802.3u 100Base-TX / 100Base-FX IEEE 802.3z Gigabit SX/LX IEEE 802.3ab Gigabit 1000T IEEE 802.3x Flow Control and Back pressure IEEE 802.3ad Port trunk with LACP IEEE 802.1D Spanning Tree Protocol IEEE 802.1w Rapid Spanning Tree Protocol IEEE 802.1s Multiple Spanning Tree Protocol IEEE 802.1p Class of service IEEE 802.1Q VLAN Tagging IEEE 802.1x Port Authentication Network Control IEEE 802.1ab LLDP RFC 768 UDP RFC 793 TFTP RFC 791 IP RFC 792 ICMP RFC 2068 HTTP RFC 1112 IGMP version 1 RFC 2236 IGMP version 2 RFC 3376 IGMP version 3 RFC 2710 MLD version 1 FRC 3810 MLD version 2
Environment	
Operating	Temperature: -40 ~ 75 degrees C Relative Humidity: 5 ~ 95% (Non-condensing)
Storage	Temperature: -40 ~ 75 degrees C Relative Humidity: 5 ~ 95% (Non-condensing)

2. INSTALLATION

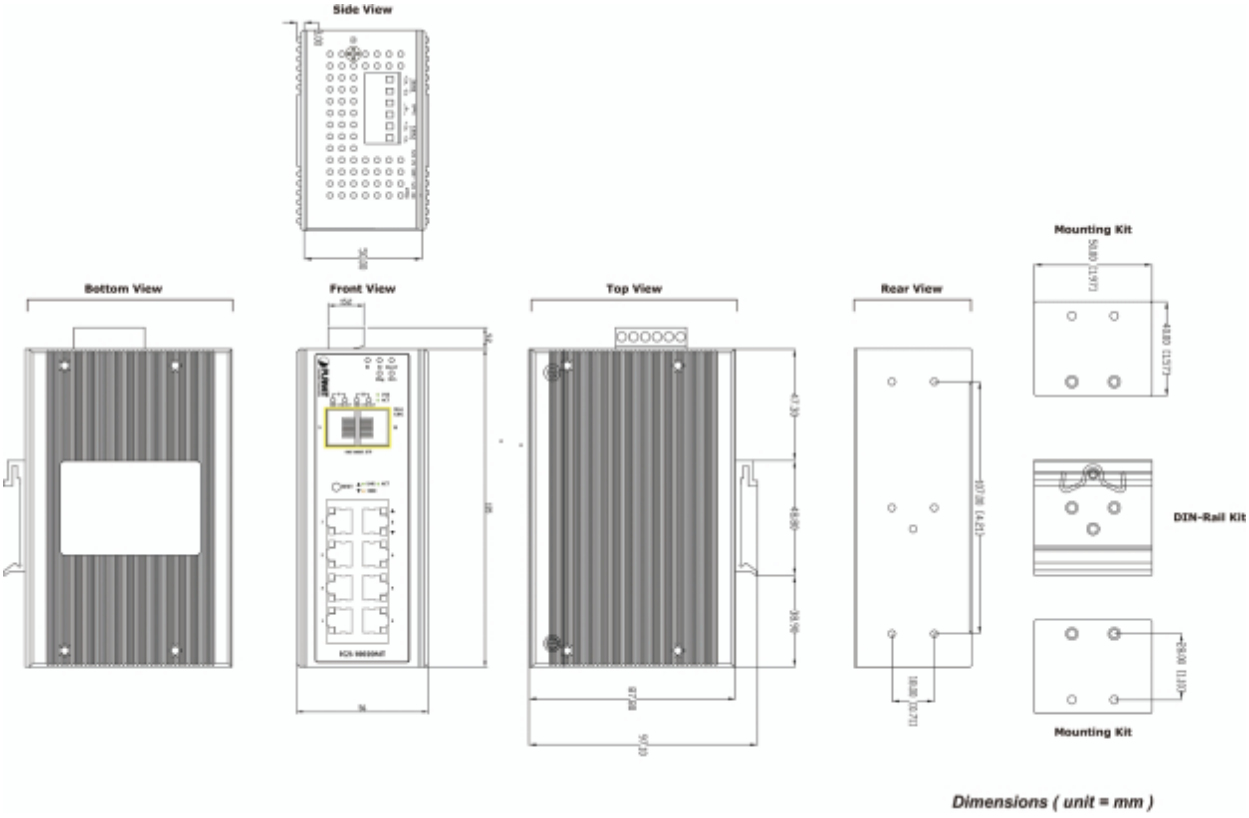
2.1 Hardware Description

The Industrial Managed Switch provides three different running speeds – 10Mbps, 100Mbps and 1000Mbps in the same Switch and automatically distinguishes the speed of incoming connection.

This section describes the hardware features of Industrial Managed Switch. For easier management and control of the Industrial Managed Switch, familiarize yourself with its display indicators, and ports. Front panel illustrations in this chapter display the unit LED indicators. Before connecting any network device to the Industrial Managed Switch, read this chapter carefully.

2.1.1 Physical Dimensions

- Dimensions (W x D x H) : 87.8 x 135 x 56mm



2.1.2 Front Panel

Figure 2-1 shows the front panel of **Industrial Managed Switch**.

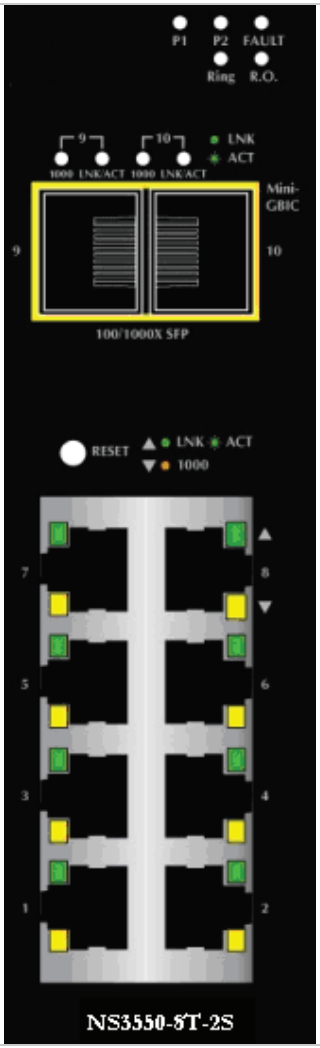


Figure 2-1: NS3550-8T-2S Switch Front Panel

■ **Reset Button**

On the left of the front panel, the reset button is designed for rebooting the **Industrial Managed Switch** without turning off and on the power. It also can reset the **Industrial Managed Switch** to factory default mode.

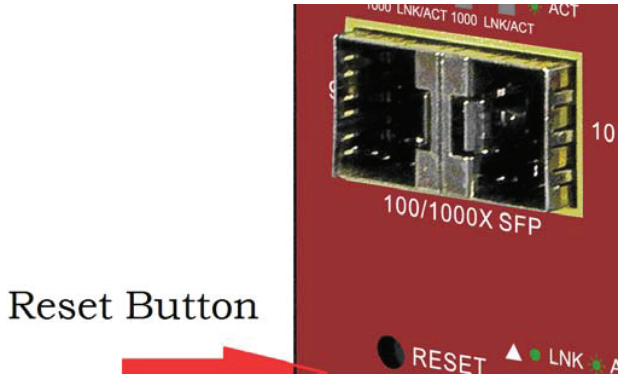


Figure 2-2: Reset Button of **Industrial Managed Switch**

Reset Button Pressed and Released	Function
< 5 sec: System Reboot	Reboot the Industrial Managed Switch
> 10 sec: Factory Default	Reset the Industrial Managed Switch to Factory Default configuration. The Industrial Managed Switch will then reboot and load the default settings as below: ■ Default Username: **admin** ■ Default Password: **admin** ■ Default IP address: **192.168.0.100** ■ Subnet mask: **255.255.255.0** ■ Default Gateway: **192.168.0.254**

2.1.3 LED Indicators

■ **System**

LED	Color	Function
P1	**Green**	Indicates power 1 has power.
P2	**Green**	Indicates power 2 has power.
Fault	**Green**	Indicates either power 1 or power 2 has no power.
Ring	**Green**	**Lights** to indicate that the ERPS Ring has been created successfully.
R.O.*	**Green**	**Lights** to indicate that Switch has enabled Ring Owner.

■ **Per 10/100/1000Base-T Port**

LED	Color	Function	
LNK / ACT	**Green**	**Light**	Indicates the link through that port is successfully established.
		Blink	Indicates that the Switch is actively sending or receiving data over that port.
1000	**Orange**	**Light**	Indicates that the port is successfully connecting to the network at 1000Mbps.
		Off	Indicates that the port is successfully connecting to the network at 10Mbps or 100Mbps.

■ **Per SFP Interface**

LED	Color	Function	
LNK / ACT	Green	Light	Indicates the link through that port is successfully established.
		Blink	Indicates that the Switch is actively sending or receiving data over that port.
1000	Orange	Light	Indicates that the port is successfully connecting to the network at 1000Mbps.
		Off	Indicates that the port is successfully connecting to the network at 100Mbps.

2.1.4 Switch Upper Panel

The Upper Panel of the **Industrial Managed Switch** indicates a DC inlet power socket and consists of one terminal block connector within 6-contacts. It accepts input power from 12 to 48V DC, and also AC 24V.

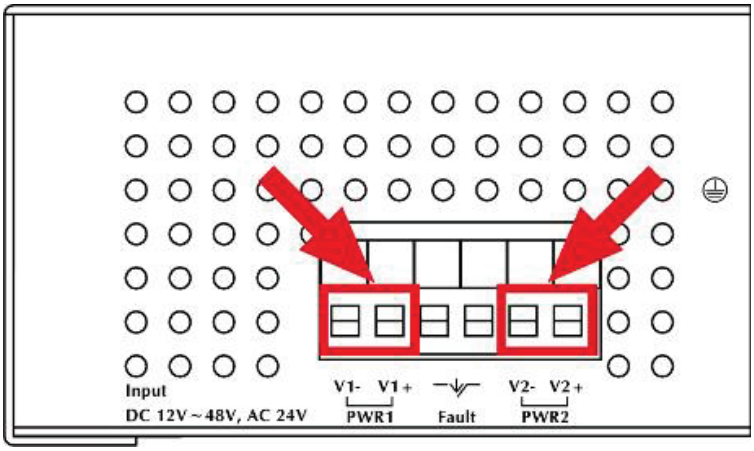


Figure 2-3: NS3550-8T-2S Upper Panel

2.2 Installing Industrial Managed Switch

This section describes how to install your **Industrial Managed Switch** and make connections to the **Industrial Managed Switch**. Please read the following topics and perform the procedures in the order being presented. To install your **Industrial Managed Switch** on a desktop or shelf, simply complete the following steps.

In this paragraph, we will describe how to install the **Industrial Managed Switch** and the installation points attended to it.

2.2.1 Installation Steps

1. **Unpack the Industrial Managed Switch**
2. **Check if the DIN-Rail is screwed on the Industrial Managed Switch or not**. If the DIN-Rail is not screwed on the **Industrial Managed Switch**, please refer to **DIN-Rail Mounting** section for DIN-Rail installation. If users want to wall-mount the **Industrial Managed Switch**, please refer to the **Wall Mount Plate Mounting** section for wall mount plate installation**.**
3. **To hang the Industrial Managed Switch on the DIN-Rail track or wall.**
4. **Power on the Industrial Managed Switch**. Please refer to the **Wiring the Power Inputs** section for knowing the information about how to wire the power. The power LED on the **Industrial Managed Switch** will light up. Please refer to the **LED Indicators** section for indication of LED lights**.**
5. **Prepare the twisted-pair, straight through Category 5 cable for Ethernet connection.**
6. **Insert one side of RJ-45 cable (category 5) into the Industrial Managed Switch Ethernet port** (RJ-45 port) and the other side of RJ-45 cable (category 5) to the network device's Ethernet port (RJ-45 port), e.g. Switch PC or Server. The UTP port (RJ-45) LED on the **Industrial Managed Switch** will light up when the cable is connected with the network device. Please refer to the **LED Indicators** section for LED light indication**.**

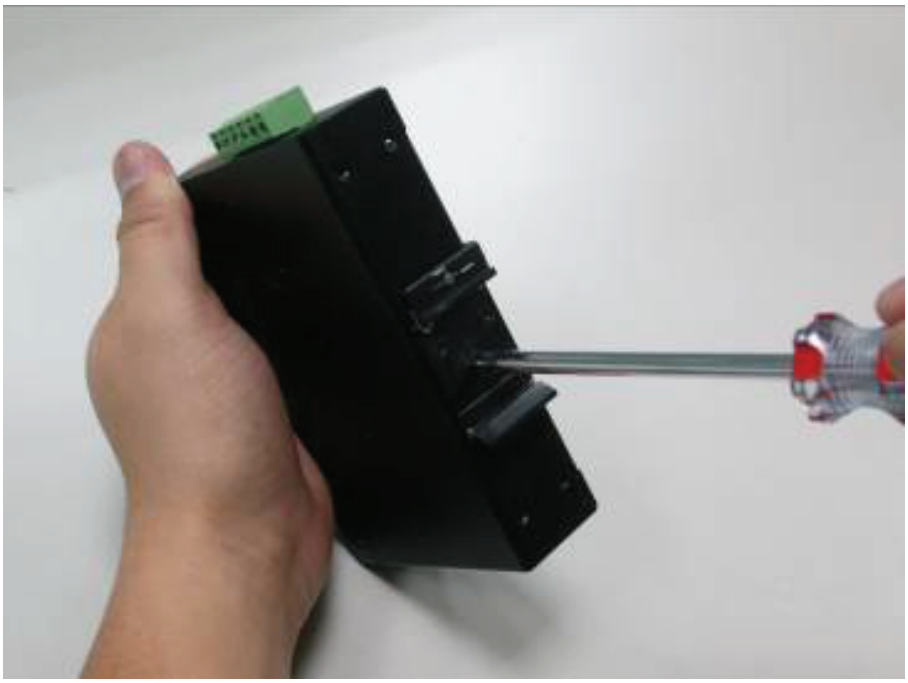
Make sure that the connected network devices support MDI/MDI-X. If it does not support, use the crossover category-5 cable.

7. **When all connections are set and LED lights all show normally, the installation is completed.**

2.2.2 DIN-Rail Mounting

This section describes how to install the **Industrial Managed Switch**.
There are two methods to install the **Industrial Managed Switch**. DIN-Rail Mounting and Wall Mount Plate Mounting. Please read the following topics and perform the procedures in the order being presented.

Step 1: Screw the DIN-Rail on the **Industrial Managed Switch**.



Step 2: Lightly press the bottom of DIN-Rail into the track.

Step 3: Check the DIN-Rail is tightly on the track.

Please refer to following procedures to remove the **Industrial Managed Switch** from the track.

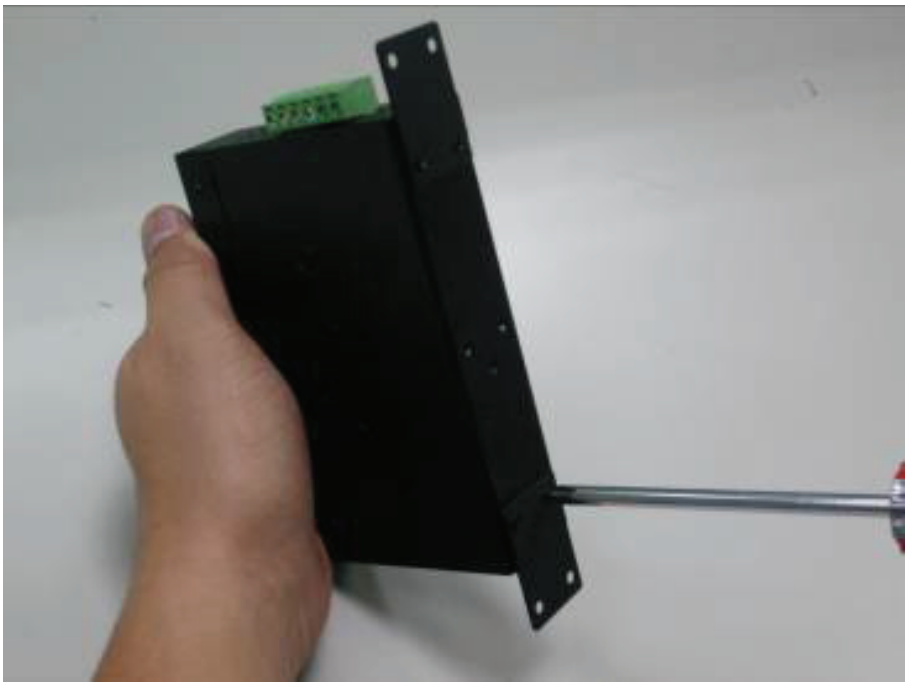
Step 4: Lightly press the bottom of DIN-Rail to remove it from the track.

2.2.3 Wall Mount Plate Mounting

To install the **Industrial Managed Switch** on the wall. Please follow the instructions below.

Step 1: Remove the DIN-Rail from the **Industrial Managed Switch**. Use the screwdriver to loosen the screws and remove the DIN-Rail.

Step 2: Place the wall mount plate on the rear panel of the **Industrial Managed Switch**.



Step 3: Use the screwdriver to screw the wall mount plate on the **Industrial Managed Switch**.

Step 4: Use the hook holes at the corners of the wall mount plate to hang the **Industrial Managed Switch** on the wall.

Step 5: To remove the wall mount plate, reverse the steps above.

2.3 Wiring the Power Inputs

The 6-contacts terminal block connector on the top panel of **Industrial Managed Switch** is used for two DC redundant power inputs. Please follow the steps to insert the power wire. The PWR1 is 1(-) & 2(+) and PWR2 is 5(-) & 6(+) contact.

Remember: Tighten the wire-clamp screws for preventing the wires from loosening..

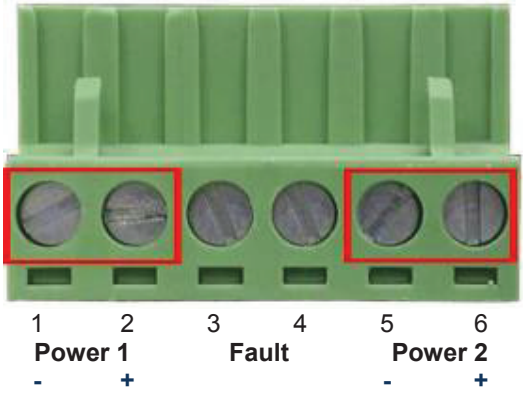


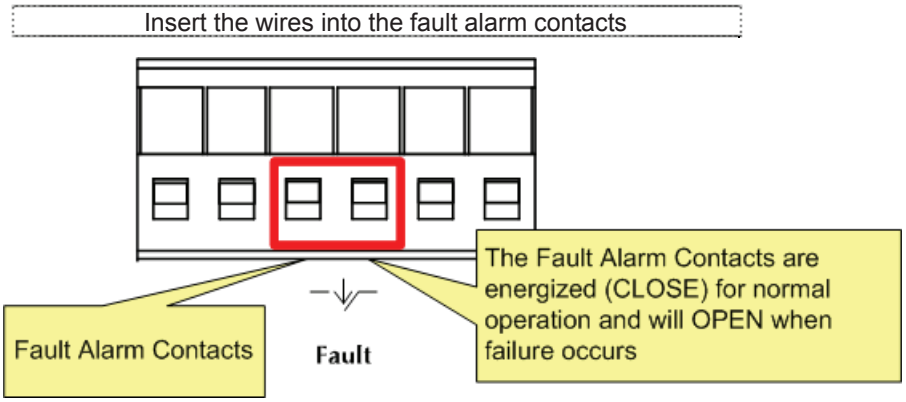
Figure 2-4: 6-Contacts of Terminal Block Connector

Note

1. The wire gauge for the terminal block should be in the range of 12 ~ 24 AWG.
2. Follow any of the procedures like inserting the wires or tighten the wire-clamp screws. Ensure the power is OFF to prevent from getting an electric shock.

2.4 Wiring the Fault Alarm Contact

The fault alarm contacts are in the middle (3 & 4) of the terminal block connector as the picture shows below. Inserting the wires, the **Industrial Managed Switch** will detect the fault status of the power failure, or port link failure (available for managed model). The following illustration shows an application example for wiring the fault alarm contacts



Note

1. The wire gauge for the terminal block should be in the range of 12 ~ 24 AWG.
2. Follow any of the procedures like inserting the wires or tighten the wire-clamp screws. Ensure the power is OFF to prevent to get an electric shock.

2.5 Cabling

- **10/100/1000Base-T and 100Base-FX / 1000Base-SX/LX**

All 10/100/1000Base-T ports come with Auto-Negotiation capability. They automatically support 1000Base-T, 100Base-TX and 10Base-T networks. Users only need to plug a working network device into one of the 10/100/1000Base-T ports, and then turn on the **Industrial Managed Switch**. The port will automatically runs in 10Mbps, 20Mbps, 100Mbps or 200Mbps and 1000Mbps or 2000Mbps after the negotiation with the connected device.

The **Industrial Managed Switch** has two SFP interfaces that support 100/1000 dual speed mode (Optional Multi-mode / Single-mode 100Base-FX / 1000Base-SX/LX SFP module)

- **Cabling**

Each 10/100/1000Base-T port uses RJ-45 sockets -- similar to phone jacks -- for connection of unshielded twisted-pair cable (UTP). The IEEE 802.3 / 802.3u 802.3ab Fast / Gigabit Ethernet standard requires Category 5 UTP for 100Mbps 100Base-TX. 10Base-T networks can use Cat.3, 4, 5 or 1000Base-T use 5/5e/6 UTP (see table below). Maximum distance is 100meters (328 feet). The 100Base-FX / 1000Base-SX/LX SFP slot is used as LC connector with optional SFP module. Please see table below and know more about the cable specifications.

Port Type	Cable Type	Connector
10Base-T	Cat 3, 4, 5, 2-pair	RJ-45
100Base-TX	Cat.5 UTP, 2-pair	RJ-45
1000Base-T	Cat.5/5e/6 UTP, 2-pair	RJ-45
100Base-FX	50 / 125μm or 62.5 / 125μm multi-mode 9 / 125μm single-mode	LC (Multi / Single mode)
1000Base-SX/LX	50 / 125μm or 62.5 / 125μm multi-mode 9 / 125μm single-mode	LC (Multi / Single mode)

Any Ethernet devices like hubs/ PCs can connect to the **Industrial Managed Switch** by using straight-through wires. The eight-10/100/1000Mbps ports are auto-MDI/MDI-X and can be used on straight-through or crossover cable.

2.5.1 Installing the SFP Transceiver

The sections describe how to insert an SFP transceiver into an SFP slot.
The SFP transceivers are hot-pluggable and hot-swappable. You can plug-in and out the transceiver to/from any SFP port without having to power down the **Industrial Managed Switch** as the Figure 2-5 shows.

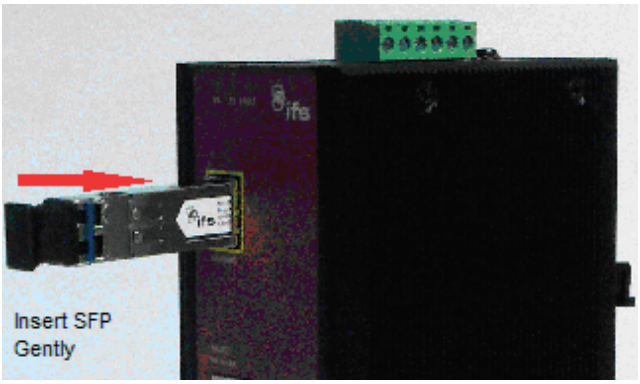


Figure 2-5: Plug-in the SFP Transceiver

- **Approved IFS SFP Transceivers**

  IFS **Industrial Managed Switch** supports 100/1000 dual mode with both Single mode and Multi-mode SFP transceiver.
  The following list of approved IFS SFP transceivers is correct at the time of publication:

Gigabit SFP Transceiver Modules

S30-1SLC/A-10	SFP, LC Connector, Single Mode, Gigabit, 1 fiber, 1310nm/1550nm, 10km , A End
S30-1SLC/A-20	SFP, LC Connector, Single Mode, Gigabit, 1 fiber, 1310nm/1550nm, 20km, A End
S30-1SLC/A-60	SFP, LC Connector, Single Mode, Gigabit, 1 fiber, 1310nm/1550nm, 60km, A End
S30-1SLC/B-10	SFP, LC Connector, Single Mode, Gigabit, 1 fiber, 1550nm/1310nm, 10km , B End
S30-1SLC/B-20	SFP, LC Connector, Single Mode, Gigabit, 1 fiber, 1550nm/1310nm, 20km, B End
S30-1SLC/B-60	SFP, LC Connector, Single Mode, Gigabit, 1 fiber, 1550nm/1310nm, 60km, B End
S30-2MLC	SFP, LC Connector, Multi-Mode, Gigabit, 2 fiber,850nm/850nm, 550m
S30-2MLC-2	SFP, LC Connector, Multi-Mode, Gigabit, 2 fiber,1310nm/1310nm, 2km
S30-2SLC-10	SFP, LC Connector, Single Mode, Gigabit, 2 fiber,1310nm/1310nm, 10km
S30-2SLC-30	SFP, LC Connector, Single Mode, Gigabit, 2 fiber,1310nm/1310nm, 30km
S30-2SLC-70	SFP, LC Connector, Single Mode, Gigabit, 2 fiber,1550nm/1550nm, 70km
S30-RJ	SFP, RJ-45, Gigabit, 100m
S35-2MLC	SFP, LC Connector, Multi-Mode, Gigabit, 2 fiber,850nm/850nm, 550m, Hardened -40~75°C
S35-2SLC-10	SFP, LC Connector, Single Mode, Gigabit, 2 fiber,1310nm/1310nm, 10km, Hardened -40~75°C
S35-2SLC-30	SFP, LC Connector, Single Mode, Gigabit, 2 fiber,1310nm/1310nm, 30km, Hardened -40~75°C
S35-2SLC-70	SFP, LC Connector, Single Mode, Gigabit, 2 fiber,1550nm/1550nm, 70km, Hardened -40~75°C

Fast Ethernet SFP Transceiver Modules

S20-1SLC/A-20	SFP, LC Connector, Single Mode, 10/100 Fast Ethernet, 1 fiber, 1310nm/1550nm, 20km , A End
S20-1SLC/B-20	SFP, LC Connector, Single Mode, 10/100 Fast Ethernet, 1 fiber, 1310nm/1550nm, 20km , B End
S20-2MLC-2	SFP, LC Connector, Multi Mode, 10/100 Fast Ethernet, 2 fiber,1310nm/1310nm, 2km
S20-2SLC-20	SFP, LC Connector, Single Mode, 10/100 Fast Ethernet, 2 fiber,1310nm/1310nm, 20km

S25-2MLC-2	SFP, LC Connector, Multi Mode, 10/100 Fast Ethernet, 2 fiber,1310nm/1310nm, 2km, Hardened -40~75°C
S25-2SLC-20	SFP, LC Connector, Single Mode, 10/100 Fast Ethernet, 2 fiber,1310nm/1310nm, 20km, Hardened -40~75°C

It is recommended to use IFS SFPs on the **Industrial Managed Switch**. If you insert an SFP transceiver that is not supported, the **Industrial Managed Switch** will not recognize it.

1000Base-SX/LX:

Before connecting the other switches, workstation or media converter,

1. Make sure both sides of the SFP transceiver are with the same media type; for example, 1000Base-SX to 1000Base-SX, 1000Bas-LX to 1000Base-LX.
2. Check the fiber-optic cable type that matches the SFP transceiver model.
   - To connect to 1000Base-SX SFP transceiver, use the Multi-mode fiber cable with one side being male duplex LC connector type.
   - To connect to 1000Base-LX SFP transceiver, use the Single-mode fiber cable with one side being male duplex LC connector type.

Connecting the fiber cable

1. Attach the duplex LC connector to the network cable and put into the SFP transceiver.
2. Connect the other end of the cable to a device – switches with SFP installed, fiber NIC to a workstation or a media converter.
3. Check the LNK/ACT LED of the SFP slot on the front of the **Industrial Managed Switch**. Make sure that the SFP transceiver is operating correctly.

100Base-FX:

Before connecting the other switches, workstation or media converter,

1. Make sure both sides of the SFP transceiver are with the same media type or WDM pair, for example: 100Base-FX to 100Base-FX, 100Base-BX20-U to 100Base-BX20-D.
2. Check the fiber-optic cable type that matches the SFP transceiver model.
   - To connect to 1000Base-SX SFP transceiver, use the Multi-mode fiber cable with one side being male duplex LC connector type.
   - To connect to 1000Base-LX SFP transceiver, use the Single-mode fiber cable with one side being male duplex LC connector type.

Connecting the fiber cable

1 Attach the duplex LC connector to the network cable and put into the SFP transceiver.
2 Connect the other end of the cable to a device – switches with SFP installed, fiber NIC to a workstation or a media converter.
3. Check the LNK/ACT LED of the SFP slot on the front of the **Industrial Managed Switch**. Make sure that the SFP transceiver is operating correctly.
4. Check the Link mode of the SFP port if the link failed. Co works with some fiber-NICs or Media Converters, set the Link mode to "**100 Force**" is needed.

2.5.2 Removing the Module

1. Make sure there is no network activity by consulting or checking with the network administrator. Or through the management interface of the switch/converter (if available) to disable the port in advance.
2. Remove the Fiber Optic Cable gently.
3. Turn the handle of the MGB / MFB module to horizontal.
4. Pull out the module gently through the lever..

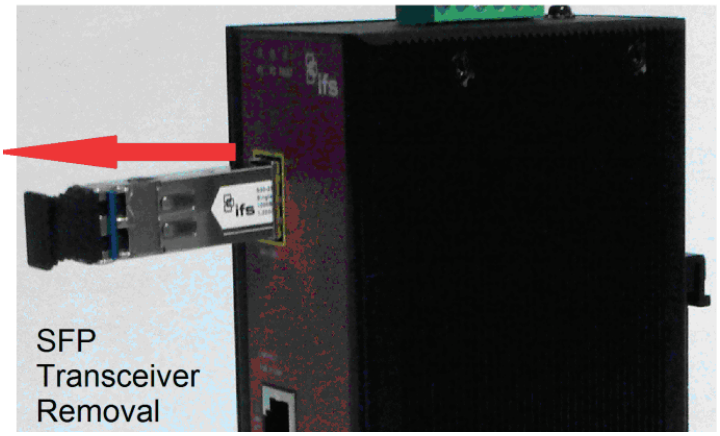


Figure 2-6: Pull Out the SFP Transceiver Module

Note

Never pull out the module without pulling the lever or the push bolts on the module. Directly pulling out the module with forcecould damage the module and SFP module slot of the device.

3. SWITCH MANAGEMENT

This chapter explains the methods that you can use to configure management access to the **Industrial Managed Switch**. It describes the types of management applications and the communication and management protocols that deliver data between your management device (workstation or personal computer) and the system. It also contains information about port connection options.

This chapter covers the following topics:

- Requirements
- Management Access Overview
- Remote Telnet Access
- Web Management Access
- SNMP Access
- Standards, Protocols, and Related Reading

3.1 Requirements

- Workstations running Windows XP/2003, Vista, Windows 7, MAC OS X, Linux, Fedora, Ubuntu or other platforms compatible with **TCP/IP** protocols.
- **Workstation** is installed with **Ethernet NIC** (Network Interface Card)
- Ethernet Port connection
  - Network cables - Use standard network (UTP) cables with RJ45 connectors.
  - The above workstation is installed with **WEB Browser** and **JAVA runtime environment** Plug-in

It is recommended to use Internet Explore 7.0 or above to access **Industrial Managed Switch**.

3.2 Management Access Overview

The **Industrial Managed Switch** gives you the flexibility to access and manage it using any or all of the following methods:

- Remote Telnet Interface
- **Web browser** Interface
- An external **SNMP-based network management application**

The Remote Telnet and Web browser interface support is embedded in the **Industrial Managed Switch** software and is available for immediate use. Each of these management methods has their own advantages. Table 3-1 compares the three management methods.

Method	Advantages	Disadvantages
Remote Telnet	• Text-based • Telnet functionality built into Windows XP/2003, Vista, Windows 7 operating systems • Can be accessed from any location	• Security can be compromised (hackers need only know the IP address)
Web Browser	• Ideal for configuring the switch remotely • Compatible with all popular browsers • Can be accessed from any location • Most visually appealing	• Security can be compromised (hackers need only know the IP address and subnet mask) • May encounter lag times on poor connections
SNMP Agent	• Communicates with switch functions at the MIB level • Based on open standards	• Requires SNMP manager software • Least visually appealing of all three methods • Some settings require calculations • Security can be compromised (hackers need only know the community name)

Table 3-1: Management Methods Comparison

3.3 Remote Telnet

The Remote Telnet is an IP-based command line user interface for performing system administration such as displaying statistics or changing option settings. Using this method, you can access the **Industrial Managed Switch** remote telnet interface from personal computer, or workstation in the same Ethernet environment as long as you know the current IP address of the **Industrial Managed Switch**.

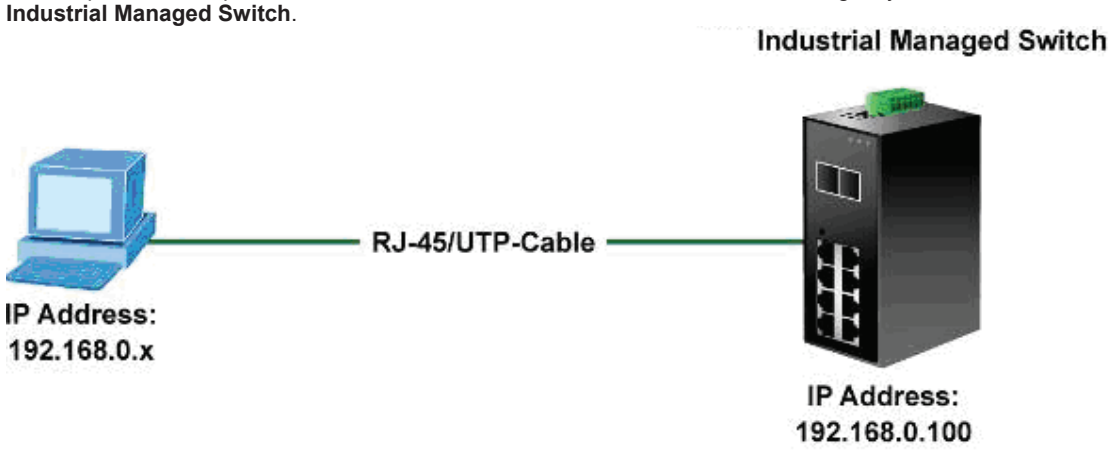


Figure 3-1: Remote Telnet Interface Management

In Windows system, you may click **"Start"** and then choose **"Acessories"**and **"Command Prompt"**. Please input **"telnet 192.168.0.100"** and press **"enter'** from your keyboard. You will see the following screen appear:

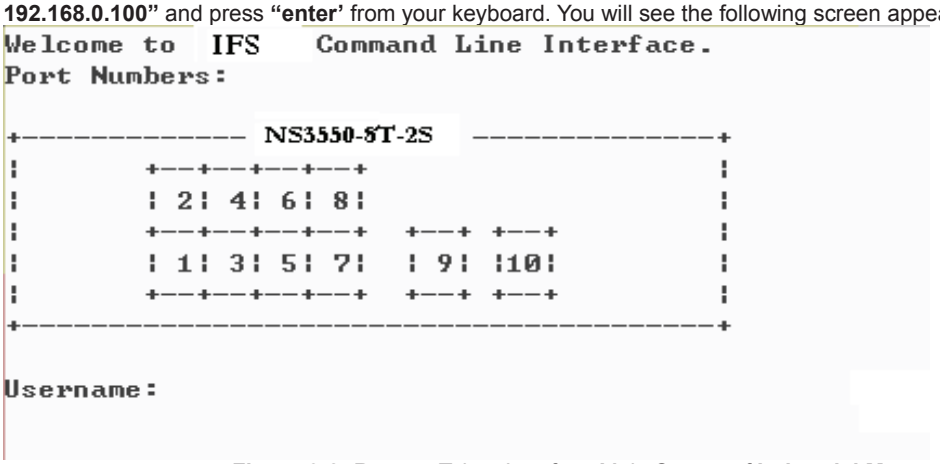


Figure 3-2: Remote Telnet Interface Main Screen of **Industrial Managed Switch**

For more information about using the Remote Telnet interface, refer to **Chapter 5 Remote Telnet Interface Management**.

3.4 Web Management

The **Industrial Managed Switch** offers management features that allow users to manage the **Industrial Managed Switch** from anywhere on the network through a standard browser such as Microsoft Internet Explorer. After you set up your IP address for the **Industrial Managed Switch**, you can access the **Industrial Managed Switch**'s Web interface applications directly in your Web browser by entering the IP address of the **Industrial Managed Switch**.

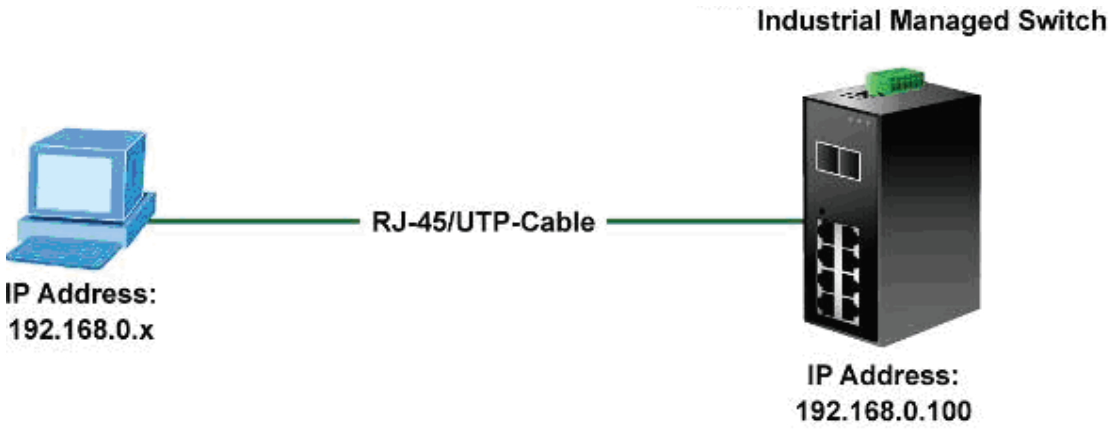


Figure 3-3: Web Management

You can then use your Web browser to list and manage the **Industrial Managed Switch** configuration parameters from one central location; the Web Management requires either **Microsoft Internet Explorer 7.0** or later, **Safari** or **Mozilla Firefox 1.5** or later.

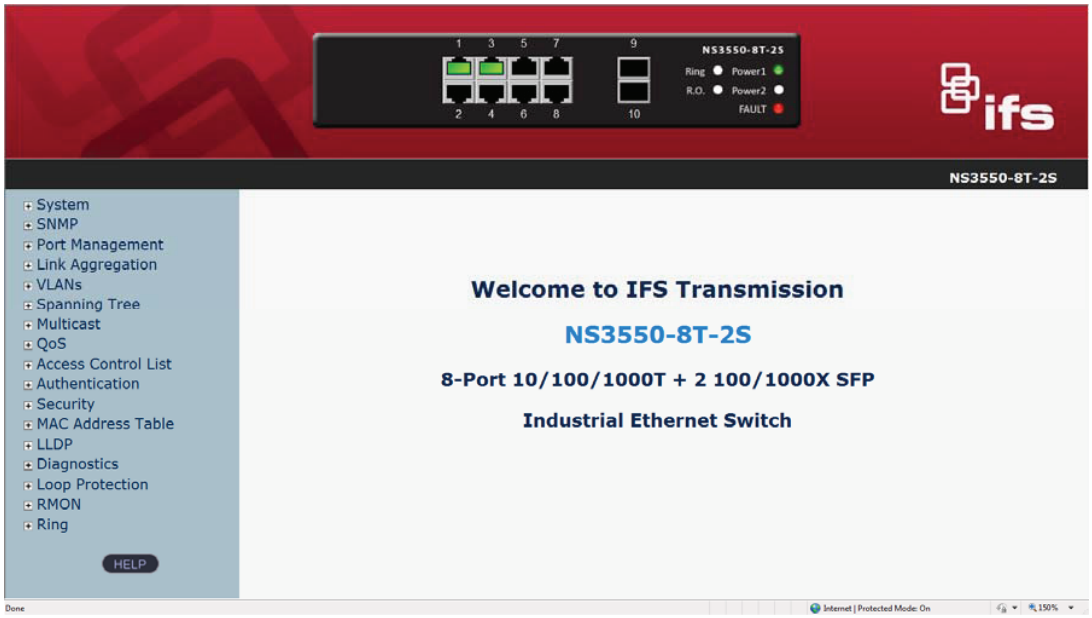


Figure 3-4: Web Main Screen of **Industrial Managed Switch**

3.5 SNMP-Based Network Management

You can use an external SNMP-based application to configure and manage the **Industrial Managed Switch**, such as SNMP Network Manager, HP Openview Network Node Management (NNM) or What's Up Gold. This management method requires the SNMP agent on the **Industrial Managed Switch** and the SNMP Network Management Station to use the **same community string**. This management method, in fact, uses two community strings: the **get community** string and the **set community** string. If the SNMP Net-work management Station only knows the set community string, it can read and write to the MIBs. However, if it only knows the get community string, it can only read MIBs. The default gets and sets community strings for the **Industrial Managed Switch** are public.

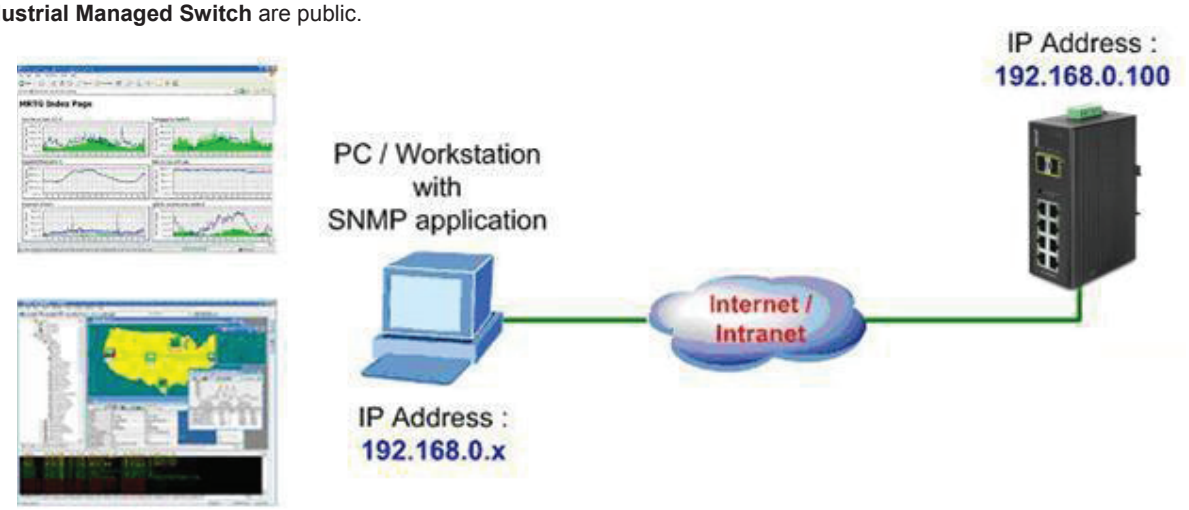


Figure 3-5: SNMP Management

4. WEB CONFIGURATION

This section introduces the configuration and functions of the Web-based management.

About Web-based Management

The Industrial Managed Switch offers management features that allow users to manage the Industrial Managed Switch from anywhere on the network through a standard browser such as Microsoft Internet Explorer.

The Web-based Management supports Internet Explorer 7.0. It is based on Java Applets with an aim to reduce network bandwidth consumption, enhance access speed and present an easy viewing screen.

By default, IE7.0 or later version does not allow Java Applets to open sockets. The user has to explicitly modify the browser setting to enable Java Applets to use network ports.

The Industrial Managed Switch can be configured through an Ethernet connection, making sure the manager PC must be set on the same the IP subnet address as the Industrial Managed Switch.

For example, the default IP address of the Industrial Managed Switch is ***192.168.0.100***, then the manager PC should be set at **192.168.0.x** (where x is a number between 1 and 254, except 100), and the default subnet mask is 255.255.255.0.

If you have changed the default IP address of the Industrial Managed Switch to 192.168.1.1 with subnet mask 255.255.255.0 via console, then the manager PC should be set at 192.168.1.x (where x is a number between 2 and 254) to do the relative configuration on manager PC.

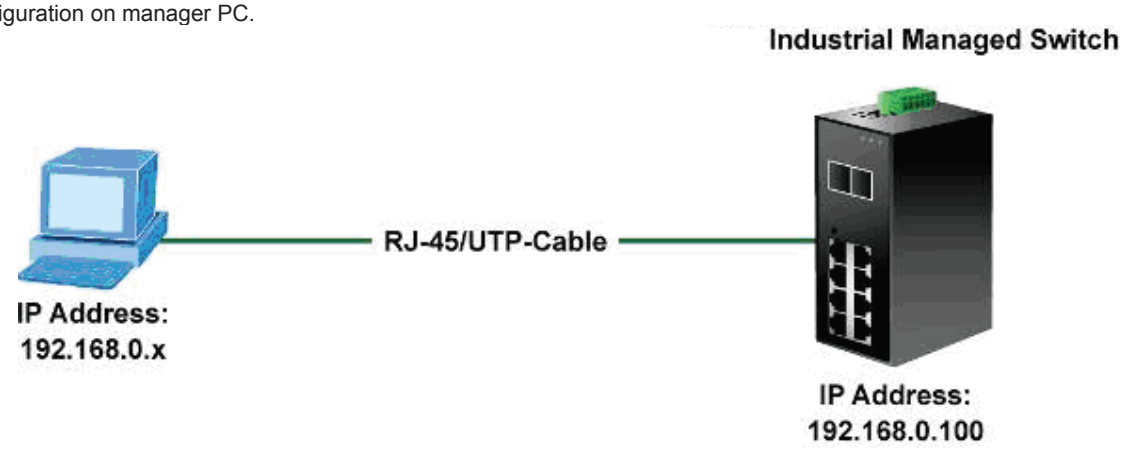


Figure 4-1-1: Web Management

■ **Logging on the Industrial Managed Switch**

1. Use Internet Explorer 7.0 or above Web browser and enter the factory-default IP address to access the Web interface. The factory-default IP Address is as follows:

http://192.168.0.100

2. When the following login screen appears, please enter the default username **"admin"** with password "**admin**" (or the username/password you have changed via console) to login the main screen of Industrial Managed Switch. The login screen in Figure 4-1-2 appears.

Figure 4-1-2: Login Screen

Default User name: **admin**
Default Password: **admin**

After entering the username and password, the main screen appears as Figure 4-1-3.

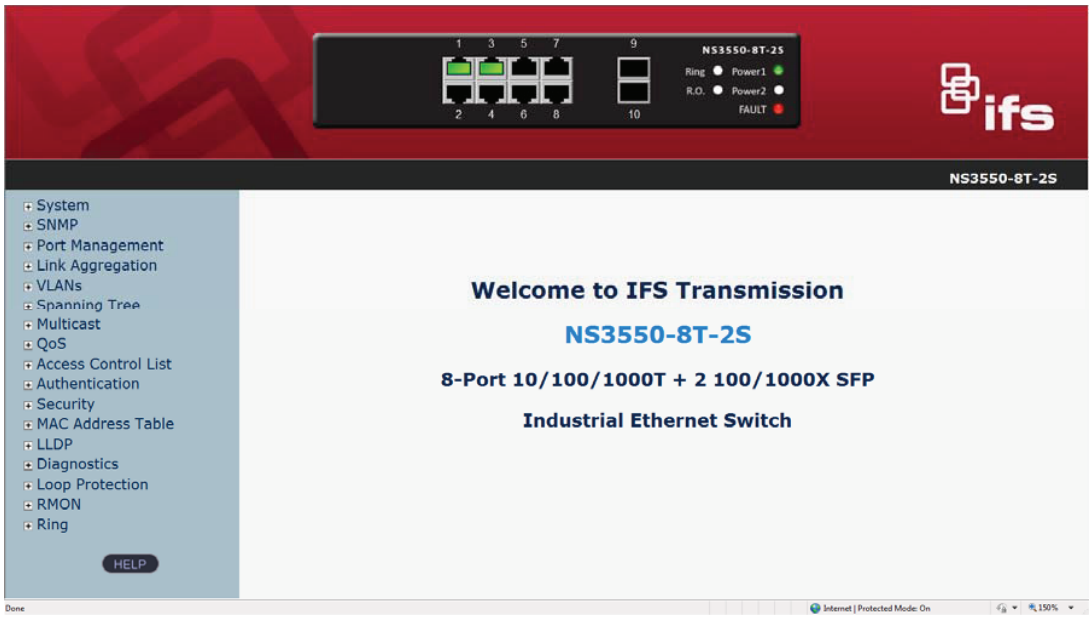


Figure 4-1-3: Default Main Page

Now, you can use the Web management interface to continue the switch management or manage the Industrial Managed Switch by Web interface. The Switch Menu on the left of the web page let you access all the commands and statistics the Managed Switch provides.

1. It is recommended to use Internet Explore 7.0 or above to access Industrial Managed Switch.
2. The changed IP address take effect immediately after clicking on the **Save** button. You need to use the new IP address to access the Web interface.
3. For security reason, please change and memorize the new password after this first setup.
4. Only accept command in lowercase letter under web interface.

4.1 Main Web Page

The Industrial Managed Switch provides a Web-based browser interface for configuring and managing it. This interface allows you to access the Industrial Managed Switch using the Web browser of your choice. This chapter describes how to use the Industrial Managed Switch's Web browser interface to configure and manage it.

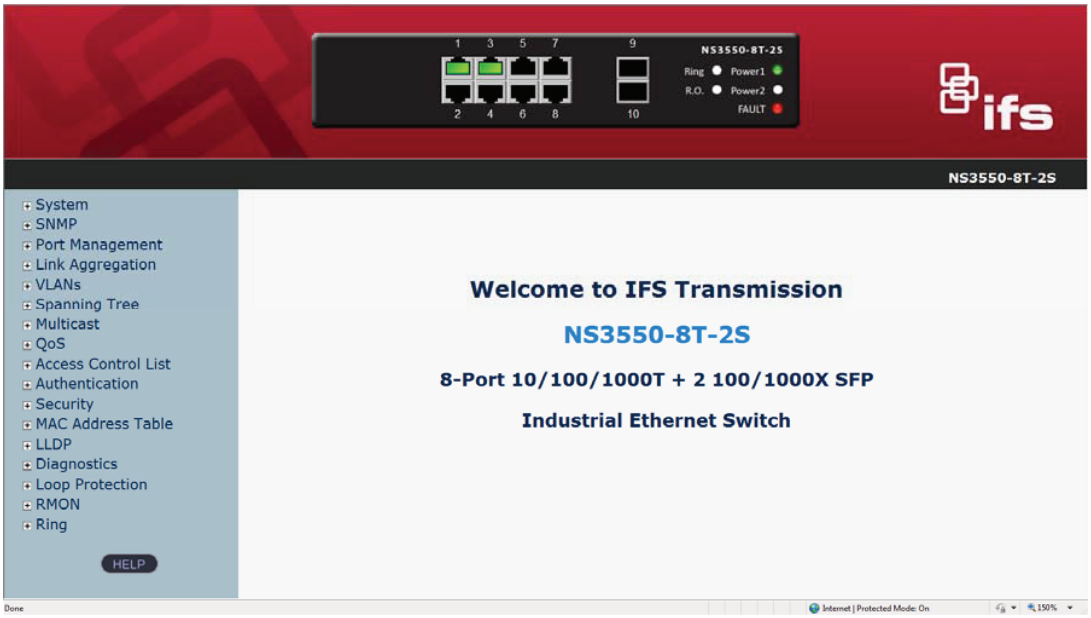


Figure 4-1-4: Main Page

Panel Display
The web agent displays an image of the Industrial Managed Switch's ports. The Mode can be set to display different information for the ports, including Link up or Link down. Clicking on the image of a port opens the **Port Statistics** page.
The port status is illustrated as follows:

State	Disabled	Down	Link
RJ-45 Ports			
SFP Ports			

Main Menu

Using the onboard web agent, you can define system parameters, manage and control the Industrial Managed Switch, and all its ports, or monitor network conditions. Via the Web-Management, the administrator can set up the Industrial Managed Switch by selecting the functions those listed in the Main Function. The screen in Figure 4-1-5 appears.

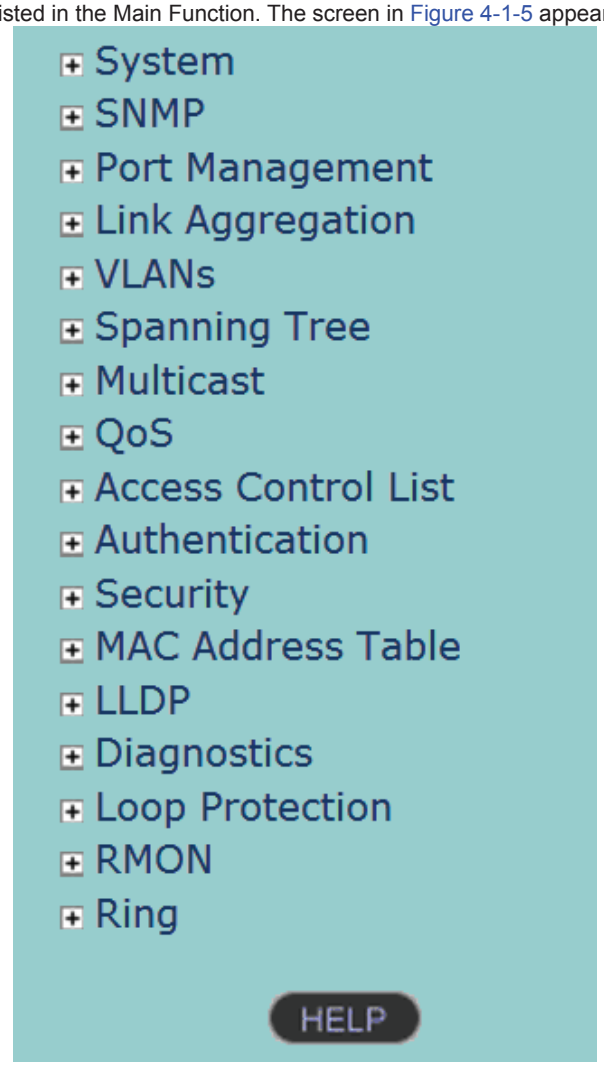


Figure 4-1-5: Industrial Managed Switch Main Functions Menu

4.2 System

Use the System menu items to display and configure basic administrative details of the Industrial Managed Switch. Underr the System, the following topics are provided to configure and view the system information: This section has the following items:

System Information	The switch system information is provided here.
IP Configuration	Configure the switch-managed IP information on this page.
IPv6 Configuration	Configure the switch-managed IPv6 information on this page.
Users Configuration	This page provides an overview of the current users. Currently the only way to login as another user on the web server is to close and reopen the browser.
Privilege Levels	This page provides an overview of the privilege levels.
NTP Configuration	Configure NTP on this page.
UPnP	Configure UPnP on this page.
DHCP Relay	Configure DHCP Relay on this page.
DHCP Relay Statistics	This page provides statistics for DHCP relay.
CPU Load	This page displays the CPU load, using a SVG graph.
System Log	The switch system log information is provided here.
Detailed Log	The switch system detailed log information is provided here.
Remote Syslog	Configure remote syslog on this page.
SMTP Configuration	Configure SMTP function on this page.
EEE Power Reduction	Configuration energy efficient ethernet power reduction on this page
Thermal Protection	Configure thermal protection on this page.
Web Firmware Upgrade	This page facilitates an update of the firmware controlling the switch.
TFTP Firmware Upgrade	Upgrade the firmware via TFTP server
Configuration Backup	You can save the switch configuration. The configuration file is in XML format with a hierarchy of tags.
Configuration Upload	You can load the switch configuration. The configuration file is in XML format with a hierarchy of tags.
Image Select	Configuration active or alternate firmware on this page.
Factory Default	You can reset the configuration of the switch on this page. Only the IP configuration is retained.
System Reboot	You can restart the switch on this page. After restart, the switch will boot normally.

4.2.1 System Information

The System Info page provides information for the current device information. System Info page helps a switch administrator to identify the hardware MAC address, software version and system uptime. The screen in Figure 4-2-1 appears.

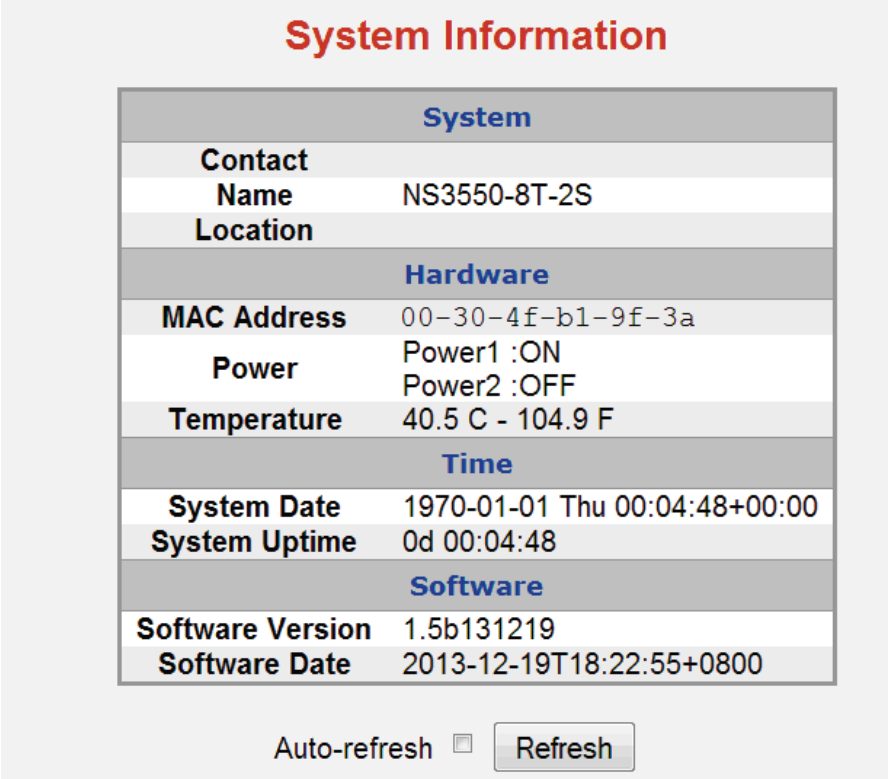


Figure 4-2-1: System Information Page Screenshot

The page includes the following fields:

Object	Description
• **Contact**	The system contact is configured in Configuration | System | Information | System Contact.
• **Name**	The system name is configured in Configuration | System | Information | System Name.
• **Location**	The system location is configured in Configuration | System | Information | System Location.
• **MAC Address**	The MAC Address of this Industrial Managed Switch.
• **Power**	The Power 1 and Power 2 ON/OFF Status display.
• **Temperature**	The Temperature shows the current temperature status of the switch
• **System Date**	The current (GMT) system time and date. The system time is obtained through the configured SNTP Server, if any.
• **System Uptime**	The period of time the device has been operational.
• **Software Version**	The software version of the Industrial Managed Switch.
• **Software Date**	The date when the switch software was produced.

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

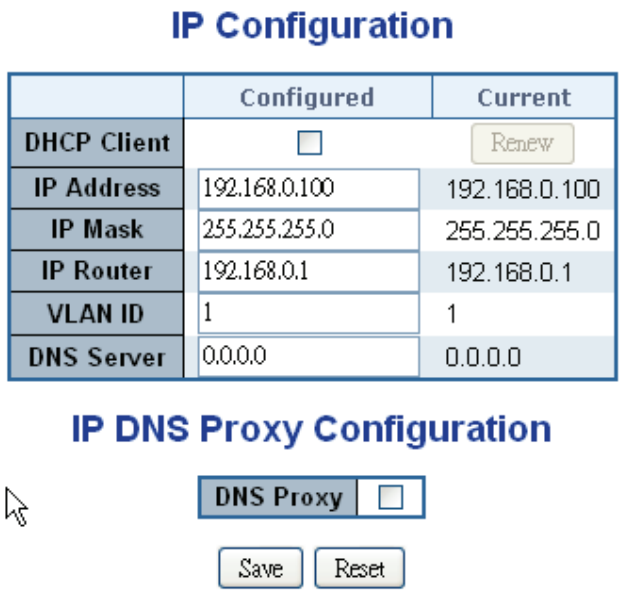


Figure 4-2-2: IP Configuration Page Screenshot

The current column is used to show the active IP configuration.

Object	Description
• **DHCP Client**	Enable the DHCP client by checking this box. If DHCP fails and the configured IP address is zero, DHCP will retry. If DHCP server does not respond around 35 seconds and the configured IP address is non-zero, DHCP will stop and the configured IP settings will be used. The DHCP client will announce the configured System Name as host name to provide DNS lookup.
• **IP Address**	Provide the IP address of this switch in dotted decimal notation.
• **IP Mask**	Provide the IP mask of this switch dotted decimal notation.
• **IP Router**	Provide the IP address of the router in dotted decimal notation.
• **VLAN ID**	Provide the managed VLAN ID. The allowed range is `1` through `4095`.
• **DNS Server**	Provide the IP address of the DNS Server in dotted decimal notation.
• **DNS Proxy**	When DNS proxy is enabled, DUT will relay DNS requests to the current configured DNS server on DUT, and reply as a DNS resolver to the client device on the network.

Buttons

[redacted]: Click to save changes.

[redacted]: Click to undo any changes made locally and revert to previously saved values.

[redacted]: Click to renew DHCP Client. This button is only available if DHCP Client is enabled.

4.2.3 IPv6 Configuration

Configure the switch-managed IPv6 information on this page.
The Configured column is used to view or change the IPv6 configuration. The Current column is used to show the active IPv6 configuration. The screen in Figure 4-2-3 appears.

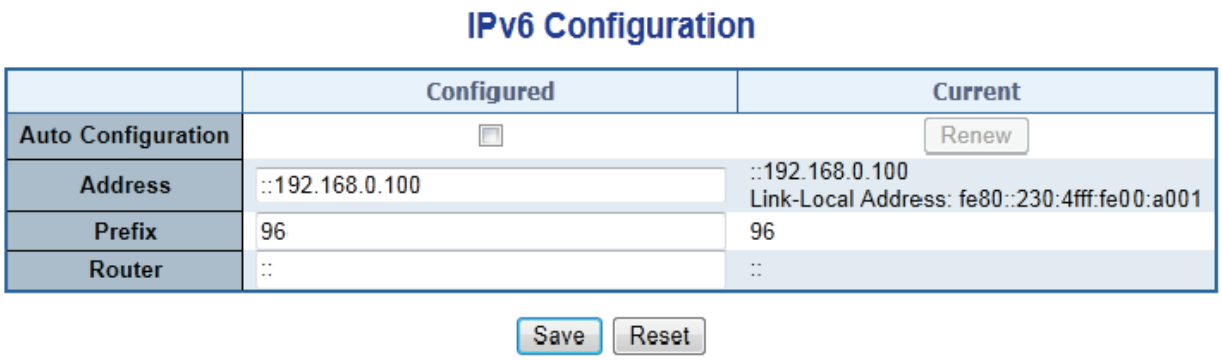


Figure 4-2-3: IPv6 Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Auto Configuration**	Enable IPv6 auto-configuration by checking this box. If system cannot obtain the stateless address in time, the configured IPv6 settings will be used. The router may delay responding to a router solicitation for a few seconds. The total time needed to complete auto-configuration can be significantly longer.
• **Address**	Provide the IPv6 address of this switch. IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can appear only once. It can also represent a legally valid IPv4 address. For example, '::192.1.2.34'.
• **Prefix**	Provide the IPv6 Prefix of this switch. The allowed range is `1` to `128`.
• **Router**	Provide the IPv6 gateway address of this switch. IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can appear only once. It can also represent a legally valid IPv4 address. . For example, '::192.1.2.34'.

Buttons

[redacted]: Click to save changes.

[redacted]: Click to undo any changes made locally and revert to previously saved values.

[redacted]: Click to renew IPv6 Auto Configuration. This button is only available if IPv6 Auto Configuration is enabled.

4.2.4 Users Configuration

This page provides an overview of the current users. Currently the only way to login as another user on the web server is to close and reopen the browser. After setup is completed, please press **"Save"** button to take effect. Please login web interface with new user name and password, the screen in Figure 4-2-4 appears.

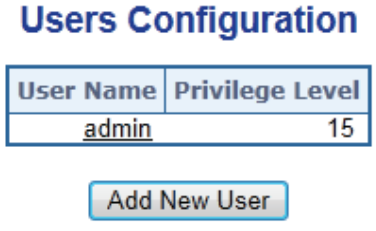


Figure 4-2-4: Users Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **User Name**	The name identifies the user.
• **Privilege Level**	The privilege level of the user. The allowed range is 1 to 15. If the privilege level value is 15, it can access all groups, i.e. granted the full control of the device. But others value need to refer to each group privilege level. User's privilege should be the same or greater than the group privilege level to have the access to that group. By default setting, almost group privilege level 5 has the read-only access and privilege level 10 has the read-write access. And the system maintenance (software upload, factory defaults, etc.) needs user privilege level 15. Generally, the privilege level 15 can be used for an administrator account, privilege level 10 for a standard user account and privilege level 5 for a guest account.

Buttons

[redacted]: Click to add a new user.

Add / Edit User

This page configures a user – add, edit or delete user.

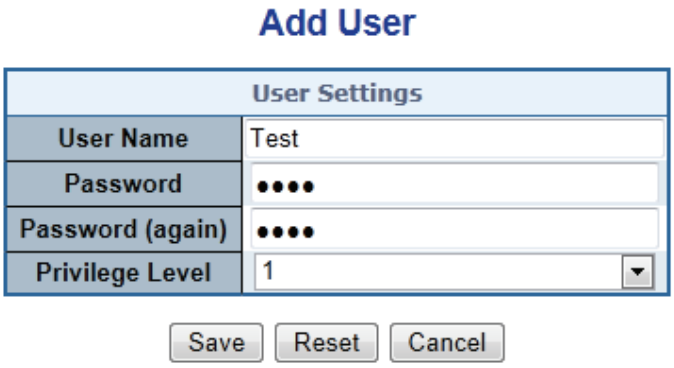


Figure 4-2-5: Add / Edit User Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **User Name**	A string identifies the user name whose entry should belong to. The allowed string length is 1 to 32. The valid user name is a combination of letters, numbers and underscores.
• **Password**	The password of the user. The allowed string length is 0 to 32.
• **Privilege Level**	The privilege level of the user. The allowed range is 1 to 15. If the privilege level value is 15, it can access all groups, i.e. granted the full control of the device. But others value need to refer to each group privilege level. User's privilege should be same or greater than the group privilege level to have the access to that group. By default setting, most groups privilege level 5 has the read-only access and privilege level 10 has the read-write access. And the system maintenance (software upload, factory defaults and etc.) need user privilege level 15. Generally, the privilege level 15 can be used for an administrator account, privilege level 10 for a standard user account and privilege level 5 for a guest account.

Buttons

[redacted]: Click to save changes.

[redacted]: Click to undo any changes made locally and revert to previously saved values.

[redacted]: Click to undo any changes made locally and return to the Users.

[redacted]: Delete the current user. This button is not available for new configurations (Add new user)

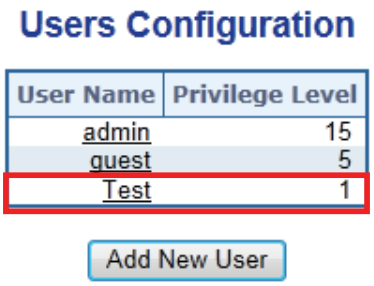


Figure 4-2-6: User Configuration Page Screenshot

Note

After changing the default password, if you forget the password, please press the "Reset" button on the front panel of the Industrial Managed Switch over 10 seconds and then release. The current setting includes VLAN, and will be lost and the Industrial Managed Switch will restore to the default mode.

4.2.5 Privilege Levels

This page provides an overview of the privilege levels. After setup is completed, please press **"Save"** button to take effect. Please login web interface with new user name and password, the screen in Figure 4-2-7 appears.

Privilege Level Configuration

Group Name	Privilege Levels			
	Configuration Read-only	Configuration/Execute Read/write	Status/Statistics Read-only	Status/Statistics Read/write
Aggregation	5	10	5	10
Diagnostics	5	10	5	10
EEE	5	10	5	10
IP	5	10	5	10
LACP	5	10	5	10
LLDP	5	10	5	10
LLDP_MED	5	10	5	10
Loop_Protect	5	10	5	10
MAC_Table	5	10	5	10
MVR	5	10	5	10
Maintenance	15	15	15	15
Mirroring	5	10	5	10
Multicast	5	10	5	10
Port_Security	5	10	5	10
Ports	5	10	1	10
Private_VLANs	5	10	5	10
Protocol_based_VLAN	5	10	5	10
QoS	5	10	5	10
SNMP	5	10	5	10
Security	5	10	5	10
Spanning_Tree	5	10	5	10
System	5	10	1	10
Timer	5	10	5	10
UPnP	5	10	5	10
VLANs	5	10	5	10
Voice_VLAN	5	10	5	10

Save Reset

Figure 4-2-7: Privilege Levels Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Group Name**	The name identifies the privilege group. In most cases, a privilege level group consists of a single module (e.g. LACP, RSTP or QoS), but a few of them contains more than one. The following description defines these privilege level groups in details: ■ **System**: Contact, Name, Location, Timezone, Log. ■ **Security**: Authentication, System Access Management, Port (contains Dot1x port, MAC based and the MAC Address Limit), ACL, HTTPS, SSH, ARP Inspection and IP source guard. ■ **IP**: Everything except 'ping'. ■ **Port**: Everything except 'VeriPHY'. ■ **Diagnostics**: 'ping' and 'VeriPHY'. ■ **Maintenance**: CLI- System Reboot, System Restore Default, System Password, Configuration Save, Configuration Load and Firmware Load. Web-Users, Privilege Levels and everything in Maintenance. ■ **Debug**: Only present in CLI.
• **Privilege Level**	Every group has an authorization Privilege level for the following sub groups: ■ **Configuration read-only** ■ **Configuration/execute read-write** ■ **Status/statistics read-only** ■ **Status/statistics read-write** (e.g. for clearing of statistics). User Privilege should be the same or greater than the authorization Privilege level to have the access to that group.

Buttons

 : Click to save changes.

 : Click to undo any changes made locally and revert to previously saved values.

4.2.6 NTP Configuration

Configuring NTP on this page.

NTP is an acronym for **Network Time Protocol**, a network protocol for synchronizing the clocks of computer systems. NTP uses UDP (data grams) as transport layer. You can specify NTP Servers and set GMT Time zone. The NTP Configuration screen in Figure 4-2-8 appears.

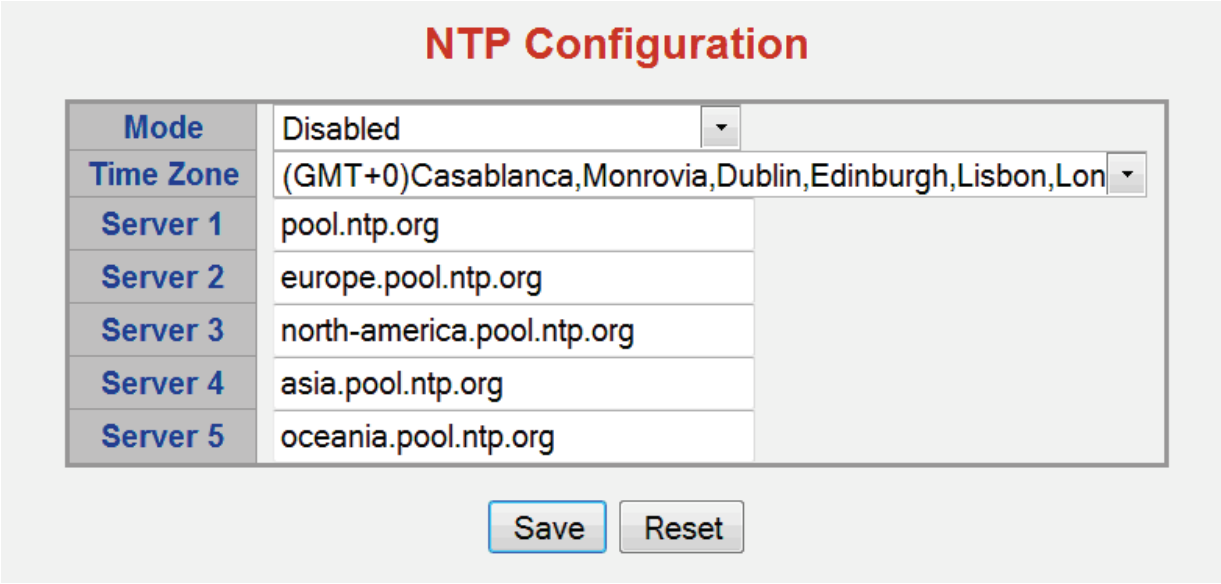


Figure 4-2-8: NTP Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Mode**	Indicates the NTP mode operation. Possible modes are: ■ **Enabled**: Enable NTP mode operation. When NTP mode operation is enabled, the agent forwards NTP messages between the clients and the server when they are not on the same subnet domain. ■ **Disabled**: Disable NTP mode operation.
• **Timezone**	Allows to select the time zone according to current location of switch.
• **Server #**	Provide the NTP IPv4 or IPv6 address of this switch. IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can appear only once. It can also represent a legally valid IPv4 address. For example, '::192.1.2.34'.

Buttons

: Click to save changes.

: Click to undo any changes made locally and revert to previously saved values.

4.2.7 UPnP

Configure UPnP on this page.
UPnP is an acronym for **Universal Plug and Play**. The goals of UPnP are to allow devices to connect seamlessly and to simplify the implementation of networks in the home (data sharing, communications, and entertainment) and in corporate environments for simplified installation of computer components. The UPnP Configuration screen in Figure 4-2-9 appears.

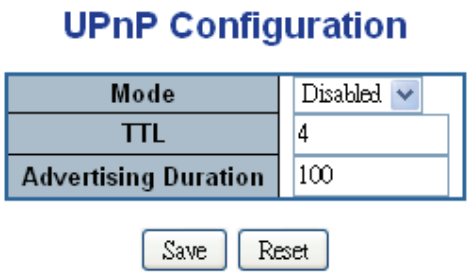


Figure 4-2-9: UPnP Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Mode**	Indicates the UPnP operation mode. Possible modes are: ■ Enabled: Enable UPnP mode operation. ■ Disabled: Disable UPnP mode operation. When the mode is enabled, two ACEs are added automatically to trap UPNP related packets to CPU. The ACEs are automatically removed when the mode is disabled.
• **TTL**	The TTL value is used by UPnP to send SSDP advertisement messages. Valid values are in the range from 1 to 255.
• **Advertising Duration**	The duration, carried in SSDP packets, is used to inform a control point or control points about how often it or they should receive an SSDP advertisement message from this switch. If a control point does not receive any message within the duration, it may suggest that the switch no longer exists. Due to the unreliable nature of UDP, as standard it is recommended that such refreshment of advertisements to be done at less than one-half of the advertising duration. In the implementation, the switch sends SSDP messages periodically at the interval one-half of the advertising duration minus 30 seconds. Valid values are in the range from 100 to 86400.

Buttons

 : Click to save changes.

 : Click to undo any changes made locally and revert to previously saved values.

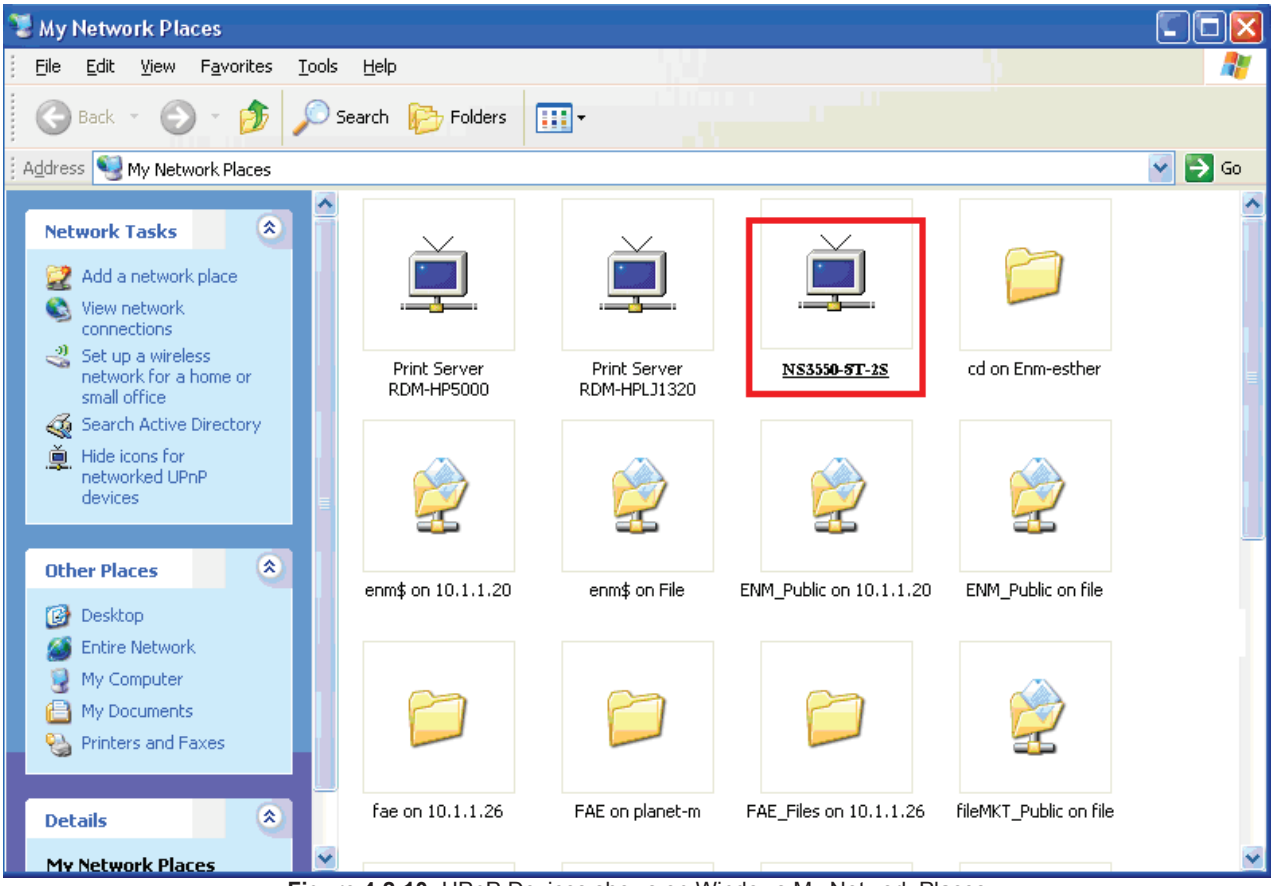


Figure 4-2-10: UPnP Devices shows on Windows My Network Places

4.2.8 DHCP Relay

Configuring DHCP Relay on this page. **DHCP Relay** is used to forward and to transfer DHCP messages between the clients and the server when they are not on the same subnet domain.

The **DHCP option 82** enables a DHCP relay agent to insert specific information into a DHCP request packets when forwarding client DHCP packets to a DHCP server and remove the specific information from a DHCP reply packets when forwarding server DHCP packets to a DHCP client. The DHCP server can use this information to implement IP address or other assignment policies. Specifically the option works by setting two sub-options:

- Circuit ID (option 1)
- Remote ID (option2).

The Circuit ID sub-option is supposed to include information specific to which circuit the request came in on.
The Remote ID sub-option was designed to carry information relating to the remote host end of the circuit.

The definition of Circuit ID in the switch is 4 bytes in length and the format is "vlan_id" "module_id" "port_no". The parameter of "vlan_id" is the first two bytes representing the VLAN ID. The parameter of "module_id" is the third byte for the module ID (in standalone switch it always equals 0; in stackable switch it means switch ID). The parameter of "port_no" is the fourth byte and it means the port number.

The Remote ID is 6 bytes in length, and the value is equal to the DHCP relay agent's MAC address. The DHCP Relay Configuration screen in Figure 4-2-11 appears.

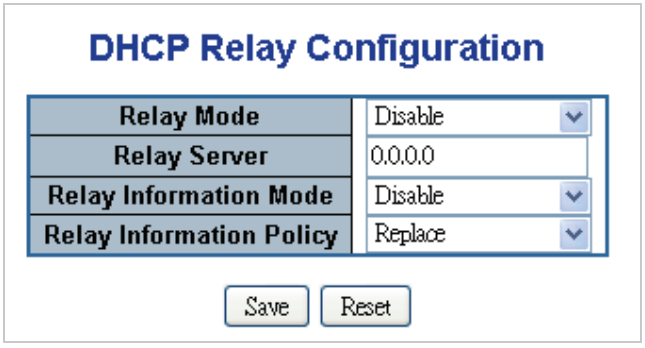


Figure 4-2-11: DHCP Relay Configuration Page Screenshot

The page includes the following fields:

Object	Description
1. Relay Mode	Indicates the DHCP relay mode operation. Possible modes are: ■ **Enabled**: Enable DHCP relay mode operation. When enable DHCP relay mode operation, the agent forward and to transfer DHCP messages between the clients and the server when they are not on the same subnet domain. And the DHCP broadcast message won't flood for security considered. ■ **Disabled**: Disable DHCP relay mode operation.
2. Relay Server	Indicates the DHCP relay server IP address. A DHCP relay agent is used to forward and to transfer DHCP messages between the clients and the server when they are not on the same subnet domain.
3. Relay Information Mode	Indicates the DHCP relay information mode option operation. Possible modes are: ■ **Enabled**: Enable DHCP relay information mode operation. When enable DHCP relay information mode operation, the agent insert specific information (option82) into a DHCP message when forwarding to DHCP server and remove it from a DHCP message when transferring to DHCP client. It only works under DHCP relay operation mode enabled. ■ **Disabled**: Disable DHCP relay information mode operation.
4. Relay Information Policy	Indicates the DHCP relay information option policy. When enable DHCP relay information mode operation, if agent receive a DHCP message that already contains relay agent information. It will enforce the policy. And it only works under DHCP relay information operation mode enabled. Possible policies are: ■ **Replace**: Replace the original relay information when receive a DHCP message that already contains it. ■ **Keep**: Keep the original relay information when receive a DHCP message that already contains it. ■ **Drop**: Drop the package when receive a DHCP message that already contains relay information.

Buttons

 : Click to save changes.

 : Click to undo any changes made locally and revert to previously saved values.

4.2.9 DHCP Relay Statistics

This page provides statistics for DHCP relay. The DHCP Relay Statistics screen in Figure 4-2-12 appears.

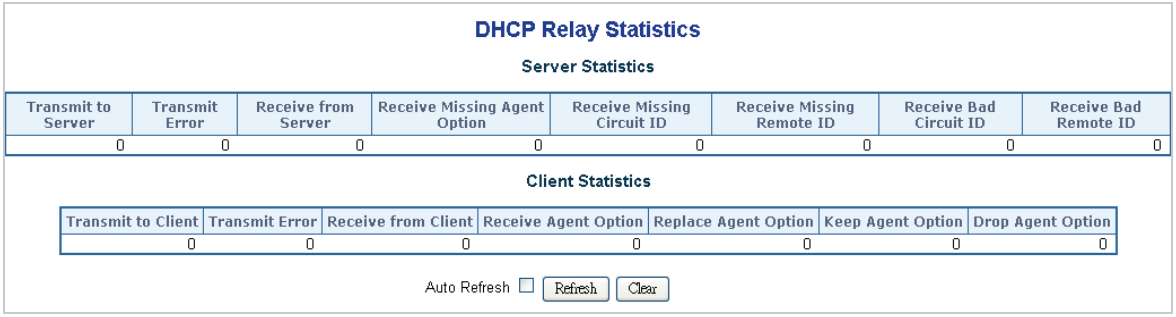


Figure 4-2-12: DHCP Relay Statistics Page Screenshot

The page includes the following fields:

Server Statistics

Object	Description
• **Transmit to Server**	The number of packets that are relayed from client to server.
• **Transmit Error**	The number of packets that resulted in errors while being sent to clients.
• **Receive form Server**	The number of packets received from server.
• **Receive Missing Agent Option**	The number of packets received without agent information options.

• **Receive Missing Circuit ID**	The number of packets received with the Circuit ID option missing.
• **Receive Missing Remote ID**	The number of packets received with the Remote ID option missing.
• **Receive Bad Circuit ID**	The number of packets whose Circuit ID option did not match known circuit ID.
• **Receive Bad Remote ID**	The number of packets whose Remote ID option did not match known Remote ID.

Client Statistics

Object	Description
• **Transmit to Client**	The number of relayed packets from server to client.
• **Transmit Error**	The number of packets that resulted in error while being sent to servers.
• **Receive from Client**	The number of received packets from server.
• **Receive Agent Option**	The number of received packets with relay agent information option.
• **Replace Agent Option**	The number of packets which were replaced with relay agent information option.
• **Keep Agent Optin**	The number of packets whose relay agent information was retained.
• **Drop Agent Option**	The number of packets that was dropped which were received with relay agent information.

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

4.2.10 CPU Load

This page displays the CPU load, using a **SVG graph**. The load is measured as averaged over the last 100ms, 1sec and 10 seconds intervals. The last 120 samples are graphed, and the last numbers are displayed as text as well.

In order to display the SVG graph, your browser must support the SVG format. Consult the SVG Wiki for more information on browser support. Specifically, at the time of writing, Microsoft Internet Explorer will need to have a plugin installed to support SVG. The CPU Load screen in Figure 4-2-13 appears.

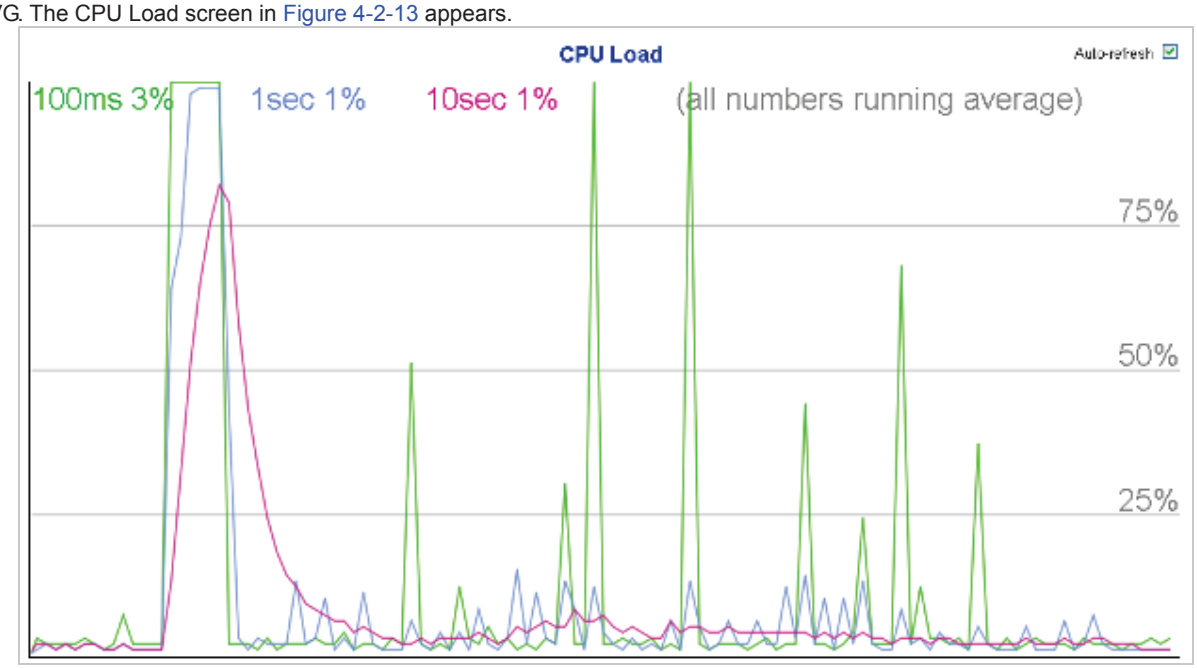


Figure 4-2-13: CPU Load Page Screenshot

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Note

If your browser cannot display anything on this page, please download Adobe SVG tool and install it in your computer.

4.2.11 System Log

The switch system log information is provided here. The System Log screen in Figure 4-2-14 appears.

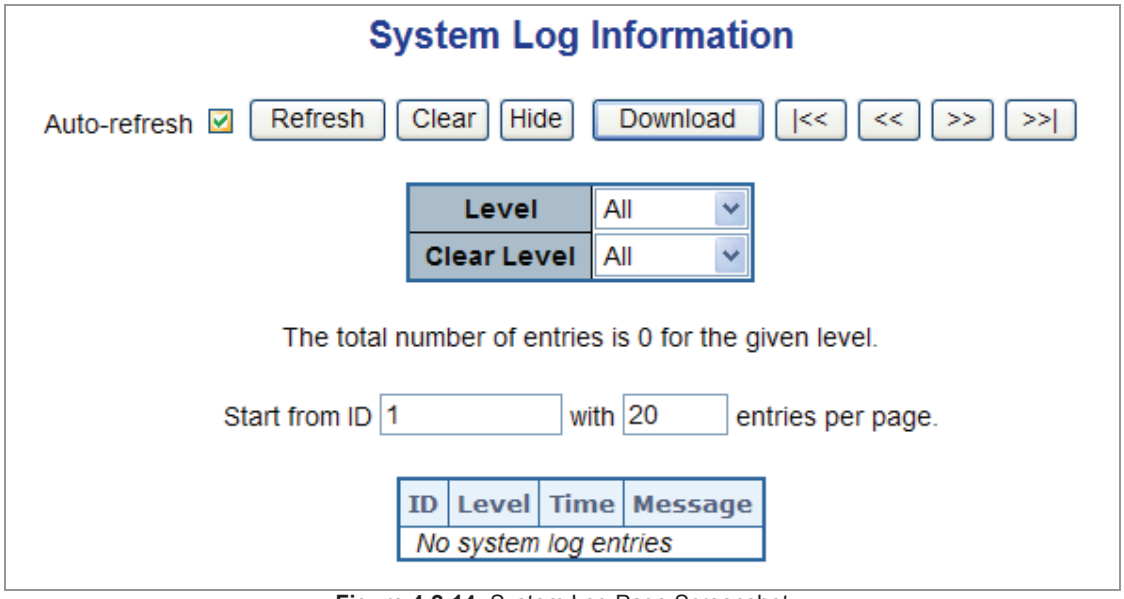


Figure 4-2-14: System Log Page Screenshot

The page includes the following fields:

Object	Description
• **ID**	The ID (>= 1) of the system log entry.
• **Level**	The level of the system log entry. The following level types are supported: ■ **Info**: Information level of the system log. ■ **Warning**: Warning level of the system log. ■ **Error**: Error level of the system log. ■ **All**: All levels.
• **Time**	The time of the system log entry.
• **Message**	The message of the system log entry.

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

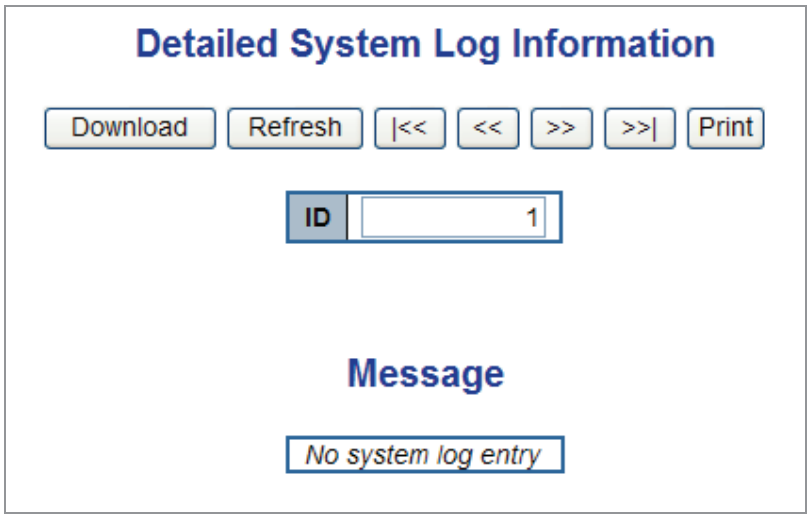


Figure 4-2-15: Detailed Log Page Screenshot

The page includes the following fields:

Object	Description
• **ID**	The ID (>= 1) of the system log entry.
• **Message**	The message of the system log entry.

Buttons

4.2.13 Remote Syslog

Configure remote syslog on this page. The Remote Syslog screen in Figure 4-2-16 appears.

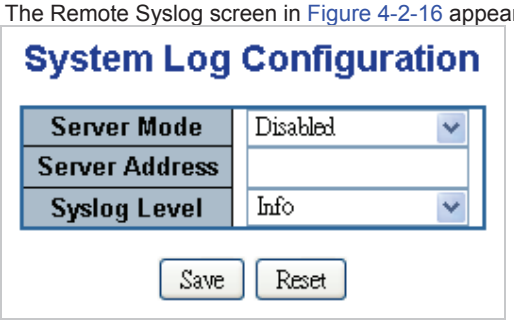


Figure 4-2-16: Remote Syslog Page Screenshot

The page includes the following fields:

Object	Description
5. Server Mode	Indicates the server mode operation. When the mode operation is enabled, the syslog message will send out to syslog server. The syslog protocol is based on UDP communication and received on UDP port 514 and the syslog server will not send acknowledgments back sender since UDP is a connectionless protocol and it does not provide acknowledgments. The syslog packet will always send out even if the syslog server does not exist. Possible modes are: ■ **Enabled**: Enable server mode operation. ■ **Disabled**: Disable server mode operation.
6. Server Address	Indicates the IPv4 host address of syslog server. If the switch provide DNS feature, it also can be a host name.
7. Syslog Level	Indicates what kind of message will send to syslog server. Possible modes are: ■ **Info**: Send information, warnings and errors. ■ **Warning**: Send warnings and errors. ■ **Error**: Send errors.

Buttons

[redacted]: Click to save changes.

[redacted]: Click to undo any changes made locally and revert to previously saved values.

4.2.14 SMTP Configuration

Configure SMTP Configuration on this page. The SMTP Configuration screen in Figure 4-2-17 appears.

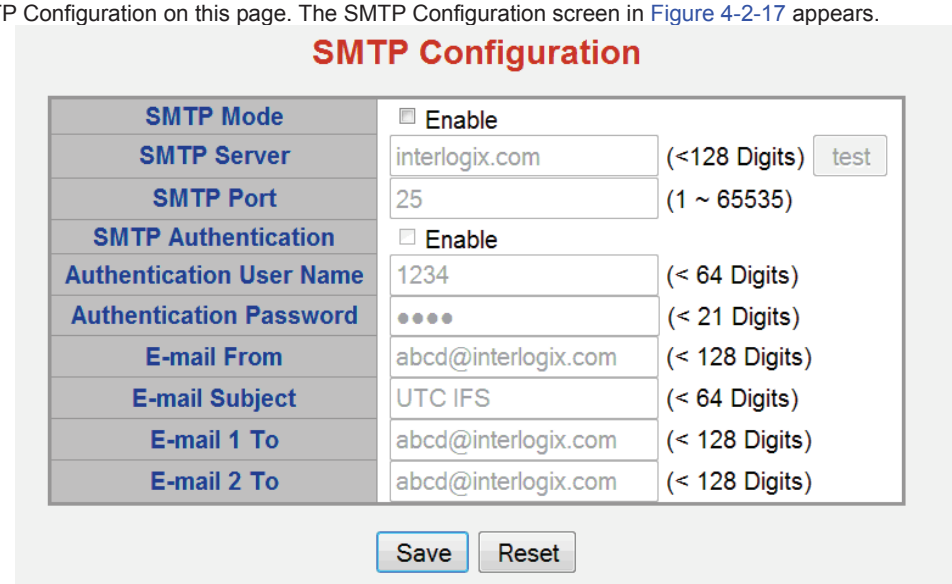


Figure 4-2-17: SMTP Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **SMTP Mode**	`Enabled` It is for you to enable SMTP mode function. This mode offers you to configure SMTP server and SMTP account information, system will refer it to send an E-mail for alarm noticing
• **SMTP Server**	It is for you to set up a specified SMTP server DNS name or IP address. If a DNS name is inputted, please remember to input DNS server IP address on the IP configuration page.
• **SMTP Port**	It is for you to input the SMTP server port number. The default is "25".
• **SMTP Authentication**	`Enabled` As usual SMTP server is denied to relay a mail from a different domain, so you have to enable this option and input your mail account and password for SMTP sever authorizing to forward a mail from a different domain. For example, you want an SMTP server, which is located on mail.123.com, to send a mail to mail.456.net.com. If you want to send the mail to a SMTP server which is located on the same domain or the same SMTP server, you don't have to enable SMTP authentication.
• **Authentic User Name**	It is for you to input your mail account name.
• **Authentication Password**	It is for you to input your mail account password.
• **E-mail From**	It is for you to input who send this mail.
• **E-mail Subject**	It is for you to input mail subject.
• **E-mail 1 To**	It is for you to input recipient mail address.
• **E-mail 2 To**	It is for you to input secondary recipient mail address.

Buttons

[redacted]: Click to test SMTP server address.

[redacted]: Click to save changes.

[redacted]: Click to undo any changes made locally and revert to previously saved values.

4.2.15 EEE Power Reduction

This page allows the user to configure the current EEE port settings.

EEE is a power saving option that reduces the power usage when there is low or no traffic utilization.

EEE works by powering down circuits when there is no traffic. When a port gets data to be transmitted, all circuits are powered up. The time it takes to power up the circuits is named wakeup time. The default wakeup time is 17 us for 1Gbit links and 30 us for other link speeds. EEE devices must agree upon the value of the wakeup time in order to make sure that both the receiving and transmitting device has all circuits powered up when traffic is transmitted. The devices can exchange wakeup time information using the LLDP protocol.

For maximizing power savings, the circuit isn't started at once transmit data is ready for a port, but is instead queued until 3000 bytes of data is ready to be transmitted. For not introducing a large delay in case that data less then 3000 bytes shall be transmitted, data are always transmitted after 48 us, giving a maximum latency of 48 us + the wakeup time.

If desired it is possible to minimize the latency for specific frames, by mapping the frames to a specific queue (done with QOS), and then mark the queue as an urgent queue. When an urgent queue gets data to be transmitted, the circuits will be powered up at once and the latency will be reduced to the wakeup time.

EEE works for ports in auto-negotiation mode, where the port is negotiated to either 1G or 100Mbps full duplex mode. The EEE Power Reduction screen in Figure 4-2-18 appears.

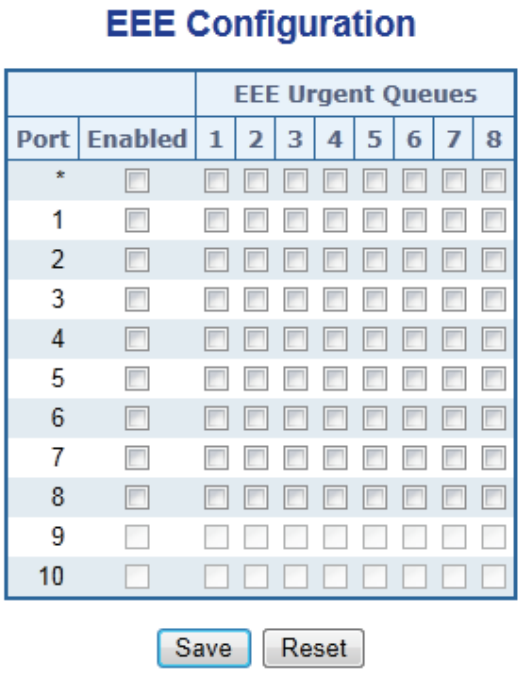


Figure 4-2-18: EEE Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Port**	The switch port number of the logical EEE port, * means to select all ports of Industrial Managed Switch.
• **EEE Enable**	Controls whether or not EEE is enabled for this switch port.
• **EEE Urgent Queues**	Queues set will activate transmission of frames as soon as any data is available. Otherwise the queue will postpone the transmsion until 3000 bytes are ready to be transmitted.

Buttons

[redacted]: Click to save changes.

[redacted]: Click to undo any changes made locally and revert to previously saved values.

4.2.16 Web Firmware Upgrade

This page facilitates an update on the firmware controlling the **Industrial Managed Switch**. The Web Firmware Upgrade screen in Figure 4-2-19 appears.

Figure 4-2-19: Web Firmware Upgrade Page Screenshot

To open **Firmware Upgrade** screen perform the folling:

1. Click **System** -> Web **Firmware Upgrade**.
2. The Firmware Upgrade screen is displayed as in Figure 4-2-19.
3. Click the "[redacted]" "button of the main page, the system would pop up the file selection menu to choose firmware.
4. Select on the firmware and then click "[redacted]", the **Software Upload Progress** would show the file upload status.
5. Once the software is loaded to the system successfully, the following screen appears. The system will load the new software after reboot.

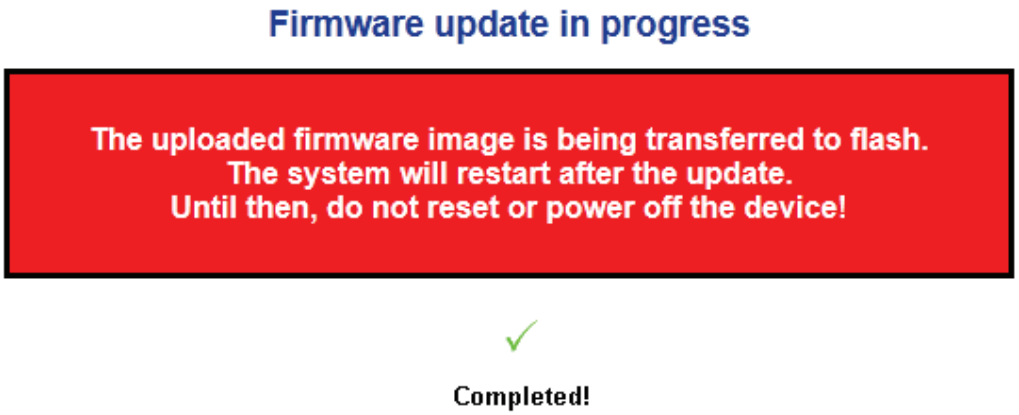


Figure 4-2-20: Software successfully Loaded Notice Screen

Note

DO NOT Power OFF the **Industrial Managed Switch** until the update progress is complete.

Note

Do not quit the Firmware Upgrade page without pressing the "**OK**" button after the image is loaded. Or the system won't apply for the new firmware. User has to repeat the firmware upgrade processes again.

4.2.17 TFTP Firmware Upgrade

The **Firmware Upgrade** page provides the functions to allow a user to update the **Industrial Managed Switch** firmware from the TFTP server in the network. Before updating, make sure you have your TFTP server ready and the firmware image is on the TFTP server. The TFTP Firmware Upgrade screen in Figure 4-2-21 appears.

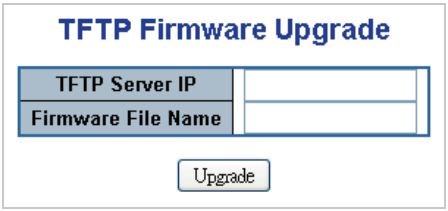


Figure 4-2-21: TFTP Firmware Update Page Screenshot

The page includes the following fields:

Object	Description
• **TFTP Server IP**	Fill in your TFTP server IP address.
• **Firmware File Name**	The name of firmware image. (Maximum length : 24 characters)

Buttons

[redacted]: Click to upgrade firmware.

Note

DO NOT Power OFF the **Industrial Managed Switch** until the update progress is complete.

Note

Do not quit the Firmware Upgrade page without press the "**OK**" button after the image is loaded. Or the system won't apply for the new firmware. User has to repeat the firmware upgrade processes again.

4.2.18 Configuration Backup

This function allows backup and reload the current configuration of the **Industrial Managed Switch** to the local management station. The Configuration Backup screen in Figure 4-2-22 appears.

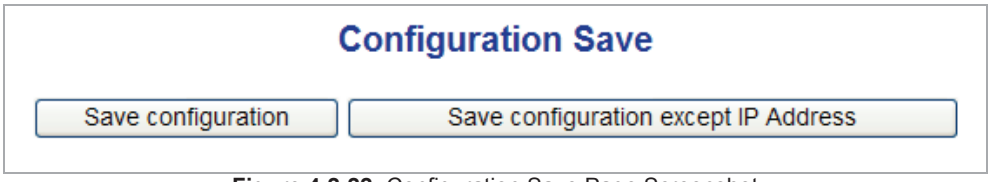


Figure 4-2-22: Configuration Save Page Screenshot

You can save/view or load the switch configuration. The configuration file is in XML format with a hierarchy of tags:

Header tags:	<?xml version="1.0"?> and <configuration>. These tags are mandatory and must be present at the beginning of the file.
Section tags:	<platform>, <global> and <switch>. The platform section must be the first section tag and this section must include the correct platform ID and version. The global section is optional and includes configuration which is not related to specific switch ports. The switch section is optional and includes configuration which is related to specific switch ports.
Module tags:	<ip>, <mac>, <port> etc. These tags identify a module controlling specific parts of the configuration.
Group tags:	<port_table>, <vlan_table> etc. These tags identify a group of parameters, typically a table.
Parameter tags:	<mode>, <entry> etc. These tags identify parameters for the specific section, module and group. The <entry> tag is used for table entries.

Configuration parameters are represented as attribute values. When saving the configuration from the switch, the entire

configuration including syntax descriptions is included in the file. The file may then be modified using an editor and loaded to a **Industrial Managed Switch**.

The examples below show a small configuration file only including configuration of the MAC address age time and the learning mode per port. When loading this file, only the included parameters will be changed. This means that the age time will be set to 200 and the learn mode will be set to automatic.

- **Save Configuration**

1. Press the ***"Save Configuration"*** button to save the current configuration in manager workstation. The following screens in Figure 4-2-23 & 4-2-24 appear

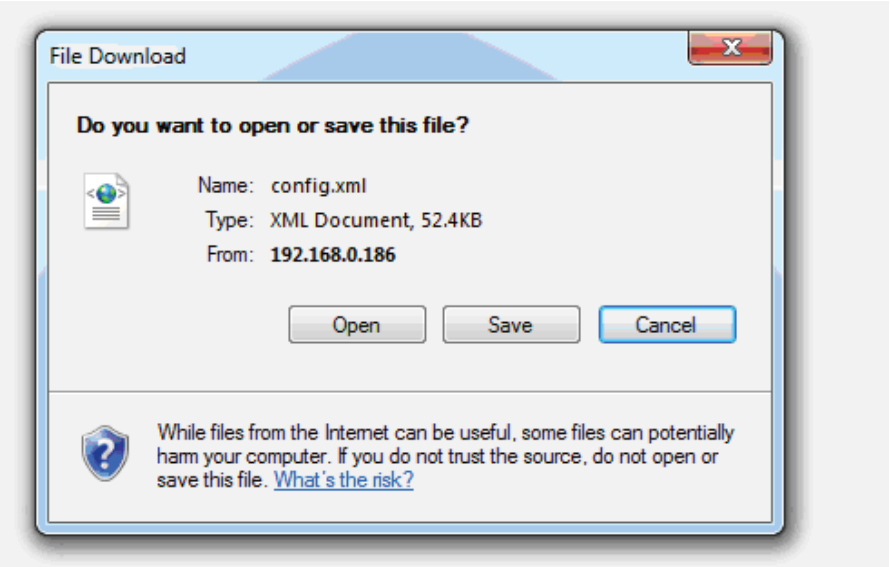


Figure 4-2-23: File Download Screen

2. Choose the file save path in management workstation.

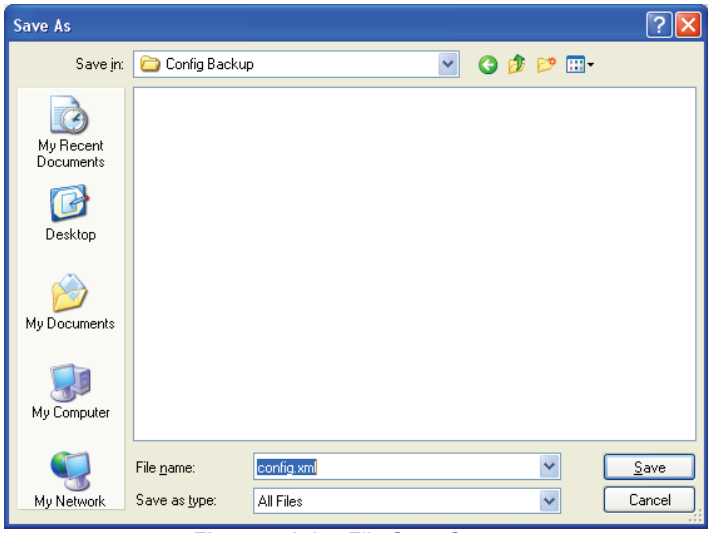


Figure 4-2-24: File Save Screen

4.2.19 Configuration Upload

This function allows backup and reload the current configuration of the **Industrial Managed Switch** to the local management station. The Configuration Upload screen in Figure 4-2-25 appears.

Figure 4-2-25: Configuration Upload Page Screenshot

- **Configuration Upload**

1. Click the "[redacted]" button of the main page, the system would pop up the file selection menu to choose saved configuration.

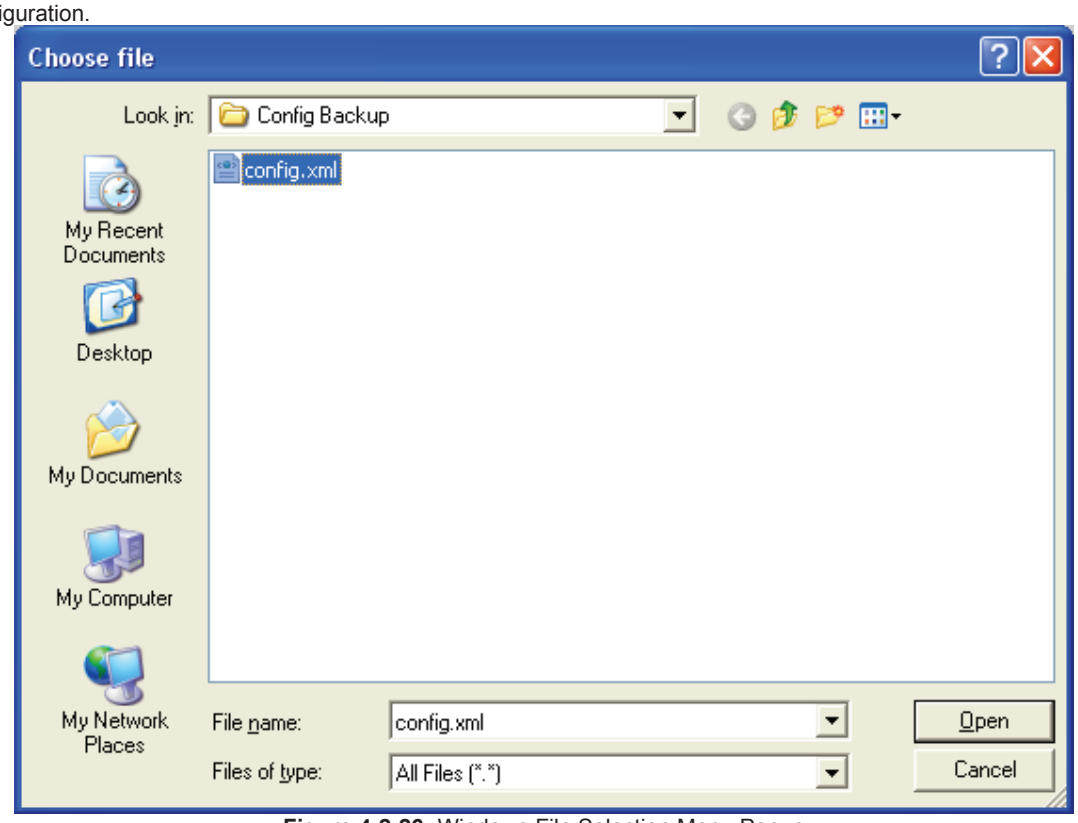


Figure 4-2-26: Windows File Selection Menu Popup

2. Select on the configuration file and then click "[redacted]", the bottom of the browser shows the upload status.
3. After down, the main screen appears "**Transfer Completed**".

4.2.20 Image Select

This function provides dual image deposit in the **Industrial Managed Switch**, user can select any one of the image as Active image of **Industrial Managed Switch.** The Image Select screen in Figure 4-2-27 appears.

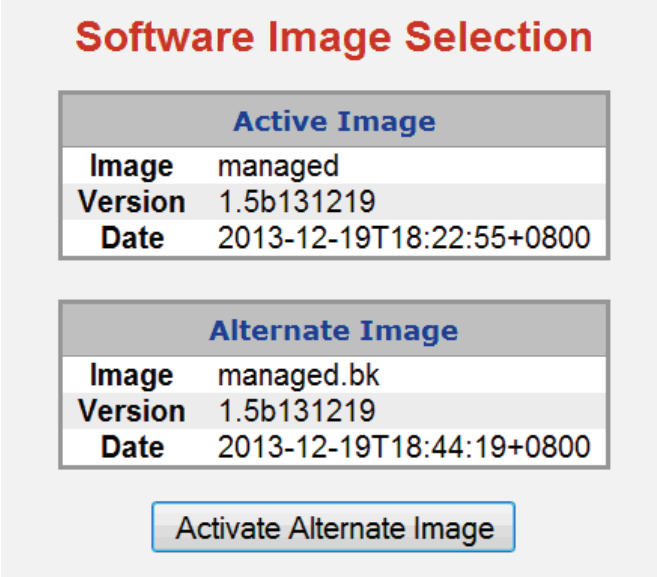


Figure 4-2-27: Image Select Page Screenshot

Button

[redacted]: Click to choose Alternate Image as Activate Image.

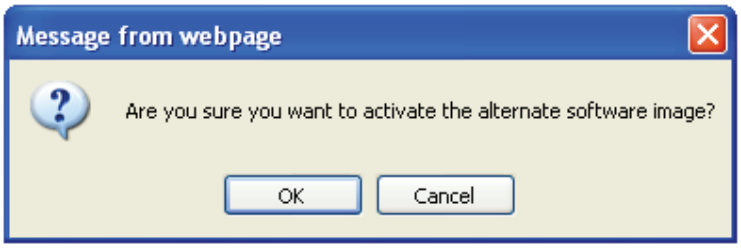


Figure 4-2-28: Image Select Page Screenshot

Figure 4-2-29: Image Select Page Screenshot

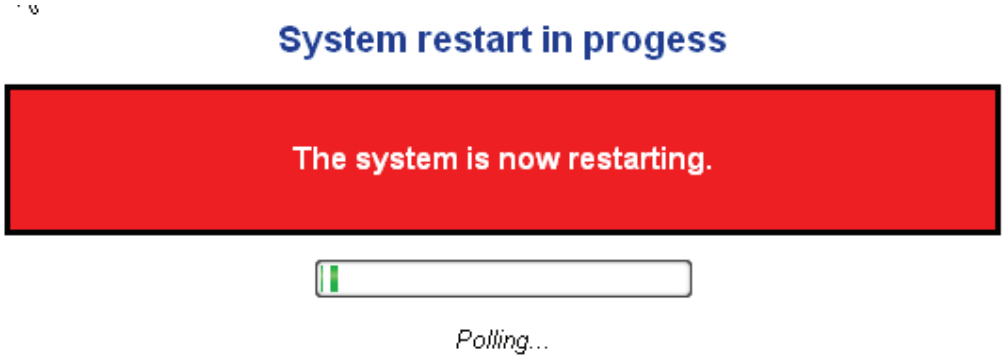


Figure 4-2-30: Image Select Page Screenshot

Figure 4-2-31: Image Select Page Screenshot

After the system reboot, you can use the Alternate Image of **Industrial Managed Switch**.

4.2.21 Factory Default

You can reset the configuration of the stack switch on this page. Only the IP configuration is retained. The new configuration is available immediately, which means that no restart is necessary. The Factory Default screen in Figure 4-2-32 appears.

Figure 4-2-32: Factory Default Page Screenshot

Buttons

: Click to reset the configuration to Factory Defaults.

Figure 4-2-33: Factory Default Page Screenshot

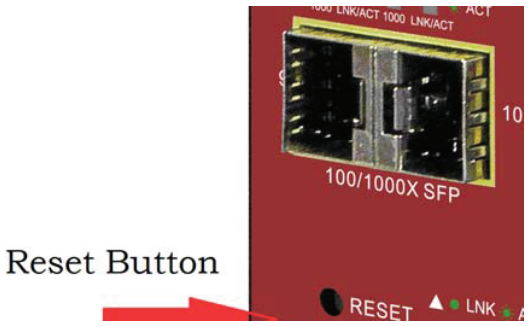
: Click to return to the web main page without resetting the configuration.

After the "**Factory**" button ispressed and rebooted, the system will load the default IP settings as following:

- Default IP address: **192.168.0.100**
- Subnet mask: **255.255.255.0**
- Default Gateway: **192.168.0.254**
- The other setting value is back to disable or none.

Note

To reset the **Industrial Managed Switch** to the Factory default setting, you can also press the hardware reset button at the front panel for more than 10 seconds. After the device is rebooted, you can login the management WEB interface within the same subnet of 192.168.0.xx.



4.2.22 System Reboot

The **Reboot** page enables the device to be rebooted from a remote location. Once the Reboot button is pressed, user will re-access the WEB interface about 60 seconds later. The System Reboot screen in Figure 4-2-34 appears.

Figure 4-2-34: System Reboot Page Screenshot

Buttons

[redacted]: Click to reboot the system.

[redacted]: Click to return to the web main page without rebooting the system.

4.2.23 Daylight Saving

The **Reboot** page enables the device to be rebooted from a remote location. Once the Reboot button is pressed, user will re-access the WEB interface about 60 seconds later, the System Reboot screen in Figure 4-2-35 appears.

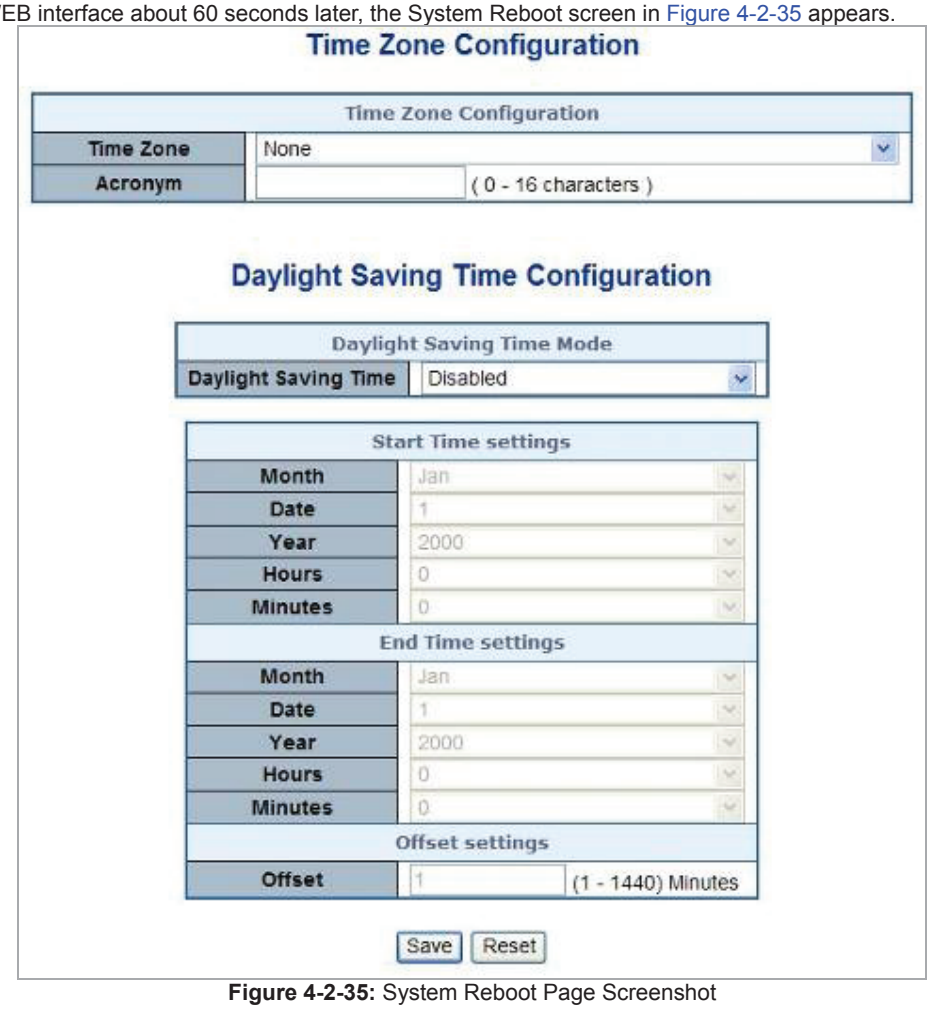


Figure 4-2-35: System Reboot Page Screenshot

The page includes the following fields:

Object	Description
• **Time Zone**	Allow select the time zone according to current location of switch.
• **Acronm**	User can set the acronym of the time zone. This is a User configurable acronym to identify the time zone. (Range : Up to 16 alpha-numeric characters and can contain '-', '_' or '.')
• **Daylight Saving Time**	is is used to set the clock forward or backward according to the configurations set below for a defined Daylight Saving Time duration. Select 'Disable' to disable the Daylight Saving Time configuration. Select 'Recurring' and configure the Daylight Saving Time duration to repeat the configuration every year. Select 'Non-Recurring' and configure the Daylight Saving Time duration for single time configuration. (Default : Disabled)

Daylight Saving Rime – **Recurring Mode**

Object	Description
• **Week (Start Time Setting)**	Select the starting week number.
• **Day (Start Time Setting)**	Select the starting day.
• **Month (Start Time Setting)**	Select the starting month.
• **Hours (Start Time Setting)**	Select the starting hour.
• **Minutes (Start Time Setting)**	Select the starting minute.

• **Week (End Time Setting)**	Select the ending week number.
• **Day (End Time Setting)**	Select the ending day.
• **Month (End Time Setting)**	Select the ending month.
• **Hours (End Time Setting)**	Select the ending hour.
• **Month (End Time Setting)**	Select the ending minute.
• **Offest**	Enter the number of minutes to add during Daylight Saving Time. (Range: 1 to 1440)

Daylight Saving Rime – N**on-Recurring Mode**

Object	Description
• **Month (Start Time Setting)**	Select the starting month.
• **Date (Start Time Setting)**	Select the starting date.
• **Year (Start Time Setting)**	Select the starting year.
• **Hours (Start Time Setting)**	Select the starting hour.
• **Minutes (Start Time Setting)**	Select the starting minute.
• **Month (End Time Setting)**	Select the ending month.
• **Date (End Time Setting)**	Select the ending date.
• **Year (End Time Setting)**	Select the ending year.
• **Hours (End Time Setting)**	Select the ending hour.
• **Minutes (End Time Setting)**	Select the ending minute.
• **Offset**	• Enter the number of minutes to add during Daylight Saving Time. (Range: 1 to 1440)

Buttons

 : Click to save changes.

 : Click to undo any changes made locally and revert to previously saved values.

4.3 Simple Network Management Protocol

4.3.1 SNMP Overview

The Simple Network Management Protocol (SNMP) is an application layer protocol that facilitates the exchange of management information between network devices. It is part of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suite. SNMP enables network administrators to manage network performance, find and solve network problems, and plan for network growth.

An SNMP-managed network consists of three key components: Network management stations (NMSs), SNMP agents, Management information base (MIB) and network-management protocol：

- **Network management stations (NMSs)：**Sometimes called consoles, these devices execute management applications that monitor and control network elements. Physically, NMSs are usually engineering workstation-caliber computers with fast CPUs, megapixel color displays, substantial memory, and abundant disk space. At least one NMS must be present in each managed environment.
- **Agents：**Agents are software modules that reside in network elements. They collect and store management information such as the number of error packets received by a network element.
- **Management information base (MIB)：**A MIB is a collection of managed objects residing in a virtual information store. Collections of related managed objects are defined in specific MIB modules.
- **network-management protocol：**A management protocol is used to convey management information between agents and NMSs. SNMP is the Internet community's de facto standard management protocol.

SNMP Operations
SNMP itself is a simple request/response protocol. NMSs can send multiple requests without receiving a response.

- **Get --** Allows the NMS to retrieve an object instance from the agent.
- **Set --** Allows the NMS to set values for object instances within an agent.
- **Trap --** Used by the agent to asynchronously inform the NMS of some event. The SNMPv2 trap message is designed to replace the SNMPv1 trap message.

SNMP community
An SNMP community is the group that devices and management stations running SNMP belong to. It helps define where information is sent. The community name is used to identify the group. A SNMP device or agent may belong to more than one SNMP community. It will not respond to requests from management stations that do not belong to one of its communities. SNMP default communities are:

- **Write** = private
- **Read** = public

Use the SNMP Menu to display or configure the Managed Switch's SNMP function. This section has the following items:

System Configuration	Configure SNMP on this page.
System Information	The system information is provides here.
SNMPv3 Communities	Configure SNMPv3 communities table on this page.
SNMPv3 Users	Configure SNMPv3 users table on this page.
SNMPv3 Groups	Configure SNMPv3 groups table on this page.
SNMPv3 Views	Configure SNMPv3 views table on this page.
SNMPv3 Accesses	Configure SNMPv3 accesses table on this page.

4.3.2 SNMP System Configuration

Configure SNMP on this page. The SNMP System Configuration screen in Figure 4-3-1 appears.

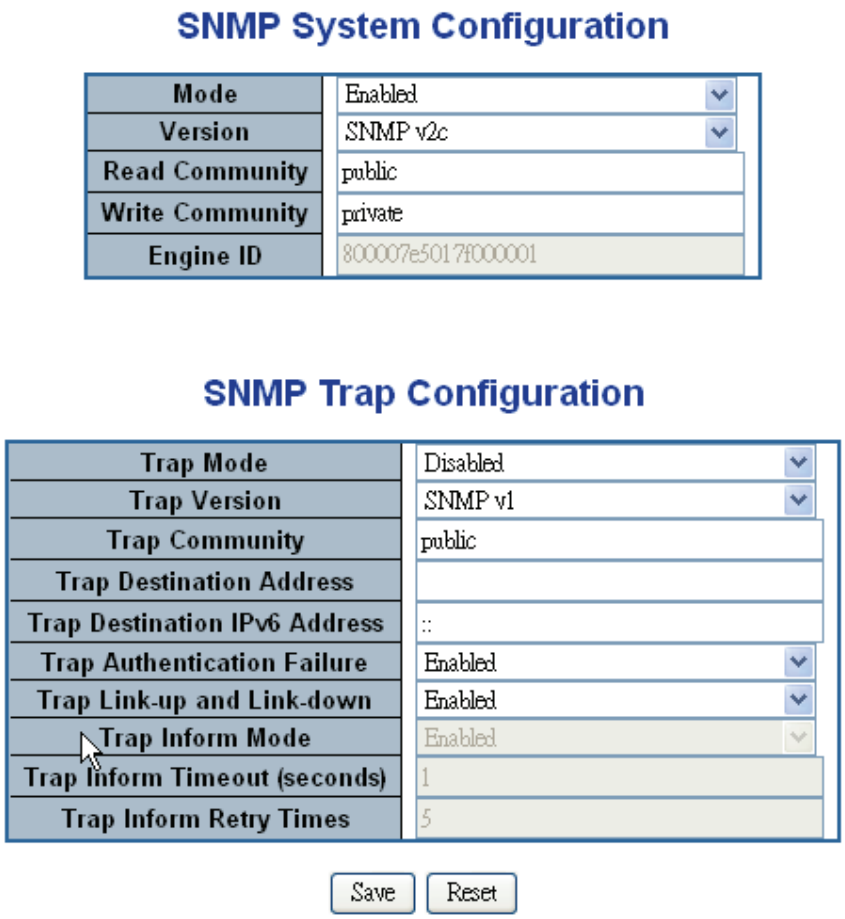


Figure 4-3-1: SNMP System Configuration Page Screenshot

The SNMP System Configuration page includes the following fields:

Object	Description
8. **Mode**	Indicates the SNMP mode operation. Possible modes are: ■ **Enabled**: Enable SNMP mode operation. ■ **Disabled**: Disable SNMP mode operation.
9. **Version**	Indicates the SNMP supported version. Possible versions are: ■ **SNMP v1**: Set SNMP supported version 1. ■ **SNMP v2c**: Set SNMP supported version 2c. ■ **SNMP v3**: Set SNMP supported version 3.
• **Read Community**	Indicates the community read access string to permit access to SNMP agent. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 33 to 126. The field is applicable only when SNMP version is SNMPv1 or SNMPv2c. If SNMP version is SNMPv3, the community string will be associated with SNMPv3 communities table. It provides more flexibility to configure security name than a SNMPv1 or SNMPv2c community string. In addition to community string, a particular range of source addresses can be used to restrict source subnet.
• **Write Community**	Indicates the community write access string to permit access to SNMP agent. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 33 to 126. The field is applicable only when SNMP version is SNMPv1 or SNMPv2c. If SNMP version is SNMPv3, the community string will be associated with SNMPv3 communities table. It provides more flexibility to configure security name than a SNMPv1 or SNMPv2c community string. In addition to community string, a particular range of source addresses can be used to restrict source subnet.
• **Engine ID**	Indicates the SNMPv3 engine ID. The string must contain an even number(in hexadecimal format) with number of digits between 10 and 64, but all-zeros and all-'F's are not allowed. Change of the Engine ID will clear all original local users.

The SNMP Trap Configuration page includes the following fields:

Object	Description
10. Trap Mode	Indicates the SNMP trap mode operation. Possible modes are: ■ **Enabled**: Enable SNMP trap mode operation. ■ **Disabled**: Disable SNMP trap mode operation.
11. Trap Version	Indicates the SNMP trap supported version. Possible versions are: ■ **SNMP v1**: Set SNMP trap supported version 1. ■ **SNMP v2c**: Set SNMP trap supported version 2c. ■ **SNMP v3**: Set SNMP trap supported version 3.
• **Trap Community**	Indicates the community access string when send SNMP trap packet. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 33 to 126.
• **Trap Destination Address**	Indicates the SNMP trap destination address. It allow a valid IP address in dotted decimal notation ('x.y.z.w'). And it also allow a valid hostname. A valid hostname is a string drawn from the alphabet (A-Za-z), digits (0-9), dot (.), dash (-). Spaces are not allowed, the first character must be an alpha character, and the first and last characters must not be a dot or a dash.
• **Trap Destination IPv6 Address**	Indicates the SNMP trap destination IPv6 address. IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can appear only once. It can also represent a legally valid IPv4 address. For example, '::192.1.2.34'.
12. Trap Authentication Failure	Indicates the SNMP entity is permitted to generate authentication failure traps. Possible modes are: ■ **Enabled**: Enable SNMP trap authentication failure. ■ **Disabled**: Disable SNMP trap authentication failure.
13. Trap Link-up and Link-down	Indicates the SNMP trap link-up and link-down mode operation. Possible modes are: ■ **Enabled**: Enable SNMP trap link-up and link-down mode operation. ■ **Disabled**: Disable SNMP trap link-up and link-down mode operation.
14. Trap Inform Mode	Indicates the SNMP trap inform mode operation. Possible modes are: ■ **Enabled**: Enable SNMP trap inform mode operation. ■ **Disabled**: Disable SNMP trap inform mode operation.
• **Trap Inform Timeout (seconds)**	Indicates the SNMP trap inform timeout. The allowed range is 0 to 2147.
• **Trap Inform Retry Times**	Indicates the SNMP trap informs retry times. The allowed range is 0 to 255.

Buttons

 : Click to save changes.

 : Click to undo any changes made locally and revert to previously saved values.

4.3.3 SNMP System Information

The switch system information is provided here. The SNMP System Information screen in Figure 4-3-2 appears.

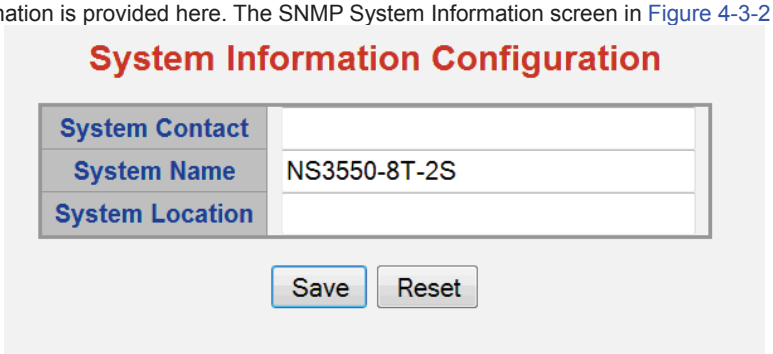


Figure 4-3-2: System Information Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **System Contact**	The textual identification of the contact person for this managed node, together with information on how to contact this person. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 32 to 126.
• **System Name**	An administratively assigned name for this managed node. By convention, this is the node's fully-qualified domain name. A domain name is a text string drawn from the alphabet (A-Za-z), digits (0-9), minus sign (-). No space characters are permitted as part of a name. The first character must be an alpha character. And the first or last character must not be a minus sign. The allowed string length is 0 to 255.
• **System Location**	The physical location of this node(e.g., telephone closet, 3rd floor). The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 32 to 126.

Buttons

[redacted]: Click to save changes.

[redacted]: Click to undo any changes made locally and revert to previously saved values.

4.3.4 SNMPv3 Configuration

4.3.4.1 SNMPv3 Communities

Configure SNMPv3 communities table on this page. The entry index key is Community. The SNMPv3 Communities screen in Figure 4-3-3 appears.

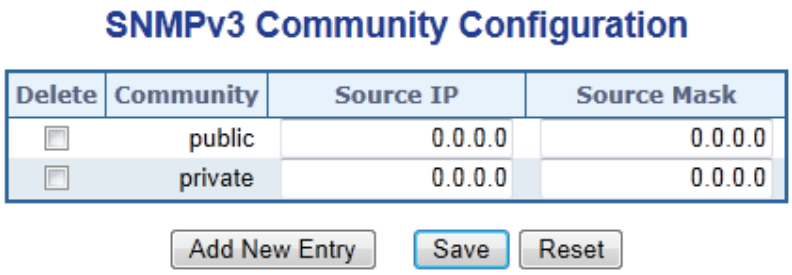


Figure 4-3-3: SNMPv3 Communities Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Delete**	Check to delete the entry. It will be deleted during the next save.
• **Community**	Indicates the community access string to permit access to SNMPv3 agent. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126. The community string will be treated as security name and map a SNMPv1 or SNMPv2c community string.
• **Source IP**	Indicates the SNMP access source address. A particular range of source addresses can be used to restrict source subnet when combined with source mask.
• **Source Mask**	Indicates the SNMP access source address mask.

Buttons

4.3.4.2 SNMPv3 Users

Configure SNMPv3 users table on this page. The entry index keys are Engine ID and User Name. The SNMPv3 Users screen in Figure 4-3-4 appears.

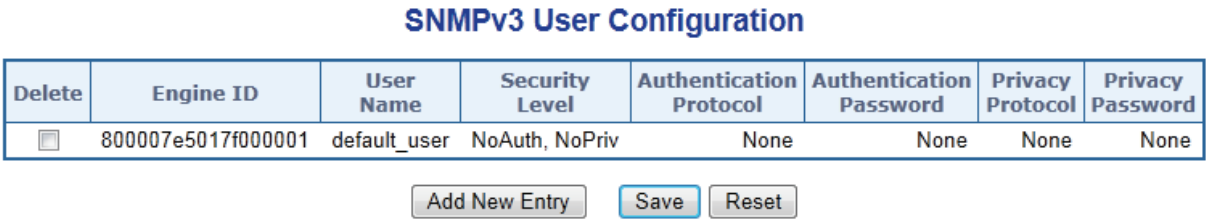


Figure 4-3-4: SNMPv3 Users Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Delete**	Check to delete the entry. It will be deleted during the next save.
• **Engine ID**	An octet string identifying the engine ID that this entry should belong to. The string must contain an even number (in hexadecimal format) with number of digits between 10 and 64, but all-zeros and all-'F's are not allowed. The SNMPv3 architecture uses the User-based Security Model (USM) for message security and the View-based Access Control Model (VACM) for access control. For the USM entry, the usmUserEngineID and usmUserName are the entry's keys. In a simple agent, usmUserEngineID is always that agent's own snmpEngineID value. The value can also take the value of the snmpEngineID of a remote SNMP engine with which this user can communicate. In other words, if user engine ID equal system engine ID then it is local user; otherwise it's remote user.
• **User Name**	A string identifying the user name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is the ASCII characters from 33 to 126.
15. **Security Level**	Indicates the security model that this entry should belong to. Possible security models are: ■ **NoAuth, NoPriv**: None authentication and none privacy. ■ **Auth, NoPriv**: Authentication and none privacy. ■ **Auth, Priv**: Authentication and privacy. The value of security level cannot be modified if entry already exist. That means must first ensure that the value is set correctly.
16. **Authentication Protocol**	Indicates the authentication protocol that this entry should belong to. Possible authentication protocol are: ■ **None**: None authentication protocol. ■ **MD5**: An optional flag to indicate that this user using MD5 authentication protocol. ■ **SHA**: An optional flag to indicate that this user using SHA authentication protocol. ■ The value of security level cannot be modified if entry already exists. That means must first ensure that the value is set correctly.
17. **Authentication Password**	A string identifying the authentication pass phrase. For MD5 authentication protocol, the allowed string length is 8 to 32. For SHA authentication protocol, the allowed string length is 8 to 40. The allowed content is the ASCII characters from 33 to 126.
18. **Privacy Protocol**	Indicates the privacy protocol that this entry should belong to. Possible privacy protocol are: ■ **None**: None privacy protocol. ■ **DES**: An optional flag to indicate that this user using DES authentication protocol.
• **Privacy Password**	A string identifying the privacy pass phrase. The allowed string length is 8 to 32, and the allowed content is the ASCII characters from 33 to 126.

Buttons

4.3.4.3 SNMPv3 Groups

Configure SNMPv3 groups table on this page. The entry index keys are Security Model and Security Name. The SNMPv3 Groups screen in Figure 4-3-5 appears.

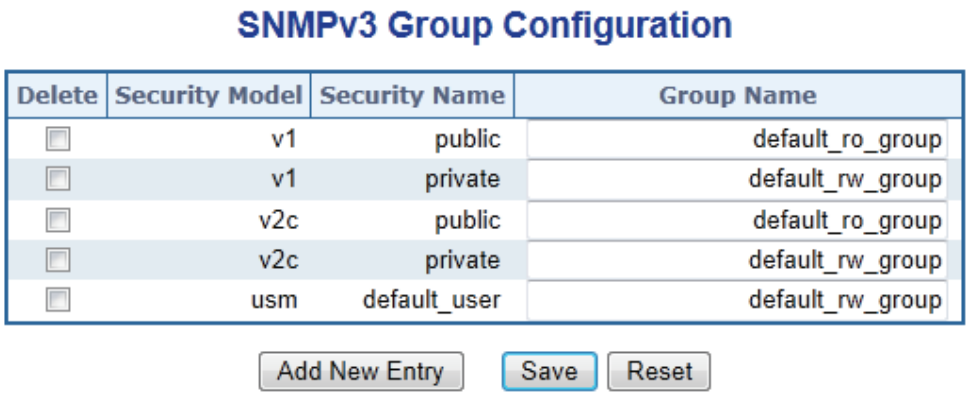


Figure 4-3-5: SNMPv3 Groups Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Delete**	Check to delete the entry. It will be deleted during the next save.
• **Security Model**	Indicates the security model that this entry should belong to. Possible security models are: ■ **v1**: Reserved for SNMPv1. ■ **v2c**: Reserved for SNMPv2c. ■ **usm**: User-based Security Model (USM).
• **Security Name**	A string identifying the security name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is the ASCII characters from 33 to 126.
• **Group Name**	A string identifying the group name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is the ASCII characters from 33 to 126.

Buttons

	to 126.
• **View Type**	Indicates the view type that this entry should belong to. Possible view type are: ■ **included**: An optional flag to indicate that this view subtree should be included. ■ **excluded**: An optional flag to indicate that this view subtree should be excluded. General, if a view entry's view type is 'excluded', it should be exist another view entry which view type is 'included' and it's OID subtree overstep the 'excluded' view entry.
• **OID Subtree**	The OID defining the root of the subtree to add to the named view. The allowed OID length is 1 to 128. The allowed string content is digital number or asterisk(*).

Buttons

Buttons

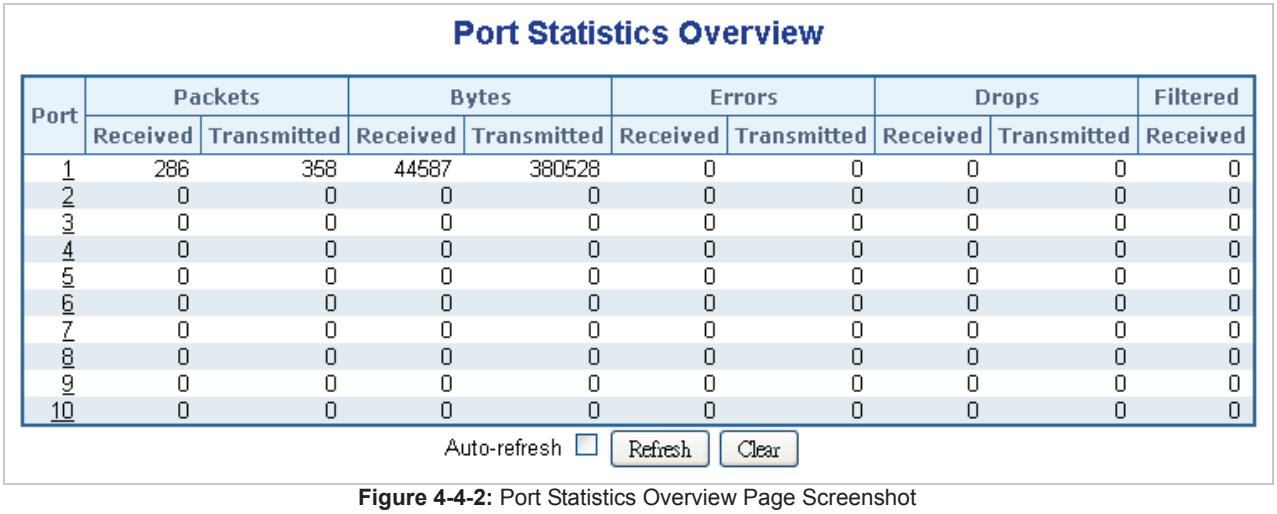
• **Configured Link Speed**	Select any available link speed for the given switch port. Draw the menu bar to select the mode. ■ **All**- Setup whole ports with the same setting. ■ **Auto Copper** - Setup Auto negotiation. ■ **Auto Fiber** - Setup Auto negotiation. ■ **10 Half** - Force sets 10Mbps/Half-Duplex mode. ■ **10 Full** - Force sets 10Mbps/Full-Duplex mode. ■ **100 Half** - Force sets 100Mbps/Half-Duplex mode. ■ **100 Full** - Force sets 100Mbps/Full-Duplex mode. ■ **1000 Full** - Force sets 10000Mbps/Full-Duplex mode. ■ **Disable** - Shutdown the port manually.
• **Flow Control**	When **Auto Speed** is selected on a port, this section indicates the flow control capability that is advertised to the link partner. When a fixed-speed setting is selected, that is what is used. The Current Rx column indicates whether pause frames on the port are obeyed, and the Current Tx column indicates whether pause frames on the port are transmitted. The Rx and Tx settings are determined by the result of the last Auto-Negotiation. Check the configured column to use flow control. This setting is related to the setting for Configured Link Speed.
• **Maximum Frame Size**	Enter the maximum frame size allowed for the switch port, including FCS. The allowed range is 1518 bytes to 9600 bytes.
• **Excessive Collision Mode**	Configure port transmit collision behavior. ■ **Discard**: Discard frame after 16 collisions (default). ■ **Restart**: Restart back off algorithm after 16 collisions.
• **Power Control**	The Usage column shows the current percentage of the power consumption per port. The Configured column allows for changing the power savings mode parameters per port. ■ **Disabled**: All power savings mechanisms disabled. ■ **ActiPHY**: Link down power savings enabled. ■ **PerfectReach**: Link up power savings enabled. ■ **Enabled**: Both link up and link down power savings enabled.

When set each port to run at 100M Full, 100M Half, 10M Full, and 10M Half-speed modes. The Auto-MDIX function will disable.

Buttons

 : Click to save changes.

 : Click to undo any changes made locally and revert to previously saved values.



Port Statistics Overview

Port	Packets		Bytes		Errors		Drops		Filtered
	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received
1	286	358	44587	380528	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0

Auto-refresh Refresh Clear

Figure 4-4-2: Port Statistics Overview Page Screenshot

The displayed counters are:

Object	Description
• **Port**	The logical port for the settings contained in the same row.
• **Packets**	The number of received and transmitted packets per port.
• **Bytes**	The number of received and transmitted bytes per port.
• **Errors**	The number of frames received in error and the number of incomplete transmissions per port.
• **Drops**	The number of frames discarded due to ingress or egress congestion.
• **Filtered**	The number of received frames filtered by the forwarding process.

Buttons

4.4.3 Port Statistics Detail

This page provides detailed traffic statistics for a specific switch port. Use the port select box to select which switch port details to display. The selected port belong to the currently selected stack unit, as reflected by the page header. The displayed counters are the totals for receive and transmit, the size counters for receive and transmit, and the error counters for receive and transmit. The Port Statistics Detail screen in Figure 4-4-3 appears.

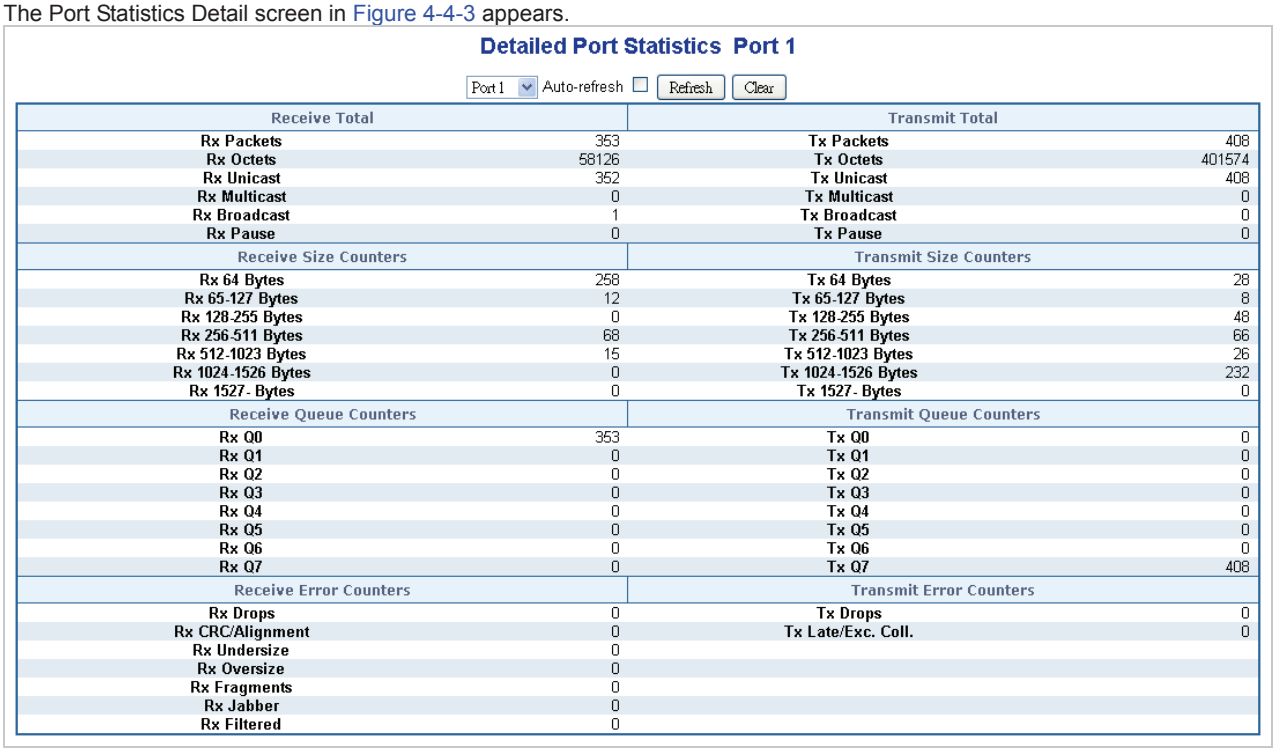


Figure 4-4-5: Detailed Port Statistics Port 1 Page Screenshot

The page includes the following fields:

Receive Total and Transmit Total

Object	Description
• **Rx and Tx Packets**	The number of received and transmitted (good and bad) packets
• **Rx and Tx Octets**	The number of received and transmitted (good and bad) bytes. Includes FCS, but excludes framing bits.
• **Rx and Tx Unicast**	The number of received and transmitted (good and bad) unicast packets.
• **Rx and Tx Multicast**	The number of received and transmitted (good and bad) multicast packets.
• **Rx and Tx Broadcast**	The number of received and transmitted (good and bad) broadcast packets.
• **Rx and Tx Pause**	A count of the MAC Control frames received or transmitted on this port that have an opcode indicating a PAUSE operation.

Receive and Transmit Size Counters

The number of received and transmitted (good and bad) packets split into categories based on their respective frame sizes.

Receive and Transmit Queue Counters

The number of received and transmitted packets per input and output queue.

Receive Error Counters

Object	Description
• **Rx Drops**	The number of frames dropped due to lack of receive buffers or egress congestion.
• **Rx CRC/Alignment**	The number of frames received with CRC or alignment errors.
• **Rx Undersize**	The number of short [1] frames received with valid CRC.
• **Rx Oversize**	The number of long [2] frames received with valid CRC.
• **Rx Fragments**	The number of short [1] frames received with invalid CRC.
• **Rx Jabber**	The number of long [2] frames received with invalid CRC.
• **Rx Filtered**	The number of received frames filtered by the forwarding process. Short frames are frames that are smaller than 64 bytes. Long frames are frames that are longer than the configured maximum frame length for this port.

1 Short frames are frames that are smaller than 64 bytes.
2 Long frames are frames that are longer than the configured maximum frame length for this port.

Transmit Error Counters

Object	Description
• **Tx Drops**	The number of frames dropped due to output buffer congestion.
• **Tx Late/Exc. Coll.**	The number of frames dropped due to excessive or late collisions.

Buttons

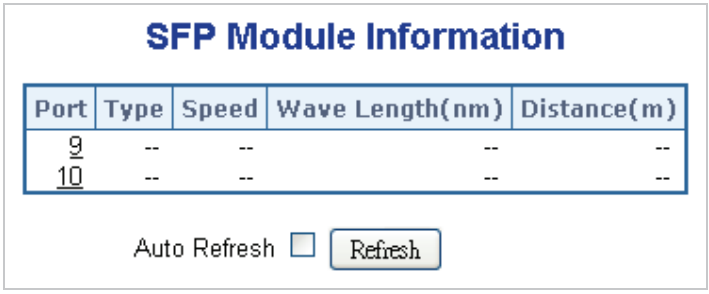


Figure 4-4-4: SFP Module Information for Switch Page Screenshot

The page includes the following fields:

Object	Description
• **Type**	Display the type of current SFP module, the possible types are: ■ 1000Base-SX ■ 1000Base-LX ■ 100Base-FX
• **Speed**	Display the spedd of current SFP module, the speed value or description is get from the SFP module. Different vendors SFP modules might shows different speed information.
• **Wave Length(nm)**	Display the wavelength of current SFP module, the wavelength value is get from the SFP module. Use this column to check if the wavelength values of two nodes are the matched while the fiber connection is failed.
• **Distance(m)**	Display the supports distance of current SFP module, the distance value is get from the SFP module.

Buttons

Auto-refresh : Check this box to enable an automatic refresh of the page at regular intervals.

4.4.5 Port Mirror

Configure port Mirroring on this page. This function provide to monitoring network traffic that forwards a copy of each incoming or outgoing packet from one port of a network Switch to another port where the packet can be studied. It enables the manager to keep close track of switch performance and alter it if necessary.

- To debug network problems, selected traffic can be copied, or mirrored, to a mirror port where a frame analyzer can be attached to analyze the frame flow.
- The Managed Switch can unobtrusively mirror traffic from any port to a monitor port. You can then attach a protocol analyzer or RMON probe to this port to perform traffic analysis and verify connection integrity.

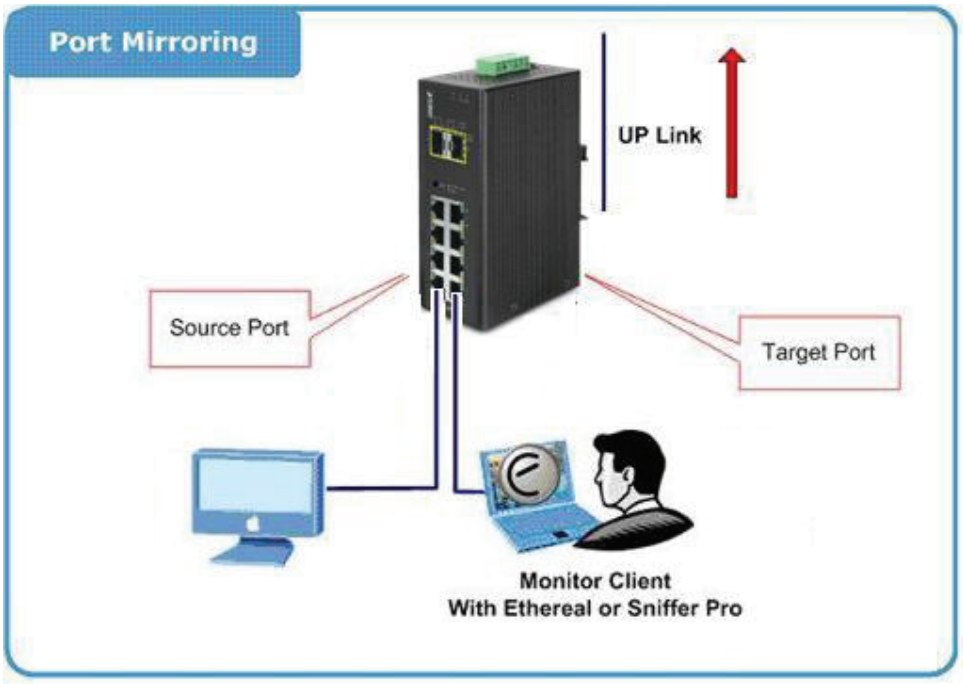


Figure 4-4-5: Port Mirror Application

The traffic to be copied to the mirror port is selected as follows:

- All frames received on a given port (also known as ingress or source mirroring).
- All frames transmitted on a given port (also known as egress or destination mirroring).

- **Mirror Port Configuration**
  The Port Mirror screen in Figure 4-4-6 appears.

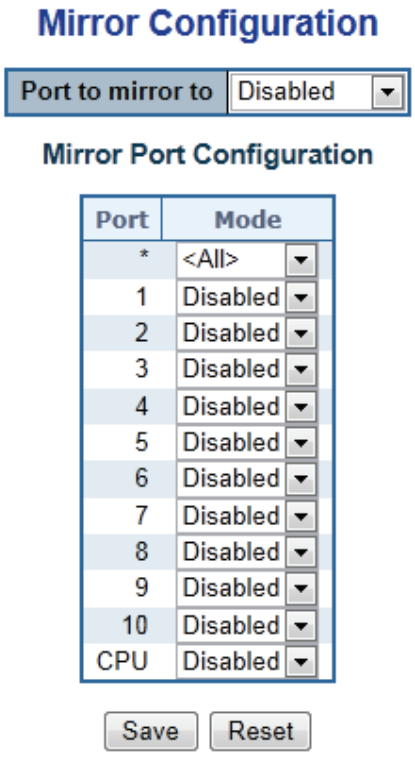


Figure 4-4-6: Mirror Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Port to mirror on**	**Port to mirror** also known as the **mirror port**. Frames from ports that have either source (rx) or destination (tx) mirroring enabled are mirrored on this port. **Disabled** disables mirroring.
• **Port**	The logical port for the settings contained in the same row.
• **Mode**	Select mirror mode. **Rx only**: Frames received at this port are mirrored to the mirroring port. Frames transmitted are not mirrored. **Tx only**: Frames transmitted from this port are mirrored to the mirroring port. Frames received are not mirrored. **Disabled**: Neither frames transmitted or frames received are mirrored. **Both**: Frames received and frames transmitted are mirrored to the mirror port.

Note

For a given port, a frame is only transmitted once. It is therefore not possible to mirror Tx frames on the **mirror port**. Because of this, **mode** for the selected mirror port is limited to **Disabled** or **Rx only**.

4.5 Link Aggregation

Port Aggregation optimizes port usage by linking a group of ports together to form a single Link Aggregated Groups (LAGs). Port Aggregation multiplies the bandwidth between the devices, increases port flexibility, and provides link redundancy.

Each LAG is composed of ports of the same speed, set to full-duplex operations. Ports in a LAG, can be of different media types (UTP/Fiber, or different fiber types), provided they operate at the same speed.

Aggregated Links can be assigned manually (**Port Trunk**) or automatically by enabling Link Aggregation Control Protocol (**LACP**) on the relevant links.

Aggregated Links are treated by the system as a single logical port. Specifically, the Aggregated Link has similar port attributes to a non-aggregated port, including auto-negotiation, speed, Duplex setting, etc.

The device supports the following Aggregation links :

- **Static LAGs** (**Port Trunk**) – Force aggregared selected ports to be a trunk group.
- **Link Aggregation Control Protocol** (**LACP**) LAGs - LACP LAG negotiate Aggregated Port links with other LACP ports located on a different device. If the other device ports are also LACP ports, the devices establish a LAG between them.

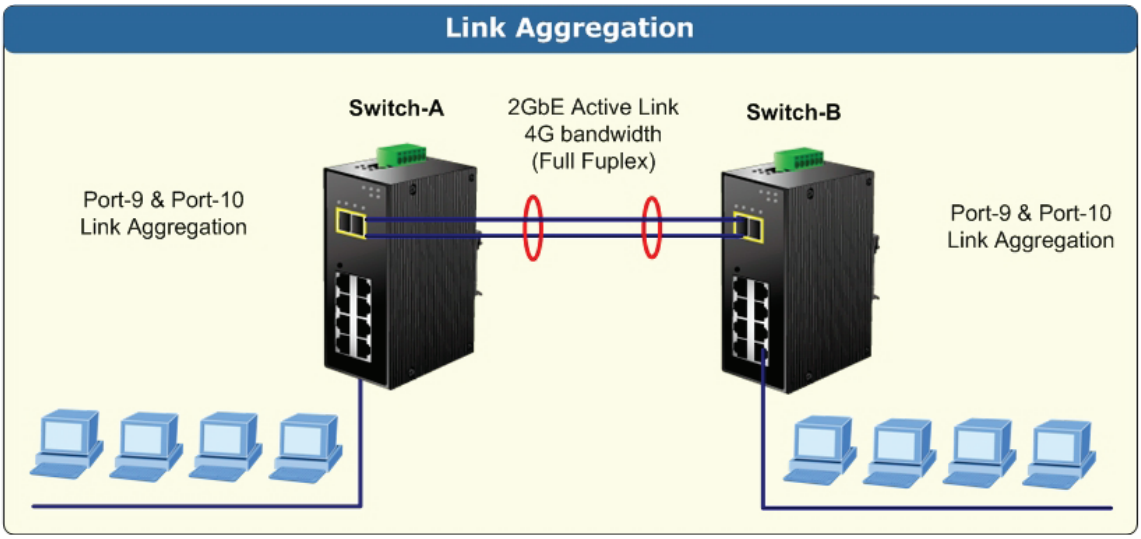


Figure 4-5-1: Link Aggregation Topology

The **Link Aggregation Control Protocol (LACP)** provides a standardized means for exchanging information between Partner Systems that require high speed redundant links. Link aggregation lets you group up to eight consecutive ports into a single dedicated connection. This feature can expand bandwidth to a device on the network. LACP operation requires full-duplex mode, more detail information refer to the IEEE 802.3ad standard.

Port link aggregations can be used to increase the bandwidth of a network connection or to ensure fault recovery. Link aggregation lets you group up to 4 consecutive ports into a single dedicated connection between any two the Switch or other Layer 2 switches. However, before making any physical connections between devices, use the Link aggregation Configuration menu to specify the link aggregation on the devices at both ends. When using a port link aggregation, note that:

- The ports used in a link aggregation must all be of the same media type (RJ-45, 100 Mbps fiber).
- The ports that can be assigned to the same link aggregation have certain other restrictions (see below).
- Ports can only be assigned to one link aggregation.
- The ports at both ends of a connection must be configured as link aggregation ports.
- None of the ports in a link aggregation can be configured as a mirror source port or a mirror target port.
- All of the ports in a link aggregation have to be treated as a whole when moved from/to, added or deleted from a VLAN.
- The Spanning Tree Protocol will treat all the ports in a link aggregation as a whole.
- Enable the link aggregation prior to connecting any cable between the switches to avoid creating a data loop.
- Disconnect all link aggregation port cables or disable the link aggregation ports before removing a port link aggregation to avoid creating a data loop.

It allows a maximum of 10 ports to be aggregated at the same time. The Managed Switch support Gigabit Ethernet ports (up to 5 groups). If the group is defined as a LACP static link aggregationing group, then any extra ports selected are placed in a standby mode for redundancy if one of the other ports fails. If the group is defined as a local static link aggregationing group, then the number of ports must be the same as the group member ports.

The aggregation code ensures that frames belonging to the same frame flow (for example, a TCP connection) are always forwarded on the same link aggregation member port. Reording of frames within a flow is therefore not possible. The aggregation code is based on the following information:

- **Source MAC**
- **Destination MAC**
- **Source and destination IPv4 address.**
- **Source and destination TCP/UDP ports for IPv4 packets**

Normally, all 5 contributions to the aggregation code should be enabled to obtain the best traffic distribution among the link aggregation member ports. Each link aggregation may consist of up to 10 member ports. Any quantity of link aggregation s may be configured for the device (only limited by the quantity of ports on the device.) To configure a proper traffic distribution, the ports within a link aggregation must use the same link speed.

4.5.1 Static Aggregation

This page is used to configure the Aggregation hash mode and the aggregation group. The aggregation hash mode settings are global, whereas the aggregation group relate to the currently selected stack unit, as reflected by the page header.

Hash Code Contributors
The Static Aggeration screen in Figure 4-5-2 appears.

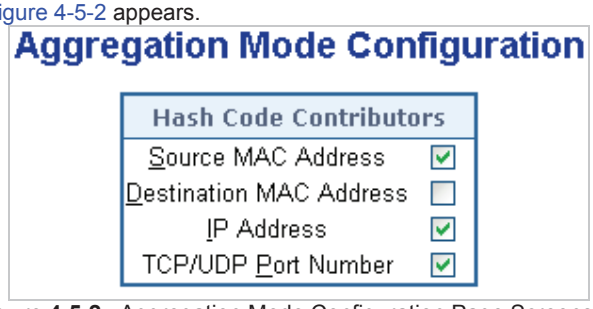


Figure 4-5-2 : Aggregation Mode Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Source MAC Address**	The Source MAC address can be used to calculate the destination port for the frame. Check to enable the use of the Source MAC address, or uncheck to disable. By default, Source MAC Address is enabled.
• **Destination MAC Address**	The Destination MAC Address can be used to calculate the destination port for the frame. Check to enable the use of the Destination MAC Address, or uncheck to disable. By default, Destination MAC Address is disabled.
• **IP Address**	The IP address can be used to calculate the destination port for the frame. Check to enable the use of the IP Address, or uncheck to disable. By default, IP Address is enabled.
• **TCP/UDP Port Number**	The TCP/UDP port number can be used to calculate the destination port for the frame. Check to enable the use of the TCP/UDP Port Number, or uncheck to disable. By default, TCP/UDP Port Number is enabled.

Static Aggregation Group Configuration
The Aggregation Group Configuration screen in Figure 4-5-3 appears.

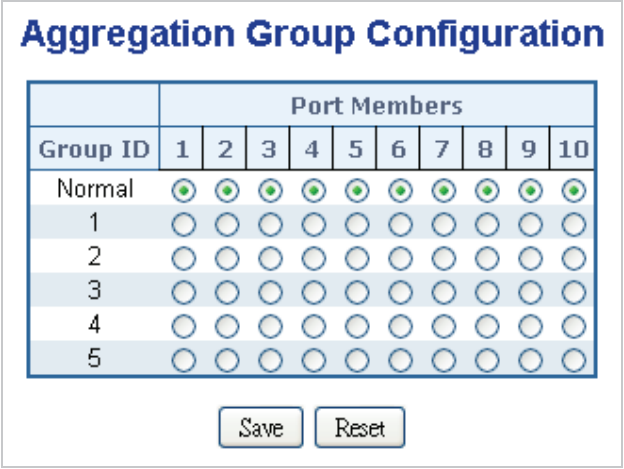


Figure 4-5-3: Aggregation Group Configuration Page Screenshot

The page includes the following fields:

.Object	Description
• **Group ID**	Indicates the group ID for the settings contained in the same row. Group ID "Normal" indicates there is no aggregation. Only one group ID is valid per port.
• **Port Members**	Each switch port is listed for each group ID. Select a radio button to include a port in an aggregation, or clear the radio button to remove the port from the aggregation. By default, no ports belong to any aggregation group. Only full duplex ports can join an aggregation and ports must be in the same speed in each group.

Buttons

: Click to save changes.

: Click to undo any changes made locally and revert to previously saved values.

4.5.2 LACP Configuration

Link Aggregation Control Protocol (LACP) - LACP LAG negotiate Aggregated Port links with other LACP ports located on a different device. LACP allows switches connected to each other to discover automatically whether any ports are member of the same LAG.

This page allows the user to inspect the current LACP port configurations, and possibly change them as well. The LACP port settings relate to the currently selected stack unit, as reflected by the page header. The LACP Configuration screen in Figure 4-5-4 appears.

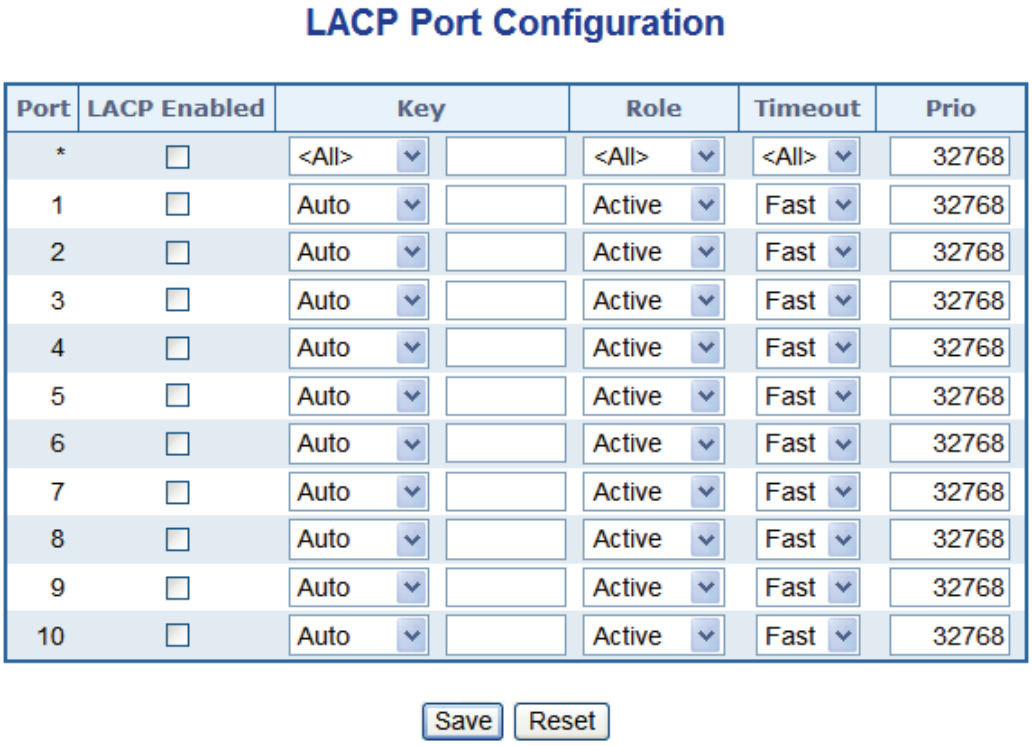


Figure 4-5-4 : LACP Port Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Port**	The switch port number, * means selection of all ports of Industrial Managed Switch.
• **LACP Enabled**	Controls whether LACP is enabled on this switch port. LACP will form an aggregation when 2 or more ports are connected to the same partner. LACP can form max 12 LLAGs per switch and 2 GLAGs per stack.
• **Key**	The Key value incurred by the port, range 1-65535 . The Auto setting will set the key as appropriate by the physical link speed, 10Mb = 1, 100Mb = 2, 1Gb = 3. Using the Specific setting, a user-defined value can be entered. Ports with the same Key value can participate in the same aggregation group, while ports with different keys cannot. The default setting is "**Auto**"
• **Role**	The Role shows the LACP activity status. The Active will transmit LACP packets each second, while Passive will wait for a LACP packet from a partner (speak if spoken to).
• **Timeout**	The Timeout controls the period between BPDU transmissions. Fast will transmit LACP packets each second, while Slow will wait for 30 seconds before sending a LACP packet.
• **Prio**	The `Prio` controls the priority of the port. If the LACP partner wants to form a larger group than is supported by this device then this parameter will control which ports will be active and which ports will be in a backup role. Lower number means greater priority.

Buttons

 : Click to save changes.

 : Click to undo any changes made locally and revert to previously saved values.

4.5.3 LACP System Status

This page provides a status overview for all LACP instances. The LACP Status page displays the current LACP aggregation Groups and LACP Port status. The LACP System Status screen in Figure 4-5-5 appears.

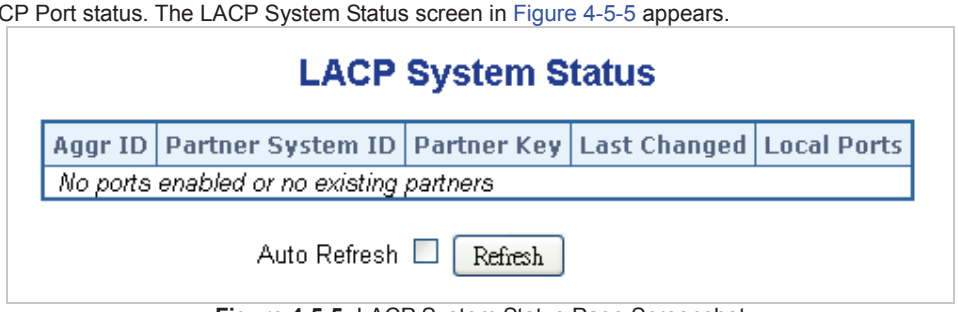


Figure 4-5-5: LACP System Status Page Screenshot

The page includes the following fields:

Object	Description
• **Aggr ID**	The Aggregation ID associated with this aggregation instance. For LLAG the id is shown as 'isid:aggr-id' and for GLAGs as 'aggr-id'
• **Partner System ID**	The system ID (MAC address) of the aggregation partner.
• **Partner Key**	The Key that the partner has assigned to this aggregation ID.
• **Last changed**	The time since this aggregation changed.
• **Local Ports**	Shows which ports are a part of this aggregation for this switch. .

Buttons

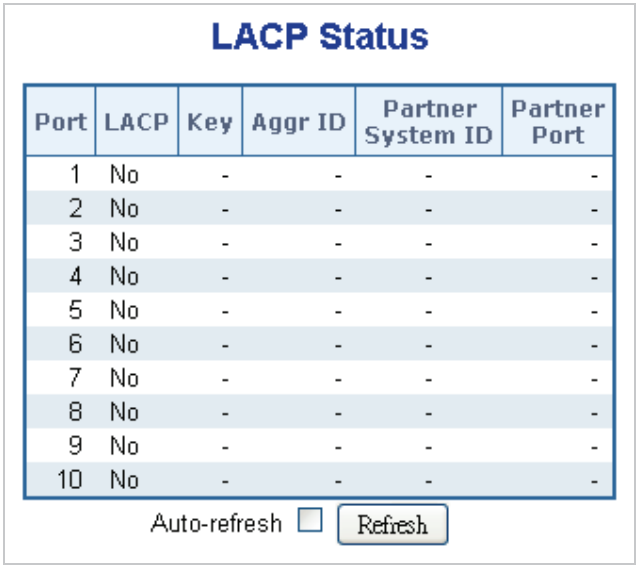


Figure 4-5-6: LACP Status Page Screenshot

The page includes the following fields:

Object	Description
• **Port**	The switch port number.
• **LACP**	'Yes' means that LACP is enabled and the port link is up. 'No' means that LACP is not enabled or that the port link is down. 'Backup' means that the port could not join the aggregation group but will join if other port leaves. Meanwhile it's LACP status is disabled.
• **Key**	The key assigned to this port. Only ports with the same key can aggregate together.
• **Aggr ID**	The Aggregation ID assigned to this aggregation group. IDs 1 and 2 are GLAGs while IDs 3-14 are LLAGs.
• **Partner System ID**	The partners System ID (MAC address).
• **Partner Port**	The partners port number connected to this port.

Buttons

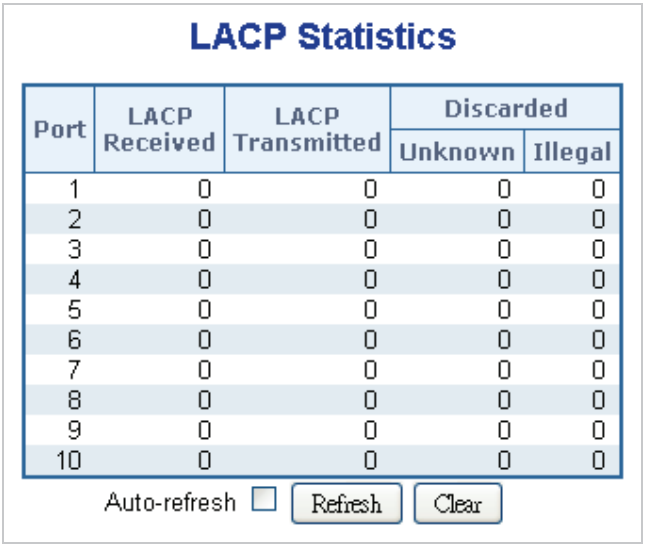


Figure 4-5-7: LACP Statistics Page Screenshot

The page includes the following fields:

Object	Description
• **Port**	The switch port number.
• **LACP Received**	Shows how many LACP frames have been sent from each port.
• **LACP Transmitted**	Shows how many LACP frames have been received at each port.
• **Discarded**	Shows how many unknown or illegal LACP frames have been discarded at each port.

Buttons

Auto-refresh : Automatic refresh occurs every 3 seconds.

4.6 VLAN

4.6.1 VLAN Overview

A Virtual Local Area Network (VLAN) is a network topology configured according to a logical scheme rather than the physical layout. VLAN can be used to combine any collection of LAN segments into an autonomous user group that appears as a single LAN. VLAN also logically segment the network into different broadcast domains so that packets are forwarded only between ports within the VLAN. Typically, a VLAN corresponds to a particular subnet, although not necessarily.

VLAN can enhance performance by conserving bandwidth, and improve security by limiting traffic to specific domains.

A VLAN is a collection of end nodes grouped by logic instead of physical location. End nodes that frequently communicate with each other are assigned to the same VLAN, regardless of where they are physically on the network. Logically, a VLAN can be equated to a broadcast domain, because broadcast packets are forwarded to only members of the VLAN on which the broadcast was initiated.

21. No matter what basis is used to uniquely identify end nodes and assign these nodes VLAN membership, packets cannot cross VLAN without a network device performing a routing function between the VLAN.
22. The Managed Switch supports IEEE 802.1Q VLAN. The port untagging function can be used to remove the 802.1 tag from packet headers to maintain compatibility with devices that are tag-unaware.
23. The Switch's default is to assign all ports to a single 802.1Q VLAN named DEFAULT_VLAN. As new VLAN is created, the member ports assigned to the new VLAN will be removed from the DEFAULT_ VLAN port member list. The DEFAULT_VLAN has a VID = 1.

This section has the following items:

VLAN Basic Information	Displays VLAN information
VLAN Port Configuration	Enables VLAN group
VLAN Memberships	Configures the VLAN membership
VLAN Membership Status	Displays VLAN membership status
VLAN Port Status	Displays VLAN port status
Private VLAN	Creates/removes primary or community VLANs
Port Isolation	Enables/disables port isolation on port
MAC-based VLAN	Configures the MAC-based VLAN entries
MAC-based VLAN Status	Displays MAC-based VLAN entries
IP Subnet-based VLAN	Configures the IP Subnet-based VLAN entries
Protocol-based VLAN	Configures the protocol-based VLAN entries
Protocol-based VLAN Membership	Displays the protocol-based VLAN entries

4.6.2 IEEE 802.1Q VLAN

In large networks, routers are used to isolate broadcast traffic for each subnet into separate domains. This Managed Switch provides a similar service at Layer 2 by using VLANs to organize any group of network nodes into separate broadcast domains. VLANs confine broadcast traffic to the originating group, and can eliminate broadcast storms in large networks. This also provides a more secure and cleaner network environment.

An IEEE 802.1Q VLAN is a group of ports that can be located anywhere in the network, but communicate as though they belong to the same physical segment.

VLANs help to simplify network management by allowing you to move devices to a new VLAN without having to change any physical connections. VLANs can be easily organized to reflect departmental groups (such as Marketing or R&D), usage groups (such as e-mail), or multicast groups (used for multimedia applications such as videoconferencing).

VLANs provide greater network efficiency by reducing broadcast traffic, and allow you to make network changes without having to update IP addresses or IP subnets. VLANs inherently provide a high level of network security since traffic must pass through a configured Layer 3 link to reach a different VLAN.

This Managed Switch supports the following VLAN features:

- Up to 255 VLANs based on the IEEE 802.1Q standard
- Port overlapping, allowing a port to participate in multiple VLANs
- End stations can belong to multiple VLANs
- Passing traffic between VLAN-aware and VLAN-unaware devices
- Priority tagging

IEEE 802.1Q Standard

IEEE 802.1Q (tagged) VLAN are implemented on the Switch. 802.1Q VLAN require tagging, which enables them to span the entire network (assuming all switches on the network are IEEE 802.1Q-compliant).

VLAN allow a network to be segmented in order to reduce the size of broadcast domains. All packets entering a VLAN will only be forwarded to the stations (over IEEE 802.1Q enabled switches) that are members of that VLAN, and this includes broadcast, multicast and unicast packets from unknown sources.

VLAN can also provide a level of security to your network. IEEE 802.1Q VLAN will only deliver packets between stations that are members of the VLAN. Any port can be configured as either **tagging** or **untagging**.:

- The untagging feature of IEEE 802.1Q VLAN allows VLAN to work with legacy switches that don't recognize VLAN tags in packet headers.
- The tagging feature allows VLAN to span multiple 802.1Q-compliant switches through a single physical connection and allows Spanning Tree to be enabled on all ports and work normally.

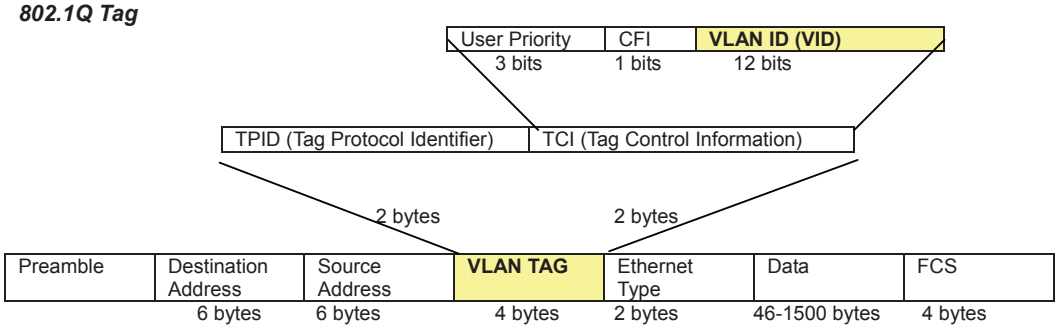
Some relevant terms:
- **Tagging** - The act of putting 802.1Q VLAN information into the header of a packet.
- **Untagging** - The act of stripping 802.1Q VLAN information out of the packet header.

802.1Q VLAN Tags

The figure below shows the 802.1Q VLAN tag. There are four additional octets inserted after the source MAC address. Their presence is indicated by a value of **0x8100** in the Ether Type field. When a packet's Ether Type field is equal to 0x8100, the packet carries the IEEE 802.1Q/802.1p tag. The tag is contained in the following two octets and consists of 3 bits of user priority, 1 bit of Canonical Format Identifier (CFI - used for encapsulating Token Ring packets so they can be carried across Ethernet backbones), and 12 bits of **VLAN ID (VID)**. The 3 bits of user priority are used by 802.1p. The VID is the VLAN identifier and is used by the 802.1Q standard. Because the VID is 12 bits long, 4094 unique VLAN can be identified.

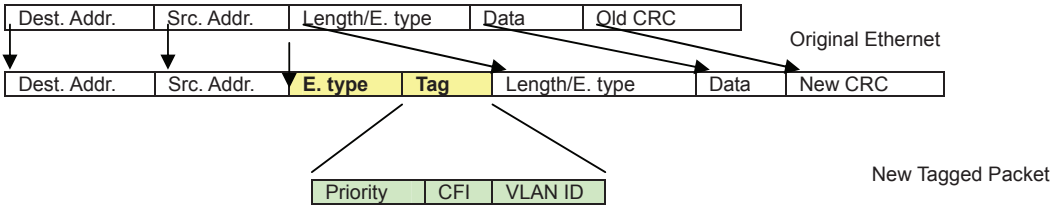
The tag is inserted into the packet header making the entire packet longer by 4 octets. All of the information originally contained in the packet is retained.

802.1Q Tag



The Ether Type and VLAN ID are inserted after the MAC source address, but before the original Ether Type/Length or Logical Link Control. Because the packet is now a bit longer than it was originally, the Cyclic Redundancy Check (CRC) must be recalculated.

Adding an IEEE802.1Q Tag



Port VLAN ID

Packets that are tagged (are carrying the 802.1Q VID information) can be transmitted from one 802.1Q compliant network device to another with the VLAN information intact. This allows 802.1Q VLAN to span network devices (and indeed, the entire network – if all network devices are 802.1Q compliant).

Every physical port on a switch has a PVID. 802.1Q ports are also assigned a PVID, for use within the switch. If no VLAN are defined on the switch, all ports are then assigned to a default VLAN with a PVID equal to 1. Untagged packets are assigned the PVID of the port on which they were received. Forwarding decisions are based upon this PVID, in so far as VLAN are concerned.

Tagged packets are forwarded according to the VID contained within the tag. Tagged packets are also assigned a PVID, but the PVID is not used to make packet forwarding decisions, the VID is.

Tag-aware switches must keep a table to relate PVID within the switch to VID on the network. The switch will compare the VID of a packet to be transmitted to the VID of the port that is to transmit the packet. If the two VID are different the switch will drop the packet. Because of the existence of the PVID for untagged packets and the VID for tagged packets, tag-aware and tag-unaware network devices can coexist on the same network.

A switch port can have only one PVID, but can have as many VID as the switch has memory in its VLAN table to store them.

Because some devices on a network may be tag-unaware, a decision must be made at each port on a tag-aware device before packets are transmitted – should the packet to be transmitted have a tag or not? If the transmitting port is connected to a tag-unaware device, the packet should be untagged. If the transmitting port is connected to a tag-aware device, the packet should be tagged.

Default VLANs

The Switch initially configures one VLAN, VID = 1, called **"default."** The factory default setting assigns all ports on the Switch to the **"default"**. As new VLAN are configured in Port-based mode, their respective member ports are removed from the "default."

Assigning Ports to VLANs

Before enabling VLANs for the switch, you must first assign each port to the VLAN group(s) in which it will participate. By default all ports are assigned to VLAN 1 as untagged ports. Add a port as a tagged port if you want it to carry traffic for one or more VLANs, and any intermediate network devices or the host at the other end of the connection supports VLANs. Then assign ports on the other VLAN-aware network devices along the path that will carry this traffic to the same VLAN(s), either manually or dynamically using GVRP. However, if you want a port on this switch to participate in one or more VLANs, but none of the intermediate network devices nor the host at the other end of the connection supports VLANs, then you should add this port to the VLAN as an untagged port.

VLAN-tagged frames can pass through VLAN-aware or VLAN-unaware network interconnection devices, but the VLAN tags should be stripped off before passing it on to any end-node host that does not support VLAN tagging.

VLAN Classification

When the switch receives a frame, it classifies the frame in one of two ways. If the frame is untagged, the switch assigns the frame to an associated VLAN (based on the default VLAN ID of the receiving port). But if the frame is tagged, the switch uses the tagged VLAN ID to identify the port broadcast domain of the frame.

Port Overlapping

Port overlapping can be used to allow access to commonly shared network resources among different VLAN groups, such as file servers or printers. Note that if you implement VLANs which do not overlap, but still need to communicate, you can connect them by enabled routing on this switch.

Untagged VLANs

Untagged (or static) VLANs are typically used to reduce broadcast traffic and to increase security. A group of network users assigned to a VLAN form a broadcast domain that is separate from other VLANs configured on the switch. Packets are forwarded only between ports that are designated for the same VLAN. Untagged VLANs can be used to manually isolate user groups or subnets.

4.6.3 VLAN Basic Information

The VLAN Basic Information page displays basic information on the VLAN type supported by the Managed Switch.
The VLAN Basic Information screen in Figure 4-6-1 appears.

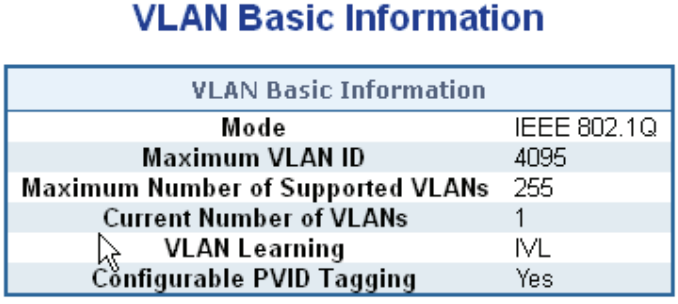


Figure 4-6-1: VLAN Basic Information Page Screenshot

The page includes the following fields:

Object	Description
• **Mode**	Display the current VLAN mode used by this Managed Switch ■ Port-Based ■ IEEE 802.1Q VLAN
• **Maximum VLAN ID**	Maximum VLAN ID recognized by this Industrial Managed Switch.
• **Maximum Number of Supported VLANs**	Maximum number of VLANs that can be configured on this Industrial Managed Switch.
• **Current number of VLANs**	Display the current number of VLANs
• **VLAN Learning**	Display the VLAN learning mode. The Industrial Managed Switch supports IVL (IVL Independent vlan learning).
• **Configurable PVID Tagging**	Indicates whether or not configurable PVID tagging is implemented.

4.6.4 VLAN Port Configuration

This page is used for configuring the Managed Switch port VLAN. The VLAN per Port Configuration page contains fields for managing ports that are part of a VLAN. The port default VLAN ID (PVID) is configured on the VLAN Port Configuration page. All untagged packets arriving to the device are tagged by the ports PVID.

Understand nomenclature of the Switch

■ IEEE 802.1Q Tagged and Untagged

Every port on an 802.1Q compliant switch can be configured as tagged or untagged.

- **Tagged:** Ports with tagging enabled will put the VID number, priority and other VLAN information into the header of all packets that flow into those ports. If a packet has previously been tagged, the port will not alter the packet, thus keeping the VLAN information intact. The VLAN information in the tag can then be used by other 802.1Q compliant devices on the network to make packet-forwarding decisions.
- **Untagged:** Ports with untagging enabled will strip the 802.1Q tag from all packets that flow into those ports. If the packet doesn't have an 802.1Q VLAN tag, the port will not alter the packet. Thus, all packets received by and forwarded by an untagging port will have no 802.1Q VLAN information. (Remember that the PVID is only used internally within the Switch). Untagging is used to send packets from an 802.1Q-compliant network device to a non-compliant network device.

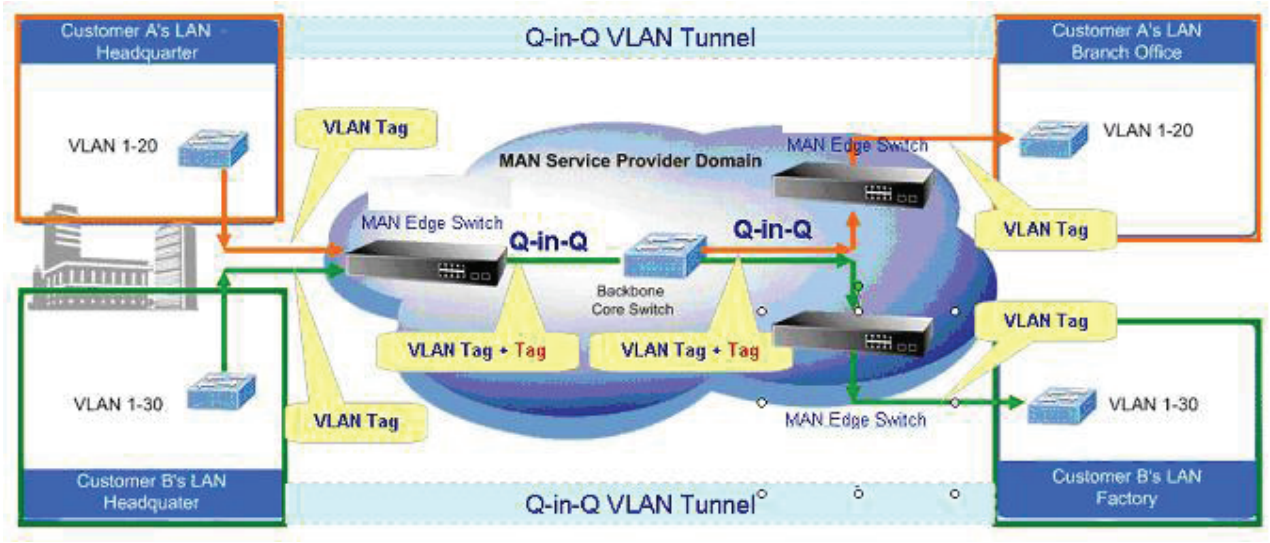
Frame Income / Frame Leave	Income Frame is **tagged**	Income Frame is **untagged**
Leave port is tagged	Frame remains tagged	Tag is inserted
Leave port is untagged	Tag is removed	Frame remain untagged

Table 4-6-1 Ingress/Egress port with VLAN VID Tag/Untag table

■ IEEE 802.1Q Tunneling (Q-in-Q)

IEEE 802.1Q Tunneling (QinQ) is designed for service providers carrying traffic for multiple customers across their networks. QinQ tunneling is used to maintain customer-specific VLAN and Layer 2 protocol configurations even when different customers use the same internal VLAN IDs. This is accomplished by inserting **Service Provider VLAN (SPVLAN)** tags into the customer's frames when they enter the service provider's network, and then stripping the tags when the frames leave the network.

A service provider's customers may have specific requirements for their internal VLAN IDs and number of VLANs supported. VLAN ranges required by different customers in the same service-provider network might easily overlap, and traffic passing through the infrastructure might be mixed. Assigning a unique range of VLAN IDs to each customer would restrict customer configurations, require intensive processing of VLAN mapping tables, and could easily exceed the maximum VLAN limit of 4095.

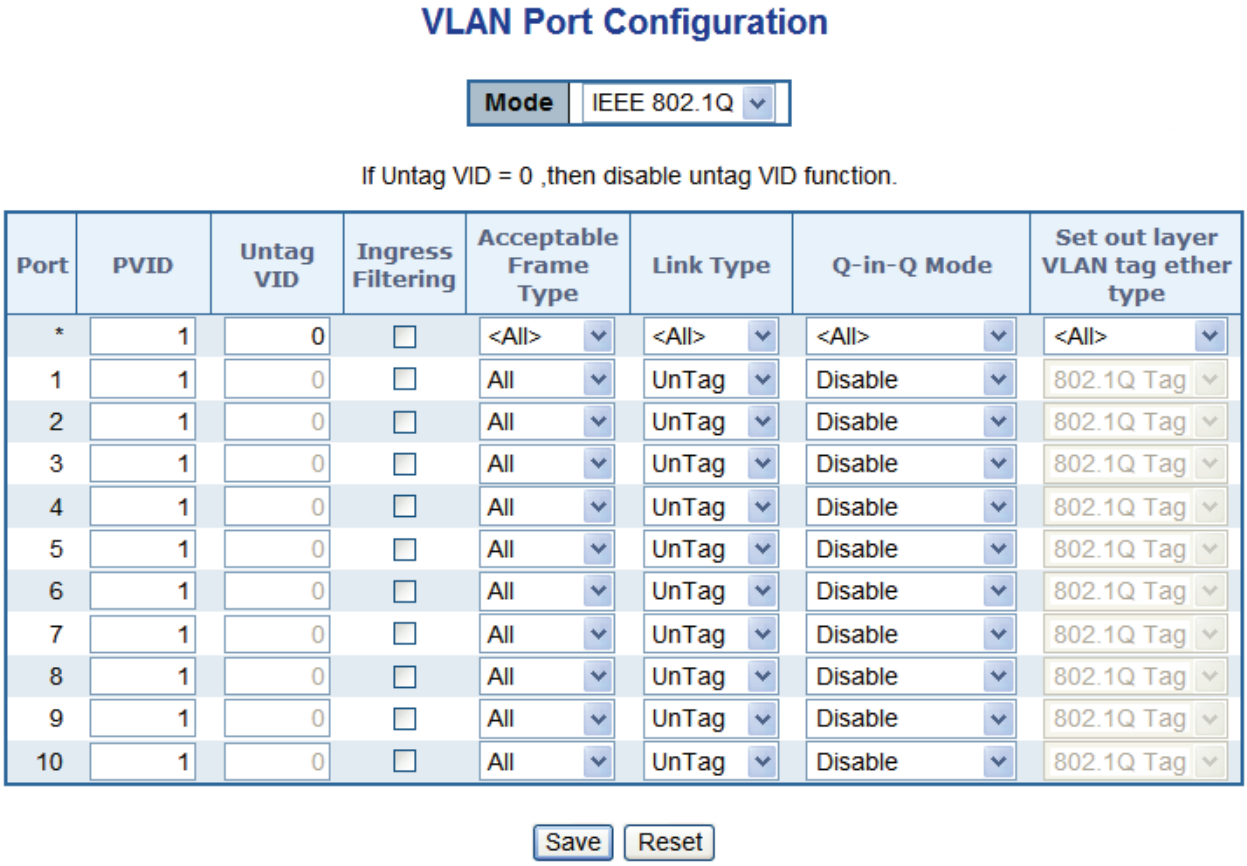


The **Industrial Managed Switch** supports multiple VLAN tags and can therefore be used in MAN applications as a provider bridge, aggregating traffic from numerous independent customer LANs into the **MAN (Metro Access Network)** space. One of the purposes of the provider bridge is to recognize and use VLAN tags so that the VLANs in the MAN space can be used independent of the customers' VLANs. This is accomplished by adding a VLAN tag with a MAN-related VID for frames entering the MAN. When leaving the MAN, the tag is stripped and the original VLAN tag with the customer-related VID is again available.

This provides a tunneling mechanism to connect remote costumer VLANs through a common MAN space without interfering with the VLAN tags. All tags use EtherType **0x8100** or **0x88A8**, where 0x8100 is used for customer tags and 0x88A8 are used for service provider tags.

In cases where a given service VLAN only has two member ports on the switch, the learning can be disabled for the particular VLAN and can therefore rely on flooding as the forwarding mechanism between the two ports. This way, the MAC table requirements is reduced.

VLAN Port Configuration
The VLAN Port Configuration screen in Figure 4-6-2 appears.



Port	PVID	Untag VID	Ingress Filtering	Acceptable Frame Type	Link Type	Q-in-Q Mode	Set out layer VLAN tag ether type
*	1	0	☐	<All>	<All>	<All>	<All>
1	1	0	☐	All	UnTag	Disable	802.1Q Tag
2	1	0	☐	All	UnTag	Disable	802.1Q Tag
3	1	0	☐	All	UnTag	Disable	802.1Q Tag
4	1	0	☐	All	UnTag	Disable	802.1Q Tag
5	1	0	☐	All	UnTag	Disable	802.1Q Tag
6	1	0	☐	All	UnTag	Disable	802.1Q Tag
7	1	0	☐	All	UnTag	Disable	802.1Q Tag
8	1	0	☐	All	UnTag	Disable	802.1Q Tag
9	1	0	☐	All	UnTag	Disable	802.1Q Tag
10	1	0	☐	All	UnTag	Disable	802.1Q Tag

Figure 4-6-2 : VLAN Port Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Port**	This is the logical port number for this row.
• **PVID**	Allows to assign PVID to selected port. The range for the PVID is 1-4094. The PVID will be inserted into all untagged frames entering the ingress port. The PVID must as the same as the VLAN ID in that the port belongs to VLAN group, or the untagged traffic will be dropped.
Ingress Filtering	Enable ingress filtering for a port by checking the box. This parameter affects VLAN ingress processing. If ingress filtering is enabled and the ingress port is not a member of the classified VLAN of the frame, the frame is discarded. By default, ingress filtering is disabled (no checkmark).
• **Accept Frame Type**	Determines whether the port accepts all frames or only tagged frames. This parameter affects VLAN ingress processing. If the port only accepts tagged frames, untagged frames received on the port are discarded. By default, the field is set to All.
24. Link Type	Allow 802.1Q Untagged or Tagged VLAN for selected port. When adding a VLAN to selected port, it tells the switch whether to keep or remove the tag from a frame on egress. ■ **Untag**: outgoing frames without VLAN-Tagged. ■ **Tagged**: outgoing frames with VLAN-Tagged.

25. Q-in-Q Mode	Sets the Managed Switch to QinQ mode, and allows the QinQ tunnel port to be configured. The default is for the Managed Switch to function in Disable mode. ■ **Disable**: The port operates in its normal VLAN mode. (This is the default.) ■ **MAN Port**: Configures IEEE 802.1Q tunneling (QinQ) for an uplink port to another device within the service provider network. ■ **Customer Port**: Configures IEEE 802.1Q tunneling (QinQ) for a client access port to segregate and preserve customer VLAN IDs for traffic crossing the service provider network.
Set Out layer VLAN tag ether type	The Tag Protocol Identifier (TPID) specifies the ethertype of incoming packets on a tunnel access port. ■ **802.1Q Tag**: 8100 ■ **vMAN Tag**: 88A8 Default : 802.1Q Tag

The port must be a member of the same VLAN as the Port VLAN ID.

Buttons

 : Click to save changes.

 : Click to undo any changes made locally and revert to previously saved values.

4.6.5 VLAN Membership

■ **Adding Static Members to VLANs (VLAN Index)**

Use the VLAN Static Table to configure port members for the selected VLAN index. The VLAN membership configuration for the selected stack switch / unit switch can be monitored and modified here. Up to 255 VLANs are supported. This page allows for adding and deleting VLANs as well as adding and deleting port members of each VLAN. The VLAN Membership screen in Figure 4-6-3 appears.

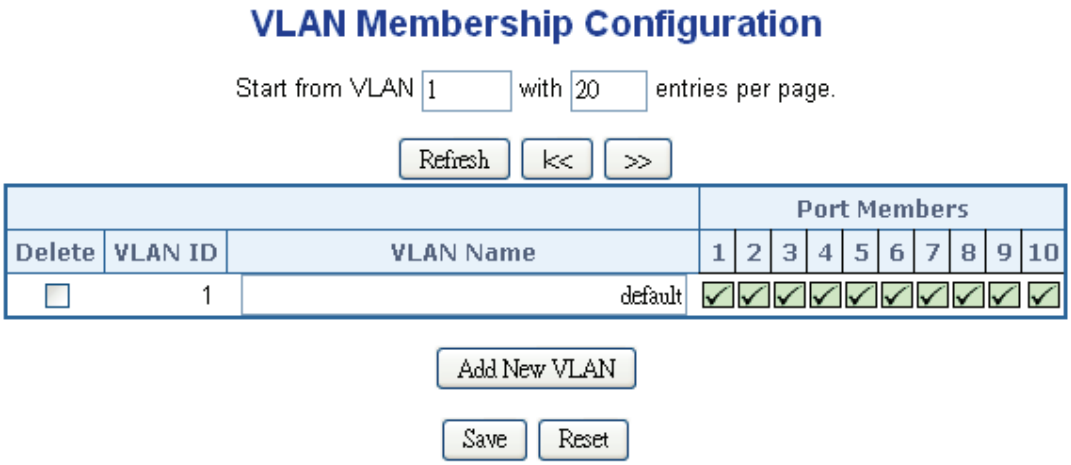


Figure 4-6-3: VLAN Membership Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Delete**	To delete a VLAN entry, check this box. The entry will be deleted on all stack switch units during the next Save.
• **VLAN ID**	Indicates the ID of this particular VLAN.
• **VLAN Name**	Indicates the name of the VLAN. Maximum length of the VLAN Name String is 32. VLAN Name can only contain alphabets or numbers. VLAN name should contain atleast one alphabet. VLAN name can be edited for the existing VLAN entries or it can be added to the new entries.
• **Port Members**	A row of check boxes for each port is displayed for each VLAN ID. To include a port in a VLAN, check the box. To remove or exclude the port from the VLAN, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.
• **Add New VLAN**	Click to add a new VLAN ID. An empty row is added to the table, and the VLAN can be configured as needed. Legal values for a VLAN ID are 1 through 4095. The VLAN is enabled on the selected stack switch unit when you click on "Save". The VLAN is thereafter present on the other stack switch units, but with no port members. A VLAN without any port members on any stack unit will be deleted when you click "Save". The button can be used to undo the addition of new VLANs.

Buttons

[redacted]: Click to add new VLAN.

[redacted]: Click to save changes.

[redacted]: Click to undo any changes made locally and revert to previously saved values.

4.6.6 VLAN Membership Status

This page provides an overview of membership status for VLAN users. The VLAN Membership Status screen in Figure 4-6-4 appears.

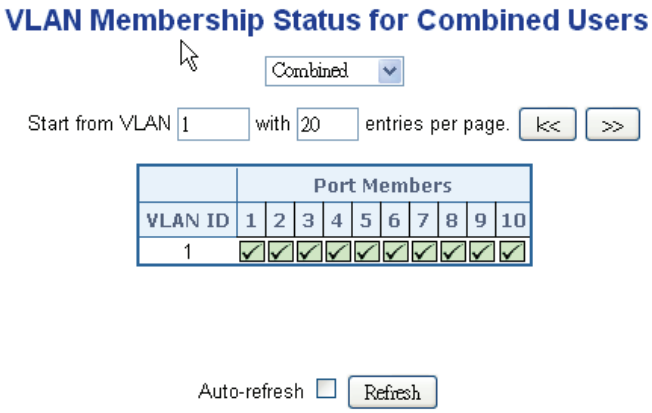


Figure 4-6-4: VLAN Membership Status for Static User Page Screenshot

The page includes the following fields:

Object	Description
• **VLAN ID**	Indicates the ID of this particular VLAN.
• **Port Members**	The VLAN Membership Status Page shall show the current VLAN port members for all VLANs configured by a selected VLAN User (selection shall be allowed by a Combo Box). When ALL VLAN Users is selected, it shall show this information for all the VLAN Users, and this is the default. VLAN membership allows the frames Classified to the VLAN ID to be forwarded to the respective VLAN member ports.
• **VLAN User**	A VLAN User is a module that uses services of the VLAN management functionality to configure VLAN memberships and VLAN port configuration such as PVID and UVID. Currently we support following VLAN : ■ **CLI/Web/SNMP** : This is refered as static. ■ **NAS** : NAS provides port-based authentication, which involves communications between a Supplicant, Authenticator, and an Authentication Server. ■ **MVR** : MVR is used to eliminate the need to duplicate multicast traffic for subscribers in each VLAN. Multicast traffic for all channels is sent only on a single (multicast) VLAN. ■ **Voice VLAN** : Voice VLAN is a VLAN configured specially for voice traffic typically originating from IP phones. ■ **MSTP** : The 802.1s Multiple Spanning Tree protocol (MSTP) uses VLANs to create multiple spanning trees in a network, which significantly improves network resource utilization while maintaining a loop-free environment.

Buttons

[redacted]: Select VLAN Users from this drop down list.

Auto-refresh [redacted]: Check this box to enable an automatic refresh of the page at regular intervals.

4.6.7 VLAN Port Status

This page provides VLAN Port Staus. The VLAN Port Status screen in Figure 4-6-5 appears.

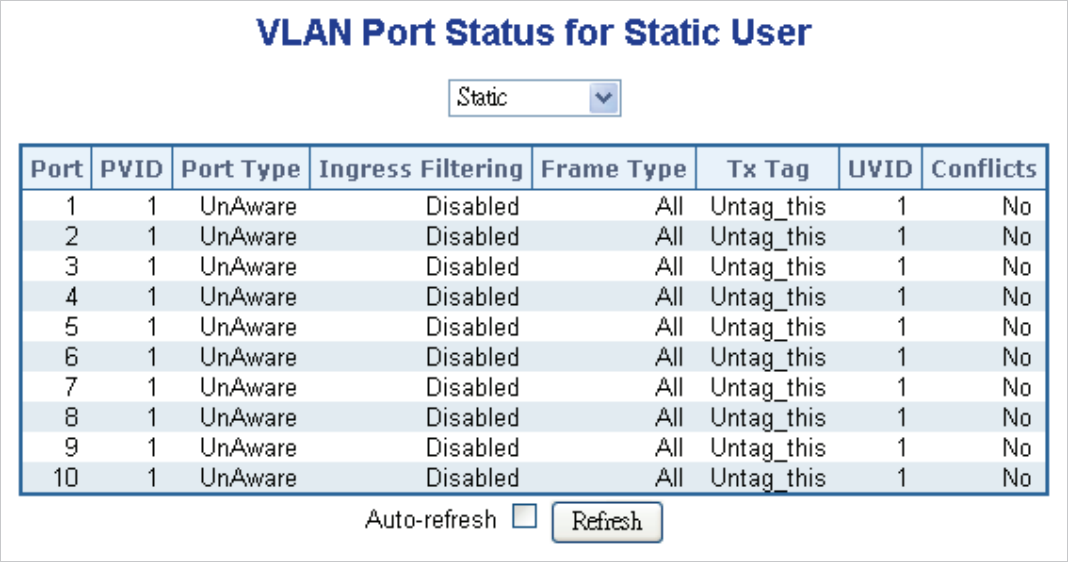


Figure 4-6-5: VLAN Port Status for Static User Page Screenshot

The page includes the following fields:

Object	Description
• **Port**	The logical port for the settings contained in the same row.
• **PVID**	Shows the VLAN identifier for that port. The allowed values are 1 through 4095. The default value is 1.
• **Port Type**	Shows the Port Type. Port type can be any of Unaware, C-port, S-port, Custom S-port. If Port Type is Unaware, all frames are classified to the Port VLAN ID and tags are not removed. C-port is Customer Port. S-port is Service port. Custom S-port is S-port with Custom TPID.
• **Ingress Filtering**	Shows the ingress filtering for a port. This parameter affects VLAN ingress processing. If ingress filtering is enabled and the ingress port is not a member of the classified VLAN of the frame, the frame is discarded.
• **Frame Type**	Shows whether the port accepts all frames or only tagged frames. This parameter affects VLAN ingress processing. If the port only accepts tagged frames, untagged frames received on that port are discarded.
• **Tx Tag**	Shows egress filtering frame status whether tagged or untagged.
• **UVID**	Shows UVID (untagged VLAN ID). Port's UVID determines the packet's behavior at the egress side.
• **Conflicts**	Shows status of Conflicts whether exists or Not. When a Volatile VLAN User requests to set VLAN membership or VLAN port configuration, the following conflicts can occur: Functional Conflicts between feature. Conflicts due to hardware limitation. Direct conflict between user modules.

Buttons

[redacted]: Select VLAN Users from this drop down list.

Auto-refresh [redacted]: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Private VLANs are based on the source port mask, and there are no connections to VLANs. This means that VLAN IDs and Private VLAN IDs can be identical.

A port must be a member of both a VLAN and a Private VLAN to be able to forward packets. By default, all ports are VLAN unaware and members of VLAN 1 and Private VLAN 1.

A VLAN unaware port can only be a member of one VLAN, but it can be a member of multiple Private VLANs.

The Private VLAN screen in Figure 4-6-6 appears.

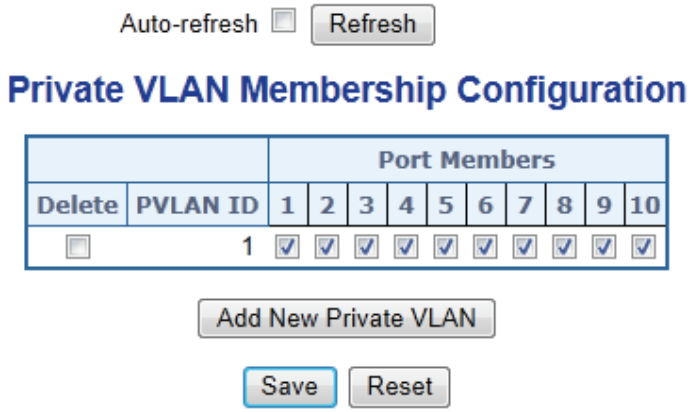


Figure 4-6-6: Private VLAN Membership Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Delete**	To delete a private VLAN entry, check this box. The entry will be deleted during the next Save.
• **Private VLAN ID**	Indicates the ID of this particular private VLAN.
• **Port Members**	A row of check boxes for each port is displayed for each private VLAN ID. To include a port in a Private VLAN, check the box. To remove or exclude the port from the Private VLAN, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.

Buttons

[redacted]: Click to add new VLAN.

[redacted]: Click to save changes.

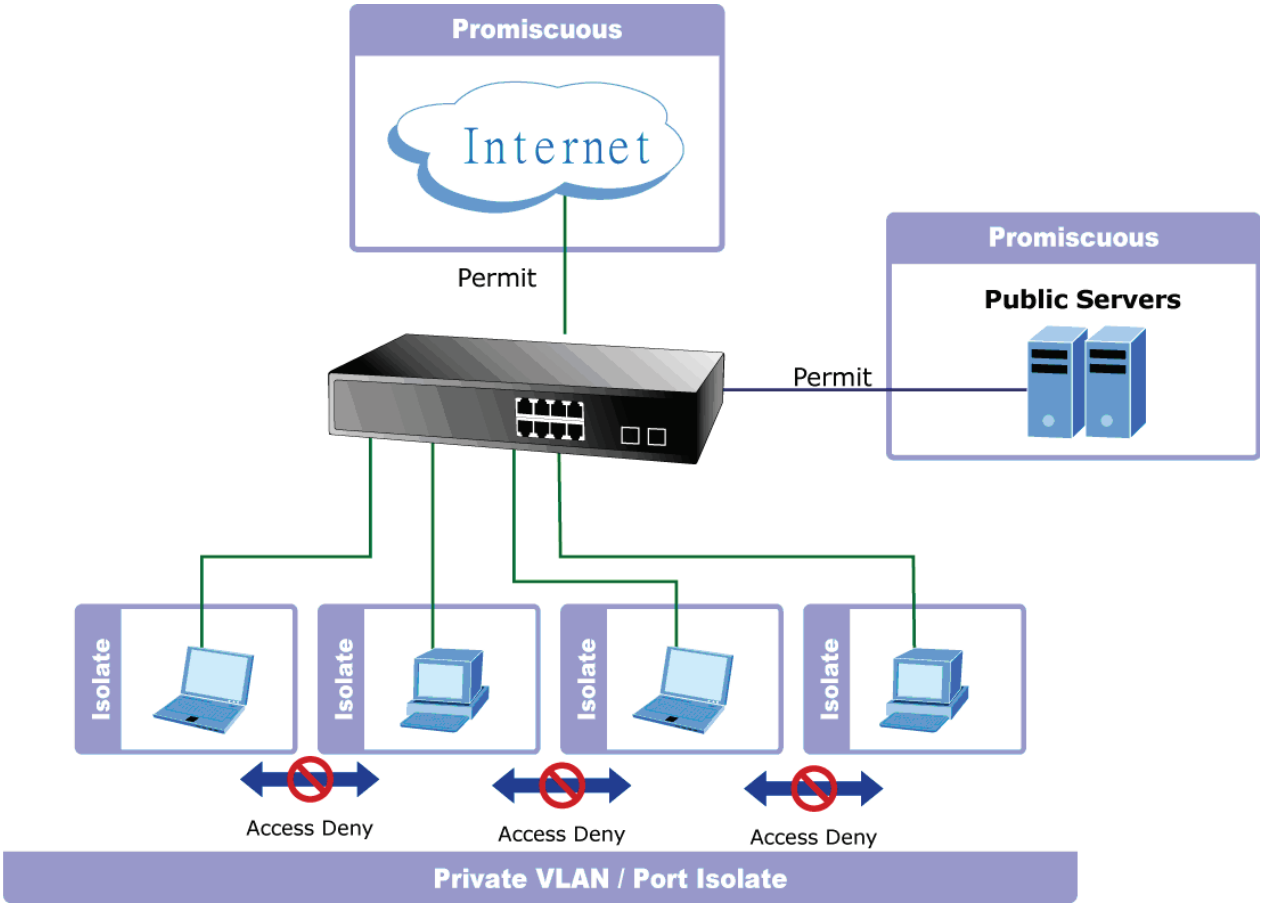
[redacted]: Click to undo any changes made locally and revert to previously saved values.

Auto-refresh [redacted]: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

4.6.9 Port Isolation

Overview
When a VLAN is configured to be a private VLAN, communication between ports within that VLAN can be prevented. Two application examples are provided in this section:

- Customers connected to an ISP can be members of the same VLAN, but they are not allowed to communicate with each other within that VLAN.
- Servers in a farm of web servers in a Demilitarized Zone (DMZ) are allowed to communicate with the outside world and with database servers on the inside segment, but are not allowed to communicate with each other



For private VLANs to be applied, the switch must first be configured for standard VLAN operation. When this is in place, one or more of the configured VLANs can be configured as private VLANs. Ports in a private VLAN fall into one of these two groups:

- **Promiscuous ports**
  - — Ports from which traffic can be forwarded to all ports in the private VLAN
  - — Ports which can receive traffic from all ports in the private VLAN
- **Isolated ports**
  - — Ports from which traffic can only be forwarded to promiscuous ports in the private VLAN
  - — Ports which can receive traffic from only promiscuous ports in the private VLAN

The configuration of promiscuous and isolated ports applies to all private VLANs. When traffic comes in on a promiscuous port in a private VLAN, the VLAN mask from the VLAN table is applied. When traffic comes in on an isolated port, the private VLAN mask is applied in addition to the VLAN mask from the VLAN table. This reduces the ports to which forwarding can be done to just the promiscuous ports within the private VLAN.

This page is used for enabling or disabling port isolation on ports in a Private VLAN. A port member of a VLAN can be isolated to other isolated ports on the same VLAN and Private VLAN. The Port Isolation screen in Figure 4-6-7 appears.

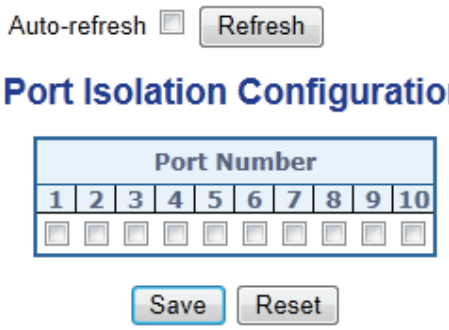


Figure 4-6-7: Port Isolation Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Port Members**	A check box is provided for each port of a private VLAN. When checked, port isolation is enabled on that port. When unchecked, port isolation is disabled on that port. By default, port isolation is disabled on all ports.

Buttons

: Click to save changes.

: Click to undo any changes made locally and revert to previously saved values.

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

4.6.10 VLAN setting example:

- Separate VLAN
- 802.1Q VLAN Trunk
- Port Isolate

4.6.10.1 Two separate 802.1Q VLAN

The diagram shows how the Industrial Managed Switch handle Tagged and Untagged traffic flow for two VLANs. VLAN Group 2 and VLAN Group 3 are separated VLAN. Each VLAN isolates network traffic so only members of the VLAN receive traffic from the same VLAN members. The screen in Figure 4-6-8 appears and Table 4-1 describes the port configuration of the **Industrial Managed Switch**.

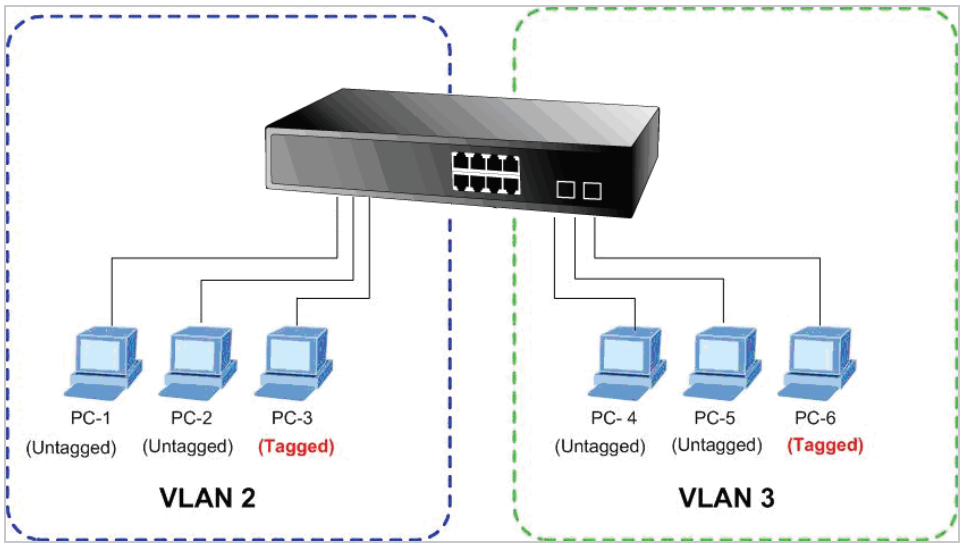


Figure 4-6-8: Two Separate VLAN Diagram

VLAN Group	VID	Untagged Members	Tagged Members
VLAN Group 1	1	Port-7 ~ Port-10	N/A
VLAN Group 2	2	Port-1,Port-2	Port-3
VLAN Group 3	3	Port-4,Port-5	Port-6

Table 4-1: VLAN and Port Configuration

The scenario described as follow:

- **Untagged packet entering VLAN 2**

1. While **[PC-1]** transmitting an **untagged** packet enters **Port-1**, the Managed Switch will tag it with a **VLAN Tag=2**. **[PC-2]** and **[PC-3]** will receive the packet through **Port-2** and **Port-3**.
2. [PC-4],[PC-5] and [PC-6] receive no packet.
3. While the packet leaves **Port-2**, it will be stripped away its tag becoming an **untagged** packet.
4. While the packet leaves **Port-3**, it will keep as a **tagged** packet with **VLAN Tag=2**.

- **Tagged packet entering VLAN 2**

5. While **[PC-3]** transmit a **tagged** packet with **VLAN Tag=2** enters **Port-3**, **[PC-1]** and **[PC-2]** will receive the packet through **Port-1** and **Port-2**.
6. While the packet leaves **Port-1** and **Port-2**, it will be stripped away its tag becoming an **untagged** packet.

- **Untagged packet entering VLAN 3**

1. While **[PC-4]** transmit an **untagged** packet enters **Port-4**, the switch will tag it with a **VLAN Tag=3**. **[PC-5]** and **[PC-6]** will receive the packet through **Port-5** and **Port-6**.
2. While the packet leaves **Port-5**, it will be stripped away it tag becoming an **untagged** packet.
3. While the packet leaves **Port-6**, it will keep as a **tagged** packet with **VLAN Tag=3**.

Note

For this example, just set VLAN Group 1 as default VLAN, but only focus on VLAN 2 and VLAN 3 traffic flow

Setup steps

1. Create VLAN Group

Set VLAN Group 1 = Default-VLAN with VID (VLAN ID) =1
Add two VLANs – VLAN 2 and VLAN 3
VLAN Group 2 with VID=*2*
VLAN Group 3 with VID=*3*

2. Assign VLAN Member :

VLAN 2 : Port-1,Port-2 and Port-3
VLAN 3 : Port-4, Port-5 and Port-6
VLAN 1 : All other ports – Port-7~Port-24

3. Remove VLAN Member for VLAN 1:

Remember to remove Port 1 – Port 6 from VLAN 1 membership, since Port 1 – Port 6 have been assigned to VLAN 2 and VLAN 3.

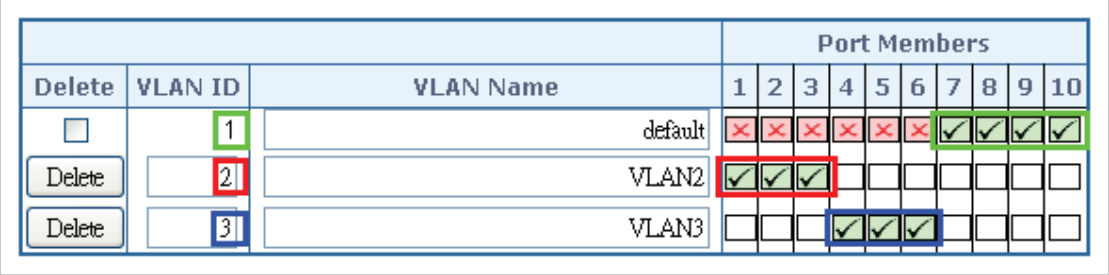


Figure 4-6-9: Add new VLAN group, assign VLAN members to VLAN 2 and VLAN 3 and remove specifed ports from VLAN1 member

Note

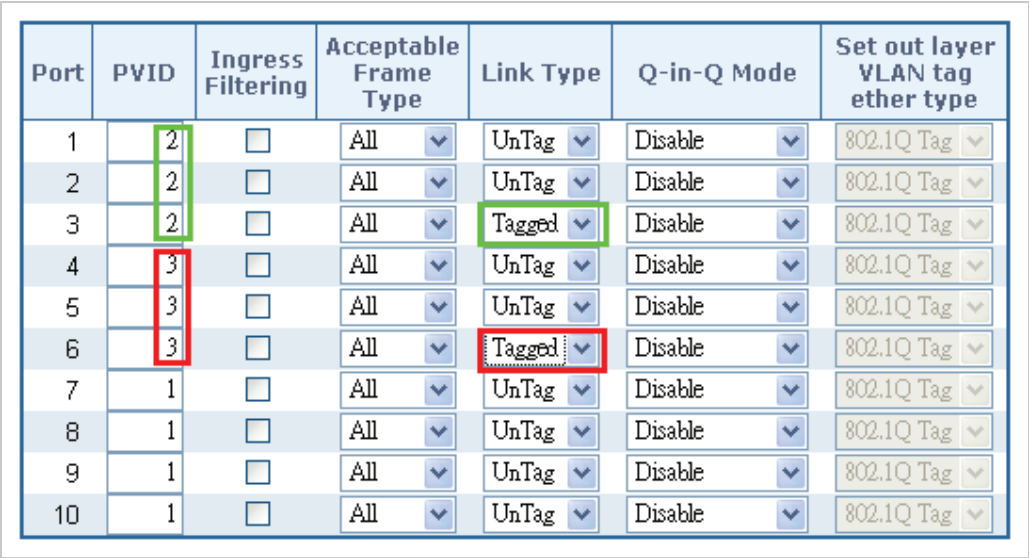
It's important to remove the VLAN members from VLAN 1 configuration. Or the ports would become overlap setting. (About the overlapped VLAN configuration, see next VLAN configure sample)

4. Assign PVID to each port:

Port-1,Port-2 and Port-3 : PVID=*2*
Port-4,Port-5 and Port-6 : PVID=*3*
Port-7~Port-24 : PVID=*1*

5. Enable VLAN Tag for specific ports

Link Type: *Port-3* (VLAN-2) and *Port-6* (VLAN-3)
The Per Port VLAN configuration in Figure 4-6-10 appears.

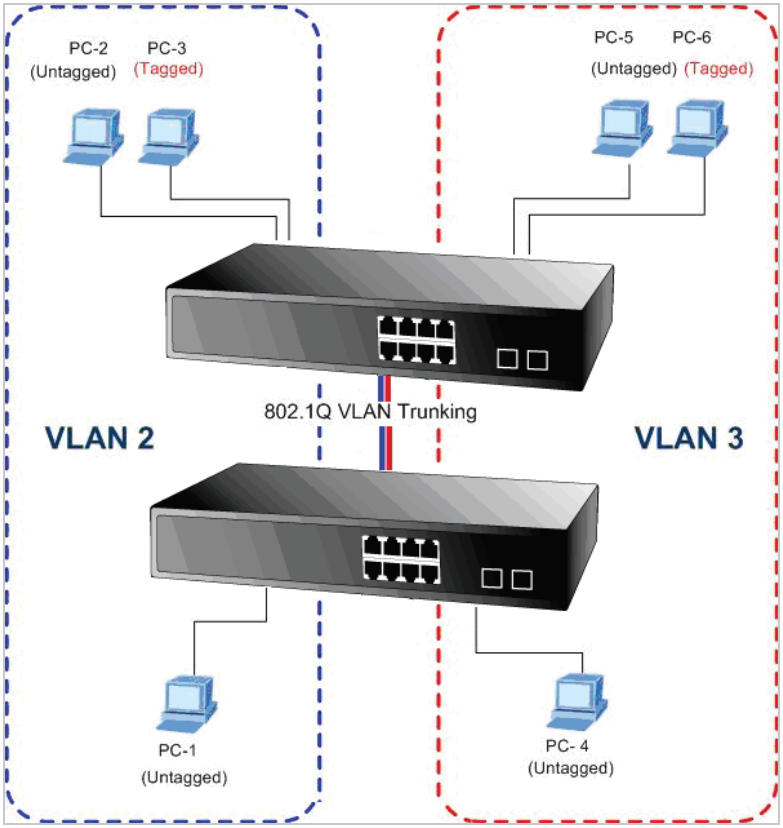


Port	PVID	Ingress Filtering	Acceptable Frame Type	Link Type	Q-in-Q Mode	Set out layer VLAN tag ether type
1	2	☐	All	UnTag	Disable	802.1Q Tag
2	2	☐	All	UnTag	Disable	802.1Q Tag
3	2	☐	All	Tagged	Disable	802.1Q Tag
4	3	☐	All	UnTag	Disable	802.1Q Tag
5	3	☐	All	UnTag	Disable	802.1Q Tag
6	3	☐	All	Tagged	Disable	802.1Q Tag
7	1	☐	All	UnTag	Disable	802.1Q Tag
8	1	☐	All	UnTag	Disable	802.1Q Tag
9	1	☐	All	UnTag	Disable	802.1Q Tag
10	1	☐	All	UnTag	Disable	802.1Q Tag

Figure 4-6-10: Port 1-Port 6 VLAN Configuration

4.6.10.2 VLAN Trunking between two 802.1Q aware Switch

In most cases, it is used for "**Uplink**" to other switches. VLANs are separated at different switches, but they need to access with other switches within the same VLAN group. The screen in Figure 4-6-11 appears.



Setup steps

1. **Create VLAN Group**

Set VLAN Group 1 = Default-VLAN with VID (VLAN ID) =1
Add two VLANs – VLAN 2 and VLAN 3
VLAN Group 2 with VID=*2*
VLAN Group 3 with VID=*3*

2. **Assign VLAN Member :**

VLAN 2 : Port-1,Port-2 and Port-3
VLAN 3 : Port-4, Port-5 and Port-6
VLAN 1 : All other ports – Port-7~Port-24

As to the VLAN ports connecting to the hosts, please refer to 4.6.10.1 examples. The following steps will focus on the VLAN **Trunk port** configuration.

1. Specify **Port-8** to be the 802.1Q VLAN **Trunk port**.
2. Assign **Port-8** to both **VLAN 2** and **VLAN 3** at the VLAN Member configuration page.
3. Define a **VLAN 1** as a **"Public Area"** that overlaps with both **VLAN 2 members** and **VLAN 3 members**.
4. Assign the VLAN Trunk Port to be the member of each VLAN, which wants to be aggregated. For this sample, assign **Port-8** to be **VLAN 2** and **VLAN 3** member port. The screen in Figure 4-6-12 appears.

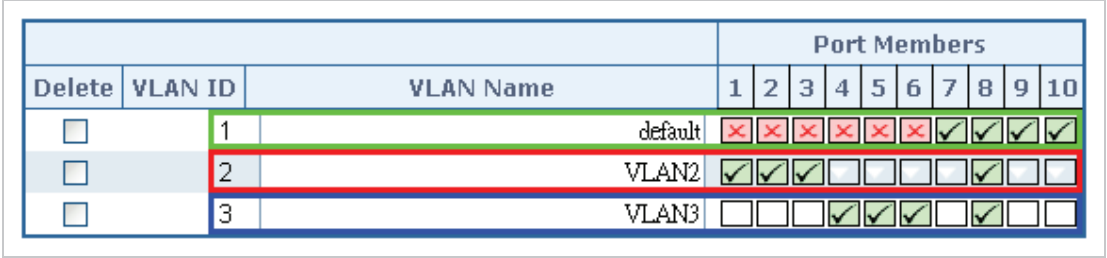


Figure 4-6-12: VLAN overlap port setting & VLAN 1 – The Public Area Member Assign

5. Specify **Port-8** to be the 802.1Q VLAN **Trunk port**, and the Trunking port must be a **Tagged** port while egress. The Port-8 configuration is shown in the following screen in Figure 4-6-13.

Figure 4-6-13: The configuration of VLAN Trunk Port

That is, although the VLAN 2 members: Port-1 to Port-3 and VLAN 3 members: Port-4 to Port-6 also belong to VLAN 1. But with different PVID settings, packets from VLAN 2 or VLAN 3 is not able to access to the other VLAN.

6. Repeat Steps 1 to 5, set up the VLAN Trunk port at the partner switch and add more VLANs to join the VLAN trunk, repeat Steps 1 to 3 to assign the Trunk port to the VLANs.

4.6.10.3 Port Isolate

The diagram shows how the Managed Switch handles isolate and promiscuous ports, and the each PCs are not able to access each other PCs of each isolate port. But they all need to access with the same server/AP/Printer. The screen in Figure 4-6-14 appears. This section will show you how to configure the port for the server – that could be accessed by each isolate port.

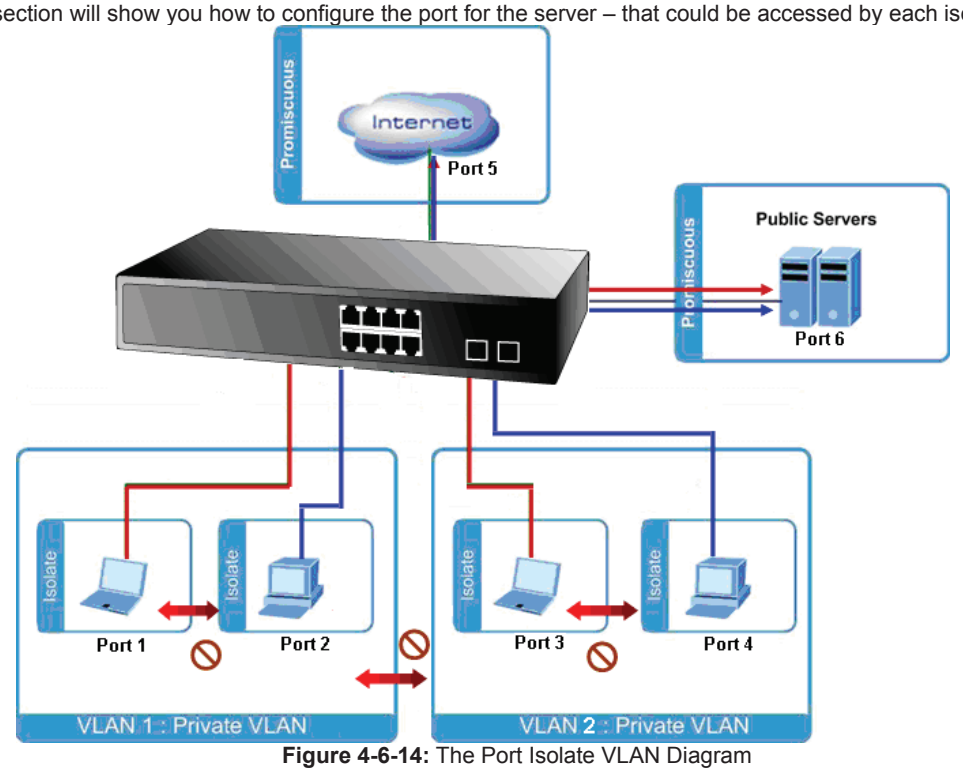


Figure 4-6-14: The Port Isolate VLAN Diagram

Setup steps

1. Assign Port Mode

Set Port-1~Port-4 in Isolate port.
Set Port5 and Port-6 in Promiscuous port. The screen in Figure 4-6-15 appears.

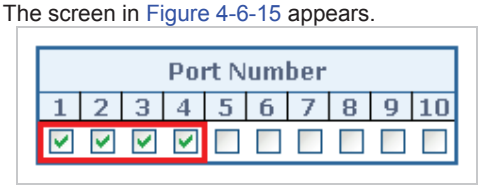


Figure 4-6-15: The Configuration of Isolate and Promiscuous Port

2. Assign VLAN Member :

VLAN 1 : Port-1,Port-2 ,Port-5 and Port-3
VLAN 2 : Port-3~Port-6. The screen in Figure 4-6-16 appears.

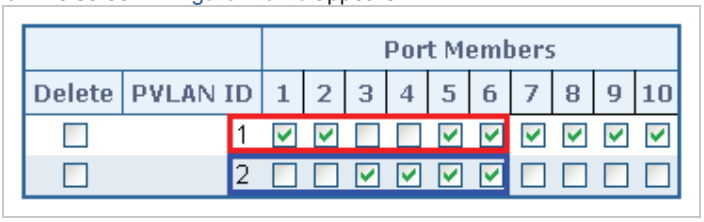


Figure 4-6-16: Private VLAN Port Setting

4.6.11 MAC-based VLAN

The MAC-based VLAN enties can be configured here. This page allows for adding and deleting MAC-based VLAN entries and assigning the entries to different ports. This page shows only static entries. The MAC-based VLAN screen in Figure 4-6-17 appears.

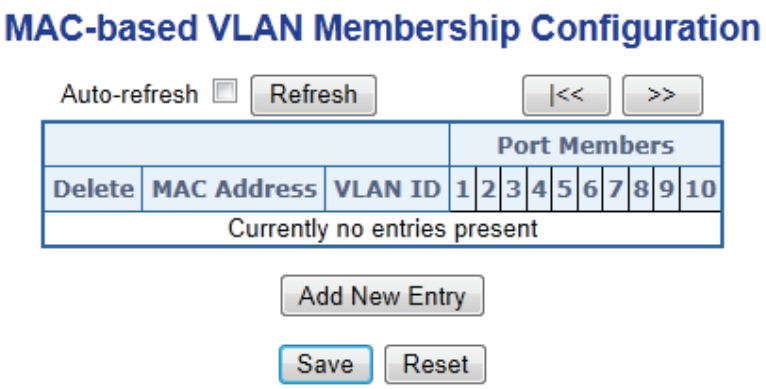


Figure 4-6-17: MAC-based VLAN Membership Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Delete**	To delete a MAC-based VLAN entry, check this box and press save. The entry will be deleted in the stack.
• **MAC Address**	Indicates the MAC address.
• **VLAN ID**	Indicates the VLAN ID.
• **Port Members**	A row of check boxes for each port is displayed for each MAC-based VLAN entry. To include a port in a MAC-based VLAN, check the box. To remove or exclude the port from the MAC-based VLAN, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.

Buttons

[redacted]: Click to add a new MAC-based VLAN entry.

[redacted]: Click to save changes.

[redacted]: Click to undo any changes made locally and revert to previously saved values.

Auto-refresh [redacted]: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

4.6.12 MAC-based VLAN Status

This page shows MAC-based VLAN entries configured by various MAC-based VLAN users. The MAC-based VLAN Status screen in Figure 4-6-18 appears.

Figure 4-6-18: MAC-based VLAN Membership Configuration for User Static Page Screenshot

The page includes the following fields:

Object	Description
• **MAC Address**	Indicates the MAC address.
• **VLAN ID**	Indicates the VLAN ID.
• **Port Members**	Port members of the MAC-based VLAN entry.

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

4.6.13 Protocol-based VLAN

This page allows you to add new protocols to Group Name (unique for each Group) mapping entries as well as allow you to see and delete already mapped entries for the switch. The Protocol-based VLAN screen in Figure 4-6-20 appears.

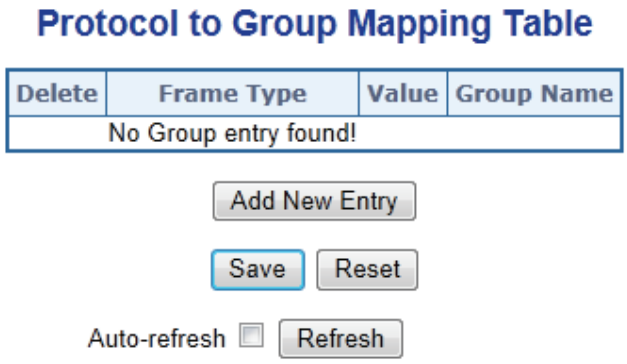


Figure 4-6-20: Protocol to Group Mapping Table Page Screenshot

The page includes the following fields:

Object	Description
• **Delete**	To delete a Protocol to Group Name map entry, check this box. The entry will be deleted on the switch during the next Save.
• **Frame Type**	Frame Type can have one of the following values: 1. **Ethernet** 2. **LLC** 3. **SNAP** Note: On changing the Frame type field, valid value of the following text field will vary depending on the new frame type you select.
• **Value**	Valid value that can be entered in this text field depends on the option selected from the the preceding Frame Type selection menu. Below is the criteria for three different Frame Types: 1. **For Ethernet**: Values in the text field when Ethernet is selected as a Frame Type is called etype. Valid values for etype ranges from 0x0600-0xffff 2. **For LLC**: Valid value in this case is comprised of two different sub-values. a. **DSAP**: 1-byte long string (0x00-0xff) b. **SSAP**: 1-byte long string (0x00-0xff) 3. **For SNAP**: Valid value in this case also is comprised of two different sub-values. a.**OUI**: OUI (Organizationally Unique Identifier) is value in format of xx-xx-xx where each pair (xx) in string is a hexadecimal value ranges from 0x00-0xff. b. **PID**: If the OUI is hexadecimal 000000, the protocol ID is the Ethernet type (EtherType) field value for the protocol running on top of SNAP; if the OUI is an OUI for a particular organization, the protocol ID is a value assigned by that organization to the protocol running on top of SNAP. In other words, if value of OUI field is 00-00-00 then value of PID will be etype (0x0600-0xffff) and if value of OUI is other than 00-00-00 then valid value of PID will be any value from 0x0000 to 0xffff.
• **Group Name**	A valid Group Name is a unique 16-character long string for every entry which consists of a combination of alphabets (a-z or A-Z) and integers(0-9). Note: special character and underscore(_) are not allowed.

Buttons

[redacted]: Click to save changes.

[redacted]: Click to undo any changes made locally and revert to previously saved values.

Auto-refresh [redacted]: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

4.6.14 Protocol-based VLAN Mambership

This page allows you to map an already configured Group Name to a VLAN for the switch. The Group Name to VLAN Mapping Table screen in Figure 4-6-21 appears.

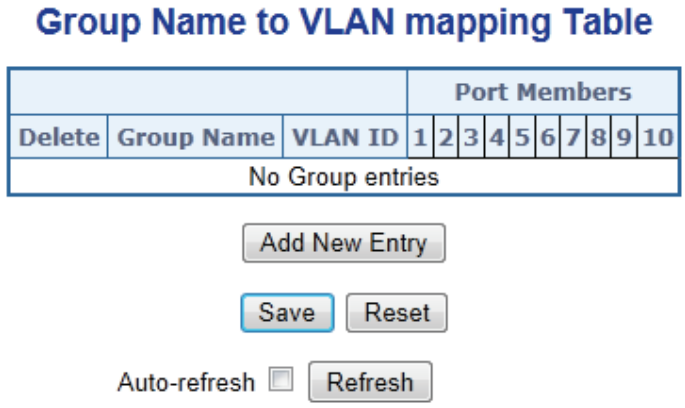


Figure 4-6-21: Group Name to VLAN Mapping Table Page Screenshot

The page includes the following fields:

Object	Description
• **Delete**	To delete a Group Name to VLAN map entry, check this box. The entry will be deleted on the switch during the next Save
• **Group Name**	A valid Group Name is a string of atmost 16 characters which consists of a combination of alphabets (a-z or A-Z) and integers(0-9), no special character is allowed. Whichever Group name you try mapping to a VLAN must be present in Protocol to Group mapping table and must not be preused by any other existing mapping entry on this page.
• **VLAN ID**	Indicates the ID to which Group Name will be mapped. A valid VLAN ID ranges from 1-4095.
• **Port Members**	A row of check boxes for each port is displayed for each Group Name to VLAN ID mapping. To include a port in a mapping, check the box. To remove or exclude the port from the mapping, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.

Buttons

established and duplicated links are blocked automatically. The reactivation of the blocked links (at the time of a primary link failure) is also accomplished automatically without operator intervention.

This automatic network reconfiguration provides maximum uptime to network users. However, the concepts of the Spanning Tree Algorithm and protocol are a complicated and complex subject and must be fully researched and understood. It is possible to cause serious degradation of the performance of the network if the Spanning Tree is incorrectly configured. Please read the following before making any changes from the default values.
The Switch STP performs the following functions:

- Creates a single spanning tree from any combination of switching or bridging elements.
- Creates multiple spanning trees – from any combination of ports contained within a single switch, in user specified groups.
- Automatically reconfigures the spanning tree to compensate for the failure, addition, or removal of any element in the tree.
- Reconfigures the spanning tree without operator intervention.

Bridge Protocol Data Units
For STP to arrive at a stable network topology, the following information is used:

- The unique switch identifier
- The path cost to the root associated with each switch port
- The port identifier

STP communicates between switches on the network using Bridge Protocol Data Units (BPDUs). Each BPDU contains the following information:

- The unique identifier of the switch that the transmitting switch currently believes is the root switch
- The path cost to the root from the transmitting port
- The port identifier of the transmitting port

The switch sends BPDUs to communicate and construct the spanning-tree topology. All switches connected to the LAN on which the packet is transmitted will receive the BPDU. BPDUs are not directly forwarded by the switch, but the receiving switch uses the information in the frame to calculate a BPDU, and, if the topology changes, initiates a BPDU transmission.
The communication between switches via BPDUs results in the following:

- One switch is elected as the root switch
- The shortest distance to the root switch is calculated for each switch
- A designated switch is selected. This is the switch closest to the root switch through which packets will be forwarded to the root.
- A port for each switch is selected. This is the port providing the best path from the switch to the root switch.
- Ports included in the STP are selected.

Creating a Stable STP Topology
It is to make the root port a fastest link. If all switches have STP enabled with default settings, the switch with the lowest MAC address in the network will become the root switch. By increasing the priority (lowering the priority number) of the best switch, STP can be forced to select the best switch as the root switch.
When STP is enabled using the default parameters, the path between source and destination stations in a switched network might not be ideal. For instance, connecting higher-speed links to a port that has a higher number than the current root port can cause a root-port change.

STP Port States
The BPDUs take some time to pass through a network. This propagation delay can result in topology changes where a port that transitioned directly from a Blocking state to a Forwarding state could create temporary data loops. Ports must wait for new network topology information to propagate throughout the network before starting to forward packets. They must also wait for the packet lifetime to expire for BPDU packets that were forwarded based on the old topology. The forward delay timer is used to allow the network topology to stabilize after a topology change. In addition, STP specifies a series of states a port must transition through to further ensure that a stable network topology is created after a topology change.

Each port on a switch using STP exists is in one of the following five states:

- **Blocking** – the port is blocked from forwarding or receiving packets
- **Listening** – the port is waiting to receive BPDU packets that may tell the port to go back to the blocking state
- **Learning** – the port is adding addresses to its forwarding database, but not yet forwarding packets
- **Forwarding** – the port is forwarding packets
- **Disabled** – the port only responds to network management messages and must return to the blocking state first

A port transitions from one state to another as follows:

- From initialization (switch boot) to blocking
- From blocking to listening or to disabled
- From listening to learning or to disabled
- From learning to forwarding or to disabled
- From forwarding to disabled
- From disabled to blocking

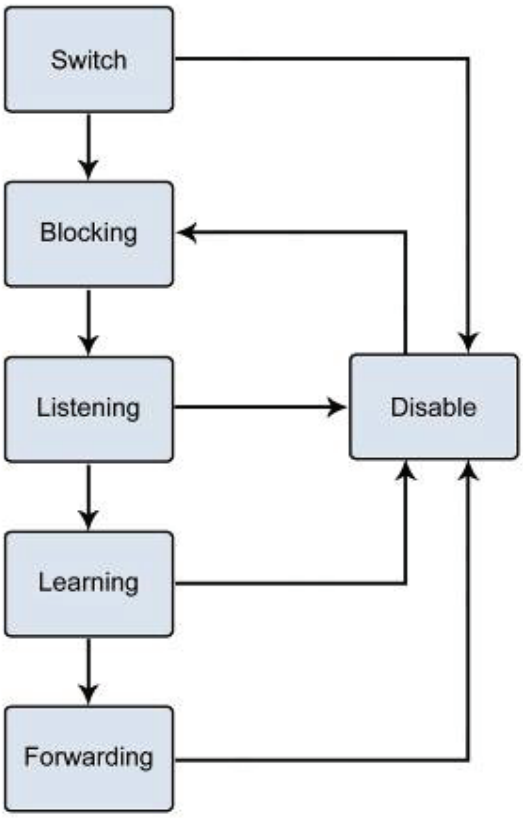


Figure 4-7-1: STP Port State Transitions

You can modify each port state by using management software. When you enable STP, every port on every switch in the network goes through the blocking state and then transitions through the states of listening and learning at power up. If properly configured, each port stabilizes to the forwarding or blocking state. No packets (except BPDUs) are forwarded from, or received by, STP enabled ports until the forwarding state is enabled for that port.

2. STP Parameters
STP Operation Levels
The Switch allows for two levels of operation: the switch level and the port level. The switch level forms a spanning tree consisting of links between one or more switches. The port level constructs a spanning tree consisting of groups of one or more ports. The STP operates in much the same way for both levels.

Note

On the switch level, STP calculates the Bridge Identifier for each switch and then sets the Root Bridge and the Designated Bridges.
On the port level, STP sets the Root Port and the Designated Ports.

The following are the user-configurable STP parameters for the switch level:

Parameter	Description	Default Value
Bridge Identifier(Not user configurable except by setting priority below)	A combination of the User-set priority and the switch's MAC address. The Bridge Identifier consists of two parts: a 16-bit priority and a 48-bit Ethernet MAC address 32768 + MAC	32768 + MAC
Priority	A relative priority for each switch – lower numbers give a higher priority and a greater chance of a given switch being elected as the root bridge	32768
Hello Time	The length of time between broadcasts of the hello message by the switch	2 seconds
Maximum Age Timer	Measures the age of a received BPDU for a	20 seconds

	port and ensures that the BPDU is discarded when its age exceeds the value of the maximum age timer.	
Forward Delay Timer	The amount time spent by a port in the learning and listening states waiting for a BPDU that may return the port to the blocking state.	15 seconds

The following are the user-configurable STP parameters for the port or port group level:

Variable	Description	Default Value
Port Priority	A relative priority for each port –lower numbers give a higher priority and a greater chance of a given port being elected as the root port	128
Port Cost	A value used by STP to evaluate paths – STP calculates path costs and selects the path with the minimum cost as the active path	200,000-100Mbps Fast Ethernet ports 20,000-1000Mbps Gigabit Ethernet ports 0 - Auto

Default Spanning-Tree Configuration

Feature	Default Value
Enable state	STP disabled for all ports
Port priority	128
Port cost	0
Bridge Priority	32,768

User-Changeable STA Parameters
The switch's factory default setting should cover the majority of installations. However, it is advisable to keep the default settings as set at the factory; unless, it is absolutely necessary. The user changeable parameters in the Switch are as follows:
Priority – A Priority for the switch can be set from 0 to 65535. 0 is equal to the highest Priority.

Hello Time – The Hello Time can be from 1 to 10 seconds. This is the interval between two transmissions of BPDU packets sent by the Root Bridge to tell all other Switches that it is indeed the Root Bridge. If you set a Hello Time for your Switch, and it is not the Root Bridge, the set Hello Time will be used if and when your Switch becomes the Root Bridge.

The Hello Time cannot be longer than the Max. Age. Otherwise, a configuration error will occur.

Max. Age – The Max Age can be from 6 to 40 seconds. At the end of the Max. Age, if a BPDU has still not been received from the Root Bridge, your Switch will start sending its own BPDU to all other Switches for permission to become the Root Bridge. If it turns out that your Switch has the lowest Bridge Identifier, it will become the Root Bridge.

Forward Delay Timer – The Forward Delay can be from 4 to 30 seconds. This is the time any port on the

Switch spends in the listening state while moving from the blocking state to the forwarding state.

Observe the following formulas when setting the above parameters:
Max. Age _ 2 x (Forward Delay - 1 second)
Max. Age _ 2 x (Hello Time + 1 second)

Port Priority – A Port Priority can be from 0 to 240. The lower the number, the greater the probability the port will be chosen as the Root Port.

Port Cost – A Port Cost can be set from 0 to 200000000. The lower the number, the greater the probability the port will be chosen to forward packets.

3. Illustration of STP
A simple illustration of three switches connected in a loop is depicted in the below diagram. In this example, you can anticipate some major network problems if the STP assistance is not applied.
If switch A broadcasts a packet to switch B, switch B will broadcast it to switch C, and switch C will broadcast it to back to switch A and so on. The broadcast packet will be passed indefinitely in a loop, potentially causing a network failure. In this example, STP breaks the loop by blocking the connection between switch B and C. The decision to block a particular connection is based on the STP calculation of the most current Bridge and Port settings.
Now, if switch A broadcasts a packet to switch C, then switch C will drop the packet at port 2 and the broadcast will end there. Setting-up STP using values other than the defaults, can be complex. Therefore, you are advised to keep the default factory settings and STP will automatically assign root bridges/ports and block loop connections. Influencing STP to choose a particular switch as the root bridge using the Priority setting, or influencing STP to choose a particular port to block using the Port Priority and Port Cost settings is, however, relatively straight forward.

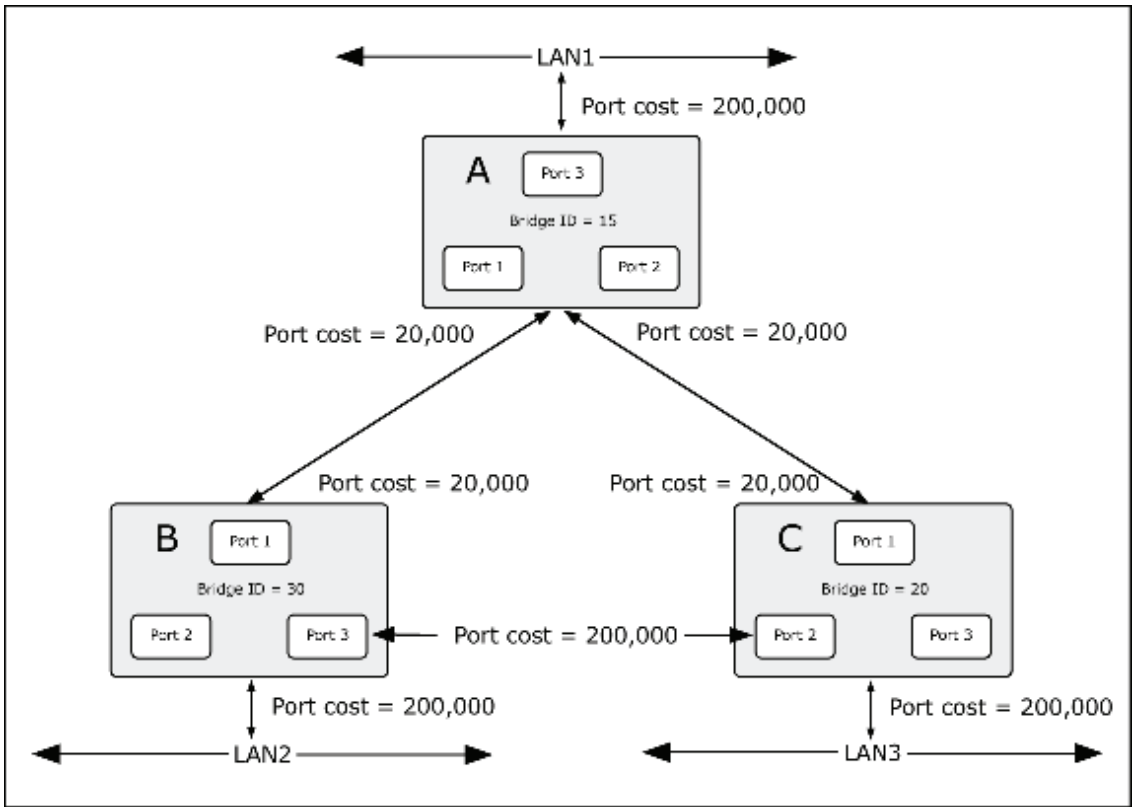


Figure 4-7-2: Before Applying the STA Rules

For this example, only the default STP values are used.

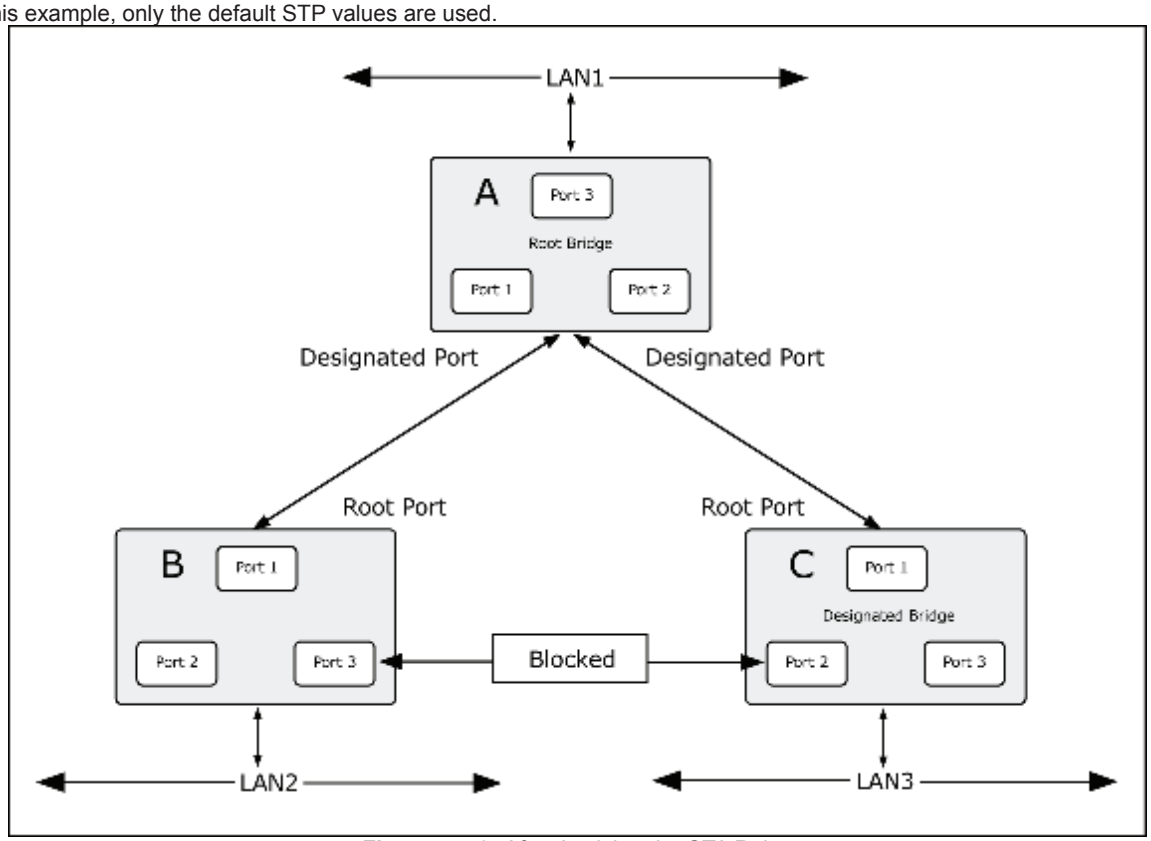


Figure 4-7-3: After Applying the STA Rules

The switch with the lowest Bridge ID (switch C) was elected the root bridge, and the ports were selected to give a high port cost between switches B and C. The two (optional) Gigabit ports (default port cost = 20,000) on switch A are connected to one (optional) Gigabit port on both switch B and C. The redundant link between switch B and C is deliberately chosen as a 100 Mbps Fast Ethernet link (default port cost = 200,000). Gigabit ports could be used, but the port cost should be increased from the

default to ensure that the link between switch B and switch C is the blocked link.

4.7.2 STP System Configuration

This page allows you to configure STP system settings. The settings are used by all STP Bridge instances in the Switch or switch Stack. The Managed Switch support the following Spanning Tree protocols:

- **Compatible -- Spanning Tree Protocol (STP):**Provides a single path between end stations, avoiding and eliminating loops.
- **Normal -- Rapid Spanning Tree Protocol (RSTP) :** Detects and uses of network topologies that provide faster spanning tree convergence, without creating forwarding loops.
- **Extension – Multiple Spanning Tree Protocol (MSTP) :** Defines an extension to RSTP to further develop the usefulness of virtual LANs (VLANs). This "Per-VLAN" Multiple Spanning Tree Protocol configures a separate Spanning Tree for each VLAN group and blocks all but one of the possible alternate paths within each Spanning Tree.

The STP System Configuration screen in Figure 4-7-4 appears.

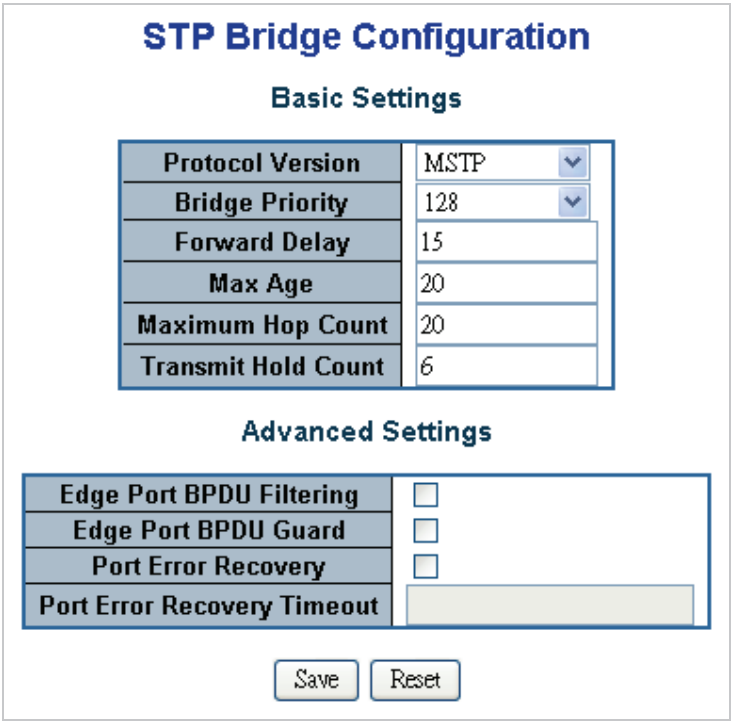


Figure 4-7-4: STP Bridge Configuration Page Screenshot

The page includes the following fields:

Basic Settings

Object	Description
• **Protocol Version**	The STP protocol version setting. Valid values are **STP**, **RSTP** and **MSTP**.
• **Bridge Priority**	Controls the bridge priority. Lower numeric values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms a Bridge Identifier. For MSTP operation, this is the priority of the CIST. Otherwise, this is the priority of the STP/RSTP bridge.
• **Forward Delay**	The delay used by STP Bridges to transition Root and Designated Ports to Forwarding (used in STP compatible mode). Valid values are in the range 4 to 30 seconds -Default: 15 -Minimum: The higher of 4 or [(Max. Message Age / 2) + 1] -Maximum: 30
• **Max Age**	The maximum age of the information transmitted by the Bridge when it is the Root Bridge. Valid values are in the range 6 to 40 seconds. -Default: 20 -Minimum: The higher of 6 or [2 x (Hello Time + 1)]. -Maximum: The lower of 40 or [2 x (Forward Delay -1)]
• **Maximum Hop Count**	This defines the initial value of remaining Hops for MSTI information generated at the boundary of an MSTI region. It defines how many bridges a root bridge can distribute its BPDU information. Valid values are in the range 6 to 40 hops.
• **Transmit Hold Count**	The number of BPDU's a bridge port can send per second. When exceeded, transmission of the next BPDU will be delayed. Valid values are in the range 1 to 10 BPDU's per second.

Advanced Settings

Object	Description
• **Edge Port BPDU Filtering**	Control whether a port explicitly configured as Edge will transmit and receive BPDUs.
• **Edge Port BPDU Guard**	Control whether a port explicitly configured as Edge will disable itself upon reception of a BPDU. The port will enter the error-disabled state, and will be removed from the active topology.
• **Port Error Recovery**	Control whether a port in the error-disabled state automatically will be enabled after a certain time. If recovery is not enabled, ports have to be disabled and re-enabled for normal STP operation. The condition is also cleared by a system reboot.
• **Port Error Recovery Timeout**	The time that has to pass before a port in the *error-disabled* state can be enabled. Valid values are between 30 and 86400 seconds (24 hours).

The **Industrial Managed Switch** implements the Rapid Spanning Protocol as the default spanning tree protocol. While selecting **"Compatible"** mode, the system uses the RSTP (802.1w) to compatible and co work with another STP (802.1D)'s BPDU control packet.

Buttons

 : Click to save changes.

 : Click to undo any changes made locally and revert to previously saved values.

4.7.3 Bridge Status

This page provides a status overview for all STP bridge instances.
The displayed table contains a row for each STP bridge instance, where the column displays the following information: The Bridge Status screen in Figure 4-7-5 appears.

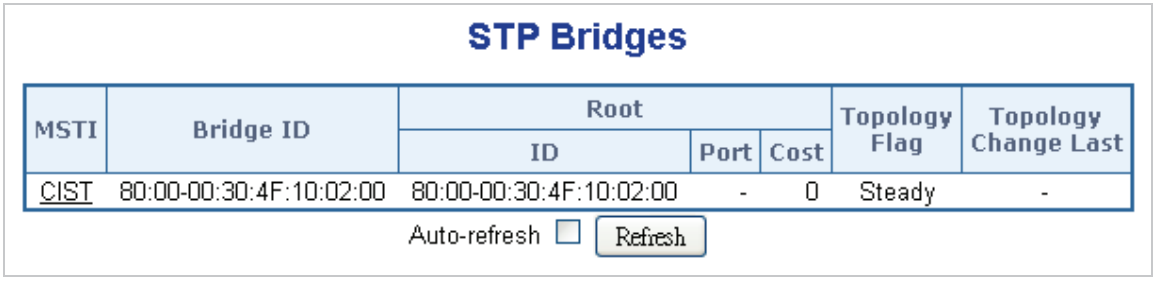


Figure 4-7-5: STP Bridge Status Page Screenshot

The page includes the following fields:

Object	Description
• **MSTI**	The Bridge Instance. This is also a link to the STP Detailed Bridge Status.
• **Bridge ID**	The Bridge ID of this Bridge instance.
• **Root ID**	The Bridge ID of the currently elected root bridge.
• **Root Port**	The switch port currently assigned the *root* port role.
• **Root Cost**	Root Path Cost. For the Root Bridge this is zero. For all other Bridges, it is the sum of the Port Path Costs on the least cost path to the Root Bridge.
• **Topology Flag**	The current state of the Topology Change Flag for this Bridge instance.
• **Topology Change Last**	The time since last Topology Change occurred.

4.7.4 CIST Port Configuration

This page allows the user to inspect the current STP CIST port configurations, and possibly change them as well. The CIST Port Configuration screen in Figure 4-7-6 appears.

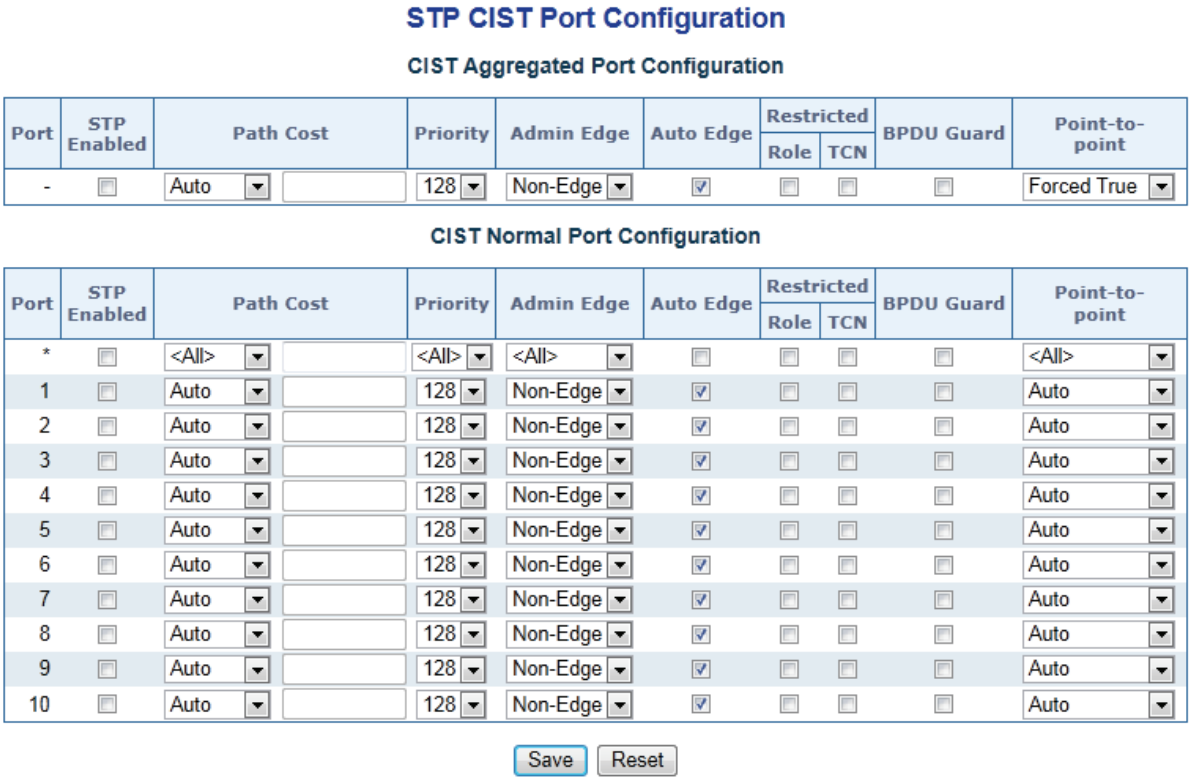


Figure 4-7-6 : STP CIST Port Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Port**	The switch port number of the logical STP port.
• **STP Enabled**	Controls whether RSTP is enabled on this switch port, * means to select all ports of Industrial Managed Switch.
• **Path Cost**	Controls the path cost incurred by the port. The **Auto** setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the **Specific** setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favor of higher path cost ports. Valid values are in the range 1 to 200000000. **All** means all ports will have one specific setting.
• **Priority**	Controls the port priority. This can be used to control priority of ports having identical port cost. (See above). Default: **128** Range: 0-240, in steps of 16 **All** means all ports will have one specific setting.
• **operEdge (state flag)**	Operational flag describing whether the port is connecting directly to edge devices. (No Bridges attached). Transition to the forwarding state is faster for edge ports (having *operEdge* true) than for other ports.The value of this flag is based on AdminEdge and AutoEdge fields. This flag is displayed as Edge in Monitor->Spanning Tree -> STP Detailed Bridge Status.
• **Admin Edge**	Controls whether the operEdge flag should start as beeing set or cleared. (The initial operEdge state when a port is initialized). **All** means all ports will have one specific setting.
• **Auto Edge**	Controls whether the bridge should enable automatic edge detection on the bridge port. This allows operEdge to be derived from whether BPDU's are received on the port or not.

• **Restricted Role**	If enabled, causes the port not to be selected as Root Port for the CIST or any MSTI, even if it has the best spanning tree priority vector. Such a port will be selected as an Alternate Port after the Root Port has been selected. If set, it can cause lack of spanning tree connectivity. It can be set by a network administrator to prevent bridges external to a core region of the network influence the spanning tree active topology, possibly because those bridges are not under the full control of the administrator. This feature is also known as **Root Guard**.
• **Restricted TCN**	If enabled, causes the port not to propagate received topology change notifications and topology changes to other ports. If set it can cause temporary loss of connectivity after changes in a spanning tree's active topology as a result of persistently incorrect learned station location information. It is set by a network administrator to prevent bridges external to a core region of the network, causing address flushing in that region, possibly because those bridges are not under the full control of the administrator or the physical link state of the attached LANs transits frequently.
• **BPDU Guard**	If enabled, causes the port to disable itself upon receiving valid BPDU's. Contrary to the similar bridge setting, the port **Edge** status does not effect this setting. A port entering error-disabled state due to this setting is subject to the bridge Port Error Recovery setting as well.
• **Point-to-Point**	Controls whether the port connects to a point-to-point LAN rather than a shared medium. This can be automatically determined, or forced either true or false. A transition to the forwarding state is faster for point-to-point LANs than for shared media. **All** means all ports will have one specific setting.

Buttons

 : Click to save changes.

 : Click to undo any changes made locally and revert to previously saved values.

By default, the system automatically detects the speed and duplex mode used on each port, and configures the path cost according to the values shown below. Path cost “0” is used to indicate auto-configuration mode. When the short path cost method is selected and the default path cost recommended by the IEEE 802.1w standard exceeds 65,535, the default is set to 65,535.

Port Type	IEEE 802.1D-1998	IEEE 802.1w-2001
Ethernet	50-600	200,000-20,000,000
Fast Ethernet	10-60	20,000-2,000,000
Gigabit Ethernet	3-10	2,000-200,000

Table 4-7-1: Recommended STP Path Cost Range

Port Type	Link Type	IEEE 802.1D-1998	IEEE 802.1w-2001
Ethernet	Half Duplex Full Duplex Trunk	100 95 90	2,000,000 1,999,999 1,000,000
Fast Ethernet	Half Duplex Full Duplex Trunk	19 18 15	200,000 100,000 50,000
Gigabit Ethernet	Full Duplex Trunk	4 3	10,000 5,000

Table 4-7-2: Recommended STP Path Costs

Port Type	Link Type	IEEE 802.1w-2001
Ethernet	Half Duplex Full Duplex Trunk	2,000,000 1,000,000 500,000
Fast Ethernet	Half Duplex Full Duplex Trunk	200,000 100,000 50,000
Gigabit Ethernet	Full Duplex Trunk	10,000 5,000

Table 4-7-3: Default STP Path Costs

4.7.5 MSTI Priorities

This page allows the user to inspect the current STP MSTI bridge instance priority configurations, and possibly change them as well. The MSTI Priority screen in Figure 4-7-7 appears.

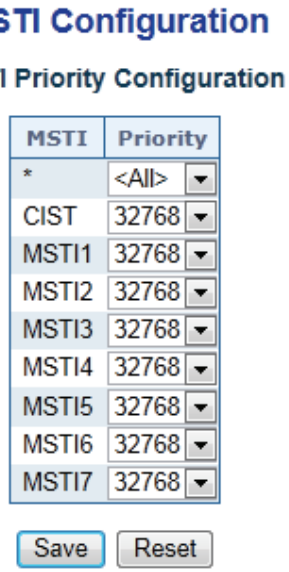


Figure 4-7-7: MSTI Priority Page Screenshot

The page includes the following fields:

Object	Description
• **MSTI**	The bridge instance. The CIST is the default instance, which is always active.
• **Priority**	The Configuration All with available values will assign to whole items. Controls the bridge priority. Lower numerical values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms a Bridge Identifier, * means all MSTI items will have one priority setting.

Buttons

 : Click to save changes.

 : Click to undo any changes made locally and revert to previously saved values.

4.7.6 MSTI Configuration

This page allows the user to inspect the current STP MSTI bridge instance priority configurations, and possibly change them as well. The MSTI Configuration screen in Figure 4-7-8 appears.

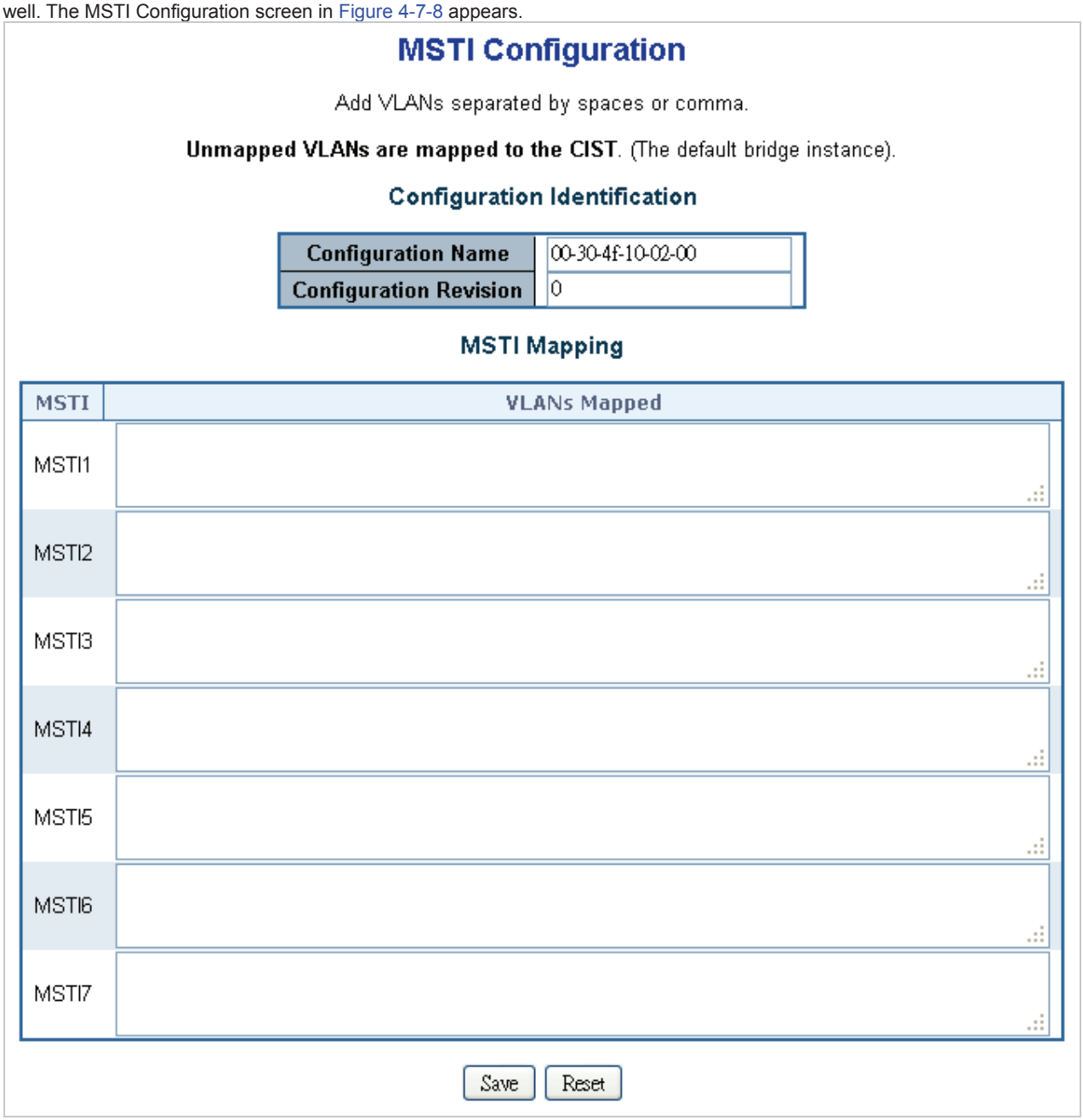


Figure 4-7-8: MSTI Configuration Page Screenshot

The page includes the following fields:

Configuration Identification

Object	Description
• **Configuration Name**	The name identifiying the VLAN to MSTI mapping. Bridges must share the name and revision (see below), as well as the VLAN-to-MSTI mapping configuration in order to share spanning trees for MSTI's. (Intra-region). The name is at most 32 characters.
• **Configuration Revision**	The revision of the MSTI configuration named above. This must be an integer between 0 and 65535.

MSTI Mapping

Object	Description
• **MSTI**	The bridge instance. The CIST is not available for explicit mapping, as it will receive the VLANs not explicitly mapped.
• **VLANs Mapped**	The list of VLAN's mapped to the MSTI. The VLANs must be separated with comma and/or space. A VLAN can only be mapped to *one* MSTI. A unused MSTI should just be left empty. (I.e. not having any VLANs mapped to it.)

Buttons

 : Click to save changes.

 : Click to undo any changes made locally and revert to previously saved values.

4.7.7 MSTI Ports Configuration

This page allows the user to inspect the current STP MSTI port configurations, and possibly change them as well.
A MSTI port is a virtual port, which is instantiated separately for each active CIST (physical) port for each MSTI instance configured and applicable for the port. The MSTI instance must be selected before displaying actual MSTI port configuration options.

This page contains MSTI port settings for physical and aggregated ports. The aggregation settings are stack global. The MSTI Port Configuration screen in Figure 4-7-9 & Figure 4-7-10 appears.

Figure 4-7-9: MSTI Port Configuration Page Screenshot

The page includes the following fields:

MSTI Port Configuration

Object	Description
• **Select MSTI**	Select the bridge instance and set more detail configuration.

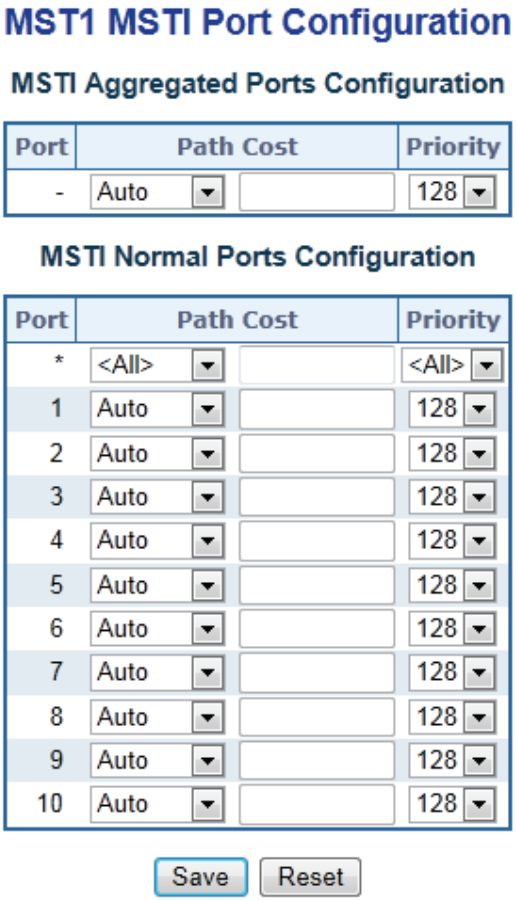


Figure 4-7-10: MST1 MSTI Port Configuration Page Screenshot

The page includes the following fields:

MSTx MSTI Port Configuration

Object	Description

• **Port**	The switch port number of the corresponding STP CIST (and MSTI) port.
• **Path Cost**	The Configuration All with available values will assign to whole items. Controls the path cost incurred by the port. The Auto setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the Specific setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favor of higher path cost ports. Valid values are in the range 1 to 200000000. **All** means all ports will have one specific setting.
• **Priority**	The Configuration All with available values will assign to whole items. Controls the port priority. This can be used to control priority of ports having identical port cost. (See above). **All** means all ports will have one specific setting.

Buttons

[redacted]: Click to set MSTx configuration

[redacted]: Click to save changes.

[redacted]: Click to undo any changes made locally and revert to previously saved values.

4.7.8 Port Status

This page displays the STP CIST port status for port physical ports in the currently selected switch.
The STP Port Status screen in Figure 4-7-11 appears.

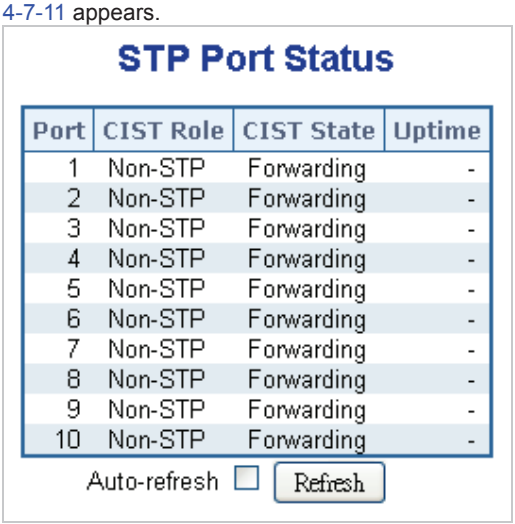


Figure 4-7-11: STP Port Status Page Screenshot

The page includes the following fields:

Object	Description
• **Port**	The switch port number of the logical STP port.
• **CIST Role**	The current STP port role of the ICST port. The port role can be one of the following values: ■ **AlternatePort** ■ **BackupPort** ■ **RootPort** ■ **DesignatedPort**
• **CIST State**	The current STP port state of the CIST port . The port state can be one of the following values: ■ **Disabled** ■ **Blocking** ■ **Learning** ■ **Forwarding** ■ **Non-STP**
• **Uptime**	The time since the bridge port was last initialized.

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

4.8 Multicast

4.8.1 IGMP Snooping

The **Internet Group Management Protocol (IGMP)** lets host and routers share information about multicast groups memberships. IGMP snooping is a switch feature that monitors the exchange of IGMP messages and copies them to the CPU for feature processing. The overall purpose of IGMP Snooping is to limit the forwarding of multicast frames to only ports that are a member of the multicast group.

About the Internet Group Management Protocol (IGMP) Snooping

Computers and network devices that want to receive multicast transmissions need to inform nearby routers that they will become members of a multicast group. The **Internet Group Management Protocol (IGMP)** is used to communicate this information. IGMP is also used to periodically check the multicast group for members that are no longer active. In the case where there is more than one multicast router on a sub network, one router is elected as the 'queried'. This router then keeps track of the membership of the multicast groups that have active members. The information received from IGMP is then used to determine if multicast packets should be forwarded to a given sub network or not. The router can check, using IGMP, to see if there is at least one member of a multicast group on a given subnet work. If there are no members on a sub network, packets will not be forwarded to that sub network.

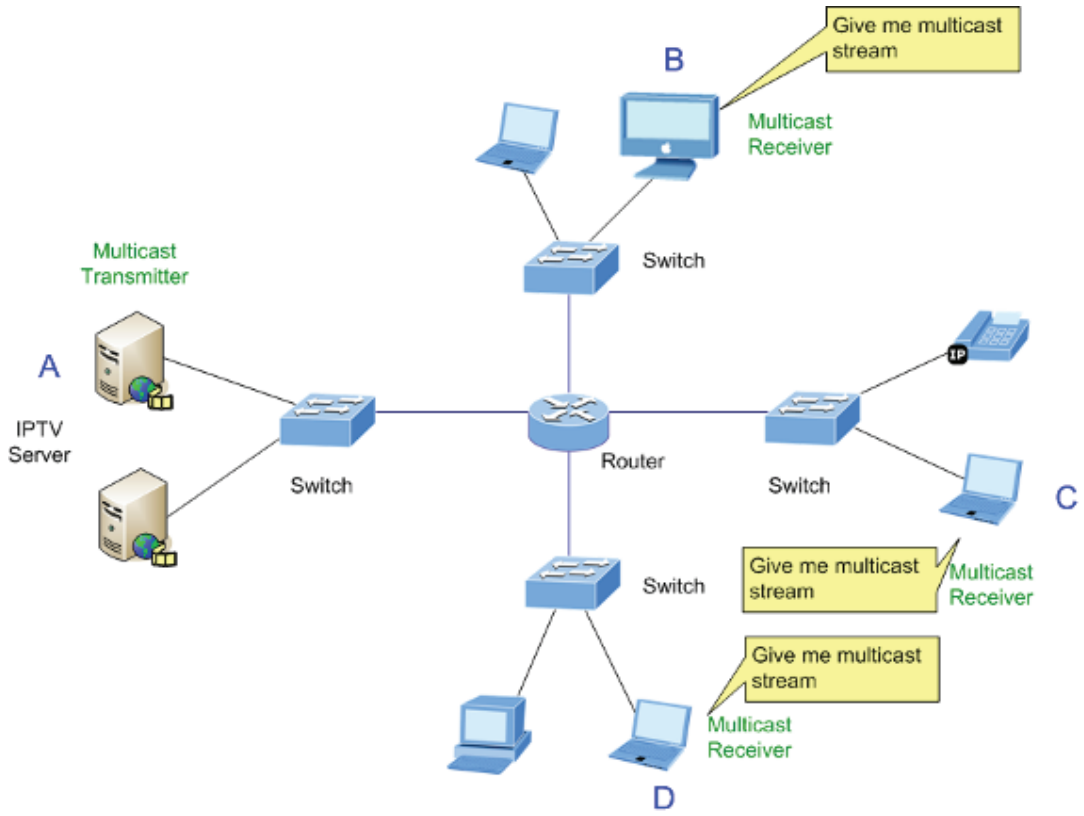


Figure 4-8-1: Multicast Service

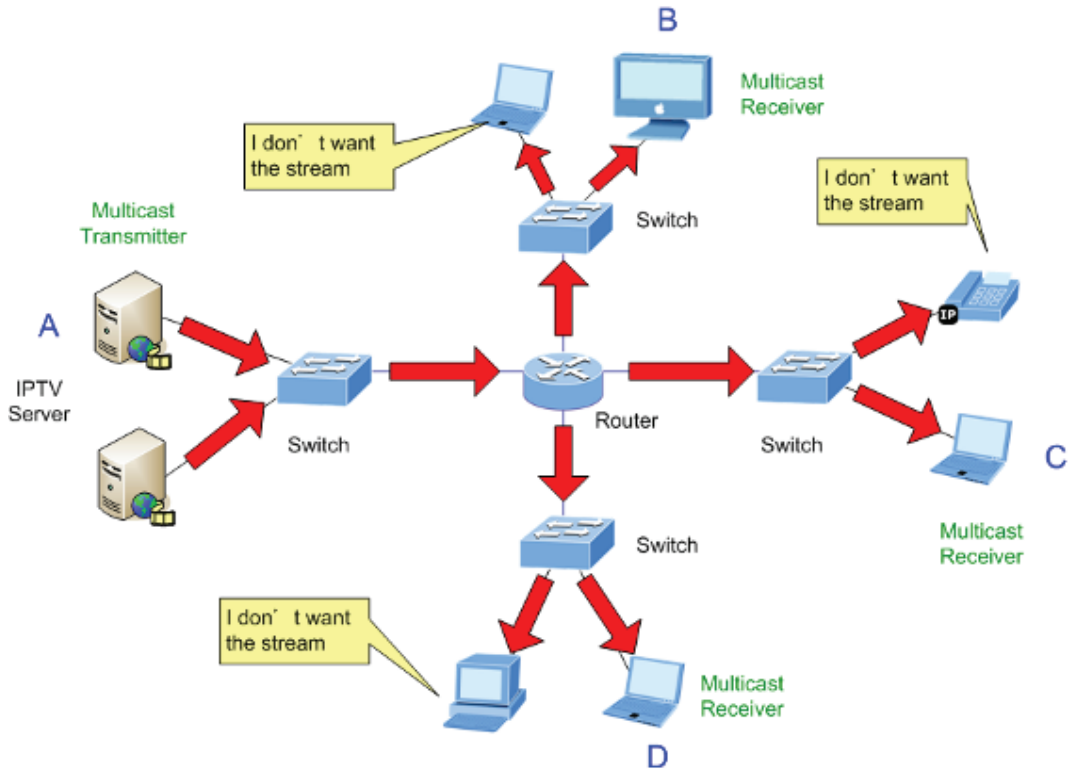


Figure 4-8-2: Multicast Flooding

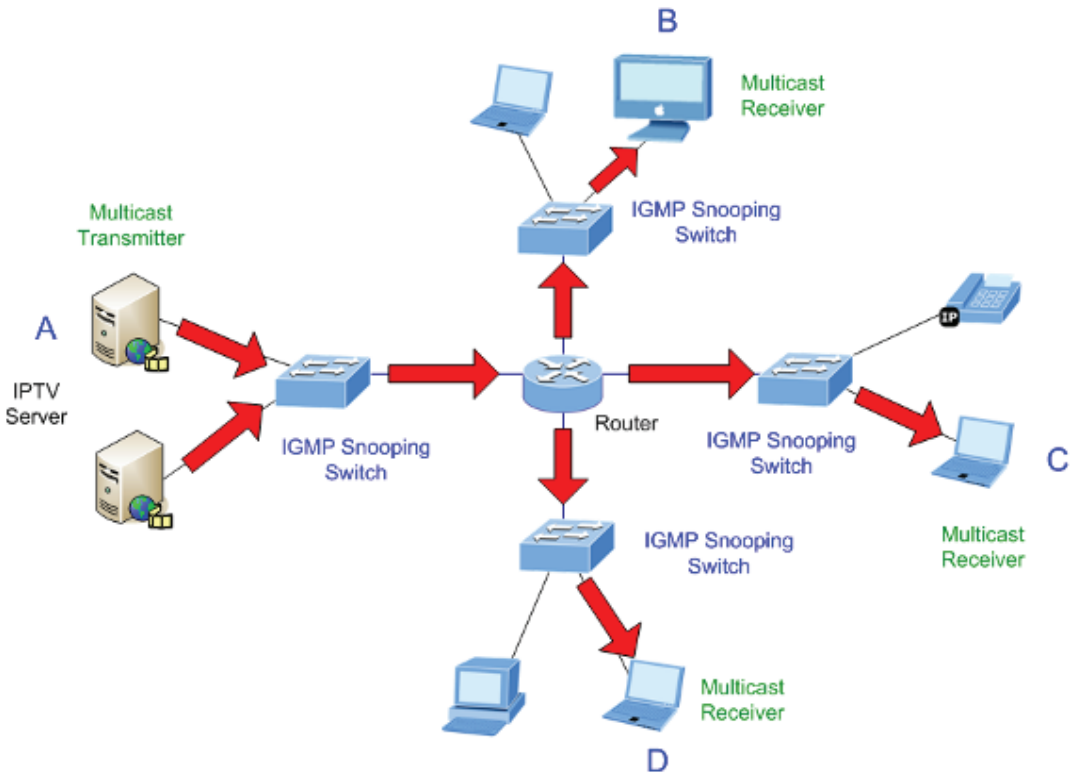


Figure 4-8-3: IGMP Snooping Multicast Stream Control

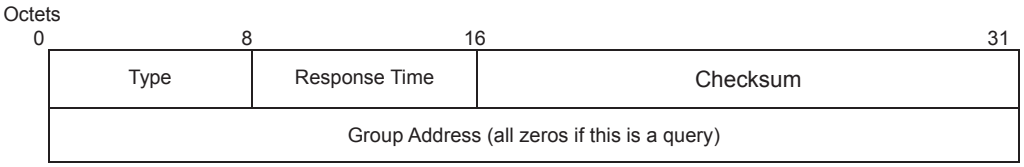
IGMP Versions 1 and 2

Multicast groups allow members to join or leave at any time. IGMP provides the method for members and multicast routers to communicate when joining or leaving a multicast group.

IGMP version 1 is defined in RFC 1112. It has a fixed packet size and no optional data.

The format of an IGMP packet is shown below:

IGMP Message Format



The IGMP Type codes are shown below:

Type	Meaning
0x11	Membership Query (if Group Address is 0.0.0.0)
0x11	Specific Group Membership Query (if Group Address is Present)
0x16	**Membership Report (version 2)**
0x17	**Leave a Group (version 2)**
0x12	**Membership Report (version 1)**

IGMP packets enable multicast routers to keep track of the membership of multicast groups, on their respective sub networks. The following outlines what is communicated between a multicast router and a multicast group member using IGMP.
A host sends an IGMP **"report"** to join a group

A host will never send a report when it wants to leave a group (for version 1).

A host will send a **"leave"** report when it wants to leave a group (for version 2).

Multicast routers send IGMP queries (to the all-hosts group address: 224.0.0.1) periodically to see whether any group members exist on their sub networks. If there is no response from a particular group, the router assumes that there are no group members on the network.

The Time-to-Live (TTL) field of query messages is set to 1 so that the queries will not be forwarded to other sub networks.

IGMP version 2 introduces some enhancements such as a method to elect a multicast queried for each LAN, an explicit leave message, and query messages that are specific to a given group.

The states a computer will go through to join or to leave a multicast group are shown below:

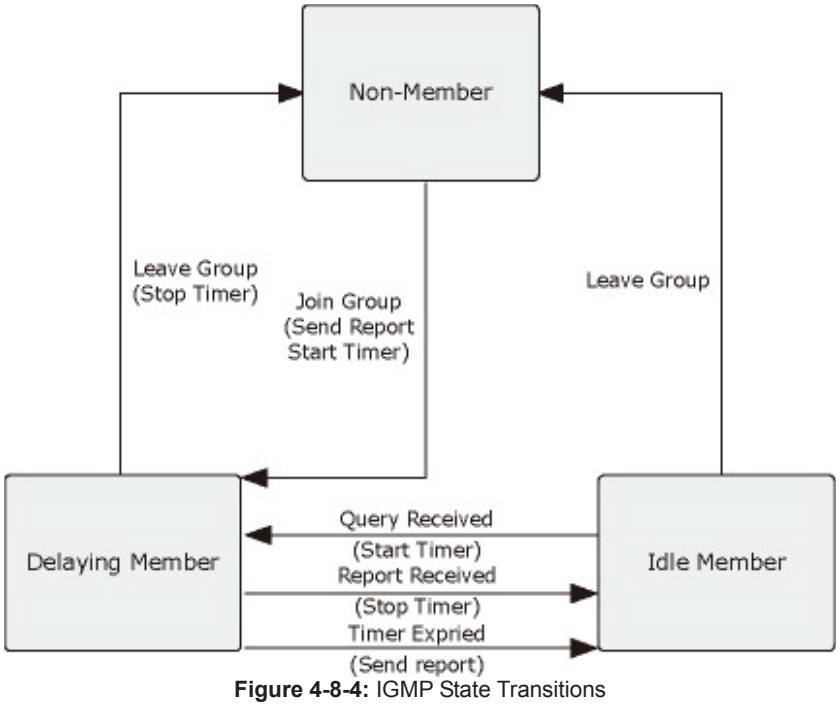


Figure 4-8-4: IGMP State Transitions

- **IGMP Querier –**
  A router, or multicast-enabled switch, can periodically ask their hosts if they want to receive multicast traffic. If there is more

than one router/switch on the LAN performing IP multicasting, one of these devices is elected "**querier**" and assumes the role of querying the LAN for group members. It then propagates the service requests on to any upstream multicast switch/router to ensure that it will continue to receive the multicast service.

Multicast routers use this information, along with a multicast routing protocol such as DVMRP or PIM, to support IP multicasting across the Internet.

4.8.2 IGMP Snooping Configuration

This page provides IGMP Snooping related configuration. The IGMP Snooping Configuration screen in Figure 4-8-5 appears.

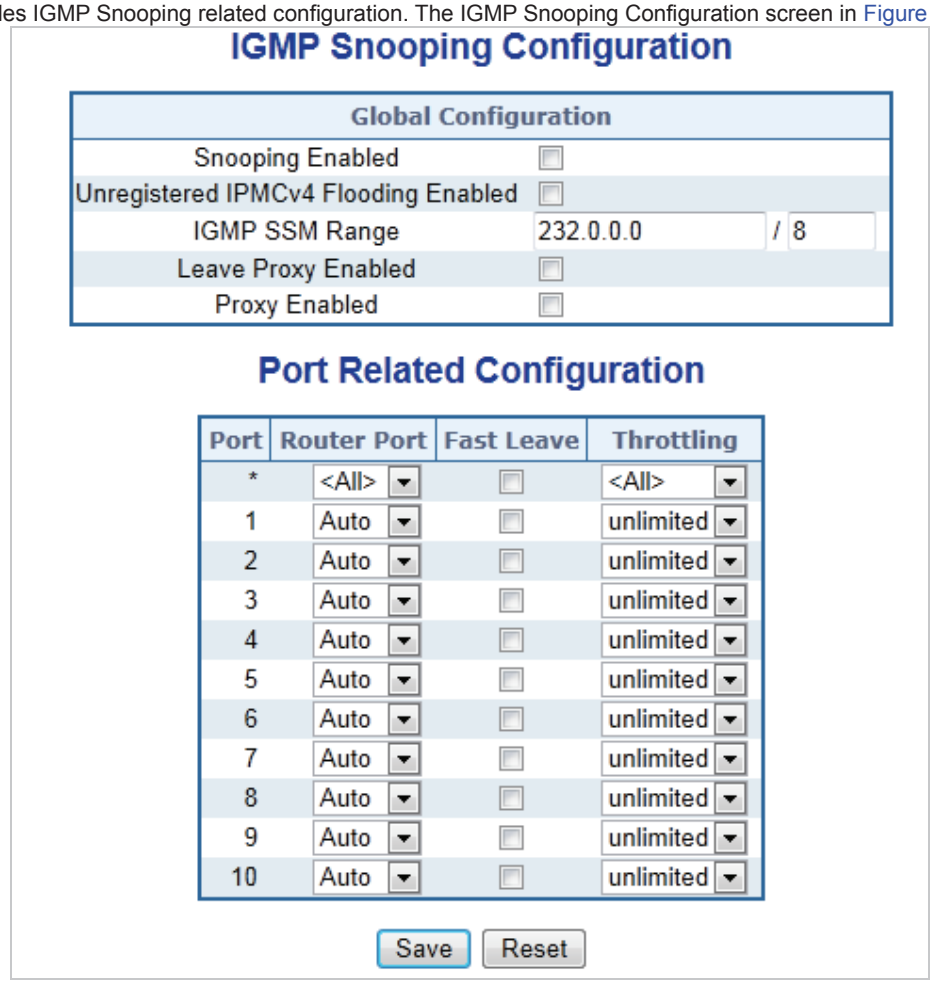


Figure 4-8-5: IGMP Snooping Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Snooping Enabled**	Enable the Global IGMP Snooping.
• **Unregistered IPMCv4 Flooding enabled**	Enable unregistered IPMCv4 traffic flooding.
• **IGMP SSM Range**	SSM (Source-Specific Multicast) Range allows the SSM-aware hosts and routers run the SSM service model for the groups in the address range.
• **Leave Proxy Enable**	Enable IGMP Leave Proxy. This feature can be used to avoid forwarding unnecessary leave messages to the router side.
• **Proxy Enable**	Enable IGMP Proxy. This feature can be used to avoid forwarding unnecessary join and leave messages to the router side.
• **Router Port**	Specify which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or IGMP querier. If an aggregation member port is selected as a router port, the whole aggregation will act as a router port. **All** means all ports will have one specific setting.
• **Fast Leave**	Enable the fast leave on the port.
• **Throtting**	The Configuration All with available values will assign to whole items. Enable to limit the number of multicast groups to which a switch port can belong. **All** means all ports will have one specific setting.

Buttons

 : Click to save changes.

 : Click to undo any changes made locally and revert to previously saved values.

4.8.3 IGMP Snooping VLAN Configuration

Each page shows up to 99 entries from the VLAN table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the VLAN Table. The first displayed will be the one with the lowest VLAN ID found in the VLAN Table.
The "VLAN" input fields allow the user to select the starting point in the VLAN Table. The IGMP Snooping VLAN Configuration screen in Figure 4-8-6 appears.

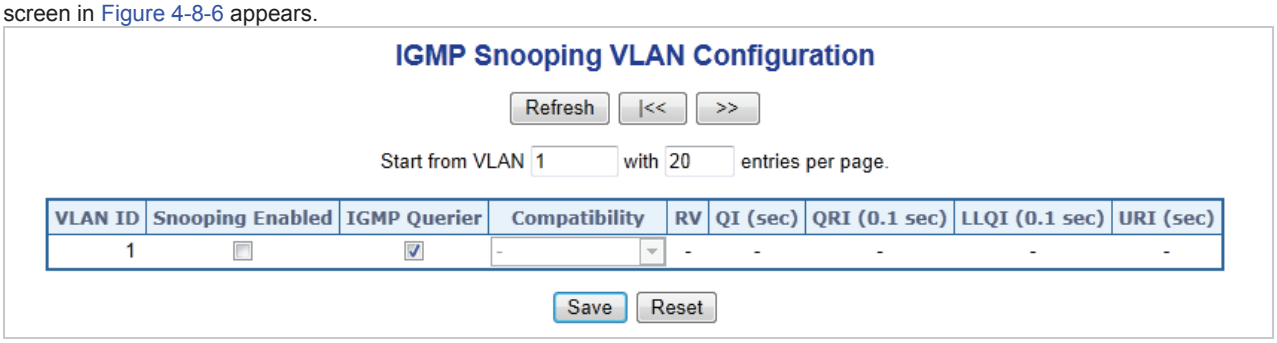


Figure 4-8-6: IGMP Snooping VLAN Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **VLAN ID**	The VLAN ID of the entry.
• **IGMP Snooping Enable**	Enable the per-VLAN IGMP Snooping. Only up to 64 VLANs can be selected.
• **IGMP Querier**	Enable the IGMP Querier in the VLAN.
• **Compatibility**	Compatibility is maintained by hosts and routers taking appropriate actions depending on the versions of IGMP operating on hosts and routers within a network. The allowed selection is IGMP-Auto, Forced IGMPv1, Forced IGMPv2, Forced IGMPv3, default compatibility value is IGMP-Auto.
• **RV**	Robustness Variable. The Robustness Variable allows tuning for the expected packet loss on a network. The allowed range is 1 to 255, default robustness variable value is 2.
• **QI**	Query Interval. The Query Interval is the interval between General Queries sent by the Querier. The allowed range is 1 to 255 seconds, default query interval is 125 seconds.
• **QRI**	Query Response Interval. The Max Response Time used to calculate the Max Resp Code inserted into the periodic General Queries. The allowed range is 0 to 31744 in tenths of seconds, default query response interval is 100 in tenths of seconds (10 seconds).
• **LLQI (LMQI for IGMP)**	Last Member Query Interval. The Last Member Query Time is the time value represented by the Last Member Query Interval, multiplied by the Last Member Query Count. The allowed range is 0 to 31744 in tenths of seconds, default last member query interval is 10 in tenths of seconds (1 second).
• **URI**	Unsolicited Report Interval. The Unsolicited Report Interval is the time between repetitions of a host's initial report of membership in a group. The allowed range is 0 to 31744 seconds, default unsolicited report interval is 1 second.

Buttons

 : Click to undo any changes made locally and revert to previously saved values.

4.8.4 IGMP Snooping Port Group Filtering

In certain switch applications, the administrator may want to control the multicast services that are available to end users. For example, an IP/TV service based on a specific subscription plan. The IGMP filtering feature fulfills this requirement by restricting access to specified multicast services on a switch port, and IGMP throttling limits the number of simultaneous multicast groups a port can join.

IGMP filtering enables you to assign a profile to a switch port that specifies multicast groups that are permitted or denied on the port. An IGMP filter profile can contain one or more, or a range of multicast addresses; but only one profile can be assigned to a port. When enabled, IGMP join reports received on the port are checked against the filter profile. If a requested multicast group is permitted, the IGMP join report is forwarded as normal. If a requested multicast group is denied, the IGMP join report is dropped.

IGMP throttling sets a maximum number of multicast groups that a port can join at the same time. When the maximum number of groups is reached on a port, the switch can take one of two actions; either “deny” or “replace”. If the action is set to deny, any new IGMP join reports will be dropped. If the action is set to replace, the switch randomly removes an existing group and replaces it with the new multicast group. The IGMP Snooping Port Group Filtering Configuration screen in Figure 4-8-7 appears.

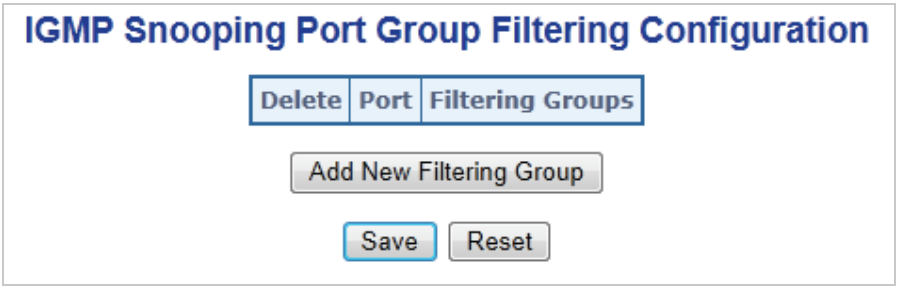


Figure 4-8-7: IGMP Snooping Port Group Filtering Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Delete**	Check to delete the entry. It will be deleted during the next save.
• **Port**	The logical port for the settings.
• **Filtering Group**	The IP Multicast Group that will be filtered.

Buttons

Add New Filtering Group: Click to add a new entry to the Group Filtering table.

 : Click to save changes.

 : Click to undo any changes made locally and revert to previously saved values.

4.8.5 IGMP Snooping Status

This page provides IGMP Snooping status. The IGMP Snooping Status screen in Figure 4-8-8 appears.

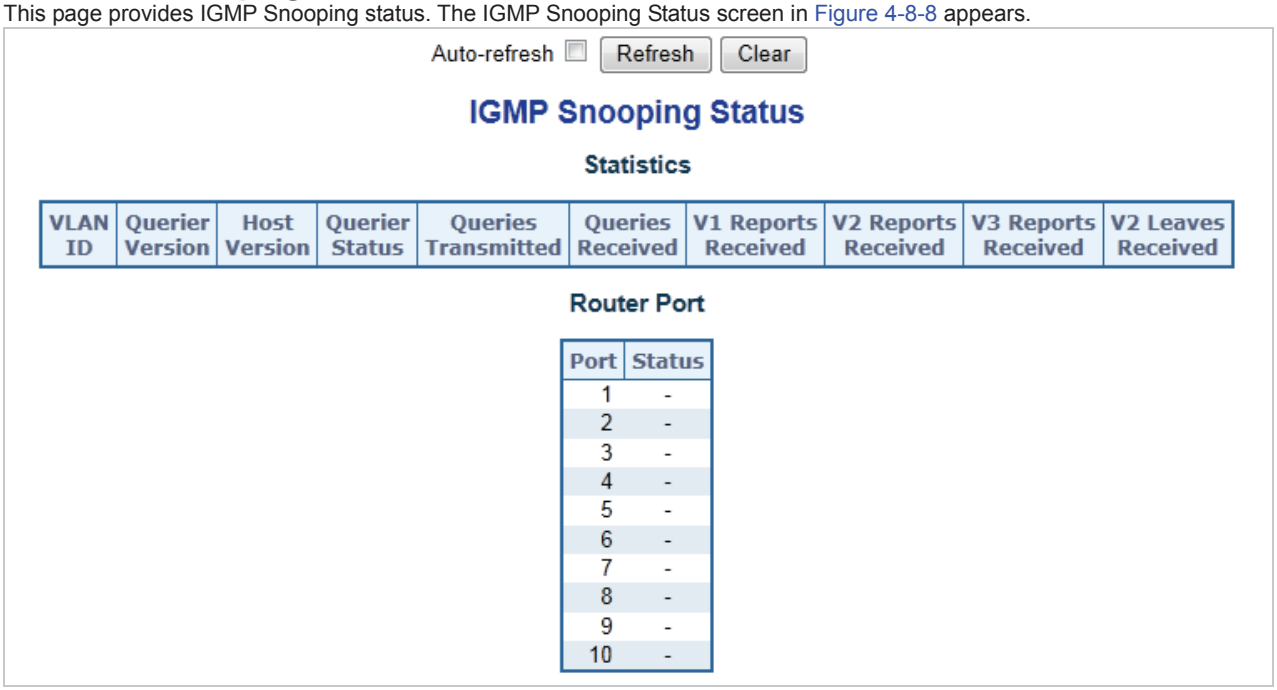


Figure 4-8-8: IGMP Snooping Status Page Screenshot

The page includes the following fields:

Object	Description
• **VLAN ID**	The VLAN ID of the entry
• **Querier Version**	Working Querier Version currently
• **Host Version**	Working Host Version currently
• **Querier Status**	Show the Querier status is "ACTIVE" or "IDLE"
• **Queriers Transmitted**	The number of Transmitted Queriers
• **Queriers Received**	The number of Received Queriers
• **V1 Reports Received**	The number of Received V1 Reports
• **V2 Reports Received**	The number of Received V2 Reports
• **V3 Reports Received**	The number of Received V3 Reports
• **V2 Leaves Received**	The number of Received V2 Leaves

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

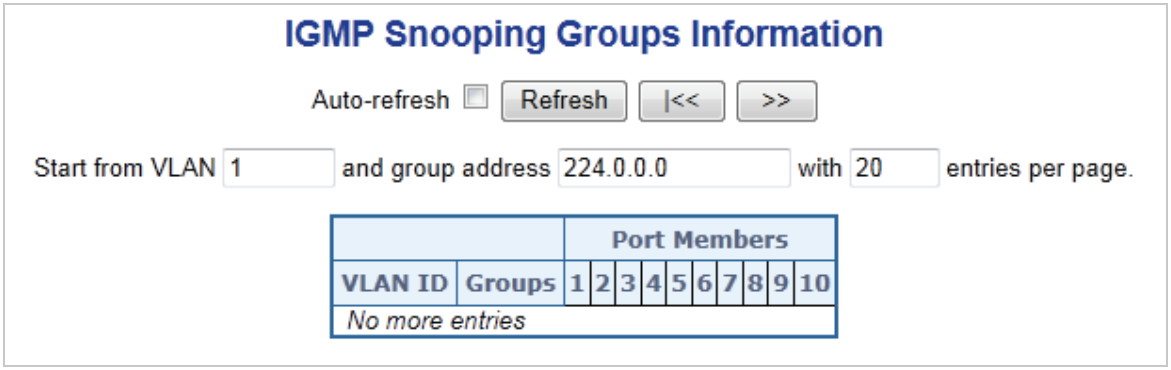


Figure 4-8-9: IGMP Snooping Groups Information Page Screenshot

The page includes the following fields:

Object	Description
• **VLAN ID**	VLAN ID of the group.
• **Groups**	Group address of the group displayed.
• **Port Members**	Ports under this group.

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

4.8.7 IGMPv3 Information

Entries in the IGMP SFM Information Table are shown on this page. The IGMP SFM (Souce-Filtered Multicast) Information Table also contains the SSM (Source-Specific Multicast) information. This table is sorted first by VLAN ID, then by group, and then by Port No. Diffrent source addresses belong to the same group are treated as single entry.
Each page shows up to 99 entries from the IGMP SFM Information table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the IGMP SFM Information Table.
The "**Start from VLAN**", and "**Group**" input fields allow the user to select the starting point in the IGMP SFM Information Table.
The IGMPv3 Information screen in Figure 4-8-10 appears.

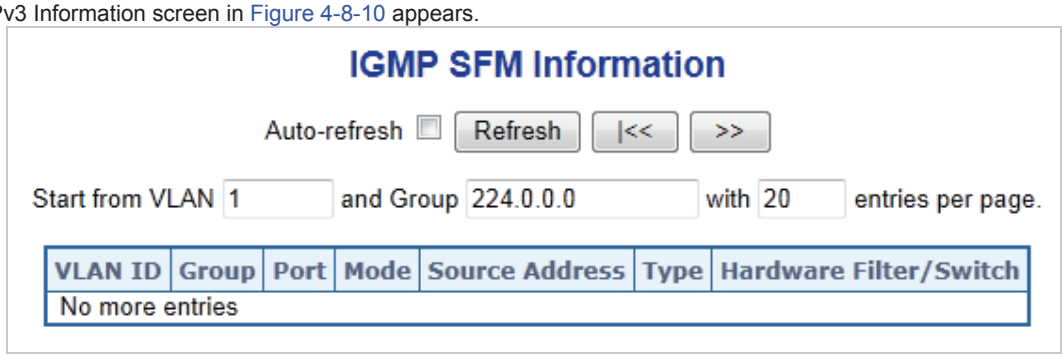


Figure 4-8-10: IGMP SFM Information Page Screenshot

The page includes the following fields:

Object	Description
• **VLAN ID**	VLAN ID of the group.
• **Group**	Group address of the group displayed.
• **Port**	Switch port number.
• **Mode**	Indicates the filtering mode maintained per (VLAN ID, port number, Group Address) basis. It can be either Include or Exclude.
• **Source Address**	IP Address of the source. Currently, system limits the total number of IP source addresses for filtering to be 128.
• **Type**	Indicates the Type. It can be either Allow or Deny.
• **Hardware Filter / Switch**	Indicates whether data plane destined to the specific group address from the source IPv4 address could be handled by chip or not.

Buttons
Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

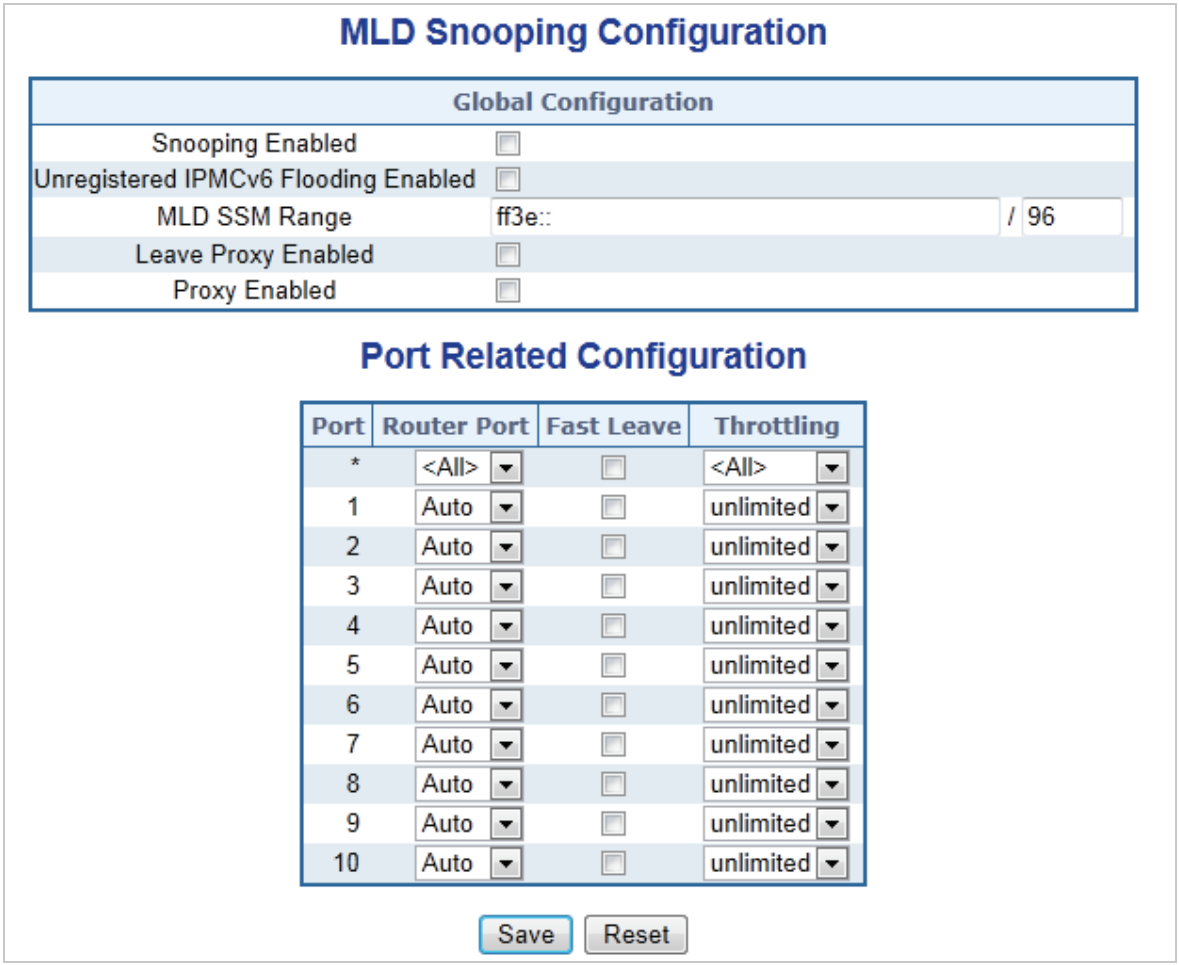


Figure 4-8-11: MLD Snooping Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Snooping Enabled**	Enable the Global MLD Snooping.
• **Unregistered IPMCv6 Flooding Enabled**	Enable unregistered IPMCv6 traffic flooding. Please note that disabling unregistered IPMCv6 traffic flooding may lead to failure of Neighbor Discovery.
• **MLD SSM Range**	SSM (Source-Specific Multicast) Range allows the SSM-aware hosts and routers run the SSM service model for the groups in the address range.
• **Leave Proxy Enable**	Enable MLD Leave Proxy. This feature can be used to avoid forwarding unnecessary leave messages to the router side.
• **Proxy Enable**	Enable MLD Proxy. This feature can be used to avoid forwarding unnecessary join and leave messages to the router side.
• **Router Port**	Specify which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or MLD querier. If an aggregation member port is selected as a router port, the whole aggregation will act as a router port. **All** means all ports will have one specific setting.
• **Fast Leave**	Enable the fast leave on the port.
• **Throtting**	The Configuration All with available values will assign to whole items. Enable to limit the number of multicast groups to which a switch port can belong. **All** means all ports will have one specific setting.

Buttons

: Click to save changes.

: Click to undo any changes made locally and revert to previously saved values.

4.8.9 MLD Snooping VLAN Configuration

Each page shows up to 99 entries from the VLAN table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the VLAN Table. The first displayed will be the one with the lowest VLAN ID found in the VLAN Table.
The "VLAN" input fields allow the user to select the starting point in the VLAN Table. The MLD Snooping VLAN Configuration screen in Figure 4-8-12 appears.

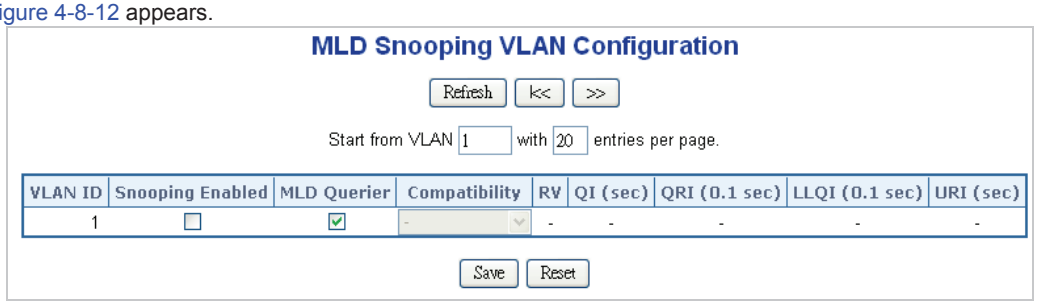


Figure 4-8-12: IGMP Snooping VLAN Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **VLAN ID**	The VLAN ID of the entry.
• **MLD Snooping Enable**	Enable the per-VLAN MLD Snooping. Only up to 64 VLANs can be selected.
• **MLD Querier**	Enable the MLD Querier in the VLAN.
• **Compatibility**	Compatibility is maintained by hosts and routers taking appropriate actions depending on the versions of MLD operating on hosts and routers within a network. The allowed selection is MLD-Auto, Forced MLDv1, Forced MLDv2, default compatibility value is MLD-Auto.
• **RV**	Robustness Variable. The Robustness Variable allows tuning for the expected packet loss on a link. The allowed range is 1 to 255, default robustness variable value is 2.
• **QI**	Query Interval. The Query Interval variable denotes the interval between General Queries sent by the Querier. The allowed range is 1 to 255 seconds, default query interval is 125 seconds.
• **QRI**	Query Response Interval. The Maximum Response Delay used to calculate the Maximum Response Code inserted into the periodic General Queries. The allowed range is 0 to 31744 in tenths of seconds, default query response interval is 100 in tenths of seconds (10 seconds).
• **LLQI**	Last Listener Query Interval. The Last Listener Query Interval is the Maximum Response Delay used to calculate the Maximum Response Code inserted into Multicast Address Specific Queries sent in response to Version 1 Multicast Listener Done messages. It is also the Maximum Response Delay used to calculate the Maximum Response Code inserted into Multicast Address and Source Specific Query messages. The allowed range is 0 to 31744 in tenths of seconds, default last listener query interval is 10 in tenths of seconds (1 second).
• **URI**	Unsolicited Report Interval. The Unsolicited Report Interval is the time between repetitions of a node's initial report of interest in a multicast address. The allowed range is 0 to 31744 seconds, default unsolicited report interval is 1 second.

Buttons

4.8.10 MLD Snooping Port Group Filtering

In certain switch applications, the administrator may want to control the multicast services that are available to end users. For example, an IP/TV service based on a specific subscription plan. The MLD filtering feature fulfills this requirement by restricting access to specified multicast services on a switch port, and MLD throttling limits the number of simultaneous multicast groups a port can join.

MLD filtering enables you to assign a profile to a switch port that specifies multicast groups that are permitted or denied on the port. A MLD filter profile can contain one or more, or a range of multicast addresses; but only one profile can be assigned to a port. When enabled, MLD join reports received on the port are checked against the filter profile. If a requested multicast group is permitted, the MLD join report is forwarded as normal. If a requested multicast group is denied, the MLD join report is dropped.

MLD throttling sets a maximum number of multicast groups that a port can join at the same time. When the maximum number of groups is reached on a port, the switch can take one of two actions; either “deny” or “replace”. If the action is set to deny, any new MLD join reports will be dropped. If the action is set to replace, the switch randomly removes an existing group and replaces it with the new multicast group. The MLD Snooping Port Group Filtering Configuration screen in Figure 4-8-13 appears.

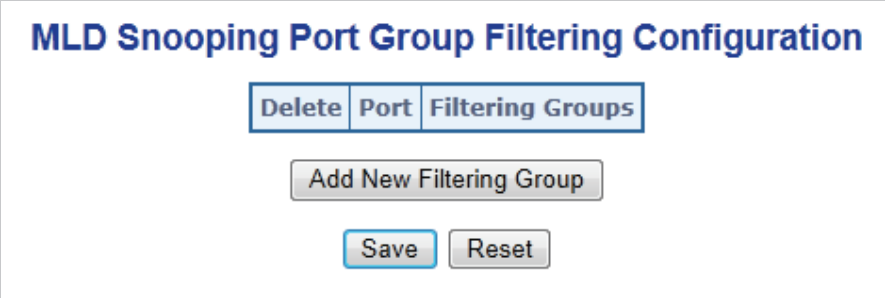


Figure 4-8-13: MLD Snooping Port Group Filtering Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Delete**	Check to delete the entry. It will be deleted during the next save.
• **Port**	The logical port for the settings.
• **Filtering Group**	The IP Multicast Group that will be filtered.

Buttons

Add New Filtering Group: Click to add a new entry to the Group Filtering table.

: Click to save changes.

: Click to undo any changes made locally and revert to previously saved values.

4.8.11 MLD Snooping Status

This page provides MLD Snooping status. The IGMP Snooping Status screen in Figure 4-8-14 appears.

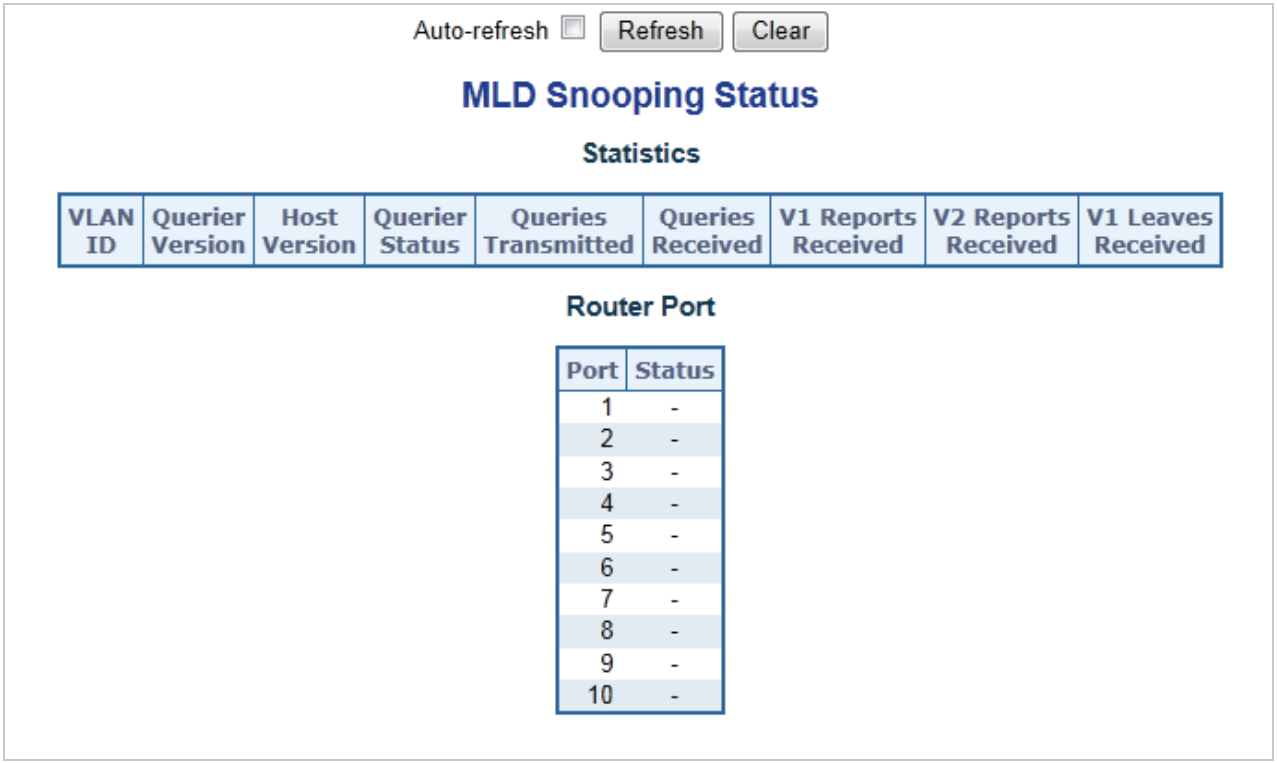


Figure 4-8-14: MLD Snooping Status Page Screenshot

The page includes the following fields:

Object	Description
• **VLAN ID**	The VLAN ID of the entry
• **Querier Version**	Working Querier Version currently
• **Host Version**	Working Host Version currently
• **Querier Status**	Show the Querier status is "ACTIVE" or "IDLE.
• **Queriers Transmitted**	The number of Transmitted Queriers
• **Queriers Received**	The number of Received Queriers
• **V1 Reports Received**	The number of Received V1 Reports
• **V2 Reports Received**	The number of Received V2 Reports
• **V1 Leave Received**	The number of Received V1 Leaves

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

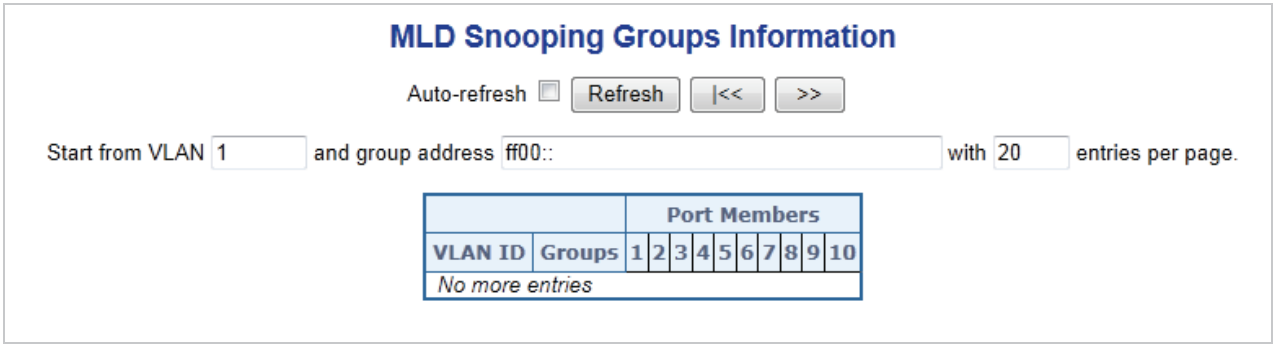


Figure 4-8-15: MLD Snooping Groups Information Page Screenshot

The page includes the following fields:

Object	Description
• **VLAN ID**	VLAN ID of the group.
• **Groups**	Group address of the group displayed.
• **Port Members**	Ports under this group.

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

4.8.13 MLDv2 Information

Entries in the MLD SFM Information Table are shown on this page. The MLD **SFM (Souce-Filtered Multicast)** Information Table also contains the **SSM (Source-Specific Multicast)** information. This table is sorted first by VLAN ID, then by group, and then by Port No. Diffrent source addresses belong to the same group are treated as single entry.

Each page shows up to 64 entries from the MLD SFM Information table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the MLD SFM Information Table.

The "**Start from VLAN**", and "**Group**" input fields allow the user to select the starting point in the MLD SSM Information Table. The MLDv2 Information screen in Figure 4-8-16 appears.

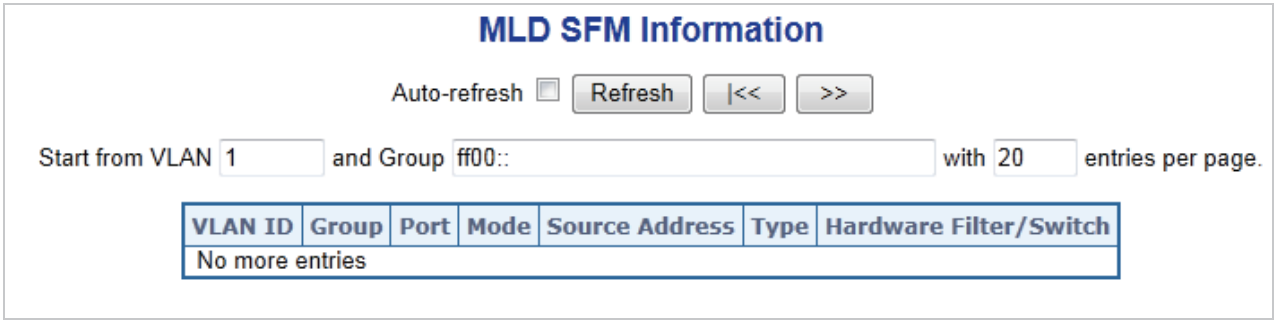


Figure 4-8-16: MLD SSM Information Page Screenshot

The page includes the following fields:

Object	Description
• **VLAN ID**	VLAN ID of the group.
• **Group**	Group address of the group displayed.
• **Port**	Switch port number.
• **Mode**	Indicates the filtering mode maintained per (VLAN ID, port number, Group Address) basis. It can be either Include or Exclude.
• **Source Address**	IP Address of the source. Currently, system limits the total number of IP source addresses for filtering to be 128.
• **Type**	Indicates the Type. It can be either Allow or Deny.
• **Hardware Filter / Switch**	Indicates whether data plane destined to the specific group address from the source IPv6 address could be handled by chip or not.

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

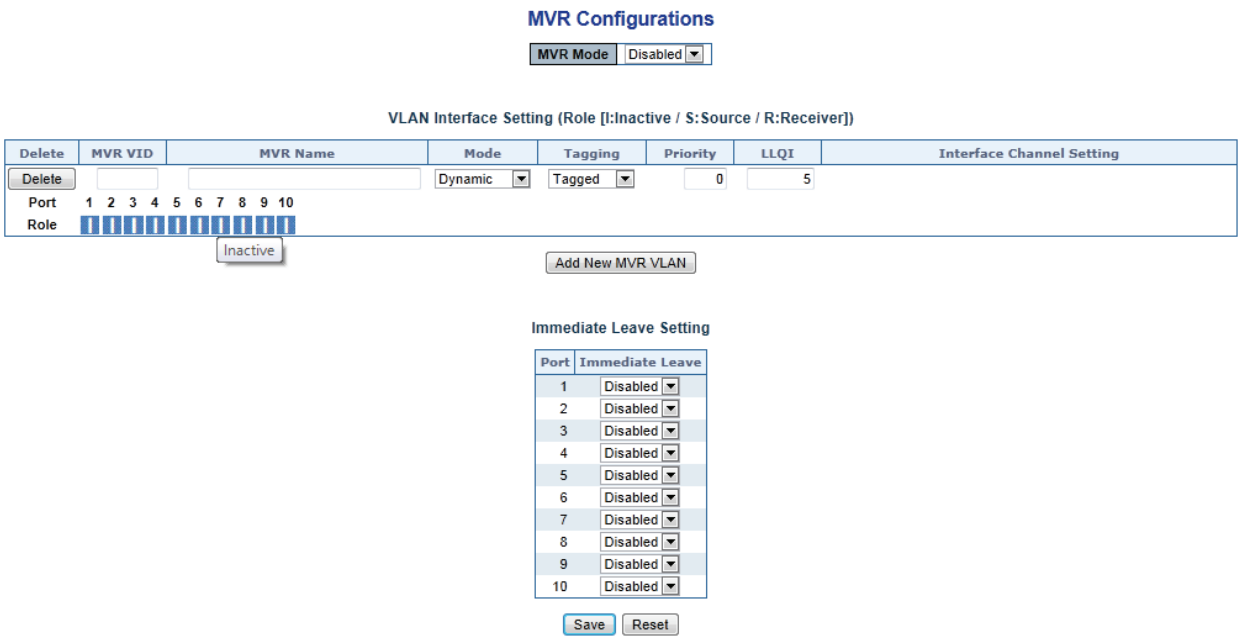


Figure 4-8-17: MVR Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **MVR Mode**	Enable/Disable the Global MVR. The Unregistered Flooding control depends on the current configuration in IGMP/MLD Snooping. It is suggested to enable Unregistered Flooding control when the MVR group table is full.
• **Delete**	Check to delete the entry. The designated entry will be deleted during the next save.
• **MVR VID**	Specify the Multicast VLAN ID. **Be Caution**: MVR source ports are not recommended to be overlapped with management VLAN ports.
• **MVR Name**	MVR Name is an optional attribute to indicate the name of the specific MVR VLAN. Maximum length of the MVR VLAN Name string is 32. MVR VLAN Name can only contain alphabets or numbers. When the optional MVR VLAN name is given, it should contain at least one alphabet. MVR VLAN name can be edited for the existing MVR VLAN entries or it can be added to the new entries.
• **Mode**	Specify the MVR mode of operation. ■ In Dynamic mode, MVR allows dynamic MVR membership reports on source ports. ■ In Compatible mode, MVR membership reports are forbidden on source ports. The default is Dynamic mode.
• **Tagging**	Specify whether the traversed IGMP/MLD control frames will be sent as Untagged or Tagged with MVR VID. The default is Tagged.
• **Priority**	Specify how the traversed IGMP/MLD control frames will be sent in prioritized manner. The default Priority is 0.
• **LLQI**	Define the maximun time to wait for IGMP/MLD report memberships on a receiver port before removing the port from multicast group membership. The value is in units of tenths of a seconds. The range is from 0 to 31744. The default LLQI is 5 tenths or one-half second.
• **Interface Channel Setting**	When the MVR VLAN is created, click the Edit symbol to expand the corresponding multicast channel settings for the specific MVR VLAN. Summary about the Interface Channel Setting (of the MVR VLAN) will be shown besides the Edit symbol.
• **Port**	The logical port for the settings.

• **Port Role**	Configure an MVR port of the designated MVR VLAN as one of the following roles. ■ **Inactive**: The designated port does not participate MVR operations. ■ **Source**: Configure uplink ports that receive and send multicast data as source ports. Subscribers cannot be directly connected to source ports. ■ **Receiver**: Configure a port as a receiver port if it is a subscriber port and should only receive multicast data. It does not receive data unless it becomes a member of the multicast group by issuing IGMP/MLD messages. **Be Caution**: MVR source ports are not recommended to be overlapped with management VLAN ports. Select the port role by clicking the Role symbol to switch the setting. I indicates Inactive; S indicates Source; R indicates Receiver The default Role is Inactive.
• **Immediate Leave**	Enable the fast leave on the port.

Buttons

[redacted]

: Click to save changes.

[redacted]: Click to undo any changes made locally and revert to previously saved values.

4.8.15 MVR Status

This page provides MVR status. The MVR Status screen in Figure 4-8-18 appears.

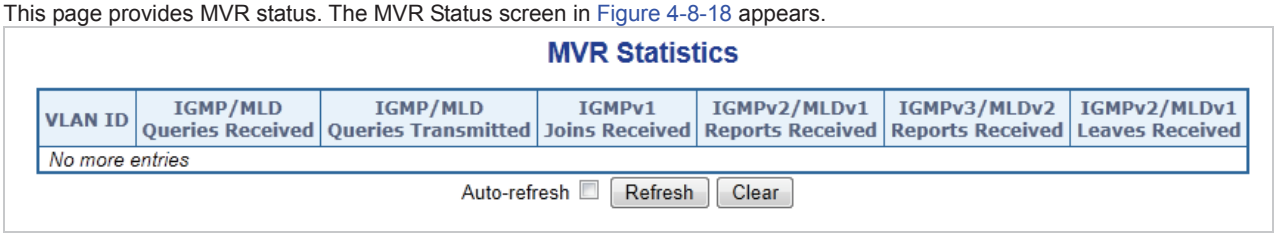


Figure 4-8-18: MVR Status Page Screenshot

The page includes the following fields:

Object	Description
• **VLAN ID**	The Multicast VLAN ID.
• **IGMP/MLD Queries Received**	The number of Received Queries for IGMP and MLD, respectively.
• **IGMP/MLD Queries Transmitted**	The number of Transmitted Queries for IGMP and MLD, respectively.
• **IGMPv1 Joins Received**	The number of Received IGMPv1 Joins.
• **IGMPv2/MLDv1 Reports Received**	The number of Received IGMPv2 Joins and MLDv1 Reports, respectively.
• **IGMPv3/MLDv2 Reports Received**	The number of Received IGMPv3 Joins and MLDv2 Reports, respectively.
• **IGMPv2/MLDv1 Leaves Received**	The number of Received IGMPv2 Leaves and MLDv1 Dones, respectively.

Buttons

Auto-refresh [redacted]: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

4.8.16 MVR Groups Information

Entries in the MVR Group Table are shown on this page. The MVR Group Table is sorted first by VLAN ID, and then by group. Each page shows up to 99 entries from the MVR Group table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the MVR Group Table.
The "Start from VLAN", and "group" input fields allow the user to select the starting point in the MVR Group Table.
The MVR Groups Information screen in Figure 4-8-19 appears.

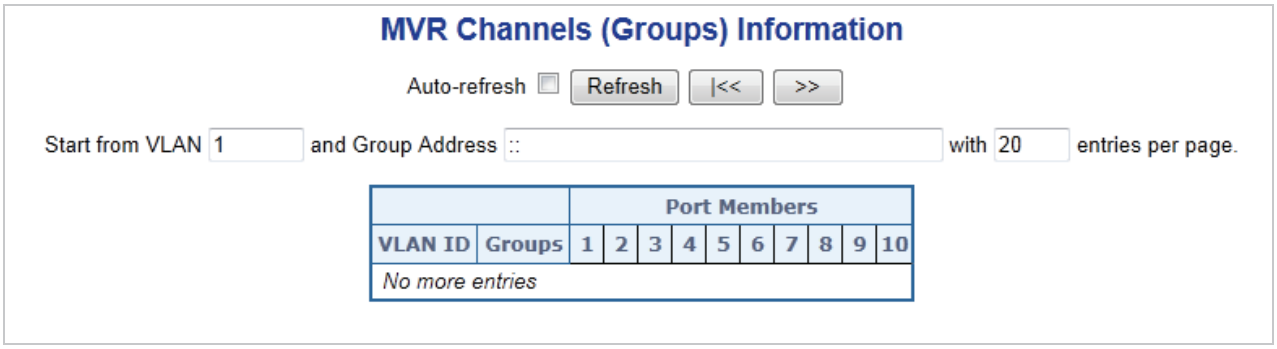


Figure 4-8-19: MVR Groups Information Page Screenshot

The page includes the following fields:

Object	Description
• **VLAN ID**	VLAN ID of the group.
• **Groups**	Group ID of the group displayed.
• **Port Members**	Ports under this group.

Buttons
Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

4.8.17 MVR SFM Information

Entries in the MVR SFM Information Table are shown on this page. The MVR SFM (Source-Filtered Multicast) Information Table also contains the SSM (Source-Specific Multicast) information. This table is sorted first by VLAN ID, then by group, and then by Port. Different source addresses belong to the same group are treated as single entry.
The MVR Groups Information screen in Figure 4-8-20 appears.

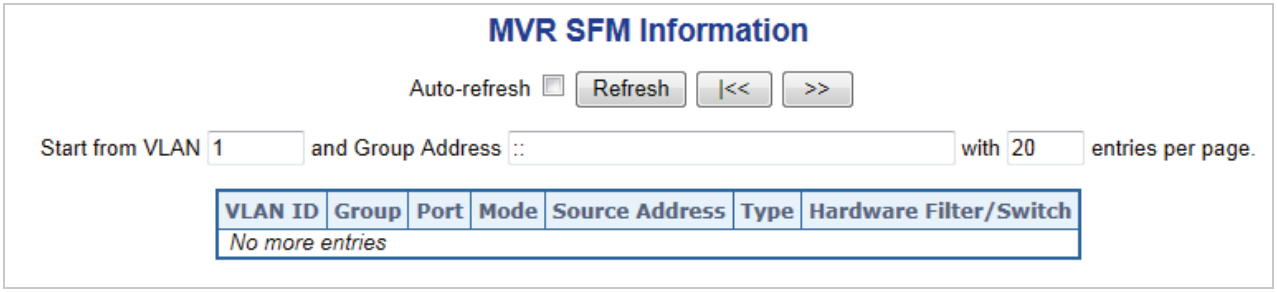


Figure 4-8-20: MVR Groups Information Page Screenshot

The page includes the following fields:

Object	Description
• **VLAN ID**	VLAN ID of the group.
• **Group**	Group ID of the group displayed.
• **Port**	Switch port number.
• **Mode**	Indicates the filtering mode maintained per (VLAN ID, port number, Group Address) basis. It can be either Include or Exclude.
• **Source Address**	IP Address of the source. Currently, system limits the total number of IP source addresses for filtering to be 128. When there is no any source filtering address, the text "None" is shown in the Source Address field.
• **Type**	Indicates the Type. It can be either Allow or Deny.
• **Hardware Filter / Switch**	Indicates whether data plane destined to the specific group address from the source IPv6 address could be handled by chip or not.

Buttons
Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

4.9 Quality of Service

4.9.1 Understand QOS

Quality of Service (QoS) is an advanced traffic prioritization feature that allows you to establish control over network traffic. QoS enables you to assign various grades of network service to different types of traffic, such as multi-media, video, protocol-specific, time critical, and file-backup traffic.

QoS reduces bandwidth limitations, delay, loss, and jitter. It also provides increased reliability for delivery of your data and allows you to prioritize certain applications across your network. You can define exactly how you want the switch to treat selected applications and types of traffic. You can use QoS on your system to:

- Control a wide variety of network traffic by:
- Classifying traffic based on packet attributes.
- Assigning priorities to traffic (for example, to set higher priorities to time-critical or business-critical applications).
- Applying security policy through traffic filtering.
- Provide predictable throughput for multimedia applications such as video conferencing or voice over IP by minimizing delay and jitter.
- Improve performance for specific types of traffic and preserve performance as the amount of traffic grows.
- Reduce the need to constantly add bandwidth to the network.
- Manage network congestion.

QoS Terminology

- **Classifier**—classifies the traffic on the network. Traffic classifications are determined by protocol, application, source, destination, and so on. You can create and modify classifications. The Switch then groups classified traffic in order to schedule them with the appropriate service level.
- **DiffServ Code Point (DSCP)** — is the traffic prioritization bits within an IP header that are encoded by certain applications and/or devices to indicate the level of service required by the packet across a network.
- **Service Level**—defines the priority that will be given to a set of classified traffic. You can create and modify service levels.
- **Policy**—comprises a set of “rules” that are applied to a network so that a network meets the needs of the business. That is, traffic can be prioritized across a network according to its importance to that particular business type.
- **QoS Profile**—consists of multiple sets of rules (classifier plus service level combinations). The QoS profile is assigned to a port(s).
- **Rules**—comprises a service level and a classifier to define how the Switch will treat certain types of traffic. Rules are associated with a QoS Profile (see above).

To implement QoS on your network, you need to carry out the following actions:

1. Define a service level to determine the priority that will be applied to traffic.
2. Apply a classifier to determine how the incoming traffic will be classified and thus treated by the Switch.
3. Create a QoS profile which associates a service level and a classifier.
4. Apply a QoS profile to a port(s).

4.9.2 Port Policing

This page allows you to configure the Policer settings for all switch ports. The Port Policing screen in Figure 4-9-1 appears.

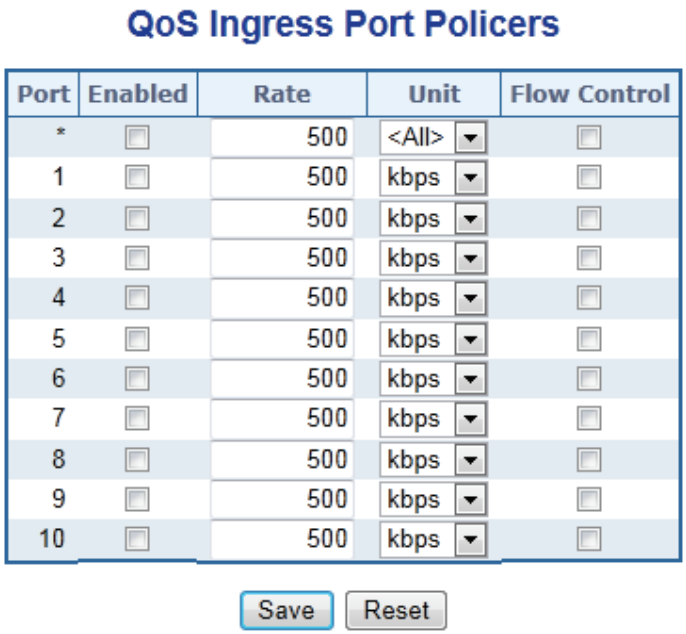


Figure 4-9-1: QoS Ingress Port Policers Page Screenshot

The page includes the following fields:

Object	Description
• **Port**	The port number for which the configuration below applies.
• **Enabled**	Controls whether the policer is enabled on this switch port, * means selection all ports of Industrial Managed Switch.
• **Rate**	Controls the rate for the policer. The default value is 500. This value is restricted to 100-1000000 when the **"Unit"** is **"kbps"** or **"fps"**, and it is restricted to 1-3300 when the **"Unit"** is **"Mbps"** or **"kfps"**.
• **Unit**	The Configuration All with available options will assign to whole ports. Controls the unit of measure for the policer rate as kbps, Mbps, fps or kfps. The default value is **"kbps"**. **All** means all ports will have one specific setting.
• **Flow Control**	If flow control is enabled and the port is in flow control mode, then pause frames are sent instead of discarding frames.

Buttons

 : Click to save changes.

 : Click to undo any changes made locally and revert to previously saved values.

4.9.3 Port Classification

This page allows you to configure the basic QoS Ingress Classification settings for all switch ports. The Port Classification screen in Figure 4-9-2 appears.

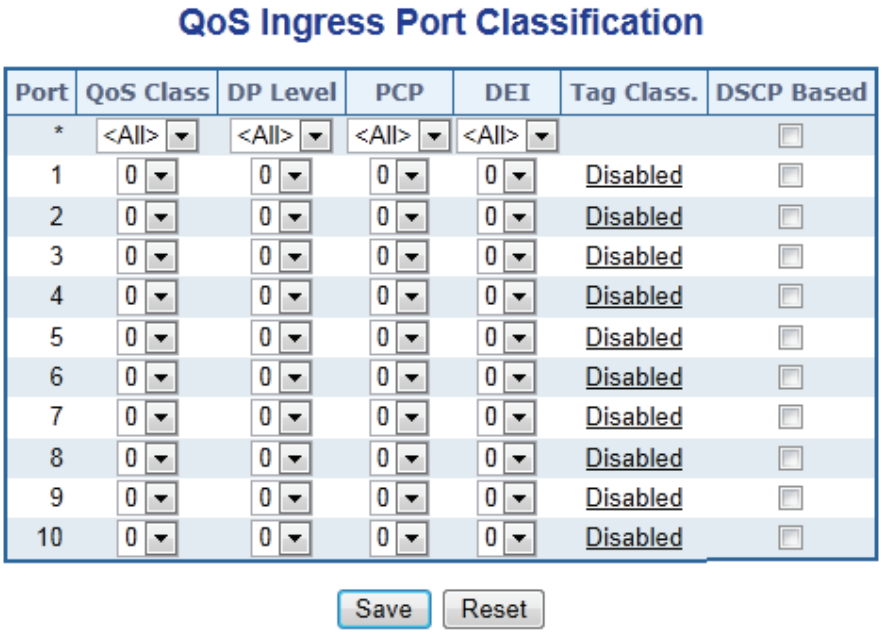


Figure 4-9-2 : QoS Ingress Port Classification Page Screenshot

The page includes the following fields:

Object	Description
• **Port**	The port number for which the configuration below applies.
• **QoS Class**	The Configuration All with available values will assign to whole ports. Controls the default QoS class, i.e., the QoS class for frames not classified in any other way. There is a one to one mapping between QoS class, queue and priority. A QoS class of 0 (zero) has the lowest priority. **All** means all ports will have one specific setting.
• **DP Level**	The Configuration All with available values will assign to whole ports. Controls the default DP level, i.e., the DP level for frames not classified in any other way. **All** means all ports will have one specific setting.
• **PCP**	The Configuration All with available values will assign to whole ports. Controls the default PCP for untagged frames. **All** means all ports will have one specific setting.
• **DEI**	The Configuration All with available values will assign to whole ports. Controls the default DEI for untagged frames. **All** means all ports will have one specific setting.
• **Tag Class**	Shows the classification mode for tagged frames on this port. ■ **Disabled**: Use default QoS class and DP level for tagged frames. ■ **Enabled**: Use mapped versions of PCP and DEI for tagged frames. Click on the mode in order to configure the mode and/or mapping. For more detail information, please refer to chapter 4.9.3.1.
• **DSCP Based**	Click to Enable DSCP Based QoS Ingress Port Classification.

Buttons

 : Click to save changes.

 : Click to undo any changes made locally and revert to previously saved values.

4.9.3.1 QoS Ingress Port Tag Classification

The clasification modes for tagged frames are configured on this page. The QoS Ingress Port Tag Classification screen in Figure 4-9-3 appears.

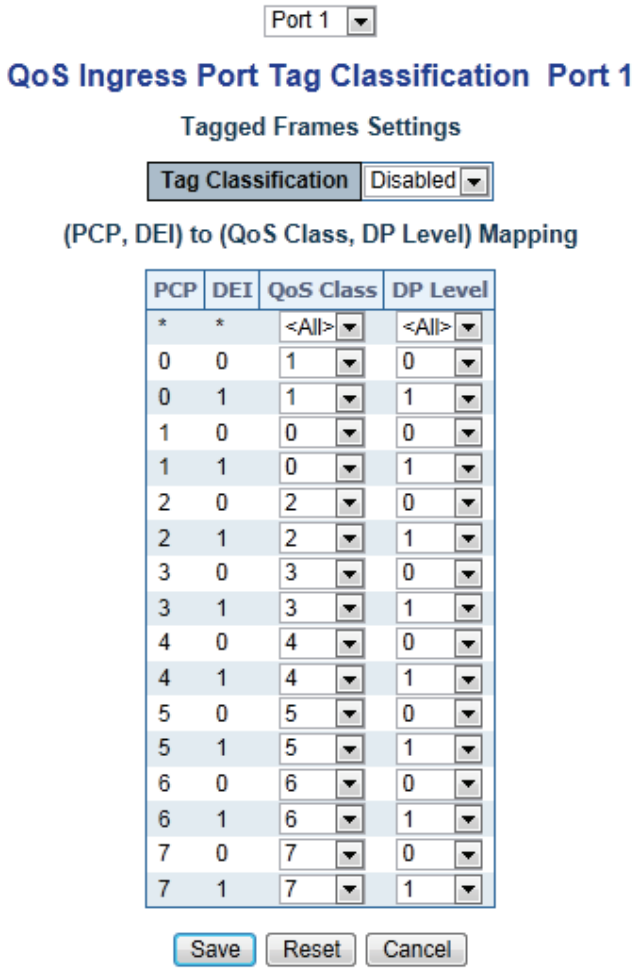


Figure 4-9-3 : QoS Ingress Port Tag Classification Page Screenshot

The page includes the following fields:

Object	Description
• **Tag Classification**	Controls the classification mode for tagged frames on this port. ■ **Disabled**: Use default QoS class and DP level for tagged frames. ■ **Enabled**: Use mapped versions of PCP and DEI for tagged frames.
• **(PCP, DEI) to (QoS class, DP level) Mapping**	The Configuration All with available values will assign to whole items. Controls the mapping of the classified (PCP, DEI) to (QoS class, DP level) values when Tag Classification is set to **Enabled**.

Buttons

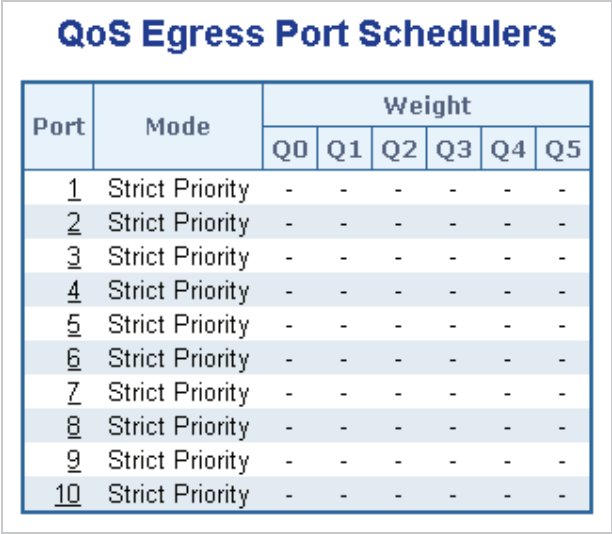
[redacted]: Click to save changes.

[redacted]: Click to undo any changes made locally and revert to previously saved values.

[redacted]: Return to the previous page.

4.9.4 Port Scheduler

This page provides an overview of QoS Egress Port Schedulers for all switch ports. The Port Scheduler screen in Figure 4-9-4 appears.



QoS Egress Port Schedulers

Port	Mode	Weight					
		Q0	Q1	Q2	Q3	Q4	Q5
1	Strict Priority	-	-	-	-	-	-
2	Strict Priority	-	-	-	-	-	-
3	Strict Priority	-	-	-	-	-	-
4	Strict Priority	-	-	-	-	-	-
5	Strict Priority	-	-	-	-	-	-
6	Strict Priority	-	-	-	-	-	-
7	Strict Priority	-	-	-	-	-	-
8	Strict Priority	-	-	-	-	-	-
9	Strict Priority	-	-	-	-	-	-
10	Strict Priority	-	-	-	-	-	-

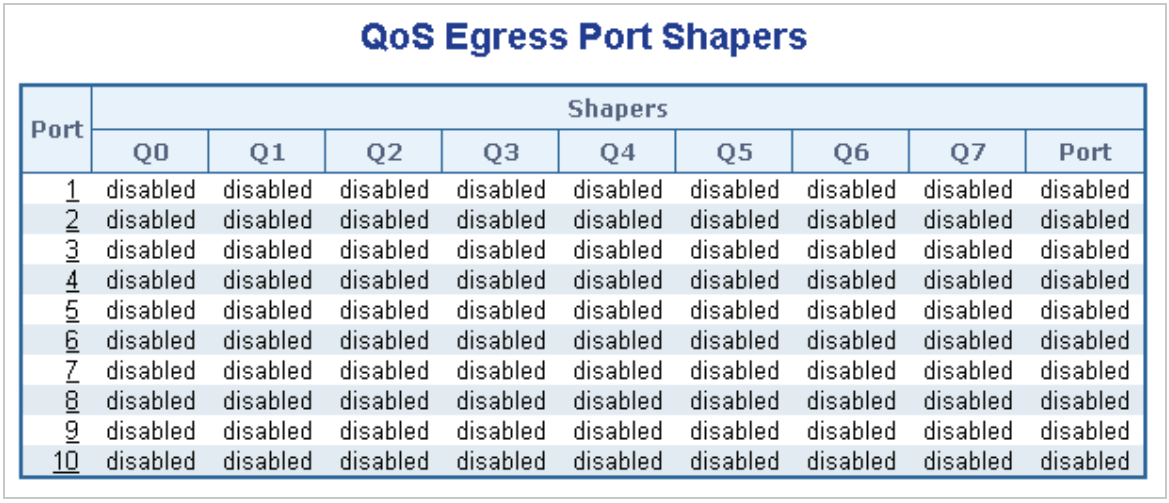
Figure 4-9-4: QoS Egress Port Schedule Page Screenshot

The page includes the following fields:

Object	Description
• **Port**	The logical port for the settings contained in the same row. Click on the port number in order to configure the schedulers. For more detail, please refer to chapter 4.9.5.1.
• **Mode**	Shows the scheduling mode for this port.
• **Q0 ~ Q5**	Shows the weight for this queue and port.

4.9.5 Port Shaping

This page provides an overview of QoS Egress Port Shapers for all switch ports. The Port Shapping screen in Figure 4-9-5 appears.



QoS Egress Port Shapers

Port	Shapers								
	Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Port
1	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
2	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
3	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
4	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
5	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
6	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
7	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
8	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
9	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
10	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled

Figure 4-9-5: QoS Egress Port Shapers Page Screenshot

The page includes the following fields:

Object	Description
• **Port**	The logical port for the settings contained in the same row. Click on the port number in order to configure the shapers. For more detail, please refer to chapter 4.9.5.1.
• **Q0 ~Q7**	Shows "disabled" or actual queue shaper rate - e.g. "800 Mbps".
• **Port**	Shows "disabled" or actual port shaper rate - e.g. "800 Mbps".

4.9.5.1 QoS Egress Port Schedule and Shapers

The Port Scheduler and Shapers for a specific port are configured on this page. The QoS Egress Port Schedule and Shaper sscreen in Figure 4-9-6 appears.

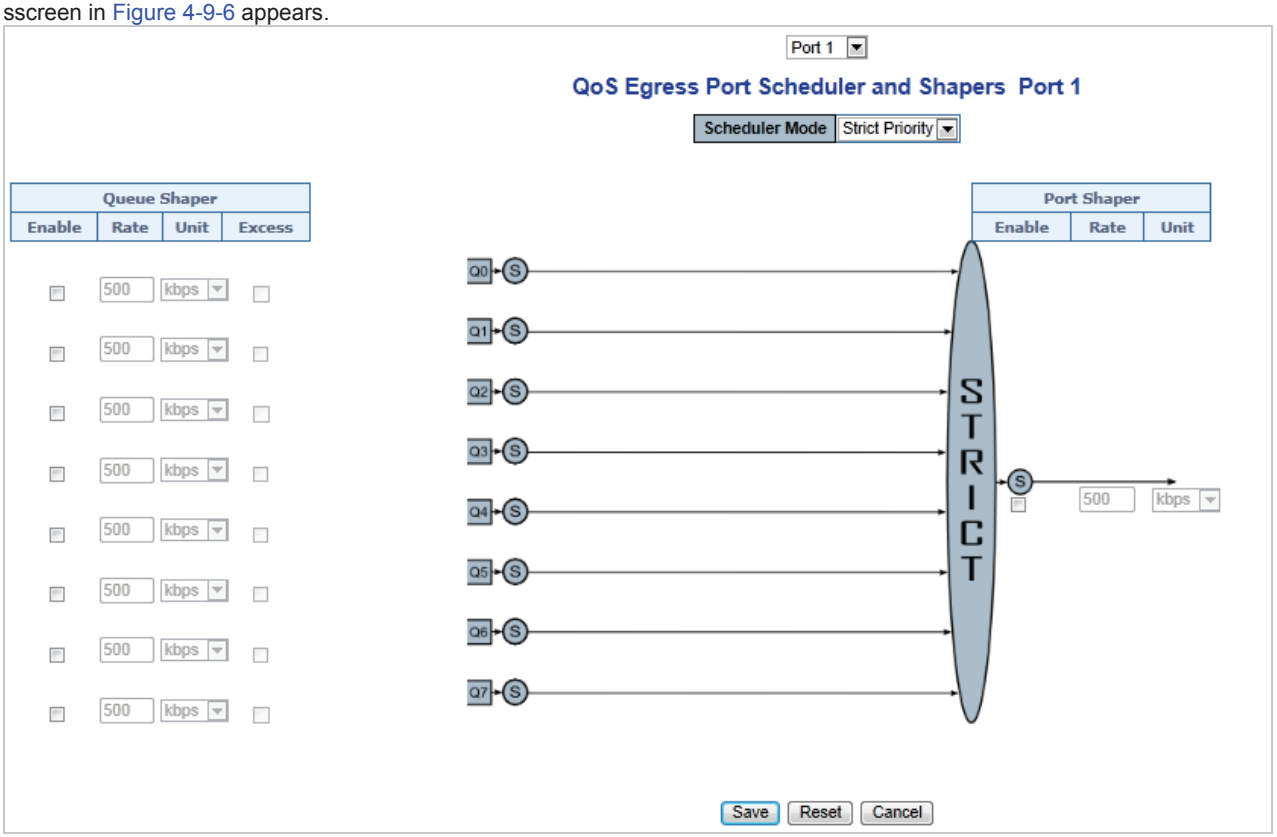


Figure 4-9-6: QoS Egress Port Schedule and Shapers Page Screenshot

The page includes the following fields:

Object	Description
• **Schedule Mode**	Controls whether the scheduler mode is **"Strict Priority"** or **"Weighted"** on this switch port.
• **Queue Shaper Enable**	Controls whether the queue shaper is enabled for this queue on this switch port.
• **Queue Shaper Rate**	Controls the rate for the queue shaper. The default value is 500. This value is restricted to 100-1000000 when the **"Unit"** is **"kbps"**, and it is restricted to 1-3300 when the "Unit" is "Mbps".
• **Queue Shaper Unit**	Controls the unit of measure for the queue shaper rate as **"kbps"** or **"Mbps"**. The default value is **"kbps"**.
• **Queue Shaper Excess**	Controls whether the queue is allowed to use excess bandwidth.
• **Queue Scheduler Weight**	Controls the weight for this queue. The default value is **"17"**. This value is restricted to 1-100. This parameter is only shown if **"Scheduler Mode"** is set to **"Weighted"**.
• **Queue Scheduler Percent**	Shows the weight in percent for this queue. This parameter is only shown if **"Scheduler Mode"** is set to **"Weighted".**
• **Port Shaper Enable**	Controls whether the port shaper is enabled for this switch port.
• **Port Shaper Rate**	Controls the rate for the port shaper. The default value is 500. This value is restricted to 100-1000000 when the **"Unit"** is **"kbps"**, and it is restricted to 1-3300 when the **"Unit"** is **"Mbps"**.
• **Port Shaper Unit**	Controls the unit of measure for the port shaper rate as **"kbps"** or **"Mbps"**. The default value is **"kbps"**.

Buttons

[redacted]: Click to save changes.

[redacted]: Click to undo any changes made locally and revert to previously saved values.

[redacted]: Click to undo any changes made locally and return to the previous page.

4.9.6 Port Tag Remarking

This page provides an overview of QoS Egress Port Tag Remarking for all switch ports. The Port Tag Remarking screen in Figure 4-9-7 appears.

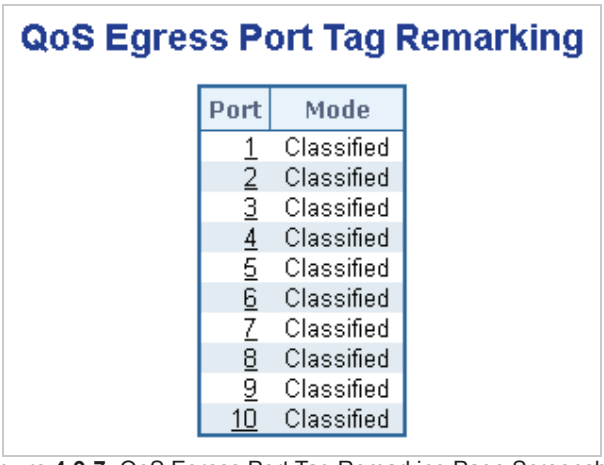


Figure 4-9-7: QoS Egress Port Tag Remarking Page Screenshot

The page includes the following fields:

Object	Description
• **Port**	The logical port for the settings contained in the same row. Click on the port number in order to configure tag remarking. For more detail, please refer to chapter 4.9.6.1.
• **Mode**	Shows the tag remarking mode for this port. ■ **Classified**: Use classified PCP/DEI values. ■ **Default**: Use default PCP/DEI values. ■ **Mapped**: Use mapped versions of QoS class and DP level.

4.9.6.1 QoS Egress Port Tag Remarking

The QoS Egress Port Tag Remarking for a specific port are configured on this page. The QoS Egress Port Tag Remarking sscreen in Figure 4-9-8 appears.

Figure 4-9-8: QoS Egress Port Tag Remarking Page Screenshot

The page includes the following fields:

Object	Description
• **Mode**	Controls the tag remarking mode for this port. ■ **Classified**: Use classified PCP/DEI values. ■ **Default**: Use default PCP/DEI values. ■ **Mapped**: Use mapped versions of QoS class and DP level.
• **PCP/DEI Configuration**	Controls the default PCP and DEI values used when the mode is set to **Default**.
• **(QoS class, DP level) to (PCP, DEI) Mapping**	Controls the mapping of the classified (QoS class, DP level) to (PCP, DEI) values when the mode is set to **Mapped**.

Buttons

[redacted]: Click to save changes.

[redacted]: Click to undo any changes made locally and revert to previously saved values.

[redacted]: Click to undo any changes made locally and return to the previous page.

4.9.7 Port DSCP

This page allows you to configure the basic QoS Port DSCP Configuration settings for all switch ports. The Port DSCP screen in Figure 4-9-9 appears.

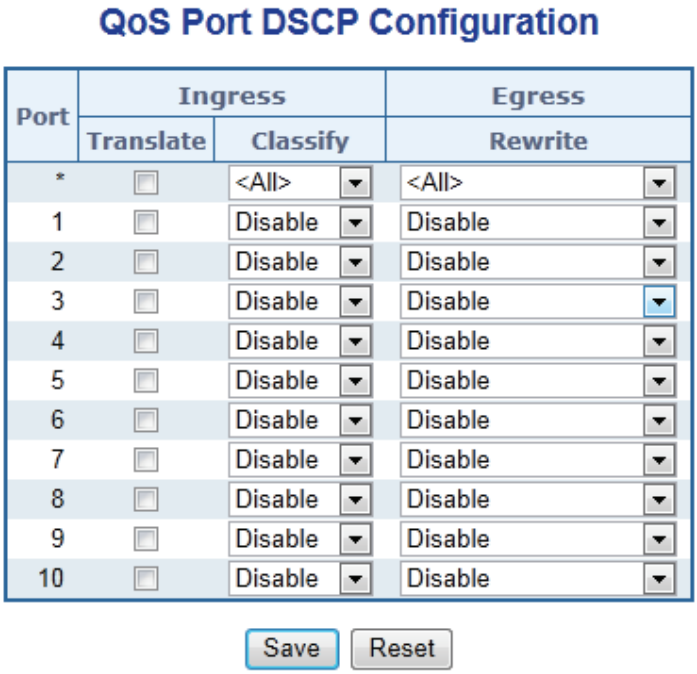


Figure 4-9-9 : QoS Port DSCP Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Port**	The Port coulmn shows the list of ports for which you can configure dscp ingress and egress settings.
• **Ingress**	In Ingress settings you can change ingress translation and classification settings for individual ports. There are two configuration parameters available in Ingress: ■ **Translate** ■ **Classify**
• **Translate**	To Enable the Ingress Translation click the checkbox. * means to select all ports of Industrial Managed Switch.
• **Classify**	The Configuration All with available options will assign to whole ports. Classification for a port has 4 different values. All means all ports will have one specific setting. ■ **Disable**: No Ingress DSCP Classification. ■ **DSCP=0**: Classify if incoming (or translated if enabled) DSCP is 0. ■ **Selected**: Classify only selected DSCP for which classification is enabled as specified in DSCP Translation window for the specific DSCP. ■ **All**: Classify all DSCP.

• **Egress**	The Configuration All with available options will assign to whole ports. Port Egress Rewriting can be one of –. All means all ports will have one specific setting. ■ **Disable**: No Egress rewrite. ■ **Enable**: Rewrite enabled without remapping. ■ **Remap DP Unaware**: DSCP from analyzer is remapped and frame is remarked with remapped DSCP value. The remapped DSCP value is always taken from the 'DSCP Translation->Egress Remap DP0' table. ■ **Remap DP Aware**: DSCP from analyzer is remapped and frame is remarked with remapped DSCP value. Depending on the DP level of the frame, the remapped DSCP value is either taken from the 'DSCP Translation->Egress Remap DP0' table or from the 'DSCP Translation->Egress Remap DP1' table.

Buttons

 : Click to save changes.

 : Click to undo any changes made locally and revert to previously saved values.

4.9.8 DSCP-Based QoS

This page allows you to configure the basic QoS DSCP based QoS Ingress Classification settings for all switches. The DSCP-Based QoS screen in Figure 4-9-10 appears.

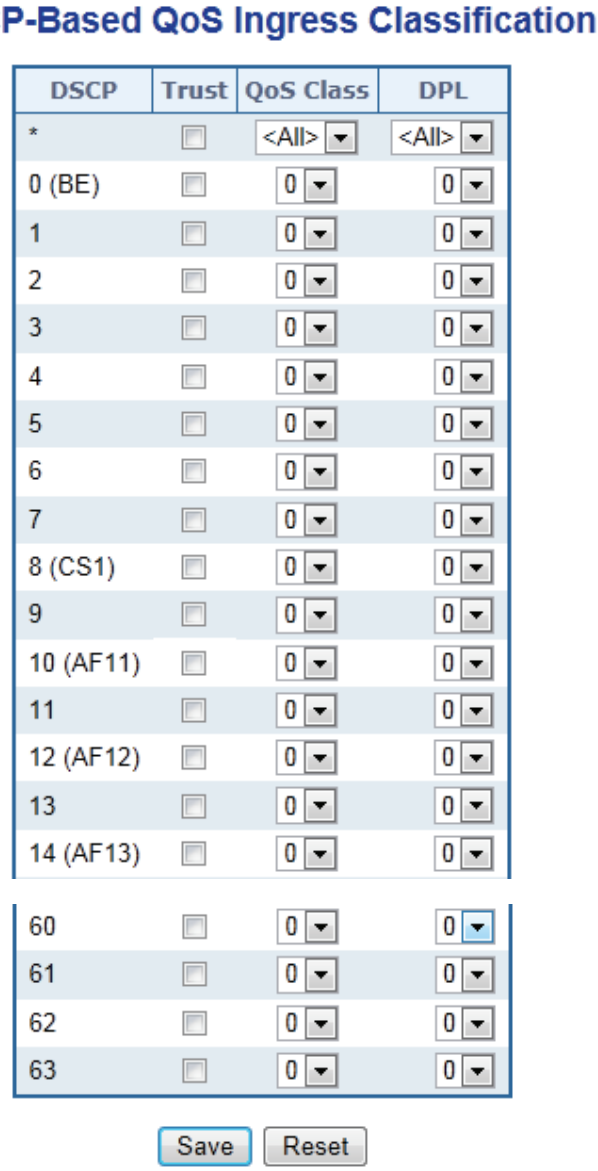


Figure 4-9-10: DSCP-Based QoS Ingress Classification Page Screenshot

The page includes the following fields:

Object	Description
• **DSCP**	Maximum number of support ed DSCP values are 63.
• **Trust**	Click to check if the DSCP value is trusted. * means to select all ports of Industrial Managed Switch.
• **QoS Class**	The Configuration All with available values will assign to whole DSCP values. QoS Class value can be any of (0-7)
• **DPL**	The Configuration All with available values will assign to whole DSCP values. Drop Precedence Level (0-1)

Buttons

: Click to save changes.

 : Click to undo any changes made locally and revert to previously saved values.

4.9.9 DSCP Translation

This page allows you to configure the basic QoS DSCP Translation settings for all switches. DSCP translation can be done in Ingress or Egress. The DSCP Translation screen in Figure 4-9-11 appears.

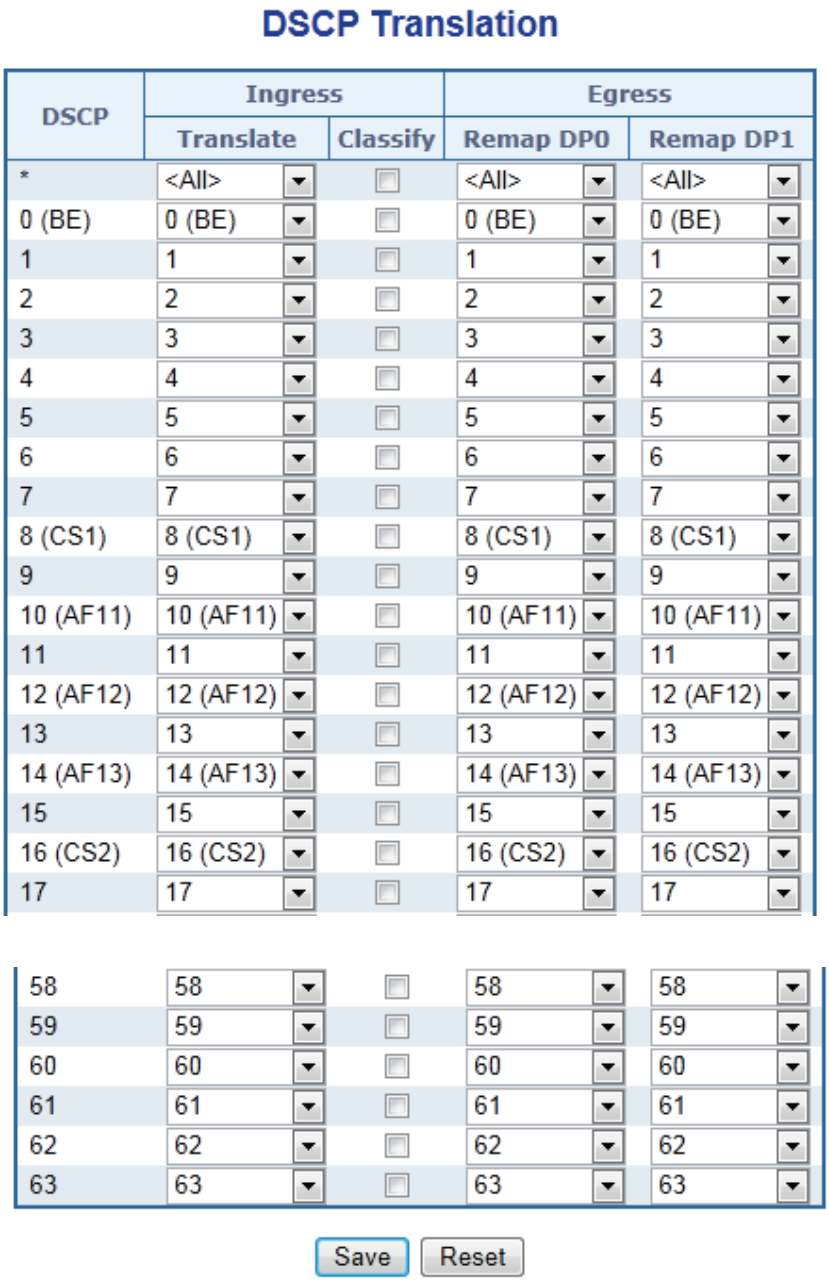


Figure 4-9-11: DSCP Translation Page Screenshot

The page includes the following fields:

Object	Description
• **DSCP**	Maximum numbers of supported DSCP values are 64 and valid DSCP value ranges from 0 to 63.
• **Ingress**	Ingress side DSCP can be first translated to new DSCP before using the DSCP for QoS class and DPL map. There are two configuration parameters for DSCP Translation – ■ **Translate**

	■ **Classify**
• **Translate**	The Configuration All with available values will assign to whole DSCP values. DSCP at Ingress side can be translated to any of (0-63) DSCP values.
• **Classify**	Click to enable Classification at Ingress side.
• **Egress**	There are the following configurable parameters for Egress side – ■ **Remap DP0** Controls the remapping for frames with DP level 0. ■ **Remap DP1** Controls the remapping for frames with DP level 1.
• **Remap DP0**	The Configuration All with available values will assign to whole DSCP values. Select the DSCP value from select menu to which you want to remap. DSCP value ranges form 0 to 63.
• **Remap DP1**	The Configuration All with available values will assign to whole DSCP values. Select the DSCP value from select menu to which you want to remap. DSCP value ranges form 0 to 63.

Buttons

 : Click to save changes.

 : Click to undo any changes made locally and revert to previously saved values.

4.9.10 DSCP Classification

This page allows you to map DSCP value to a QoS Class and DPL value. The DSCP Classification screen in Figure 4-9-12 appears.

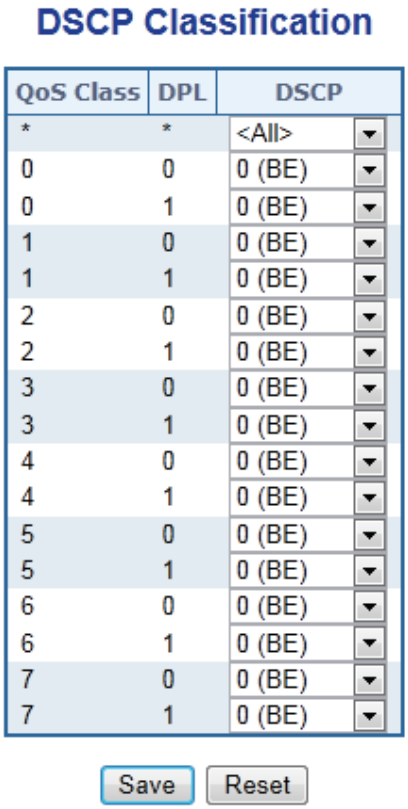


Figure 4-9-12: DSCP Classification Page Screenshot

The page includes the following fields:

Object	Description
• **QoS Class**	Available QoS Class value ranges from 0 to 7. QoS Class (0-7) can be mapped to followed parameters.
• **DPL**	Drop Precedence Level (0-1) can be configured for all available QoS Classes.
• **DSCP**	The Configuration All with available values will assign to whole QoS Class. Select DSCP value (0-63) from DSCP menu to map DSCP to corresponding QoS Class and DPL value

Buttons

 : Click to save changes.

 : Click to undo any changes made locally and revert to previously saved values.

4.9.11 QoS Control List

This page shows the QoS Control List(QCL), which is made up of the QCEs. Each row describes a QCE that is defined. The maximum number of QCEs is 256 on each switch.
Click on the lowest plus sign to add a new QCE to the list.
The QoS Control List screen in Figure 4-9-13 appears.

Figure 4-9-13: QoS Control List Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **QCE#**	Indicates the index of QCE.
• **Port**	Indicates the list of ports configured with the QCE.
26. Frame Type	Indicates the type of frame to look for incomming frames. Possible frame types are: ■ **Any**: The QCE will match all frame type. ■ **Ethernet**: Only Ethernet frames (with Ether Type 0x600-0xFFFF) are allowed. ■ **LLC**: Only (LLC) frames are allowed. ■ **SNAP**: Only (SNAP) frames are allowed. ■ **IPv4**: The QCE will match only IPV4 frames. ■ **IPv6**: The QCE will match only IPV6 frames.
27. SMAC	Displays the OUI field of Source MAC address, i.e. first three octet (byte) of MAC address.
28. DMAC	Specify the type of Destination MAC addresses for incoming frame. Possible values are: ■ **Any**: All types of Destination MAC addresses are allowed. ■ **Unicast**: Only Unicast MAC addresses are allowed. ■ **Multicast**: Only Multicast MAC addresses are allowed. ■ **Broadcast**: Only Broadcast MAC addresses are allowedd. The default value is 'Any'.
• **VID**	Indicates (VLAN ID), either a specific VID or range of VIDs. VID can be in the range 1-4095 or 'Any'
• **PCP**	Priority Code Point: Valid value PCP are specific(0, 1, 2, 3, 4, 5, 6, 7) or range(0-1, 2-3, 4-5, 6-7, 0-3, 4-7) or 'Any'.
• **DEI**	Drop Eligible Indicator: Valid value of DEI can be any of values between 0, 1 or 'Any'.
• **Action**	Indicates the classification action taken on ingress frame if parameters configured are matched with the frame's content. There are three action fields: Class, DPL and DSCP. ■ **Class**: Classified QoS Class; if a frame matches the QCE it will be put in the queue. ■ **DPL**: Drop Precedence Level; if a frame matches the QCE then DP level will set to value displayed under DPL column. ■ **DSCP**: If a frame matches the QCE then DSCP will be classified with the value displayed under DSCP column.
• **Modification Buttons**	You can modify each QCE in the table using the following buttons: : Inserts a new QCE before the current row. : Edits the QCE. : Moves the QCE up the list. : Moves the QCE down the list. : Deletes the QCE. : The lowest plus sign adds a new entry at the bottom of the list of QCL.

4.9.11.1 QoS Control Entry Configuration

The QCE Configuration screen in Figure 4-9-14 appears.

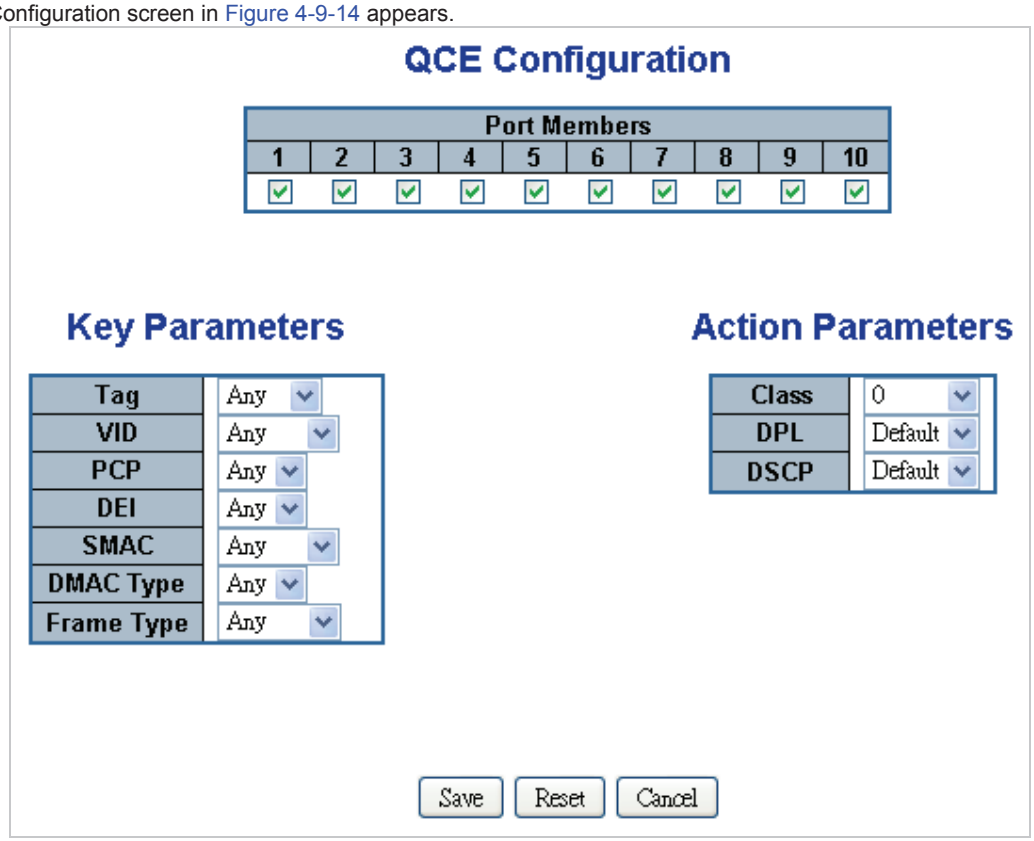


Figure 4-9-14: QCE Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Port Members**	Check the checkbox button in case you what to make any port member of the QCL entry. By default all ports will be checked
• **Key Parameters**	Key configuration is described as below: ■ **Tag** Value of Tag field can be 'Any', 'Untag' or 'Tag'. ■ **VID** Valid value of VLAN ID can be any value in the range 1-4095 or 'Any'; user can enter either a specific value or a range of VIDs. ■ **PCP** Priority Code Point: Valid value PCP are specific(0, 1, 2, 3, 4, 5, 6, 7) or range(0-1, 2-3, 4-5, 6-7, 0-3, 4-7) or 'Any'. ■ **DEI** Drop Eligible Indicator: Valid value of DEI can be any of values between 0, 1 or 'Any'. ■ **SMAC** Source MAC address: 24 MS bits (OUI) or 'Any'. ■ **DMAC Type** Destination MAC type: possible values are unicast(UC), multicast(MC), broadcast(BC) or 'Any'. ■ **Frame Type** Frame Type can have any of the following values: 1. **Any** 2. **Ethernet** 3. **LLC** 4. **SNAP** 5. **IPv4** 6. **IPv6** Note: All frame types are explained below.
• **Any**	Allow all types of frames.
• **Ethernet**	**Ethernet Type** Valid ethernet type can have value within 0x600-0xFFFF or 'Any' but excluding 0x800(IPv4) and 0x86DD(IPv6), default value is 'Any'.
• **LLC**	■ **SSAP Address** Valid SSAP(Source Service Access Point) can vary from 0x00 to 0xFF or 'Any', the default value is 'Any' ■ **DSAP Address** Valid DSAP(Destination Service Access Point) can vary from

	0x00 to 0xFF or 'Any', the default value is 'Any' ■ **Control Address** Valid Control Address can vary from 0x00 to 0xFF or 'Any', the default value is 'Any'
• **SNAP**	**PID** Valid PID(a.k.a ethernet type) can have value within 0x00-0xFFFF or 'Any', default value is 'Any'
• **IPv4**	■ **Protocol** IP protocol number: (0-255, TCP or UDP) or 'Any' ■ **Source IP** Specific Source IP address in value/mask format or 'Any'. IP and Mask are in the format x.y.z.w where x, y, z, and w are decimal numbers between 0 and 255. When Mask is converted to a 32-bit binary string and read from left to right, all bits following the first zero must also be zero **DSCP** Diffserv Code Point value(DSCP): It can be specific value, range of value or 'Any'. DSCP values are in the range 0-63 including BE, CS1-CS7, EF or AF11-AF43 ■ **IP Fragment** IPv4 frame fragmented option: yes|no|any ■ **Sport** Source TCP/UDP port:(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP ■ **Dport** Destination TCP/UDP port:(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP
29. IPv6	■ **Protocol** IP protocol number: (0-255, TCP or UDP) or 'Any' ■ **Source IP** IPv6 source address: (a.b.c.d) or 'Any', 32 LS bits ■ **DSCP** Diffserv Code Point value(DSCP): It can be specific value, range of value or 'Any'. DSCP values are in the range 0-63 including BE, CS1-CS7, EF or AF11-AF43 ■ **Sport** Source TCP/UDP port:(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP ■ **Dport** Destination TCP/UDP port:(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP
30. Action Parameters	■ **Class** QoS class: (0-7) or 'Default'. ■ **DP** Valid Drop Precedence Level can be (0-1) or 'Default'. ■ **DSCP** Valid DSCP value can be (0-63, BE, CS1-CS7, EF or AF11-AF43) or 'Default'. 'Default' means that the default classified value is not modified by this QCE.

Buttons

[redacted]: Click to save the configuration and move to main QCL page

[redacted]: Click to undo any changes made locally and revert to previously saved values

[redacted]: Return to the previous page without saving the configuration change

4.9.12 QoS Status

This page shows the QCL status by different QCL users. Each row describes the QCE that is defined. It is a conflict if a specific QCE is not applied to the hardware due to hardware limitations. The maximum number of QCEs is **256** on each switch. The QoS Control List Status screen in Figure 4-9-15 appears.

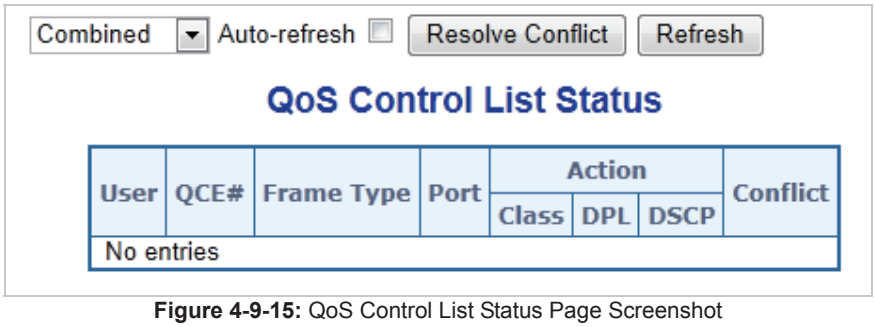


Figure 4-9-15: QoS Control List Status Page Screenshot

The page includes the following fields:

Object	Description
• **User**	Indicates the QCL user.

• **QCE#**	Indicates the index of QCE.
31. Frame Type	Indicates the type of frame to look for incomming frames. Possible frame types are: ■ **Any**: The QCE will match all frame type. ■ **Ethernet**: Only Ethernet frames (with Ether Type 0x600-0xFFFF) are allowed. ■ **LLC**: Only (LLC) frames are allowed. ■ **SNAP**: Only (SNAP) frames are allowed. ■ **IPv4**: The QCE will match only IPV4 frames. ■ **IPv6**: The QCE will match only IPV6 frames.
32. Port	Indicates the list of ports configured with the QCE
33. Action	Indicates the classification action taken on ingress frame if parameters configured are matched with the frame's content. There are three action fields: Class, DPL and DSCP. ■ **Class**: Classified QoS Class; if a frame matches the QCE it will be put in the queue. ■ **DPL**: Drop Precedence Level; if a frame matches the QCE then DP level will set to value displayed under DPL column. ■ **DSCP**: If a frame matches the QCE then DSCP will be classified with the value displayed under DSCP column.
• **Conflict**	Displays QCE status. It may happen that resources required to add a QCE may not available, in that case it shows conflict status as 'Yes', otherwise it is always 'No'.Please note that conflict can be resolved by releaseing the resource required by the QCE and pressing 'Refresh' button.

Buttons

[redacted]: Select the QCL status from this drop down list.

Auto-refresh [redacted]: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

[redacted]: Click to release the resources required to add QCL entry, incase conflict status for any QCL entry is 'yes'.

4.9.13 Storm Control Configuration

Storm control for the switch is configured on this page.

There is a unicast storm rate control, multicast storm rate control, and a broadcast storm rate control. These only affect flooded frames, i.e. frames with a (VLAN ID, DMAC) pair not present on the MAC Address table.
The configuration indicates the permitted packet rate for unicast, multicast or broadcast traffic across the switch. The Storm Control Configuration screen in Figure 4-9-16 appears.

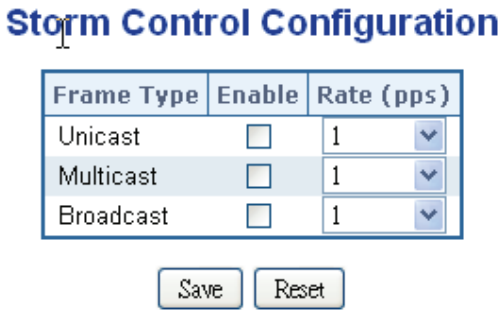


Figure 4-9-16: Storm Control Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Frame Type**	The settings in a particular row apply to the frame type listed here: ■ **unicast** ■ **multicast** ■ **Broadcast**
• **Enable**	Enable or disable the storm control status for the given frame type.
• **Rate**	The rate unit is packets per second (pps). Valid values are: 1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1K, 2K, 4K, 8K, 16K, 32K, 64K, 128K, 256K, 512K , 1024K, 2048K, 4096K, 8192K, 16384K or 32768K.

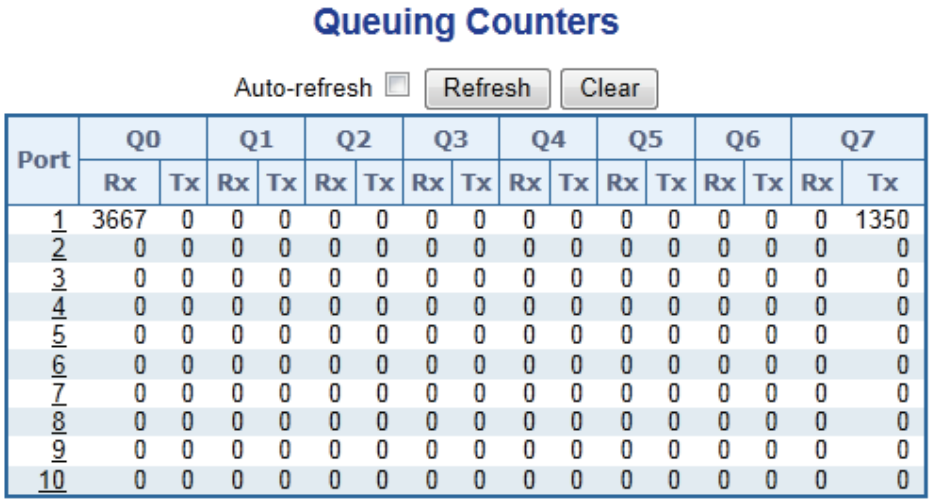
Buttons

[redacted]: Click to save changes.

[redacted]: Click to undo any changes made locally and revert to previously saved values.

4.9.14 QoS Statistics

This page provides statistics for the different queues for all switch ports. The QoS Statistics screen in Figure 4-9-17 appears.



Port	Q0		Q1		Q2		Q3		Q4		Q5		Q6		Q7	
	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx
1	3667	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1350
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Figure 4-9-17: Queuing Counters Page Screenshot

The page includes the following fields:

Object	Description
• **Port**	The logical port for the settings contained in the same row.
• **Q0 ~ Q7**	There are 8 QoS queues per port. Q0 is the lowest priority queue.
• **Rx/Tx**	The number of received and transmitted packets per queue.

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

4.9.15 Voice VLAN Configuration

The Voice VLAN feature enables voice traffic forwarding on the Voice VLAN, then the switch can classify and schedule network traffic. It is recommended that there be two VLANs on a port - one for voice, one for data. Before connecting the IP device to the switch, the IP phone should configure the voice VLAN ID correctly. It should be configured through its own GUI. The Voice VLAN Configuration screen in Figure 4-9-18 appears.

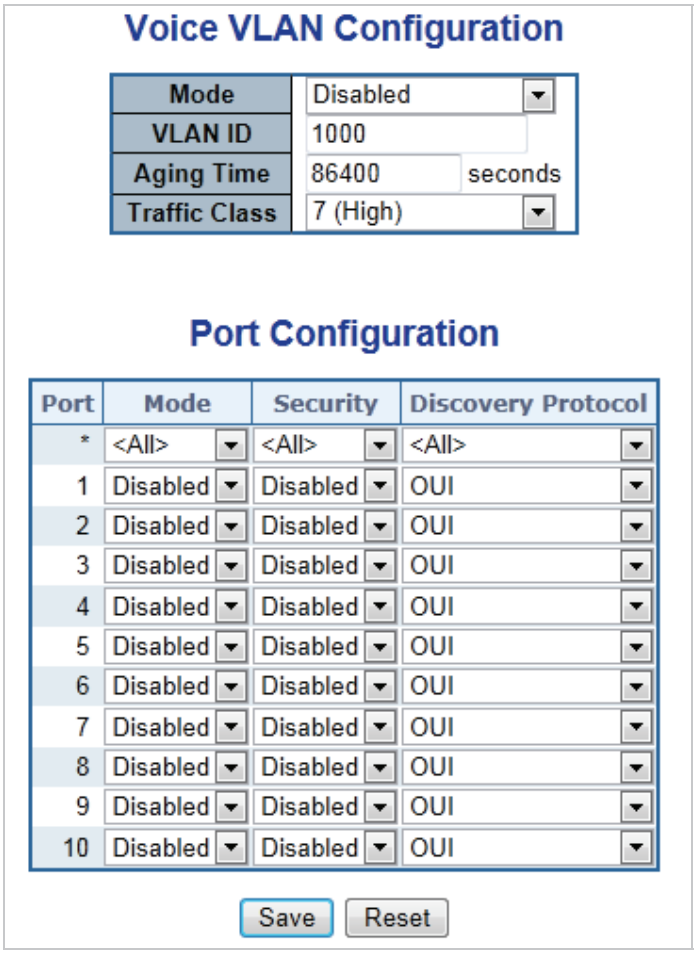


Figure 4-9-18: Voice VLAN Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Mode**	Indicates the Voice VLAN mode operation. We must disable MSTP feature before we enable Voice VLAN. It can avoid the conflict of ingress filter. Possible modes are: ■ **Enabled**: Enable Voice VLAN mode operation. ■ **Disabled**: Disable Voice VLAN mode operation.
• **VLAN ID**	Indicates the Voice VLAN ID. It should be a unique VLAN ID in the system and cannot equal each port PVID. It is conflict configuration if the value equal management VID, MVR VID, PVID etc. The allowed range is 1 to 4095.
• **Age Time**	Indicates the Voice VLAN secure learning age time. The allowed range is 10 to 10000000 seconds. It used when security mode or auto detect mode is enabled. In other cases, it will based hardware age time. The actual age time will be situated in the [age_time; 2 * age_time] interval.
• **Traffic Class**	Indicates the Voice VLAN traffic class. All traffic on Voice VLAN will apply this class.
34. Port Mode	Indicates the Voice VLAN port mode. When the port mode isn't disabled, we must disable MSTP feature before we enable Voice VLAN. It can avoid the conflict of ingress filter. Possible port modes are: ■ **Disabled**: Disjoin from Voice VLAN. ■ **Auto**: Enable auto detect mode. It detects whether there is VoIP phone attached on the specific port and configure the Voice VLAN members

	automatically. ■ **Forced**: Forced join to Voice VLAN. ■ **All** means all ports will have one specific setting.
35. Port Security	Indicates the Voice VLAN port security mode. When the function is enabled, all non-telephone MAC address in Voice VLAN will be blocked 10 seconds. Possible port modes are: ■ **Enabled**: Enable Voice VLAN security mode operation. ■ **Disabled**: Disable Voice VLAN security mode operation. ■ **All** means all ports will have one specific setting.
36. Port Discovery Protocol	Indicates the Voice VLAN port discovery protocol. It will only work when auto detect mode is enabled. We should enable LLDP feature before configuring discovery protocol to "LLDP" or "Both". Changing the discovery protocol to "OUI" or "LLDP" will restart auto detect process. Possible discovery protocols are: ■ **OUI**: Detect telephony device by OUI address. ■ **LLDP**: Detect telephony device by LLDP. ■ **Both**: Both OUI and LLDP. ■ **All** means all ports will have one specific setting.

Buttons

 : Click to save changes.

 : Click to undo any changes made locally and revert to previously saved values.

4.9.16 Voice VLAN OUI Table

Configure VOICE VLAN OUI table on this page. The maximum entry number is 16. Modifying the OUI table will restart auto detection of OUI process. The Voice VLAN OUI Table screen in Figure 4-9-19 appears.

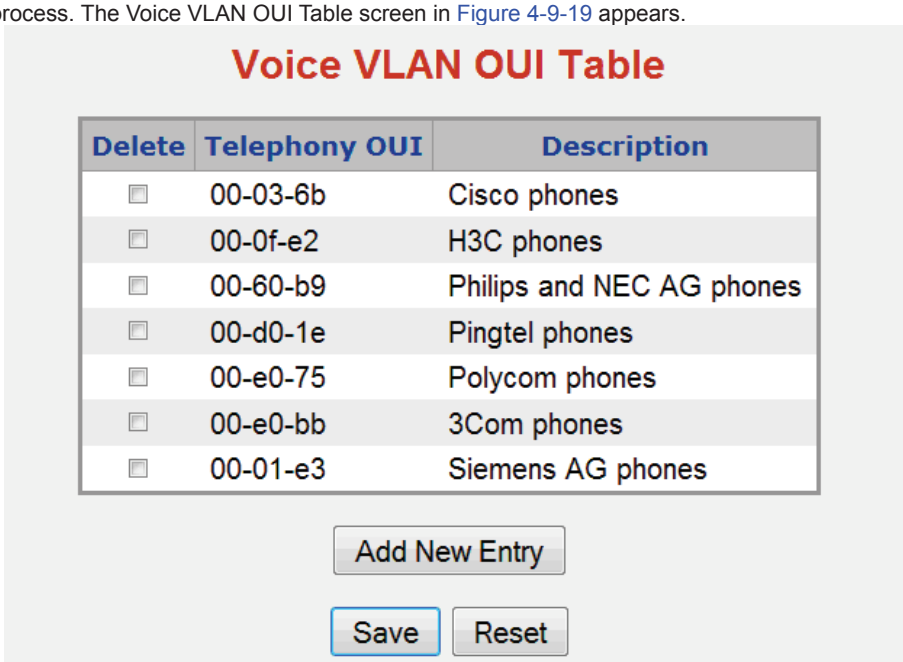


Figure 4-9-19 : Voice VLAN OUI Table Page Screenshot

The page includes the following fields:

Object	Description
• **Delete**	Check to delete the entry. It will be deleted during the next save.
• **Telephony OUI**	An telephony OUI address is a globally unique identifier assigned to a vendor by IEEE. It must be 6 characters long and the input format is "xx-xx-xx" (x is a hexadecimal digit).
• **Description**	The description of OUI address. Normaly, it descript which vendor telephony device. The allowed string length is 0 to 32.

Buttons

4.10.1 Access Control List Status

This page shows the ACL status by different ACL users. Each row describes the ACE that is defined. It is a conflict if a specific ACE is not applied to the hardware due to hardware limitations. The maximum number of ACEs is **256** on each switch. The Voice VLAN OUI Table screen in Figure 4-10-1 appears.

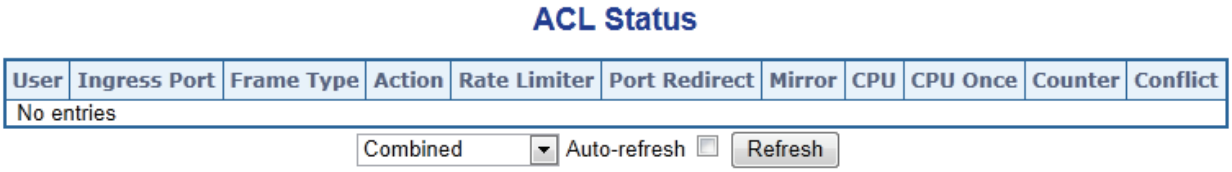


Figure 4-10-1: ACL Status Page Screenshot

The page includes the following fields:

Object	Description
37. User	Indicates the ACL user.
38. Ingress Port	Indicates the ingress port of the ACE. Possible values are: ■ **All**: The ACE will match all ingress port. ■ **Port**: The ACE will match a specific ingress port.
39. Frame Type	Indicates the frame type of the ACE. Possible values are: ■ **Any**: The ACE will match any frame type. ■ **EType**: The ACE will match Ethernet Type frames. Note that an Ethernet Type based ACE will not get matched by IP and ARP frames. ■ **ARP**: The ACE will match ARP/RARP frames. ■ **IPv4**: The ACE will match all IPv4 frames. ■ **IPv4/ICMP**: The ACE will match IPv4 frames with ICMP protocol. ■ **IPv4/UDP**: The ACE will match IPv4 frames with UDP protocol. ■ **IPv4/TCP**: The ACE will match IPv4 frames with TCP protocol. ■ **IPv4/Other**: The ACE will match IPv4 frames, which are not ICMP/UDP/TCP. ■ **IPv6**: The ACE will match all IPv6 standard frames.
40. Action	Indicates the forwarding action of the ACE. ■ **Permit**: Frames matching the ACE may be forwarded and learned. ■ **Deny**: Frames matching the ACE are dropped.
41. Rate Limiter	Indicates the rate limiter number of the ACE. The allowed range is 1 to 16. When Disabled is displayed, the rate limiter operation is disabled.
42. Port Redirect	Indicates the port redirect operation of the ACE. Frames matching the ACE are redirected to the port number. The allowed values are **Disabled** or a specific port number. When **Disabled** is displayed, the port redirect operation is disabled.
43. Mirror	Specify the mirror operation of this port. The allowed values are: ■ **Enabled**: Frames received on the port are mirrored. ■ **Disabled**: Frames received on the port are not mirrored. The default value is **"Disabled"**.
44. CPU	Forward packet that matched the specific ACE to CPU.
45. CPU Once	Forward first packet that matched the specific ACE to CPU.
46. Counter	The counter indicates the number of times the ACE was hit by a frame.
47. Conflict	Indicates the hardware status of the specific ACE. The specific ACE is not applied to the hardware due to hardware limitations.

Buttons

[redacted]: Select the ACL status from this drop down list.

Auto-refresh [redacted]: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

4.10.2 Access Control List Configuration

This page shows the Access Control List (ACL), which is made up of the ACEs defined on this switch. Each row describes the ACE that is defined. The maximum number of ACEs is **256** on each switch.
Click on the lowest plus sign to add a new ACE to the list. The reserved ACEs used for internal protocol, cannot be edited or deleted, the order sequence cannot be changed and the priority is highest.
The Access Control List Configuration screen in Figure 4-10-2 appears.

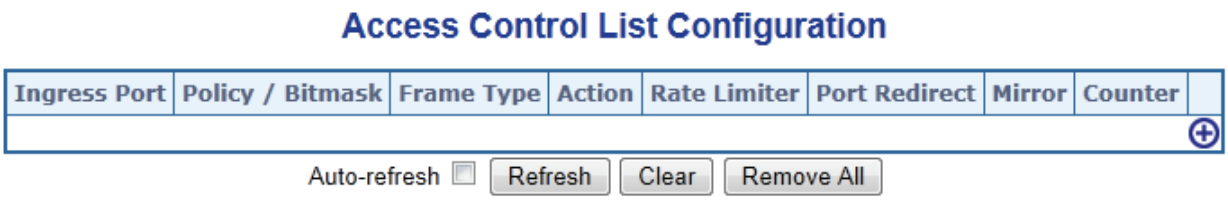


Figure 4-10-2: Access Control List Configuration Page Screenshot

The page includes the following fields:

Object	Description
48. Ingress Port	Indicates the ingress port of the ACE. Possible values are: ■ **All:** The ACE will match all ingress port. ■ **Port:** The ACE will match a specific ingress port.
49. Policy / Bitmask	Indicates the policy number and bitmask of the ACE.
50. Frame Type	Indicates the frame type of the ACE. Possible values are: ■ **Any**: The ACE will match any frame type. ■ **EType**: The ACE will match Ethernet Type frames. Note that an Ethernet Type based ACE will not get matched by IP and ARP frames. ■ **ARP**: The ACE will match ARP/RARP frames. ■ **IPv4**: The ACE will match all IPv4 frames. ■ **IPv4/ICMP**: The ACE will match IPv4 frames with ICMP protocol. ■ **IPv4/UDP**: The ACE will match IPv4 frames with UDP protocol. ■ **IPv4/TCP**: The ACE will match IPv4 frames with TCP protocol. ■ **IPv4/Other**: The ACE will match IPv4 frames, which are not ICMP/UDP/TCP. ■ **IPv6**: The ACE will match all IPv6 standard frames.
51. Action	Indicates the forwarding action of the ACE. ■ **Permit**: Frames matching the ACE may be forwarded and learned. ■ **Deny**: Frames matching the ACE are dropped.
• **Rate Limiter**	Indicates the rate limiter number of the ACE. The allowed range is 1 to 16. When Disabled is displayed, the rate limiter operation is disabled.
• **Port Redirect**	Indicates the port redirect operation of the ACE. Frames matching the ACE are redirected to the port number. The allowed values are **Disabled** or a specific port number. When **Disabled** is displayed, the port redirect operation is disabled.
• **Mirror**	Specify the mirror operation of this port. Frames matching the ACE are mirrored to the destination mirror port. The allowed values are: ■ **Enabled:** Frames received on the port are mirrored. ■ **Disabled:** Frames received on the port are not mirrored. The default value is "Disabled".v
• **Counter**	The counter indicates the number of times the ACE was hit by a frame.
• **Modification Buttons**	You can modify each ACE (Access Control Entry) in the table using the following buttons: : Inserts a new ACE before the current row. : Edits the ACE row. : Moves the ACE up the list. : Moves the ACE down the list. : Deletes the ACE. : The lowest plus sign adds a new entry at the bottom of the ACE listings.

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

: Click to remove all ACEs.

4.10.3 ACE Configuration

Configure an ACE (Access Control Entry) on this page.

An ACE consists of several parameters. These parameters vary according to the frame type that you select. First select the ingress port for the ACE, and then select the frame type. Different parameter options are displayed depending on the frame type selected.

A frame that hits this ACE matches the configuration that is defined here. The ACE Configuration screen in Figure 4-10-3 appears.

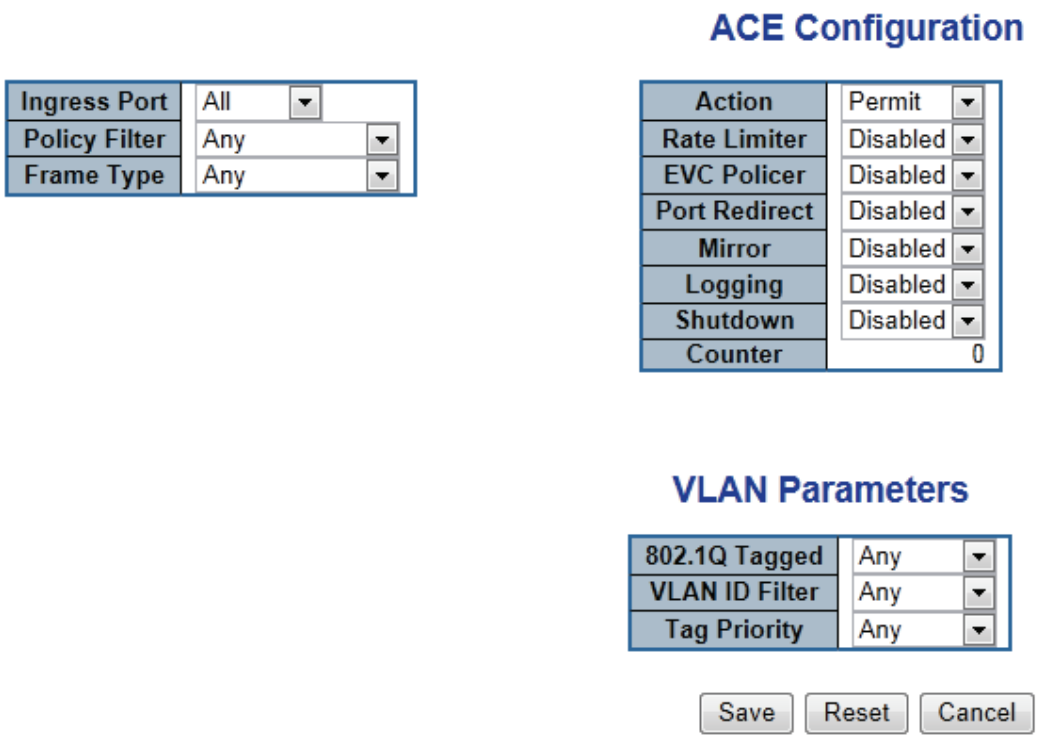


Figure 4-10-3: ACE Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Ingress Port**	Select the ingress port for which this ACE applies. `All`: The ACE applies to all port. `Port n`: The ACE applies to this port number, where *n* is the number of the switch port.
• **Policy Filter**	Specify the policy number filter for this ACE. **Any:** No policy filter is specified. (policy filter status is "don't-care".) **Specific:** If you want to filter a specific policy with this ACE, choose this value. Two field for entering an policy value and bitmask appears.
• **Policy Value**	When **"Specific"** is selected for the policy filter, you can enter a specific policy value. The allowed range is **0** to **255**.
• **Policy Bitmask**	When **"Specific"** is selected for the policy filter, you can enter a specific policy bitmask. The allowed range is **0x0** to **0xff**.
• **Frame Type**	Select the frame type for this ACE. These frame types are mutually exclusive. **Any**: Any frame can match this ACE. **Ethernet Type**: Only Ethernet Type frames can match this ACE. The IEEE 802.3 describes the value of Length/Type Field specifications to be greater than or equal to 1536 decimal (equal to 0600 hexadecimal). **ARP**: Only ARP frames can match this ACE. Notice the ARP frames won't match the ACE with ethernet type. **IPv4**: Only IPv4 frames can match this ACE. Notice the IPv4 frames won't match the ACE with ethernet type.

• **Action**	Specify the action to take with a frame that hits this ACE. **Permit**: The frame that hits this ACE is granted permission for the ACE operation. **Deny**: The frame that hits this ACE is dropped.
• **Rate Limiter**	Specify the rate limiter in number of base units. The allowed range is 1 to 16. Disabled indicates that the rate limiter operation is disabled.
• **EVC Policer**	Select whether EVC policer is enabled or disabled. The default value is **"Disabled"**.
• **EVC Policer ID**	Select which EVC policer ID to apply on this ACE. The allowed values are `Disabled` or the values `1` through `128`.
• **Port Redirect**	Frames that hit the ACE are redirected to the port number specified here. The allowed range is the same as the switch port number range. **Disabled** indicates that the port redirect operation is disabled.
• **Mirror**	Specify the mirror operation of this port. The allowed values are: **Enabled**: Frames received on the port are mirrored. **Disabled**: Frames received on the port are not mirrored. The default value is "Disabled".
• **Logging**	Specify the logging operation of the ACE. The allowed values are: **Enabled**: Frames matching the ACE are stored in the System Log. **Disabled**: Frames matching the ACE are not logged. Please note that the System Log memory size and logging rate is limited.
• **Shutdown**	Specify the port shut down operation of the ACE. The allowed values are: **Enabled**: If a frame matches the ACE, the ingress port will be disabled. **Disabled**: Port shut down is disabled for the ACE.
• **Counter**	The counter indicates the number of times the ACE was hit by a frame.

■ MAC Parameters

Object	Description
• **SMAC Filter**	(Only displayed when the frame type is Ethernet Type or ARP.) Specify the source MAC filter for this ACE. **Any**: No SMAC filter is specified. (SMAC filter status is "don't-care".) **Specific**: If you want to filter a specific source MAC address with this ACE, choose this value. A field for entering an SMAC value appears.
• **SMAC Value**	When "Specific" is selected for the SMAC filter, you can enter a specific source MAC address. The legal format is "xx-xx-xx-xx-xx-xx". A frame that hits this ACE matches this SMAC value.
• **DMAC Filter**	Specify the destination MAC filter for this ACE. **Any**: No DMAC filter is specified. (DMAC filter status is "don't-care".) **MC**: Frame must be multicast. **BC**: Frame must be broadcast. **UC**: Frame must be unicast. **Specific**: If you want to filter a specific destination MAC address with this ACE, choose this value. A field for entering a DMAC value appears.
• **DMAC Value**	When **"Specific"** is selected for the DMAC filter, you can enter a specific destination MAC address. The legal format is "xx-xx-xx-xx-xx-xx". A frame that hits this ACE matches this DMAC value.

■ VLAN Parameters

Object	Description
• **802.1Q Tagged**	Specify whether frames can hit the action according to the 802.1Q tagged. The allowed values are: **Any**: Any value is allowed ("don't-care"). **Enabled**: Tagged frame only. **Disabled**: Untagged frame only. The default value is "Any".
• **VLAN ID Filter**	Specify the VLAN ID filter for this ACE. **Any**: No VLAN ID filter is specified. (VLAN ID filter status is "don't-care".) **Specific**: If you want to filter a specific VLAN ID with this ACE, choose this value. A field for entering a VLAN ID number appears.
• **VLAN ID**	When **"Specific"** is selected for the VLAN ID filter, you can enter a specific VLAN ID number. The allowed range is 1 to 4095. A frame that hits this ACE matches this VLAN ID value.
• **Tag Priority**	Specify the tag priority for this ACE. A frame that hits this ACE matches this tag priority. The allowed number range is 0 to 7. The value Any means that no tag priority is specified (tag priority is "don't-care".)

■ ARP Parameters

The ARP parameters can be configured when Frame Type "ARP" is selected.

Object	Description
• **ARP/RARP**	Specify the available ARP/RARP opcode (OP) flag for this ACE. **Any**: No ARP/RARP OP flag is specified. (OP is "don't-care".) **ARP**: Frame must have ARP/RARP opcode set to ARP. **RARP**: Frame must have ARP/RARP opcode set to RARP. **Other**: Frame has unknown ARP/RARP Opcode flag.
• **Request/Reply**	Specify the available ARP/RARP opcode (OP) flag for this ACE. **Any**: No ARP/RARP OP flag is specified. (OP is "don't-care".) **Request**: Frame must have ARP Request or RARP Request OP flag set. **Reply**: Frame must have ARP Reply or RARP Reply OP flag.
• **Sender IP Filter**	Specify the sender IP filter for this ACE. **Any**: No sender IP filter is specified. (Sender IP filter is "don't-care".) **Host**: Sender IP filter is set to Host. Specify the sender IP address in the SIP Address field that appears. **Network**: Sender IP filter is set to Network. Specify the sender IP address and sender IP mask in the SIP Address and SIP Mask fields that appear.
• **Sender IP Address**	When "Host" or "Network" is selected for the sender IP filter, you can enter a specific sender IP address in dotted decimal notation.
• **Sender IP Mask**	When "Network" is selected for the sender IP filter, you can enter a specific sender IP mask in dotted decimal notation.
• **Target IP Filter**	Specify the target IP filter for this specific ACE. **Any**: No target IP filter is specified. (Target IP filter is "don't-care".) **Host**: Target IP filter is set to Host. Specify the target IP address in the Target IP

	Address field that appears. **Network**: Target IP filter is set to Network. Specify the target IP address and target IP mask in the Target IP Address and Target IP Mask fields that appear.
• **Target IP Address**	When "Host" or "Network" is selected for the target IP filter, you can enter a specific target IP address in dotted decimal notation.
• **Target IP Mask**	When "Network" is selected for the target IP filter, you can enter a specific target IP mask in dotted decimal notation.
• **ARP SMAC Match**	Specify whether frames can hit the action according to their sender hardware address field (SHA) settings. **0**: ARP frames where SHA is not equal to the SMAC address. **1**: ARP frames where SHA is equal to the SMAC address. **Any**: Any value is allowed ("don't-care").
• **RARP SMAC Match**	Specify whether frames can hit the action according to their target hardware address field (THA) settings. **0**: RARP frames where THA is not equal to the SMAC address. **1**: RARP frames where THA is equal to the SMAC address. **Any**: Any value is allowed ("don't-care").
• **IP/Ethernet Length**	Specify whether frames can hit the action according to their ARP/RARP hardware address length (HLN) and protocol address length (PLN) settings. **0**: ARP/RARP frames where the HLN is equal to Ethernet (0x06) and the (PLN) is equal to IPv4 (0x04). **1**: ARP/RARP frames where the HLN is equal to Ethernet (0x06) and the (PLN) is equal to IPv4 (0x04). **Any**: Any value is allowed ("don't-care").
• **IP**	Specify whether frames can hit the action according to their ARP/RARP hardware address space (HRD) settings. **0**: ARP/RARP frames where the HLD is equal to Ethernet (1). **1**: ARP/RARP frames where the HLD is equal to Ethernet (1). **Any**: Any value is allowed ("don't-care").
• **Ethernet**	Specify whether frames can hit the action according to their ARP/RARP protocol address space (PRO) settings. **0**: ARP/RARP frames where the PRO is equal to IP (0x800). **1**: ARP/RARP frames where the PRO is equal to IP (0x800). **Any**: Any value is allowed ("don't-care").

■ IP Parameters

The IP parameters can be configured when Frame Type "IPv4" is selected.

Object	Description
• **IP Protocol Filter**	Specify the IP protocol filter for this ACE. **Any**: No IP protocol filter is specified ("don't-care"). **Specific**: If you want to filter a specific IP protocol filter with this ACE, choose this value. A field for entering an IP protocol filter appears. **ICMP**: Select ICMP to filter IPv4 ICMP protocol frames. Extra fields for defining ICMP parameters will appear. These fields are explained later in this help file. **UDP**: Select UDP to filter IPv4 UDP protocol frames. Extra fields for defining UDP parameters will appear. These fields are explained later in this help file. **TCP**: Select TCP to filter IPv4 TCP protocol frames. Extra fields for defining TCP parameters will appear. These fields are explained later in this help file.
• **IP Protocol Value**	When "Specific" is selected for the IP protocol value, you can enter a specific value. The allowed range is **0** to **255**. A frame that hits this ACE matches this IP protocol value.
• **IP TTL**	Specify the Time-to-Live settings for this ACE. **zero**: IPv4 frames with a Time-to-Live field greater than zero must not be able to match this entry. **non-zero**: IPv4 frames with a Time-to-Live field greater than zero must be able to match this entry. **Any**: Any value is allowed ("don't-care").
• **IP Fragment**	Specify the fragment offset settings for this ACE. This involves the settings for the More Fragments (MF) bit and the Fragment Offset (FRAG OFFSET) field for an IPv4 frame. **No**: IPv4 frames where the MF bit is set or the FRAG OFFSET field is greater than zero must not be able to match this entry. **Yes**: IPv4 frames where the MF bit is set or the FRAG OFFSET field is greater than zero must be able to match this entry. **Any**: Any value is allowed ("don't-care").

• **IP Option**	Specify the options flag setting for this ACE. **No**: IPv4 frames where the options flag is set must not be able to match this entry. **Yes**: IPv4 frames where the options flag is set must be able to match this entry. **Any**: Any value is allowed ("don't-care").
• **SIP Filter**	Specify the source IP filter for this ACE. **Any**: No source IP filter is specified. (Source IP filter is "don't-care".) **Host**: Source IP filter is set to Host. Specify the source IP address in the SIP Address field that appears. **Network**: Source IP filter is set to Network. Specify the source IP address and source IP mask in the SIP Address and SIP Mask fields that appear.
• **SIP Address**	When "Host" or "Network" is selected for the source IP filter, you can enter a specific SIP address in dotted decimal notation.
• **SIP Mask**	When "Network" is selected for the source IP filter, you can enter a specific SIP mask in dotted decimal notation.
• **DIP Filter**	Specify the destination IP filter for this ACE. **Any**: No destination IP filter is specified. (Destination IP filter is "don't-care".) **Host**: Destination IP filter is set to Host. Specify the destination IP address in the DIP Address field that appears. **Network**: Destination IP filter is set to Network. Specify the destination IP address and destination IP mask in the DIP Address and DIP Mask fields that appear.
• **DIP Address**	When "Host" or "Network" is selected for the destination IP filter, you can enter a specific DIP address in dotted decimal notation.
• **DIP Mask**	When "Network" is selected for the destination IP filter, you can enter a specific DIP mask in dotted decimal notation.

■ ICMP Parameters

Object	Description
• **ICMP Type Filter**	Specify the ICMP filter for this ACE. **Any**: No ICMP filter is specified (ICMP filter status is "don't-care"). **Specific**: If you want to filter a specific ICMP filter with this ACE, you can enter a specific ICMP value. A field for entering an ICMP value appears.
• **ICMP Type Value**	When "Specific" is selected for the ICMP filter, you can enter a specific ICMP value. The allowed range is `0` to `255`. A frame that hits this ACE matches this ICMP value.
• **ICMP Code Filter**	Specify the ICMP code filter for this ACE. **Any**: No ICMP code filter is specified (ICMP code filter status is "don't-care"). **Specific**: If you want to filter a specific ICMP code filter with this ACE, you can enter a specific ICMP code value. A field for entering an ICMP code value appears.
• **ICMP Code Value**	When "Specific" is selected for the ICMP code filter, you can enter a specific ICMP code value. The allowed range is `0` to `255`. A frame that hits this ACE matches this ICMP code value.

■ TCP/UDP Parameters

Object	Description
• **TCP/UDP Source Filter**	Specify the TCP/UDP source filter for this ACE. **Any**: No TCP/UDP source filter is specified (TCP/UDP source filter status is "don't-care"). **Specific**: If you want to filter a specific TCP/UDP source filter with this ACE, you can enter a specific TCP/UDP source value. A field for entering a TCP/UDP source value appears. **Range**: If you want to filter a specific TCP/UDP source range filter with this ACE, you can enter a specific TCP/UDP source range value. A field for entering a TCP/UDP source value appears.
• **TCP/UDP Source No.**	When "Specific" is selected for the TCP/UDP source filter, you can enter a specific TCP/UDP source value. The allowed range is `0` to `65535`. A frame that hits this ACE matches this TCP/UDP source value.
• **TCP/UDP Source Range**	When "Range" is selected for the TCP/UDP source filter, you can enter a specific TCP/UDP source range value. The allowed range is `0` to `65535`. A frame that hits this ACE matches this TCP/UDP source value.
• **TCP/UDP Destination Filter**	Specify the TCP/UDP destination filter for this ACE. **Any**: No TCP/UDP destination filter is specified (TCP/UDP destination filter

	status is "don't-care"). **Specific**: If you want to filter a specific TCP/UDP destination filter with this ACE, you can enter a specific TCP/UDP destination value. A field for entering a TCP/UDP destination value appears. **Range**: If you want to filter a specific range TCP/UDP destination filter with this ACE, you can enter a specific TCP/UDP destination range value. A field for entering a TCP/UDP destination value appears.
• **TCP/UDP Destination Number**	When "Specific" is selected for the TCP/UDP destination filter, you can enter a specific TCP/UDP destination value. The allowed range is **0** to **65535**. A frame that hits this ACE matches this TCP/UDP destination value.
• **TCP/UDP Destination Range**	When "Range" is selected for the TCP/UDP destination filter, you can enter a specific TCP/UDP destination range value. The allowed range is **0** to **65535**. A frame that hits this ACE matches this TCP/UDP destination value.
• **TCP FIN**	Specify the TCP "No more data from sender" (FIN) value for this ACE. **0**: TCP frames where the FIN field is set must not be able to match this entry. **1**: TCP frames where the FIN field is set must be able to match this entry. **Any**: Any value is allowed ("don't-care").
• **TCP SYN**	Specify the TCP "Synchronize sequence numbers" (SYN) value for this ACE. **0**: TCP frames where the SYN field is set must not be able to match this entry. **1**: TCP frames where the SYN field is set must be able to match this entry. **Any**: Any value is allowed ("don't-care").
• **TCP RST**	Specify the TCP "Reset the connection" (RST) value for this ACE. **0**: TCP frames where the RST field is set must not be able to match this entry. **1**: TCP frames where the RST field is set must be able to match this entry. **Any**: Any value is allowed ("don't-care").
• **TCP PSH**	Specify the TCP "Push Function" (PSH) value for this ACE. **0**: TCP frames where the PSH field is set must not be able to match this entry. **1**: TCP frames where the PSH field is set must be able to match this entry. **Any**: Any value is allowed ("don't-care").
• **TCP ACK**	Specify the TCP "Acknowledgment field significant" (ACK) value for this ACE. **0**: TCP frames where the ACK field is set must not be able to match this entry. **1**: TCP frames where the ACK field is set must be able to match this entry. **Any**: Any value is allowed ("don't-care").
• **TCP URG**	Specify the TCP "Urgent Pointer field significant" (URG) value for this ACE. **0**: TCP frames where the URG field is set must not be able to match this entry. **1**: TCP frames where the URG field is set must be able to match this entry. **Any**: Any value is allowed ("don't-care").

■ Ethernet Type Parameters

The Ethernet Type parameters can be configured when Frame Type "Ethernet Type" is selected.

Object	Description
• **EtherType Filter**	Specify the Ethernet type filter for this ACE. **Any**: No EtherType filter is specified (EtherType filter status is "don't-care"). **Specific**: If you want to filter a specific EtherType filter with this ACE, you can enter a specific EtherType value. A field for entering a EtherType value appears.
• **Ethernet Type Value**	When "Specific" is selected for the EtherType filter, you can enter a specific EtherType value. The allowed range is **0x600** to **0xFFFF** but excluding 0x800(IPv4), 0x806(ARP) and 0x86DD(IPv6). A frame that hits this ACE matches this EtherType value.

Buttons

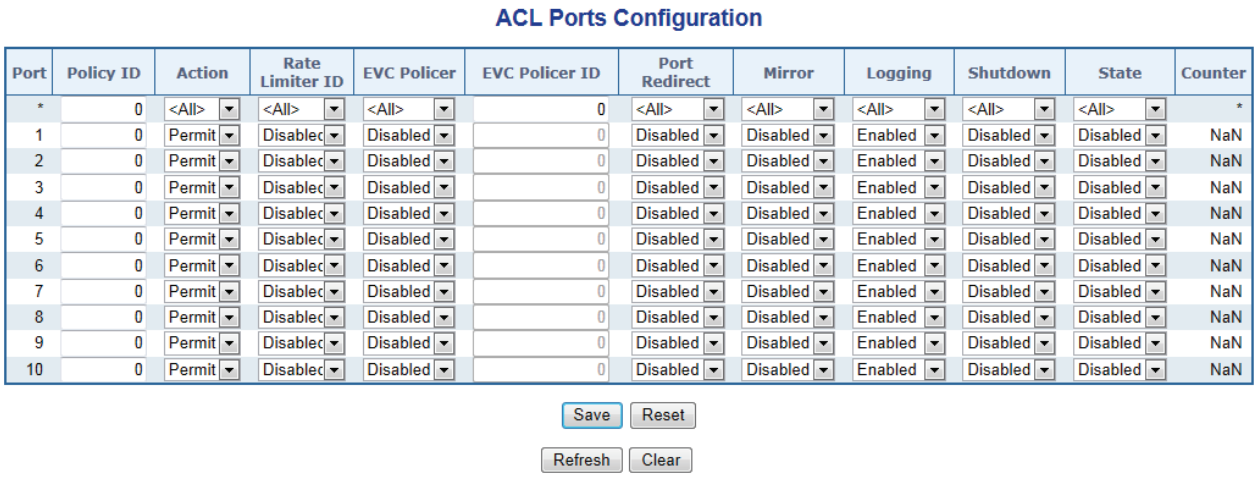
[redacted]: Click to save changes.

[redacted]: Click to undo any changes made locally and revert to previously saved values.

[redacted]: Return to the previous page.

4.10.4 ACL Ports Configuration

Configure the ACL parameters (ACE) of each switch port. These parameters will affect frames received on a port unless the frame matches a specific ACE.
The ACL Ports Configuration screen in Figure 4-10-4 appears.



ACL Ports Configuration

Port	Policy ID	Action	Rate Limiter ID	EVC Policer	EVC Policer ID	Port Redirect	Mirror	Logging	Shutdown	State	Counter
*	0	<All>	<All>	<All>	0	<All>	<All>	<All>	<All>	<All>	*
1	0	Permit	Disablec	Disabled	0	Disabled	Disabled	Enabled	Disabled	Disabled	NaN
2	0	Permit	Disablec	Disabled	0	Disabled	Disabled	Enabled	Disabled	Disabled	NaN
3	0	Permit	Disablec	Disabled	0	Disabled	Disabled	Enabled	Disabled	Disabled	NaN
4	0	Permit	Disablec	Disabled	0	Disabled	Disabled	Enabled	Disabled	Disabled	NaN
5	0	Permit	Disablec	Disabled	0	Disabled	Disabled	Enabled	Disabled	Disabled	NaN
6	0	Permit	Disablec	Disabled	0	Disabled	Disabled	Enabled	Disabled	Disabled	NaN
7	0	Permit	Disablec	Disabled	0	Disabled	Disabled	Enabled	Disabled	Disabled	NaN
8	0	Permit	Disablec	Disabled	0	Disabled	Disabled	Enabled	Disabled	Disabled	NaN
9	0	Permit	Disablec	Disabled	0	Disabled	Disabled	Enabled	Disabled	Disabled	NaN
10	0	Permit	Disablec	Disabled	0	Disabled	Disabled	Enabled	Disabled	Disabled	NaN

Save Reset

Refresh Clear

Figure 4-10-4: ACL Ports Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Port**	The logical port for the settings contained in the same row.
• **Policy ID**	Select the policy to apply to this port. The allowed values are `1` through `8`. The default value is **1**.
• **Action**	Select whether forwarding is permitted ("Permit") or denied ("Deny"). The default value is **"Permit"**. **All** means all ports will have one specific setting.
• **Rate Limiter ID**	Select which rate limiter to apply to this port. The allowed values are `Disabled` or the values `1` through `15`. The default value is **"Disabled"**. **All** means all ports will have one specific setting.
• **EVC Policer**	Select whether EVC policer is enabled or disabled. The default value is **"Disabled"**. **All** means all ports will have one specific setting.
• **EVC Policer ID**	Select which EVC policer ID to apply on this port. The allowed values are **Disabled** or the values **1** through **128**.
• **Port Redirect**	Select which port frames are redirected on. The allowed values are **Disabled** or a specific port number. The default value is **"Disabled"**. **All** means all ports will have one specific setting.
• **Mirror**	Specify the mirror operation of this port. The allowed values are: **Enabled**: Frames received on the port are mirrored. **Disabled**: Frames received on the port are not mirrored. The default value is **"Disabled".** **All** means all ports will have one specific setting.
• **Logging**	Specify the logging operation of this port. The allowed values are: **Enabled**: Frames received on the port are stored in the System Log. **Disabled**: Frames received on the port are not logged. The default value is **"Disabled"**. Please note that the System Log memory size and logging rate is limited. **All** means all ports will have one specific setting.
• **Shutdown**	Specify the port shut down operation of this port. The allowed values are: **Enabled**: If a frame is received on the port, the port will be disabled. **Disabled**: Port shut down is disabled. The default value is **"Disabled"**. **All** means all ports will have one specific setting.
• **State**	Specify the port state of this port. The allowed values are: **Enabled**: To reopen ports by changing the volatile port configuration of the ACL user module. **Disabled**: To close ports by changing the volatile port configuration of the ACL user module. The default value is **"Enabled"**. **All** means all ports will have one specific setting.
• **Counter**	Counts the number of frames that match this ACE.

Buttons

 : Click to save changes.

 : Click to undo any changes made locally and revert to previously saved values.

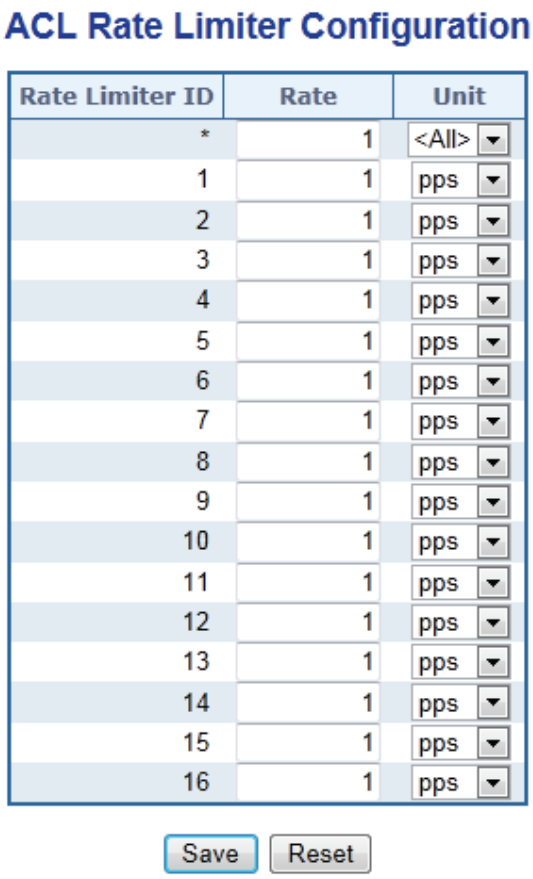


Figure 4-10-5: ACL Rate Limiter Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Rate Limiter ID**	The rate limiter ID for the settings contained in the same row.
• **Rate**	The allowed values are: 0-3276700 in pps or 0, 100, 200, 300, ..., 1000000 in kbps.
• **Unit**	Specify the rate unit. The allowed values are: **pps**: packets per second. **kbps**: Kbits per second. **All** means all ports will have one specific setting.

Buttons

[redacted]: Click to save changes.

[redacted]: Click to undo any changes made locally and revert to previously saved values.

4.11 Authentication

This section is to control the access of the Managed Switch, includes the user access and management control.
The Authentication section contains links to the following main topics:

- **IEEE 802.1X Port-Based Network Access Control**
- **MAC-Based Authentication**
- **User Authentication**

Overview of 802.1X (Port-Based) Authentication

In the 802.1X-world, the user is called the supplicant, the switch is the authenticator, and the RADIUS server is the authentication server. The switch acts as the man-in-the-middle, forwarding requests and responses between the supplicant and the authentication server. Frames sent between the supplicant and the switch are special 802.1X frames, known as **EAPOL (EAP Over LANs)** frames. EAPOL frames encapsulate **EAP PDU**s (RFC3748). Frames sent between the switch and the RADIUS server are RADIUS packets. RADIUS packets also encapsulate EAP PDUs together with other attributes like the switch's IP address, name, and the supplicant's port number on the switch. EAP is very flexible, in that it allows for different authentication methods, like **MD5-Challenge**, **PEAP**, and **TLS**. The important thing is that the authenticator (the switch) doesn't need to know which authentication method the supplicant and the authentication server are using, or how many information exchange frames are needed for a particular method. The switch simply encapsulates the EAP part of the frame into the relevant type (EAPOL or RADIUS) and forwards it.

When authentication is complete, the RADIUS server sends a special packet containing a success or failure indication. Besides forwarding this decision to the supplicant, the switch uses it to open up or block traffic on the switch port connected to the supplicant.

Overview of MAC-Based Authentication

Unlike 802.1X, MAC-based authentication is not a standard, but merely a best-practices method adopted by the industry. In MAC-based authentication, users are called clients, and the switch acts as the supplicant on behalf of clients. The initial frame (any kind of frame) sent by a client is snooped by the switch, which in turn uses the client's MAC address as both username and password in the subsequent EAP exchange with the RADIUS server. The 6-byte MAC address is converted to a string on the following form "xx-xx-xx-xx-xx-xx", that is, a dash (-) is used as separator between the lower-cased hexadecimal digits. The switch only supports the MD5-Challenge authentication method, so the RADIUS server must be configured accordingly.

When authentication is complete, the RADIUS server sends a success or failure indication, which in turn causes the switch to open up or block traffic for that particular client, using static entries into the MAC Table. Only then will frames from the client be forwarded on the switch. There are no EAPOL frames involved in this authentication, and therefore, MAC-based Authentication has nothing to do with the 802.1X standard.

The advantage of MAC-based authentication over 802.1X is that several clients can be connected to the same port (e.g. through a 3rd party switch or a hub) and still require individual authentication, and that the clients don't need special supplicant software to authenticate. The disadvantage is that MAC addresses can be spoofed by malicious users, equipment whose MAC address is a valid RADIUS user can be used by anyone, and only the MD5-Challenge method is supported.
The 802.1X and MAC-Based Authentication configuration consists of two sections, a system- and a port-wide.

Overview of User Authentication

It is allowed to configure the Managed Switch to authenticate users logging into the system for management access using local or remote authentication methods, such as telnet and Web browser. This Managed Switch provides secure network management access using the following options:

- **Remote Authentication Dial-in User Service (RADIUS)**
- **Terminal Access Controller Access Control System Plus (TACACS+)**
- **Local user name and Priviledge Level control**

RADIUS and TACACS+ are logon authentication protocols that use software running on a central server to control access to RADIUS-aware or TACACS-aware devices on the network. An **authentication server** contains a database of multiple user name / password pairs with associated privilege levels for each user that requires management access to the Managed Switch.

4.11.1 Understanding IEEE 802.1X Port-Based Authentication

The IEEE 802.1X standard defines a client-server-based access control and authentication protocol that restricts unauthorized clients from connecting to a LAN through publicly accessible ports. The authentication server authenticates each client connected to a switch port before making available any services offered by the switch or the LAN.

Until the client is authenticated, 802.1X access control allows only **Extensible Authentication Protocol over LAN (EAPOL)** traffic through the port to which the client is connected. After authentication is successful, normal traffic can pass through the port.

This section includes this conceptual information:

- Device Roles
- Authentication Initiation and Message Exchange
- Ports in Authorized and Unauthorized States

■ **Device Roles**

With 802.1X port-based authentication, the devices in the network have specific roles as shown below.

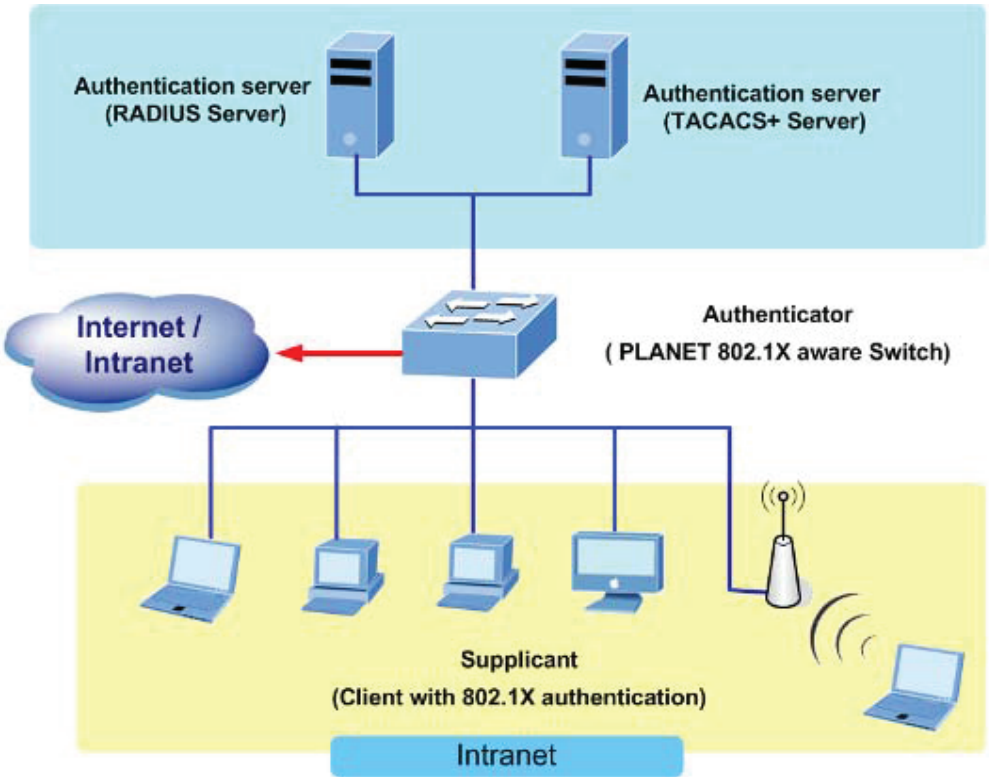


Figure 4-11-1

- ***Client***—the device (workstation) that requests access to the LAN and switch services and responds to requests from the switch. The workstation must be running 802.1X-compliant client software such as that offered in the Microsoft Windows XP operating system. (The client is the *supplicant* in the IEEE 802.1X specification.)

- ***Authentication server***—performs the actual authentication of the client. The authentication server validates the identity of the client and notifies the switch whether or not the client is authorized to access the LAN and switch services. Because the switch acts as the proxy, the authentication service is transparent to the client. In this release, the Remote Authentication Dial-In User Service (RADIUS) security system with **Extensible Authentication Protocol (EAP)** extensions is the only supported authentication server; it is available in Cisco Secure Access Control Server version 3.0. RADIUS operates in a client/server model in which secure authentication information is exchanged between the RADIUS server and one or more RADIUS clients.

- ***Switch* (802.1X device)**—controls the physical access to the network based on the authentication status of the client. The switch acts as an intermediary (proxy) between the client and the authentication server, requesting identity information from the client, verifying that information with the authentication server, and relaying a response to the client. The switch includes the RADIUS client, which is responsible for encapsulating and decapsulating the Extensible Authentication Protocol (EAP) frames and interacting with the authentication server. When the switch receives EAPOL frames and relays them to the authentication server, the Ethernet header is stripped and the remaining EAP frame is re-encapsulated in the RADIUS format. The EAP frames are not modified or examined during encapsulation, and the authentication server must support EAP within the native frame format. When the switch receives frames from the authentication server, the server's frame header is removed, leaving the EAP frame, which is then encapsulated for Ethernet and sent to the client.

■ **Authentication Initiation and Message Exchange**

The switch or the client can initiate authentication. If you enable authentication on a port by using the **dot1x port-control auto** interface configuration command, the switch must initiate authentication when it determines that the port link state transitions from down to up. It then sends an EAP-request/identity frame to the client to request its identity (typically, the switch sends an initial identity/request frame followed by one or more requests for authentication information). Upon receipt of the frame, the client responds with an EAP-response/identity frame.

However, if during bootup, the client does not receive an EAP-request/identity frame from the switch, the client can initiate authentication by sending an EAPOL-start frame, which prompts the switch to request the client's identity

If 802.1X is not enabled or supported on the network access device, any EAPOL frames from the client are dropped. If the client does not receive an EAP-request/identity frame after three attempts to start authentication, the client transmits frames as if the port was in the authorized state. A port in the authorized state effectively means that the client has been successfully authenticated.

When the client supplies its identity, the switch begins its role as the intermediary, passing EAP frames between the client and the authentication server until authentication succeeds or fails. If the authentication succeeds, the switch port becomes authorized.

The specific exchange of EAP frames depends on the authentication method being used. "Figure 4-11-2" shows a message exchange initiated by the client using the One-Time-Password (OTP) authentication method with a RADIUS server.

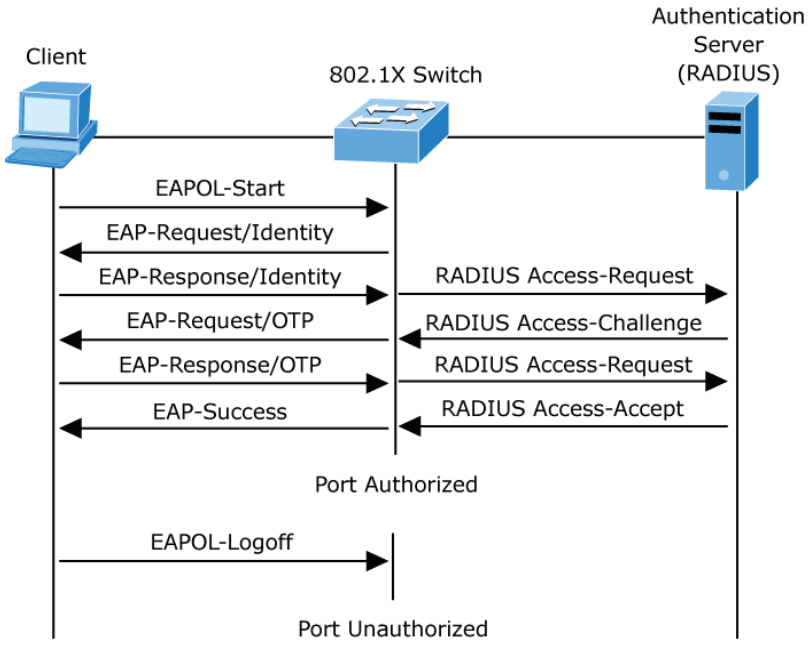


Figure 4-11-2: EAP Message Exchange

■ **Ports in Authorized and Unauthorized States**

The switch port state determines whether or not the client is granted access to the network. The port starts in the *unauthorized* state. While in this state, the port disallows all ingress and egress traffic except for 802.1X protocol packets. When a client is successfully authenticated, the port transitions to the *authorized* state, allowing all traffic for the client to flow normally.

If a client that does not support 802.1X is connected to an unauthorized 802.1X port, the switch requests the client's identity. In this situation, the client does not respond to the request, the port remains in the unauthorized state, and the client is not granted access to the network.

In contrast, when an 802.1X-enabled client connects to a port that is not running the 802.1X protocol, the client initiates the authentication process by sending the EAPOL-start frame. When no response is received, the client sends the request for a fixed number of times. Because no response is received, the client begins sending frames as if the port is in the authorized state

If the client is successfully authenticated (receives an Accept frame from the authentication server), the port state changes to authorized, and all frames from the authenticated client are allowed through the port. If the authentication fails, the port remains in the unauthorized state, but authentication can be retried. If the authentication server cannot be reached, the switch can retransmit the request. If no response is received from the server after the specified number of attempts, authentication fails, and network access is not granted.

When a client logs off, it sends an EAPOL-logoff message, causing the switch port to transition to the unauthorized state.

If the link state of a port transitions from up to down, or if an EAPOL-logoff frame is received, the port returns to the unauthorized state.

4.11.2 Authentication Configuration

This page allows you to configure how a user is authenticated when he logs into the switch via one of the management client interfaces. The Authentication Method Configuration screen in Figure 4-11-3 appears.

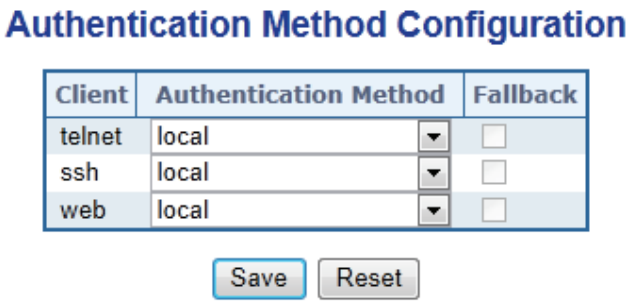


Figure 4-11-3: Authentication Method Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Client**	The management client for which the configuration below applies.
• **Authentication Method**	Authentication Method can be set to one of the following values: ■ **None**: authentication is disabled and login is not possible. ■ **local**: use the local user database on the switch stack for authentication. ■ **RADIUS**: use a remote RADIUS server for authentication. ■ **TACACSt+**: use a remote TACACS+ server for authentication.
• **Fallback**	Enable fallback to local authentication by checking this box. If none of the configured authentication servers are alive, the local user database is used for authentication. This is only possible if the Authentication Method is set to something else than 'none or 'local'.

Buttons

[redacted]: Click to save changes.

[redacted]: Click to undo any changes made locally and revert to previously saved values.

4.11.3 Network Access Server Configuration

This page allows you to configure the **IEEE 802.1X** and **MAC-based** authentication system and port settings.

The IEEE 802.1X standard defines a port-based access control procedure that prevents unauthorized access to a network by requiring users to first submit credentials for authentication. One or more central servers, the backend servers, determine whether the user is allowed access to the network. These backend (RADIUS) servers are configured on the "Configuration→Security→AAA" page. The IEEE802.1X standard defines port-based operation, but non-standard variants overcome security limitations as shall be explored below.

MAC-based authentication allows for authentication of more than one user on the same port, and doesn't require the user to have special 802.1X supplicant software installed on his system. The switch uses the user's MAC address to authenticate against the backend server. Intruders can create counterfeit MAC addresses, which makes MAC-based authentication less secure than 802.1X authentication. The NAS configuration consists of two sections, a system- and a port-wide. The Network Access Server Configuration screen in Figure 4-11-4 appears.

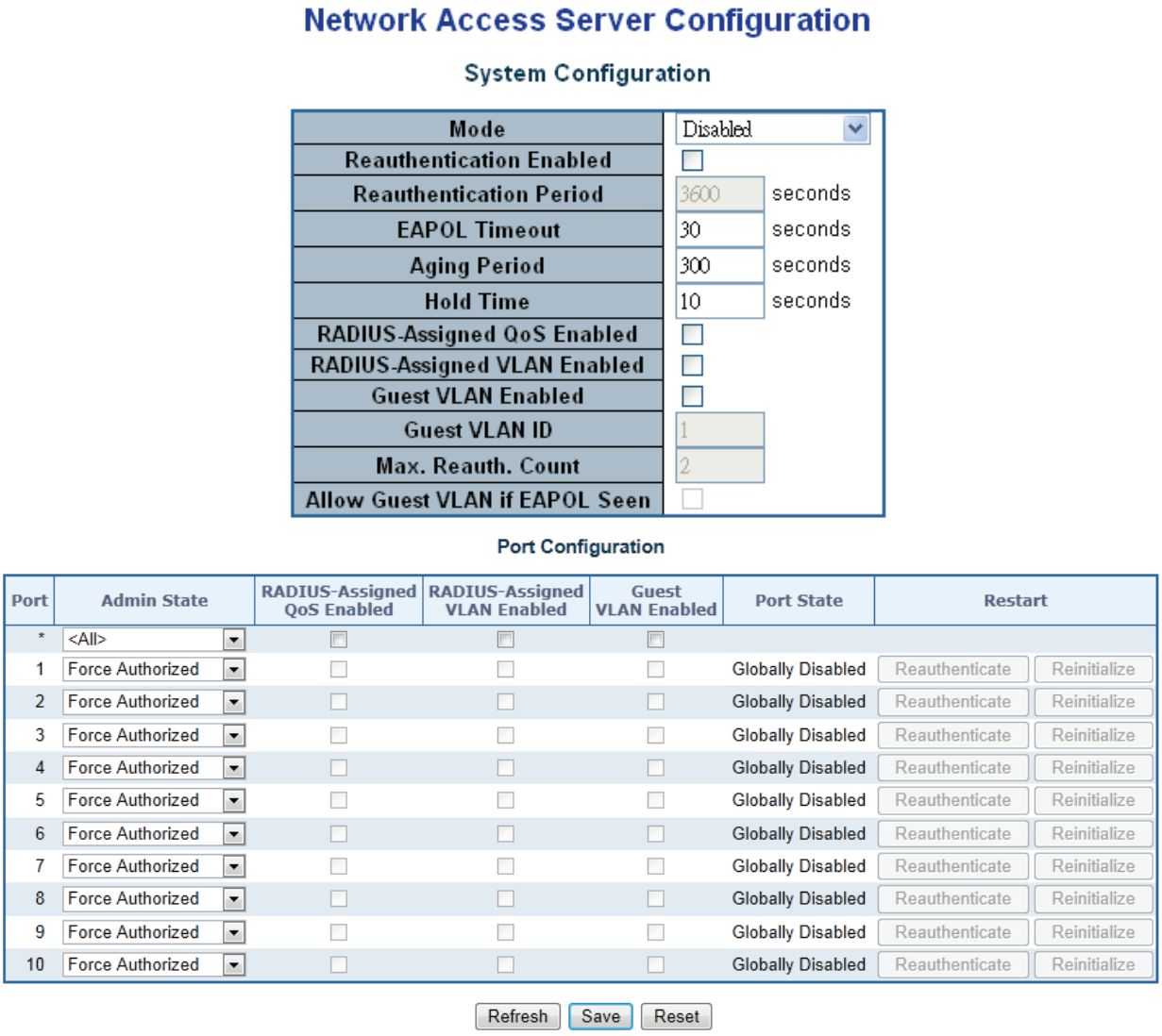


Figure 4-11-4: Network Access Server Configuration Page Screenshot

The page includes the following fields:

System Configuration

Object	Description
• **Mode**	Indicates if NAS is globally enabled or disabled on the switch. If globally disabled, all ports are allowed forwarding of frames.
• **Reauthentication Enabled**	If checked, successfully authenticated supplicants/clients are reauthenticated after the interval specified by the Reauthentication Period. Reauthentication for 802.1X-enabled ports can be used to detect if a new device is plugged into a switch port or if a supplicant is no longer attached. For MAC-based ports, reauthentication is only useful if the RADIUS server configuration has changed. It does not involve communication between the switch and the client, and therefore doesn't imply that a client is still present on a port.
• **Reauthentication Period**	Determines the period, in seconds, after which a connected client must be reauthenticated. This is only active if the Reauthentication Enabled checkbox is checked. Valid values are in the range 1 to 3600 seconds.
• **EAPOL Timeout**	Determines the time between retransmission of Request Identity EAPOL frames. Valid values are in the range 1 to 255 seconds. This has no effect for MAC-based ports.
• **Aging Period**	This setting applies to the following modes, i.e. modes using the Port Security functionality to secure MAC addresses: ■ **Single 802.1X** ■ **Multi 802.1X** ■ **MAC-Based Auth**. When the NAS module uses the Port Security module to secure MAC addresses, the Port Security module needs to check for activity on the MAC address in question at regular intervals and free resources if no activity is seen within a given period of time. This parameter controls exactly this period and can be set to a number between 10 and 1000000 seconds. If reauthentication is enabled and the port is in a 802.1X-based mode, this is not so criticial, since supplicants that are no longer attached to the port will get removed upon the next reauthentication, which will fail. But if reauthentication is not enabled, the only way to free resources is by aging the entries. For ports in MAC-based Auth. mode, reauthentication doesn't cause direct communication between the switch and the client, so this will not detect whether the client is still attached or not, and the only way to free any resources is to age the entry.
• **Hold Time**	This setting applies to the following modes, i.e. modes using the Port Security functionality to secure MAC addresses: ■ **Single 802.1X** ■ **Multi 802.1X** ■ **MAC-Based Auth**. If a client is denied access - either because the RADIUS server denies the client access or because the RADIUS server request times out (according to the timeout specified on the "Configuration→Security→AAA" page) - the client is put on hold in the Unauthorized state. The hold timer does not count during an on-going authentication. In MAC-based Auth. mode, the The switch will ignore new frames coming from the client during the hold time. The Hold Time can be set to a number between 10 and 1000000 seconds.
• **RADIUS-Assigned QoS Enabled**	RADIUS-assigned QoS provides a means to centrally control the traffic class to which traffic coming from a successfully authenticated supplicant is assigned on the switch. The RADIUS server must be configured to transmit special RADIUS attributes to take advantage of this feature (see RADIUS-Assigned QoS Enabled below for a detailed description). The "RADIUS-Assigned QoS Enabled" checkbox provides a quick way to globally enable/disable RADIUS-server assigned QoS Class functionality. When checked, the individual ports' ditto setting determine whether RADIUS-assigned

	QoS Class is enabled for that port. When unchecked, RADIUS-server assigned QoS Class is disabled for all ports.
• **RADIUS-Assigned VLAN Enabled**	RADIUS-assigned VLAN provides a means to centrally control the VLAN on which a successfully authenticated supplicant is placed on the switch. Incoming traffic will be classified to and switched on the RADIUS-assigned VLAN. The RADIUS server must be configured to transmit special RADIUS attributes to take advantage of this feature (see RADIUS-Assigned VLAN Enabled below for a detailed description). The "**RADIUS-Assigned VLAN Enabled**" checkbox provides a quick way to globally enable/disable RADIUS-server assigned VLAN functionality. When checked, the individual ports' ditto setting determine whether RADIUS-assigned VLAN is enabled for that port. When unchecked, RADIUS-server assigned VLAN is disabled for all ports.
• **Guest VLAN Enabled**	A Guest VLAN is a special VLAN - typically with limited network access - on which 802.1X-unaware clients are placed after a network administrator-defined timeout. The switch follows a set of rules for entering and leaving the Guest VLAN as listed below. The "**Guest VLAN Enabled**" checkbox provides a quick way to globally enable/disable Guest VLAN functionality. When checked, the individual ports' ditto setting determines whether the port can be moved into Guest VLAN. When unchecked, the ability to move to the Guest VLAN is disabled for all ports.
• **Guest VLAN ID**	This is the value that a port's Port VLAN ID is set to if a port is moved into the Guest VLAN. It is only changeable if the Guest VLAN option is globally enabled. Valid values are in the range [1; 4095].
• **Max. Reauth. Count**	The number of times that the switch transmits an EAPOL Request Identity frame without response before considering entering the Guest VLAN is adjusted with this setting. The value can only be changed if the Guest VLAN option is globally enabled. Valid values are in the range [1; 255].
• **Allow Guest VLAN if EAPOL Seen**	The switch remembers if an EAPOL frame has been received on the port for the life-time of the port. Once the switch considers whether to enter the Guest VLAN, it will first check if this option is enabled or disabled. If disabled (unchecked; default), the switch will only enter the Guest VLAN if an EAPOL frame has not been received on the port for the life-time of the port. If enabled (checked), the switch will consider entering the Guest VLAN even if an EAPOL frame has been received on the port for the life-time of the port. The value can only be changed if the Guest VLAN option is globally enabled.

Port Configuration

The table has one row for each port on the selected switch in the stack and a number of columns, which are:

Object	Description
• **Port**	The port number for which the configuration below applies.
• **Admin State**	The Configuration All with available options will assign to whole ports. If NAS is globally enabled, this selection controls the port's authentication mode. The following modes are available: ■ **Force Authorized** In this mode, the switch will send one EAPOL Success frame when the port link comes up, and any client on the port will be allowed network access without authentication. ■ **Force Unauthorized** In this mode, the switch will send one EAPOL Failure frame when the port link comes up, and any client on the port will be disallowed network access. ■ **Port-based 802.1X** In the 802.1X-world, the user is called the supplicant, the switch is the authenticator, and the RADIUS server is the authentication server. The authenticator acts as the man-in-the-middle, forwarding requests and

responses between the supplicant and the authentication server. Frames sent between the supplicant and the switch are special 802.1X frames, known as EAPOL (EAP Over LANs) frames. EAPOL frames encapsulate EAP PDUs (RFC3748). Frames sent between the switch and the RADIUS server are RADIUS packets. RADIUS packets also encapsulate EAP PDUs together with other attributes like the switch's IP address, name, and the supplicant's port number on the switch. EAP is very flexible, in that it allows for different authentication methods, like MD5-Challenge, PEAP, and TLS. The important thing is that the authenticator (the switch) doesn't need to know which authentication method the supplicant and the authentication server are using, or how many information exchange frames are needed for a particular method. The switch simply encapsulates the EAP part of the frame into the relevant type (EAPOL or RADIUS) and forwards it.

When authentication is complete, the RADIUS server sends a special packet containing a success or failure indication. Besides forwarding this decision to the supplicant, the switch uses it to open up or block traffic on the switch port connected to the supplicant.

Note: Suppose two backend servers are enabled and that the server timeout is configured to X seconds (using the AAA configuration page), and suppose that the first server in the list is currently down (but not considered dead). Now, if the supplicant retransmits EAPOL Start frames at a rate faster than X seconds, then it will never get authenticated, because the switch will cancel on-going backend authentication server requests whenever it receives a new EAPOL Start frame from the supplicant. And since the server hasn't yet failed (because the X seconds haven't expired), the same server will be contacted upon the next backend authentication server request from the switch. This scenario will loop forever. Therefore, the server timeout should be smaller than the supplicant's EAPOL Start frame retransmission rate.

- **Single 802.1X**
  In port-based 802.1X authentication, once a supplicant is successfully authenticated on a port, the whole port is opened for network traffic. This allows other clients connected to the port (for instance through a hub) to piggy-back on the successfully authenticated client and get network access even though they really aren't authenticated. To overcome this security breach, use the Single 802.1X variant.

  Single 802.1X is really not an IEEE standard, but features many of the same characteristics as does port-based 802.1X. In Single 802.1X, at most one supplicant can get authenticated on the port at a time. Normal EAPOL frames are used in the communication between the supplicant and the switch. If more than one supplicant is connected to a port, the one that comes first when the port's link comes up will be the first one considered. If that supplicant doesn't provide valid credentials within a certain amount of time, another supplicant will get a chance. Once a supplicant is successfully authenticated, only that supplicant will be allowed access. This is the most secure of all the supported modes. In this mode, the Port Security module is used to secure a supplicant's MAC address once successfully authenticated.

- **Multi 802.1X**
  In port-based 802.1X authentication, once a supplicant is successfully authenticated on a port, the whole port is opened for network traffic. This allows other clients connected to the port (for instance through a hub) to piggy-back on the successfully authenticated client and get network access even though they really aren't authenticated. To overcome this security breach, use the Multi 802.1X variant.

  Multi 802.1X is really not an IEEE standard, but features many of the same characteristics as does port-based 802.1X. Multi 802.1X is - like Single 802.1X - not an IEEE standard, but a variant that features many of the same characteristics. In Multi 802.1X, one or more supplicants can get authenticated on the same port at the same time. Each supplicant is authenticated individually and secured in the MAC table using the Port Security module.

  In Multi 802.1X it is not possible to use the multicast BPDU MAC address as destination MAC address for EAPOL frames sent from the switch towards the supplicant, since that would cause all supplicants attached to the port to reply to requests sent from the switch. Instead, the switch uses the supplicant's MAC address, which is obtained from the first EAPOL Start or

	EAPOL Response Identity frame sent by the supplicant. An exception to this is when no supplicants are attached. In this case, the switch sends EAPOL Request Identity frames using the BPDU multicast MAC address as destination - to wake up any supplicants that might be on the port. The maximum number of supplicants that can be attached to a port can be limited using the Port Security Limit Control functionality. ■ **MAC-based Auth.** Unlike port-based 802.1X, MAC-based authentication is not a standard, but merely a best-practices method adopted by the industry. In MAC-based authentication, users are called clients, and the switch acts as the supplicant on behalf of clients. The initial frame (any kind of frame) sent by a client is snooped by the switch, which in turn uses the client's MAC address as both username and password in the subsequent EAP exchange with the RADIUS server. The 6-byte MAC address is converted to a string on the following form "xx-xx-xx-xx-xx-xx", that is, a dash (-) is used as separator between the lower-cased hexadecimal digits. The switch only supports the MD5-Challenge authentication method, so the RADIUS server must be configured accordingly. When authentication is complete, the RADIUS server sends a success or failure indication, which in turn causes the switch to open up or block traffic for that particular client, using the Port Security module. Only then will frames from the client be forwarded on the switch. There are no EAPOL frames involved in this authentication, and therefore, MAC-based Authentication has nothing to do with the 802.1X standard. The advantage of MAC-based authentication over port-based 802.1X is that several clients can be connected to the same port (e.g. through a 3rd party switch or a hub) and still require individual authentication, and that the clients don't need special supplicant software to authenticate. The advantage of MAC-based authentication over 802.1X-based authentication is that the clients don't need special supplicant software to authenticate. The disadvantage is that MAC addresses can be spoofed by malicious users - equipment whose MAC address is a valid RADIUS user can be used by anyone. Also, only the MD5-Challenge method is supported. The maximum number of clients that can be attached to a port can be limited using the Port Security Limit Control functionality.
• **RADIUS-Assigned QoS Enabled**	When RADIUS-Assigned QoS is both globally enabled and enabled (checked) for a given port, the switch reacts to QoS Class information carried in the RADIUS Access-Accept packet transmitted by the RADIUS server when a supplicant is successfully authenticated. If present and valid, traffic received on the supplicant's port will be classified to the given QoS Class. If (re-)authentication fails or the RADIUS Access-Accept packet no longer carries a QoS Class or it's invalid, or the supplicant is otherwise no longer present on the port, the port's QoS Class is immediately reverted to the original QoS Class (which may be changed by the administrator in the meanwhile without affecting the RADIUS-assigned). This option is only available for single-client modes, i.e. • **Port-based 802.1X** • **Single 802.1X** **RADIUS attributes used in identifying a QoS Class:** Refer to the written documentation for a description of the RADIUS attributes needed in order to successfully identify a QoS Class. The User-Priority-Table attribute defined in RFC4675 forms the basis for identifying the QoS Class in an Access-Accept packet. Only the first occurrence of the attribute in the packet will be considered, and to be valid, it must follow this rule: All 8 octets in the attribute's value must be identical and consist of ASCII characters in the range '0' - '3', which translates into the desired QoS Class in the range [0; 3].
• **RADIUS-Assigned VLAN Enabled**	When RADIUS-Assigned VLAN is both globally enabled and enabled (checked) for a given port, the switch reacts to VLAN ID information carried in the RADIUS Access-Accept packet transmitted by the RADIUS server when a supplicant is successfully authenticated. If present and valid, the port's Port VLAN ID will be changed to this VLAN ID, the port will be set to be a member of that VLAN ID, and the port will be forced into VLAN unaware mode. Once assigned, all traffic

	arriving on the port will be classified and switched on the RADIUS-assigned VLAN ID. If (re-)authentication fails or the RADIUS Access-Accept packet no longer carries a VLAN ID or it's invalid, or the supplicant is otherwise no longer present on the port, the port's VLAN ID is immediately reverted to the original VLAN ID (which may be changed by the administrator in the meanwhile without affecting the RADIUS-assigned). This option is only available for single-client modes, i.e. ■ **Port-based 802.1X** ■ **Single 802.1X** For trouble-shooting VLAN assignments, use the "Monitor→VLANs→VLAN Membership and VLAN Port" pages. These pages show which modules have (temporarily) overridden the current Port VLAN configuration. **RADIUS attributes used in identifying a VLAN ID:** RFC2868 and RFC3580 form the basis for the attributes used in identifying a VLAN ID in an Access-Accept packet. The following criteria are used: - The Tunnel-Medium-Type, Tunnel-Type, and Tunnel-Private-Group-ID attributes must all be present at least once in the Access-Accept packet. - The switch looks for the first set of these attributes that have the same Tag value and fulfil the following requirements (if Tag == 0 is used, the Tunnel-Private-Group-ID does not need to include a Tag): - Value of Tunnel-Medium-Type must be set to "IEEE-802" (ordinal 6). - Value of Tunnel-Type must be set to "VLAN" (ordinal 13). - Value of Tunnel-Private-Group-ID must be a string of ASCII chars in the range '0' - '9', which is interpreted as a decimal string representing the VLAN ID. Leading '0's are discarded. The final value must be in the range [1; 4095].
• **Guest VLAN Enabled**	When Guest VLAN is both globally enabled and enabled (checked) for a given port, the switch considers moving the port into the Guest VLAN according to the rules outlined below. This option is only available for EAPOL-based modes, i.e.: ■ **Port-based 802.1X** ■ **Single 802.1X** ■ **Multi 802.1X** For trouble-shooting VLAN assignments, use the "Monitor→VLANs→VLAN Membership and VLAN Port" pages. These pages show which modules have (temporarily) overridden the current Port VLAN configuration. **Guest VLAN Operation:** When a Guest VLAN enabled port's link comes up, the switch starts transmitting EAPOL Request Identity frames. If the number of transmissions of such frames exceeds Max. Reauth. Count and no EAPOL frames have been received in the meanwhile, the switch considers entering the Guest VLAN. The interval between transmission of EAPOL Request Identity frames is configured with EAPOL Timeout. If Allow Guest VLAN if EAPOL Seen is enabled, the port will now be placed in the Guest VLAN. If disabled, the switch will first check its history to see if an EAPOL frame has previously been received on the port (this history is cleared if the port link goes down or the port's Admin State is changed), and if not, the port will be placed in the Guest VLAN. Otherwise it will not move to the Guest VLAN, but continue transmitting EAPOL Request Identity frames at the rate given by EAPOL Timeout. Once in the Guest VLAN, the port is considered authenticated, and all attached clients on the port are allowed access on this VLAN. The switch will not transmit an EAPOL Success frame when entering the Guest VLAN. While in the Guest VLAN, the switch monitors the link for EAPOL frames, and if one such frame is received, the switch immediately takes the port out of the Guest VLAN and starts authenticating the supplicant according to the port mode. If an EAPOL frame is received, the port will never be able to go back into the Guest VLAN if the "Allow Guest VLAN if EAPOL Seen" is disabled.
• **Port State**	The current state of the port. It can undertake one of the following values: ■ **Globally Disabled**: NAS is globally disabled. ■ **Link Down**: NAS is globally enabled, but there is no link on the port.

	■ **Authorized**: The port is in Force Authorized or a single-supplicant mode and the supplicant is authorized. ■ **Unauthorized**: The port is in Force Unauthorized or a single-supplicant mode and the supplicant is not successfully authorized by the RADIUS server. ■ **X Auth/Y Unauth**: The port is in a multi-supplicant mode. Currently X clients are authorized and Y are unauthorized.
• **Restart**	Two buttons are available for each row. The buttons are only enabled when authentication is globally enabled and the port's Admin State is in an EAPOL-based or MAC-based mode. Clicking these buttons will not cause settings changed on the page to take effect. ■ **Reauthenticate**: Schedules a reauthentication to whenever the quiet-period of the port runs out (EAPOL-based authentication). For MAC-based authentication, reauthentication will be attempted immediately. The button only has effect for successfully authenticated clients on the port and will not cause the clients to get temporarily unauthorized. ■ **Reinitialize**: Forces a reinitialization of the clients on the port and thereby a reauthentication immediately. The clients will transfer to the unauthorized state while the reauthentication is in progress.

Buttons

	client for MAC-based authentication.
• **Last ID**	The user name (supplicant identity) carried in the most recently received Response Identity EAPOL frame for EAPOL-based authentication, and the source MAC address from the most recently received frame from a new client for MAC-based authentication.
• **QoS Class**	QoS Class assigned to the port by the RADIUS server if enabled.
• **Port VLAN ID**	The VLAN ID that NAS has put the port in. The field is blank, if the Port VLAN ID is not overridden by NAS. ■ If the VLAN ID is assigned by the RADIUS server, "(RADIUS-assigned)" is appended to the VLAN ID. Read more about RADIUS-assigned VLANs here. ■ If the port is moved to the Guest VLAN, "(Guest)" is appended to the VLAN ID. Read more about Guest VLANs here.

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

- **EAPOL Counters**

These supplicant frame counters are available for the following administrative states:
Force Authorized
Force Unauthorized
Port-based 802.1X
Single 802.1X
Multi 802.1X

Direction	Name	IEEE Name	Description
Rx	**Total**	dot1xAuthEapolFramesRx	The number of valid EAPOL frames of any type that have been received by the switch.
Rx	**Response ID**	dot1xAuthEapolRespIdFramesRx	The number of valid EAPOL Response Identity frames that have been received by the switch.
Rx	**Responses**	dot1xAuthEapolRespFramesRx	The number of valid EAPOL response frames (other than Response Identity frames) that have been received by the switch.
Rx	**Start**	dot1xAuthEapolStartFramesRx	The number of EAPOL Start frames that have been received by the switch.
Rx	**Logoff**	dot1xAuthEapolLogoffFramesRx	The number of valid EAPOL Logoff frames that have been received by the switch.
Rx	**Invalid Type**	dot1xAuthInvalidEapolFramesRx	The number of EAPOL frames that have been received by the switch in which the frame type is not recognized.
Rx	**Invalid Length**	dot1xAuthEapLengthErrorFramesRx	The number of EAPOL frames that have been received by the switch in which the Packet Body Length field is invalid.
Tx	**Total**	dot1xAuthEapolFramesTx	The number of EAPOL frames of any type that have been transmitted by the switch.
Tx	**Request ID**	dot1xAuthEapolReqIdFramesTx	The number of EAPOL Request Identity frames that have been transmitted by the switch.
Tx	**Requests**	dot1xAuthEapolReqFramesTx	The number of valid EAPOL Request frames (other than Request Identity frames) that have been transmitted by the switch.

- **Backend Server Counters**

These backend (RADIUS) frame counters are available for the following administrative states:

- **Port-based 802.1X**
- **Single 802.1X**
- **Multi 802.1X**
- **MAC-based Auth**

Direction	Name	IEEE Name	Description
Rx	**Access Challenges**	dot1xAuthBackendAccessChallenges	**802.1X-based**: Counts the number of times that the switch receives the first request from the backend server following the first response from the supplicant. Indicates that the backend

				server has communication with the switch. **MAC-based**: Counts all Access Challenges received from the backend server for this port (left-most table) or client (right-most table).
	Rx	**Other Requests**	dot1xAuthBackendOtherRequestsToSupplicant	**802.1X-based**: Counts the number of times that the switch sends an EAP Request packet following the first to the supplicant. Indicates that the backend server chose an EAP-method. **MAC-based**: Not applicable.
	Rx	**Auth. Successes**	dot1xAuthBackendAuthSuccesses	**802.1X- and MAC-based**: Counts the number of times that the switch receives a success indication. Indicates that the supplicant/client has successfully authenticated to the backend server.
	Rx	**Auth. Failures**	dot1xAuthBackendAuthFails	**802.1X- and MAC-based**: Counts the number of times that the switch receives a failure message. This indicates that the supplicant/client has not authenticated to the backend server.
	Tx	**Responses**	dot1xAuthBackendResponses	**802.1X-based:** Counts the number of times that the switch attempts to send a supplicant's first response packet to the backend server. Indicates the switch attempted communication with the backend server. Possible retransmissions are not counted. **MAC-based:** Counts all the backend server packets sent from the switch towards the backend server for a given port (left-most table) or client (right-most table). Possible retransmissions are not counted.

- **Last Supplicant/Client Info**

Information about the last supplicant/client that attempted to authenticate. This information is available for the following administrative states:

- **Port-based 802.1X**
- **Single 802.1X**
- **Multi 802.1X**
- **MAC-based Auth**.

Name	IEEE Name	Description
MAC Address	dot1xAuthLastEapolFrameSource	The MAC address of the last supplicant/client.
VLAN ID	-	The VLAN ID on which the last frame from the last supplicant/client was received.

	Version	dot1xAuthLastEapolFrameVersion	**802.1X-based**: The protocol version number carried in the most recently received EAPOL frame. **MAC-based**: Not applicable.
	Identity	-	**802.1X-based**: The user name (supplicant identity) carried in the most recently received Response Identity EAPOL frame. **MAC-based**: Not applicable.

Selected Counters

Object	Description
• **Selected Counters**	The Selected Counters table is visible when the port is one of the following administrative states: ■ **Multi 802.1X** ■ **MAC-based Auth**. The table is identical to and is placed next to the Port Counters table, and will be empty if no MAC address is currently selected. To populate the table, select one of the attached MAC Addresses from the table below.

Attached MAC Address

Object	Description
• **Identity**	Shows the identity of the supplicant, as received in the Response Identity EAPOL frame. Clicking the link causes the supplicant's EAPOL and Backend Server counters to be shown in the Selected Counters table. If no supplicants are attached, it shows No supplicants attached. This column is not available for MAC-based Auth.
• **MAC Address**	For Multi 802.1X, this column holds the MAC address of the attached supplicant. For MAC-based Auth., this column holds the MAC address of the attached client. Clicking the link causes the client's Backend Server counters to be shown in the Selected Counters table. If no clients are attached, it shows No clients attached.
• **VLAN ID**	This column holds the VLAN ID that the corresponding client is currently secured through the Port Security module.
• **State**	The client can either be authenticated or unauthenticated. In the authenticated state, it is allowed to forward frames on the port, and in the unauthenticated state, it is blocked. As long as the backend server hasn't successfully authenticated the client, it is unauthenticated. If an authentication fails for one or the other reason, the client will remain in the unauthenticated state for Hold Time seconds.
• **Last Authentication**	Shows the date and time of the last authentication of the client (successful as well as unsuccessful).

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

• MAC-based Auth.X

Click to clear both the port counters and all of the attached client's counters. The "Last Client" will not be cleared, however.

 : This button is available in the following modes:

• Multi 802.1X

• MAC-based Auth.X

Click to clear only the currently selected client's counters.

4.11.6 Authentication Server Configuration

This page allows you to configure the Authentication Servers. The Authentication Server Configuration screen in Figure 4-11-7 appears.

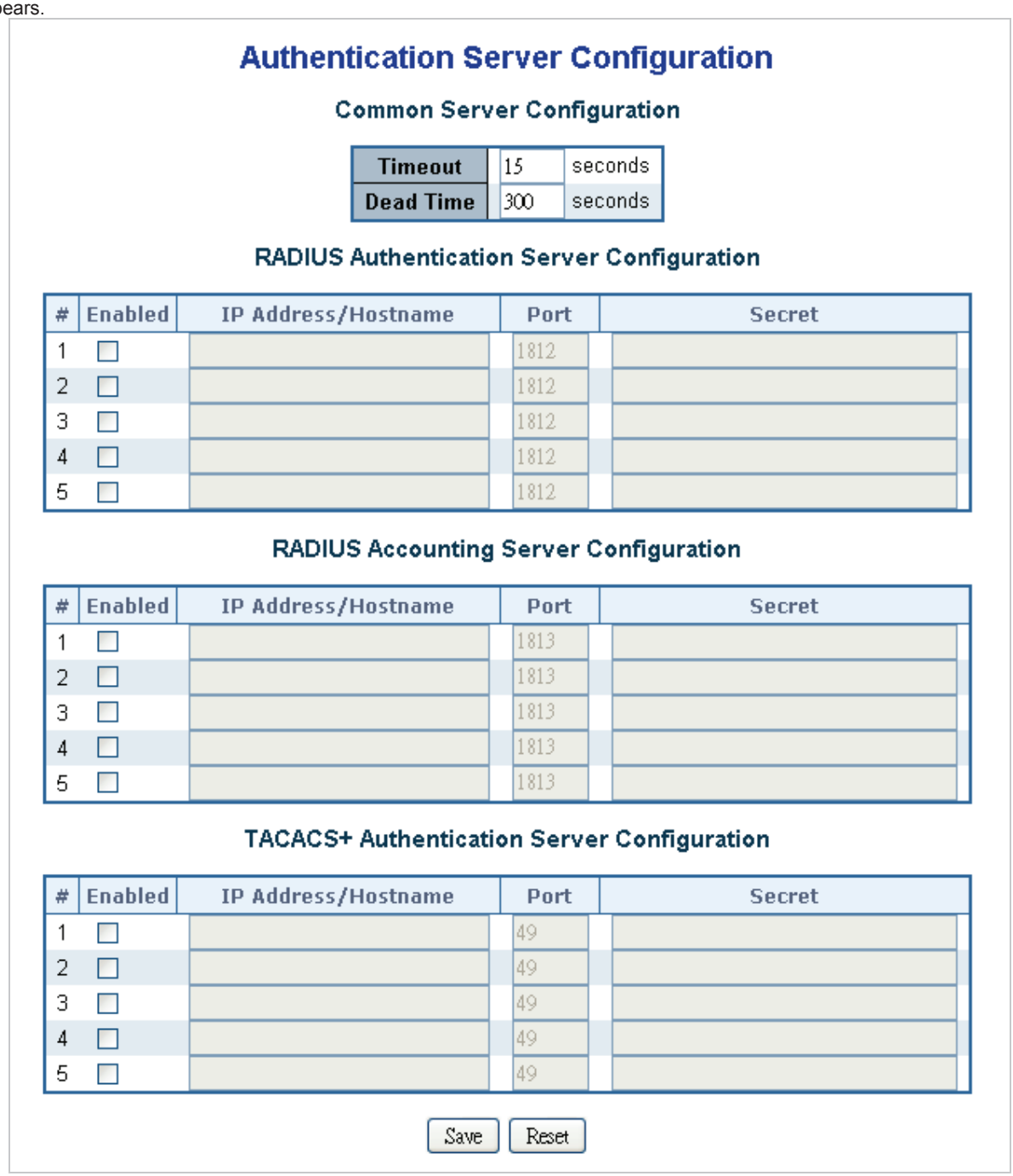


Figure 4-11-7: Authentication Server Configuration Page Screenshot

The page includes the following fields:

Port State
These settings are common for all of the Authentication Servers.

Object	Description
• **Timeout**	The Timeout, which can be set to a number between 3 and 3600 seconds, is the maximum time to wait for a reply from a server. f the server does not reply within this timeframe, we will consider it to be dead and continue with the next enabled server (if any).

	RADIUS servers are using the UDP protocol, which is unreliable by design. In order to cope with lost frames, the timeout interval is divided into 3 subintervals of equal length. If a reply is not received within the subinterval, the request is transmitted again. This algorithm causes the RADIUS server to be queried up to 3 times before it is considered to be dead.
• **Dead Time**	The Dead Time, which can be set to a number between 0 and 3600 seconds, is the period during which the switch will not send new requests to a server that has failed to respond to a previous request. This will stop the switch from continually trying to contact a server that it has already determined as dead. Setting the Dead Time to a value greater than 0 (zero) will enable this feature, but only if more than one server has been configured.

RADIUS Authentication Server Configuration

The table has one row for each RADIUS Authentication Server and a number of columns, which are:

Object	Description
• **#**	The RADIUS Authentication Server number for which the configuration below applies.
• **Enabled**	Enable the RADIUS Authentication Server by checking this box.
• **IP Address/Hostname**	The IP address or hostname of the RADIUS Authentication Server. IP address is expressed in dotted decimal notation.
• **Port**	The UDP port to use on the RADIUS Authentication Server. If the port is set to 0 (zero), the default port (1812) is used on the RADIUS Authentication Server.
• **Secret**	The secret - up to 29 characters long - shared between the RADIUS Authentication Server and the switch.

RADIUS Accounting Server Configuration

The table has one row for each RADIUS Accounting Server and a number of columns, which are:

Object	Description
• **#**	The RADIUS Accounting Server number for which the configuration below applies.
• **Enabled**	Enable the RADIUS Accounting Server by checking this box.
• **IP Address/Hostname**	The IP address or hostname of the RADIUS Accounting Server. IP address is expressed in dotted decimal notation.
• **Port**	The UDP port to use on the RADIUS Accounting Server. If the port is set to 0 (zero), the default port (1813) is used on the RADIUS Accounting Server.
• **Secret**	The secret - up to 29 characters long - shared between the RADIUS Accounting Server and the switch.

TACACS+ Authentication Server Configuration

The table has one row for each TACACS+ Authentication Server and a number of columns, which are:

Object	Description
• **#**	The TACACS+ Authentication Server number for which the configuration below applies.
• **Enabled**	Enable the TACACS+ Authentication Server by checking this box.
• **IP Address/Hostname**	The IP address or hostname of the TACACS+ Authentication Server. IP address is expressed in dotted decimal notation.
• **Port**	The TCP port to use on the TACACS+ Authentication Server. If the port is set to 0 (zero), the default port (49) is used on the TACACS+ Authentication Server.

• **Secret**	The secret - up to 29 characters long - shared between the TACACS+ Authentication Server and the switch.

Buttons

 : Click to save changes.

 : Click to undo any changes made locally and revert to previously saved values.

4.11.7 RADIUS Overview

This page provides an overview of the status of the RADIUS servers configurable on the Authentication configuration page. The RADIUS Authentication/Accounting Server Overview screen in Figure 4-11-8 appears.

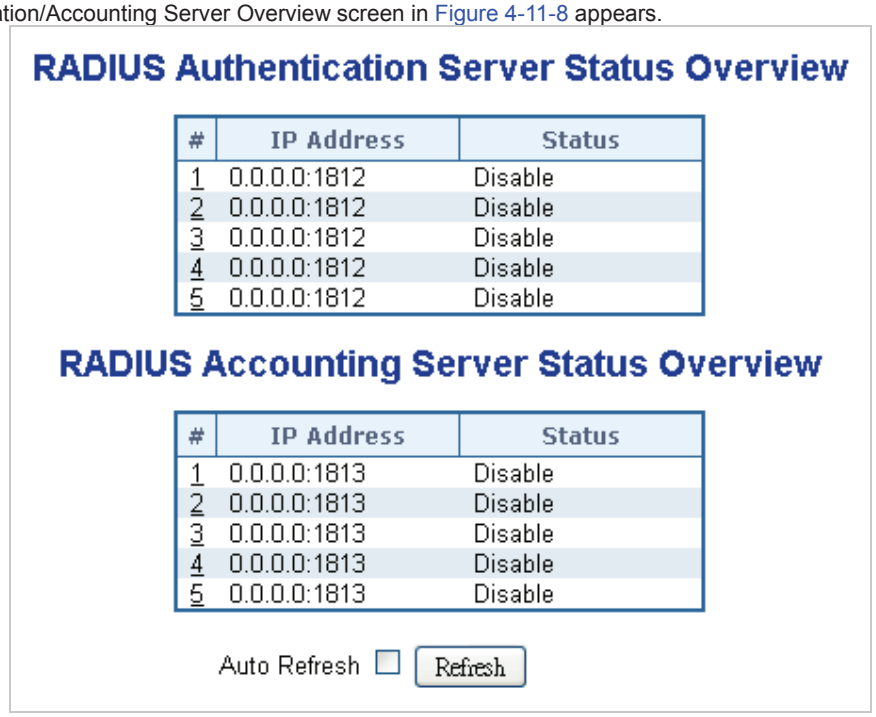


Figure 4-11-8: RADIUS Authentication/Accounting Server Overview Page Screenshot

The page includes the following fields:

RADIUS Authentication Server

Object	Description
• **#**	The RADIUS server number. Click to navigate to detailed statistics for this server.
• **IP Address**	The IP address and UDP port number (in <IP Address>:<UDP Port> notation) of this server.
• **Status**	The current state of the server. This field takes one of the following values: ■ **Disabled**: The server is disabled. ■ **Not Ready**: The server is enabled, but IP communication is not yet up and running. ■ **Ready**: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts. ■ **Dead (X seconds left)**: Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.

RADIUS Accounting Server

Object	Description
• **#**	The RADIUS server number. Click to navigate to detailed statistics for this server.
• **IP Address**	The IP address and UDP port number (in <IP Address>:<UDP Port> notation) of this server.
• **Status**	The current state of the server. This field takes one of the following values: ■ **Disabled**: The server is disabled. ■ **Not Ready**: The server is enabled, but IP communication is not yet up and running. ■ **Ready**: The server is enabled, IP communication is up and running,

	and the RADIUS module is ready to accept accounting attempts. ■ **Dead** (X seconds left): Accounting attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

4.11.8 RADIUS Details

This page provides detailed statistics for a particular RADIUS server. The RADIUS Authentication/Accounting for Server Overview screen in Figure 4-11-9 appears.

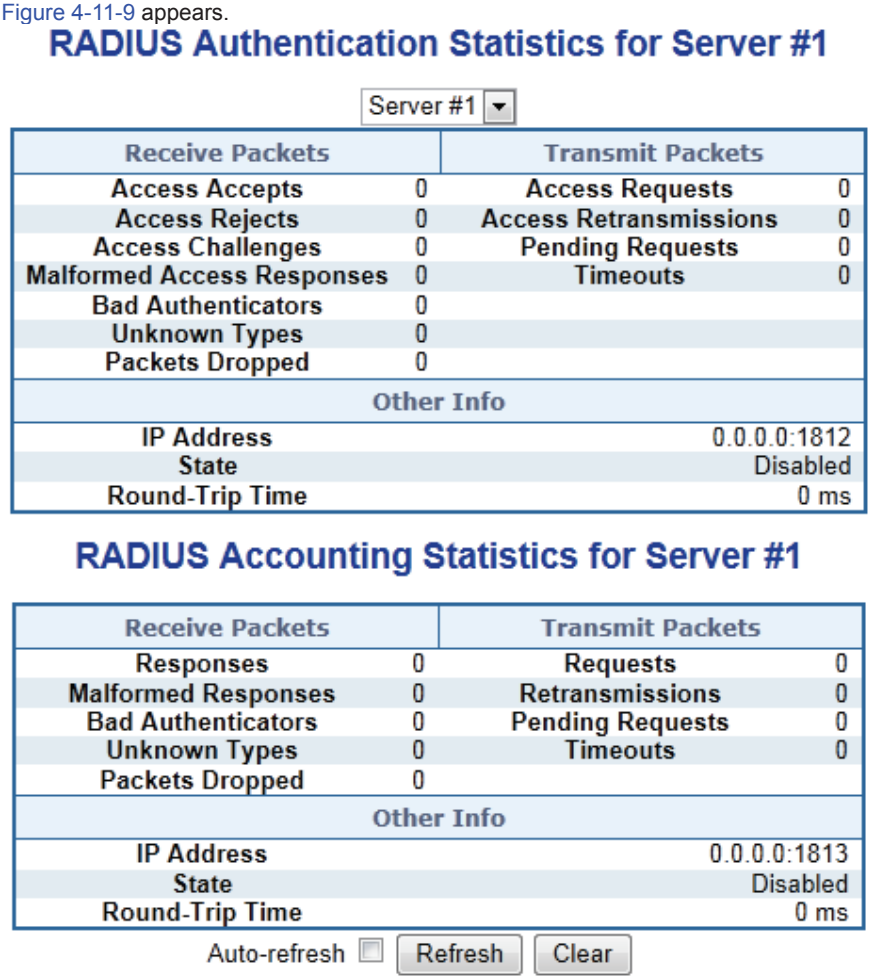


Figure 4-11-9: RADIUS Authentication/Accounting for Server Overview Page Screenshot

The page includes the following fields:

RADIUS Authentication Servers

The statistics map closely to those specified in RFC4668 - RADIUS Authentication Client MIB.

Use the server select box to switch between the backend servers to show details for.

Object	Description			
• **Packet Counters**	RADIUS authentication server packet counter. There are seven receive and four transmit counters.			
	Direction	**Name**	**RFC4668 Name**	**Description**
	Rx	**Access Accepts**	radiusAuthClientExtAccessAccepts	The number of RADIUS Access-Accept packets (valid or invalid) received from the server.
	Rx	**Access Rejects**	radiusAuthClientExtAccessRejects	The number of RADIUS Access-Reject packets (valid or invalid) received from the server.
	Rx	**Access Challenges**	radiusAuthClientExtAccessChallenges	The number of RADIUS Access-Challenge packets (valid or invalid) received from the server.

	Rx	**Malformed Access Responses**	radiusAuthClientExtMalformedAccessResponses	The number of malformed RADIUS Access-Response packets received from the server. Malformed packets include packets with an invalid length. Bad authenticators or Message Authenticator attributes or unknown types are not included as malformed access responses.
	Rx	**Bad Authenticators**	radiusAuthClientExtBadAuthenticators	The number of RADIUS Access-Response packets containing invalid authenticators or Message Authenticator attributes received from the server.
	Rx	**Unknown Types**	radiusAuthClientExtUnknownTypes	The number of RADIUS packets that were received from the server on the authentication port and dropped for some other reason.
	Rx	**Packets Dropped**	radiusAuthClientExtPacketsDropped	The number of RADIUS packets that were received from the server on the authentication port and dropped for some other reason.
	Tx	**Access Requests**	radiusAuthClientExtAccessRequests	The number of RADIUS Access-Request packets sent to the server. This does not include retransmissions.
	Tx	**Access Retransmissions**	radiusAuthClientExtAccessRetransmissions	The number of RADIUS Access-Request packets retransmitted to the RADIUS authentication server.
	Tx	**Pending Requests**	radiusAuthClientExtPendingRequests	The number of RADIUS Access-Request packets destined for the server that have not yet timed out or received a response. This variable is incremented when an Access-Request is sent and decremented due to receipt of an Access-Accept, Access-Reject, Access-Challenge, timeout, or retransmission.
	Tx	**Timeouts**	radiusAuthClientExtTimeouts	The number of authentication timeouts to the server. After a timeout, the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Request as well as a timeout.

- **Other Info**

This section contains information about the state of the server and the latest round-trip time.

Name	RFC4668 Name	Description
IP Address	-	IP address and UDP port for the accounting server in question.

	State	-	Shows the state of the server. It takes one of the following values: **Disabled**: The selected server is disabled. **Not Ready**: The server is enabled, but IP communication is not yet up and running. **Ready**: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts. **Dead (X seconds left)**: Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.
	Round-Trip Time	radiusAuthClientExtRoundTripTime	The time interval (measured in milliseconds) between the most recent Access-Reply/Access-Challenge and the Access-Request that matched it from the RADIUS authentication server. The granularity of this measurement is 100 ms. A value of 0 ms indicates that there hasn't been round-trip communication with the server yet.

RADIUS Accounting Servers

The statistics map closely to those specified in RFC4670 - RADIUS Accounting Client MIB.
Use the server select box to switch between the backend servers to show details for.

<table>
<tr><th>Object</th><th>Description</th></tr>
<tr><td>• Packet Counters</td><td>RADIUS accounting server packet counter. There are five receive and four transmit counters.
<table>
<tr><th>Direction</th><th>Name</th><th>RFC4670 Name</th><th>Description</th></tr>
<tr><td>Rx</td><td>Responses</td><td>radiusAccClientExt Responses</td><td>The number of RADIUS packets (valid or invalid) received from the server.</td></tr>
<tr><td>Rx</td><td>Malformed Responses</td><td>radiusAccClientExt MalformedResponses</td><td>The number of malformed RADIUS packets received from the server. Malformed packets include packets with an invalid length. Bad authenticators or or unknown types are not included as malformed access responses.</td></tr>
<tr><td>Rx</td><td>Bad Authenticators</td><td>radiusAcctClientExt BadAuthenticators</td><td>The number of RADIUS packets containing invalid authenticators received from the server.</td></tr>
<tr><td>Rx</td><td>Unknown Types</td><td>radiusAccClientExt UnknownTypes</td><td>The number of RADIUS packets of unknown types that were received from the server on the accounting port.</td></tr>
<tr><td>Rx</td><td>Packets Dropped</td><td>radiusAccClientExt PacketsDropped</td><td>The number of RADIUS packets that were received from the server on the accounting port and dropped for some other reason.</td></tr>
<tr><td>Tx</td><td>Requests</td><td>radiusAccClientExt Requests</td><td>The number of RADIUS packets sent to the server. This does not include retransmissions.</td></tr>
<tr><td>Tx</td><td>Retransmissions</td><td>radiusAccClientExt Retransmissions</td><td>The number of RADIUS packets retransmitted to the RADIUS accounting server.</td></tr>
<tr><td>Tx</td><td>Pending Requests</td><td>radiusAccClientExt PendingRequests</td><td>The number of RADIUS packets destined for the server that have not yet timed out or received a response. This variable is incremented when a Request is sent and decremented due to receipt of a Response, timeout, or retransmission.</td></tr>
<tr><td>Tx</td><td>Timeouts</td><td>radiusAccClientExt Timeouts</td><td>The number of accounting timeouts to the server. After a timeout, the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Request as well as a timeout.</td></tr>
</table></td></tr>
<tr><td>• Other Info</td><td>This section contains information about the state of the server and the latest round-trip time.
<table>
<tr><th>Name</th><th>RFC4670 Name</th><th>Description</th></tr>
</table></td></tr>
</table>

	IP Address	-	IP address and UDP port for the accounting server in question.
	State	-	Shows the state of the server. It takes one of the following values: **Disabled**: The selected server is disabled. **Not Ready**: The server is enabled, but IP communication is not yet up and running. **Ready**: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept accounting attempts. **Dead (X seconds left)**: Accounting attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.
	Round-Trip Time	radiusAccClientExtRoundTripTime	The time interval (measured in milliseconds) between the most recent Response and the Request that matched it from the RADIUS accounting server. The granularity of this measurement is 100 ms. A value of 0 ms indicates that there hasn't been round-trip communication with the server yet.

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

4.11.9 Windows Platform RADIUS Server Configuration

Setup the RADIUS server and assign the client IP address to the Managed switch. In this case, field in the default IP Address of the Managed Switch with 192.168.0.100. And also make sure the shared **secret key** is as same as the one you had set at the Managed Switch's 802.1x system configuration – **12345678** at this case.

1. Configure the IP Address of remote RADIUS server and secret key.

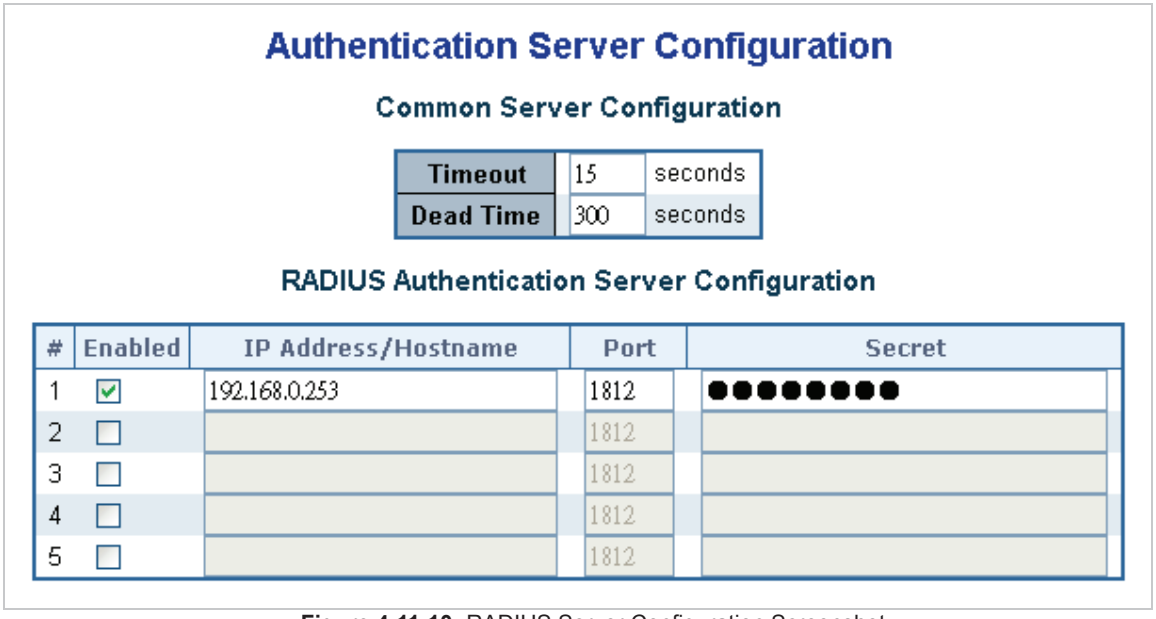


Figure 4-11-10: RADIUS Server Configuration Screenshot

2. Add New RADIUS Cleint on the Windows 2003 server

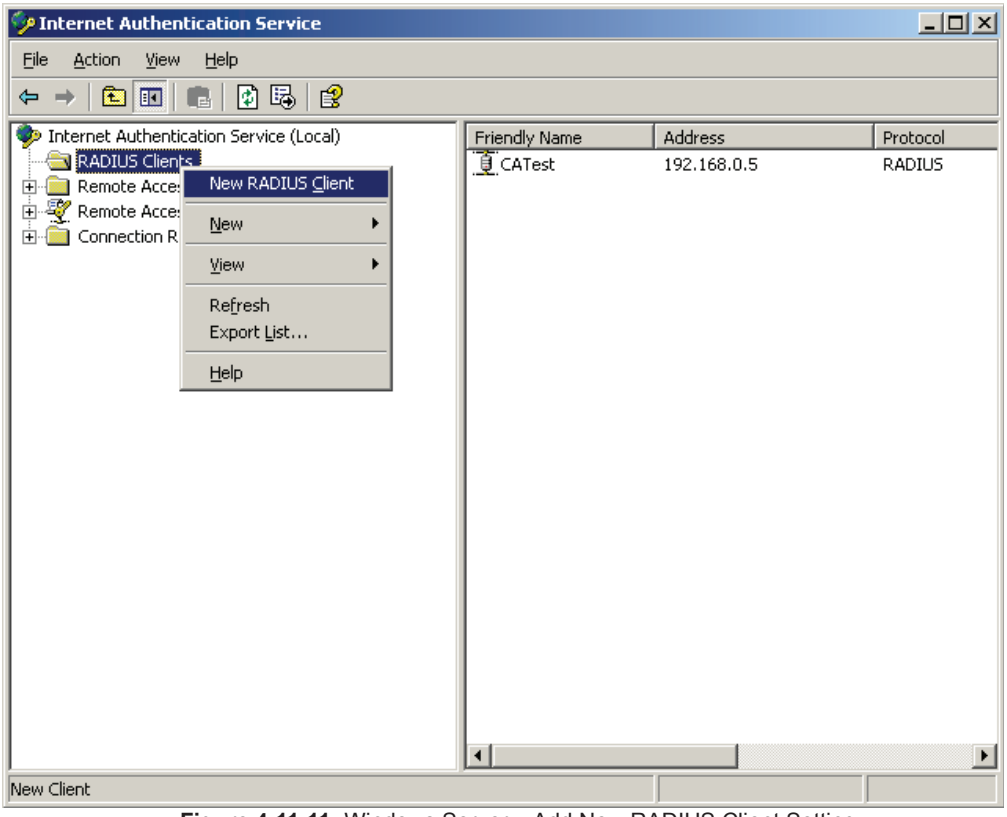


Figure 4-11-11: Windows Server – Add New RADIUS Client Setting

3. Assign the client IP address to the **Industrial Managed Switch**.

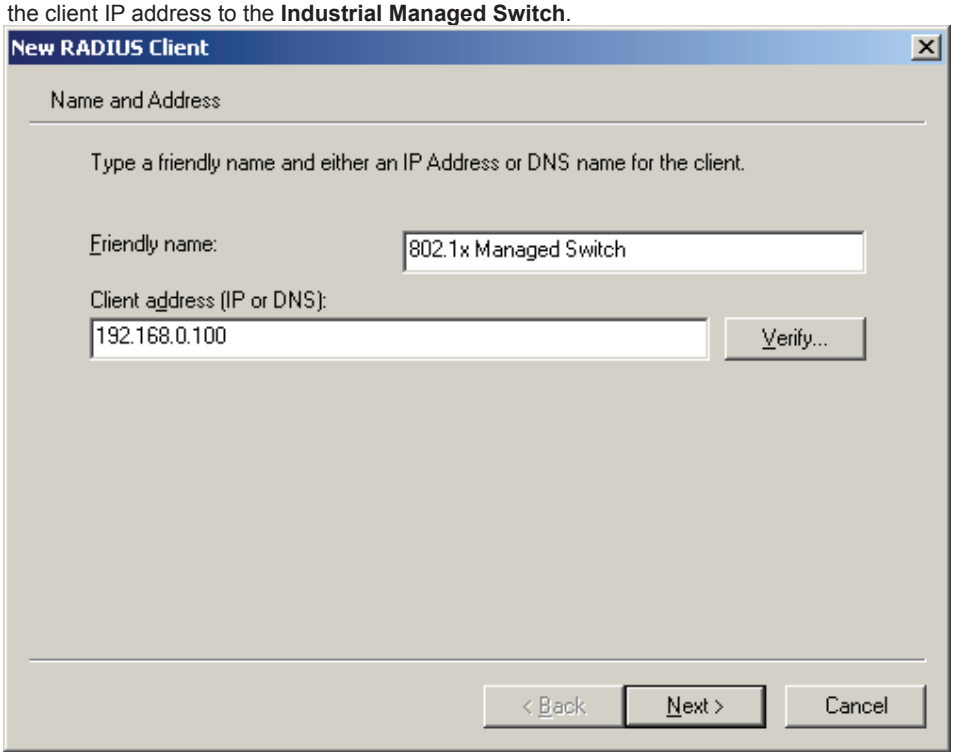


Figure 4-11-12: Windows Server RADIUS Server Setting

4. The shared **secret key** should be as same as the key configured on the **Industrial Managed Switch**.

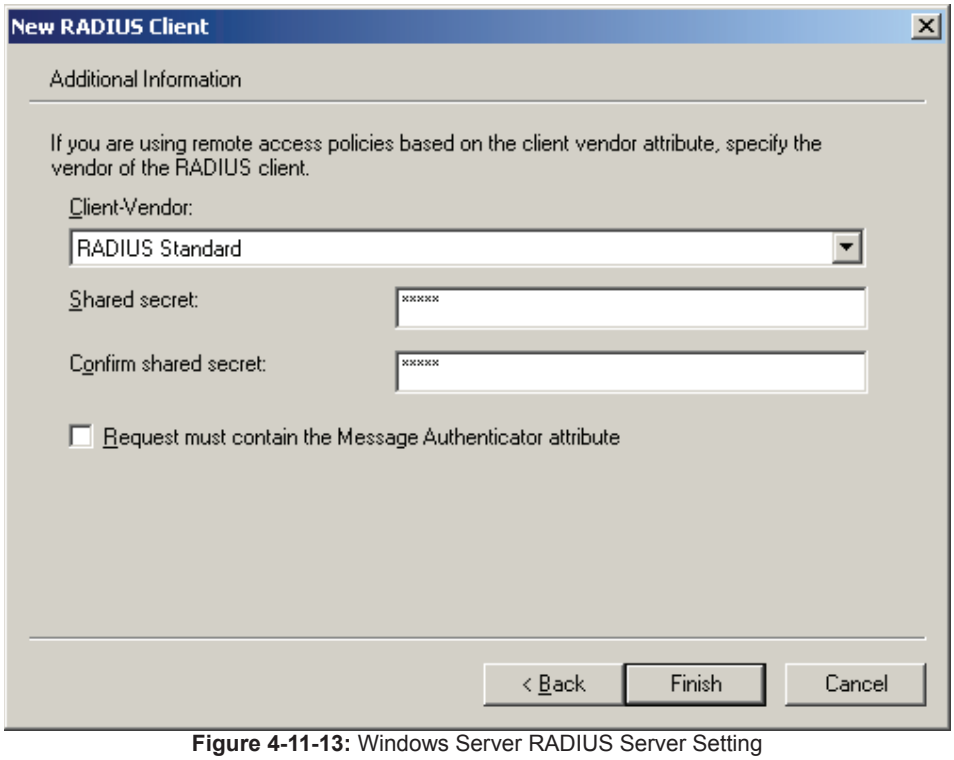


Figure 4-11-13: Windows Server RADIUS Server Setting

5. Configure ports attribute of 802.1X, the same as "802.1X Port Configuration".

Port	Admin State	RADIUS-Assigned QoS Enabled	RADIUS-Assigned VLAN Enabled	Guest VLAN Enabled	Port State	Restart
*	<Configure All>	☐	☐	☐		
1	Port-based 802.1X	☐	☐	☐	Globally Disabled	Reauthenticate Reinitialize
2	Port-based 802.1X	☐	☐	☐	Globally Disabled	Reauthenticate Reinitialize

Figure 4-11-14: 802.1x Port Configuration

6. Create user data. The establishment of the user data needs to be created on the Radius Server PC. For example, the Radius Server founded on Win2003 Server, and then:

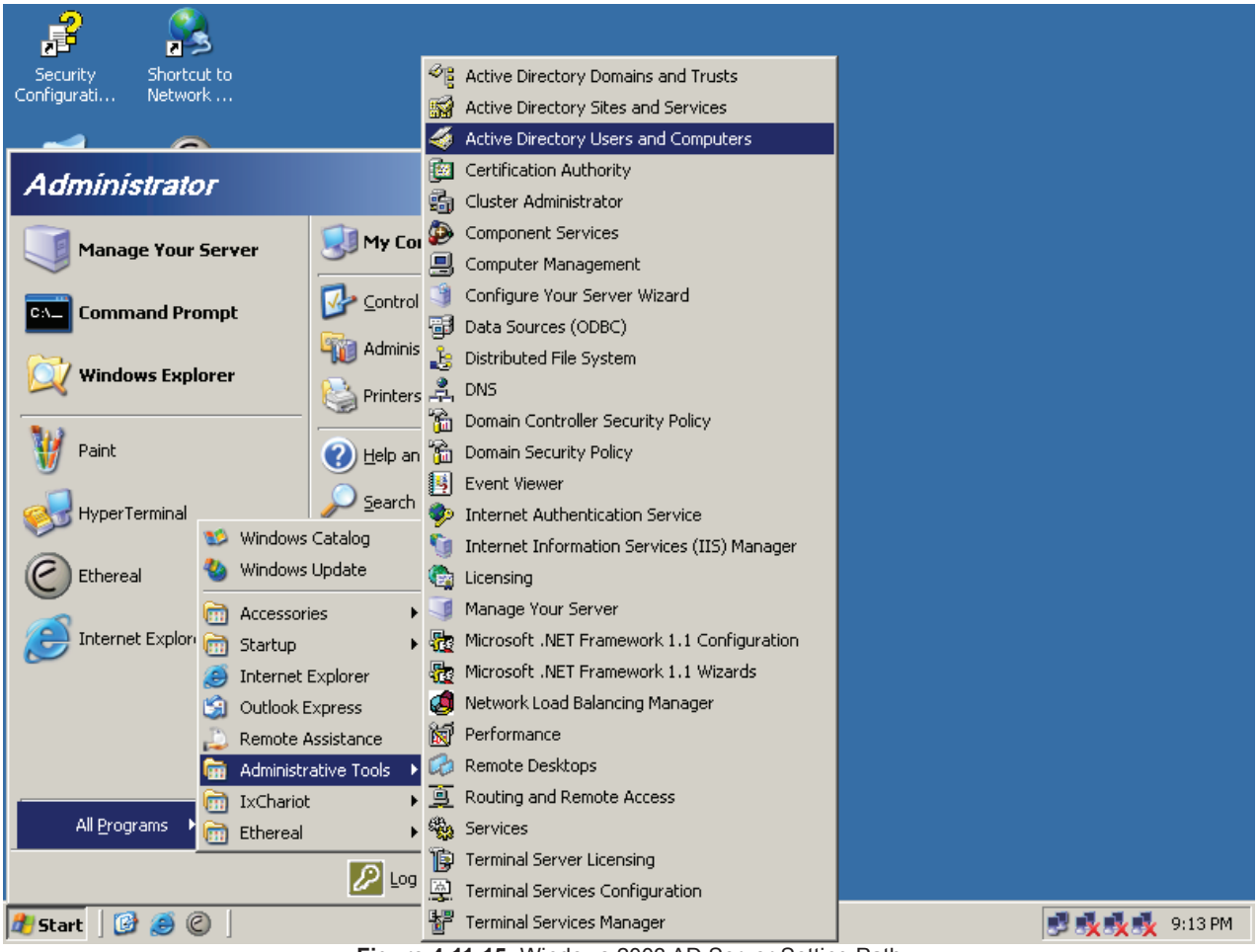


Figure 4-11-15: Windows 2003 AD Server Setting Path

7. Enter " **Active Directory Users and Computers**", create legal user data, the next, right-click a user what you created to enter properties, and what to be noticed:

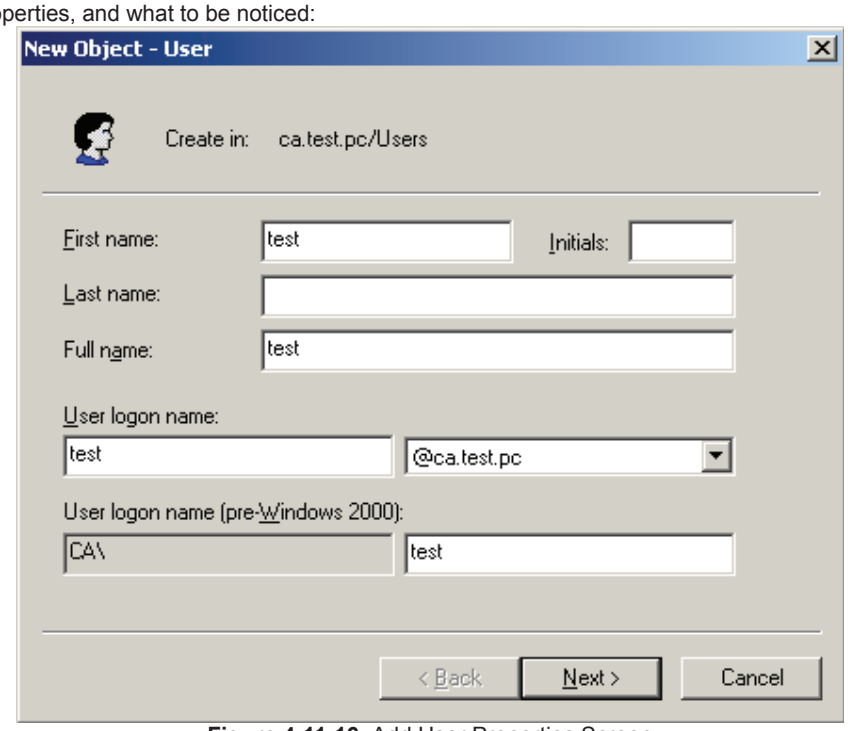


Figure 4-11-16: Add User Properties Screen

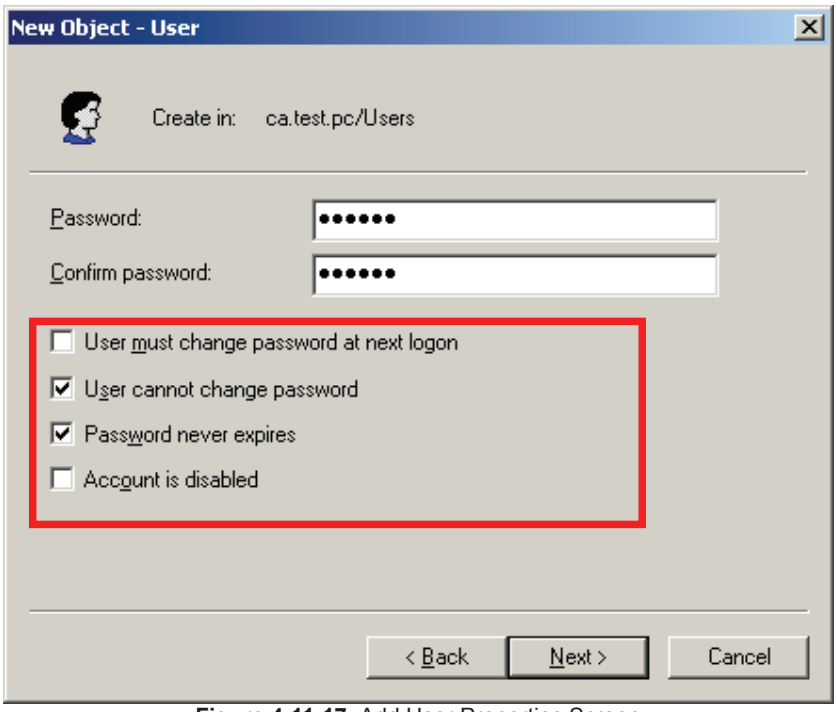


Figure 4-11-17: Add User Properties Screen

Note

Set the Ports Authenticate Status to "**Force Authorized**" if the port is connected to the RADIUS server or the port is a uplink port that is connected to another switch. Or once the 802.1X is set to work, the switch might not be able to access the RADIUS server.

4.11.10 802.1X Client Configuration

Windows XP is originally 802.1X support. As to other operating systems (windows 98SE, ME, 2000), an 802.1X client utility is needed. The following procedures show how to configure 802.1X Authentication in Windows XP.
Please note that if you want to change the 802.1x authentication type of a wireless client, i.e. switch to EAP-TLS from EAP-MD5, you must remove the current existing wireless network from your preferred connection first, and add it in again.

■ Configure Sample: EAP-MD5 Authentication

1. Go to **Start** > **Control Panel,** double-click on "**Network Connections**".
2. Right-click on the Local Network Connection.
3. Click "**Properties**" to open up the Properties setting window.

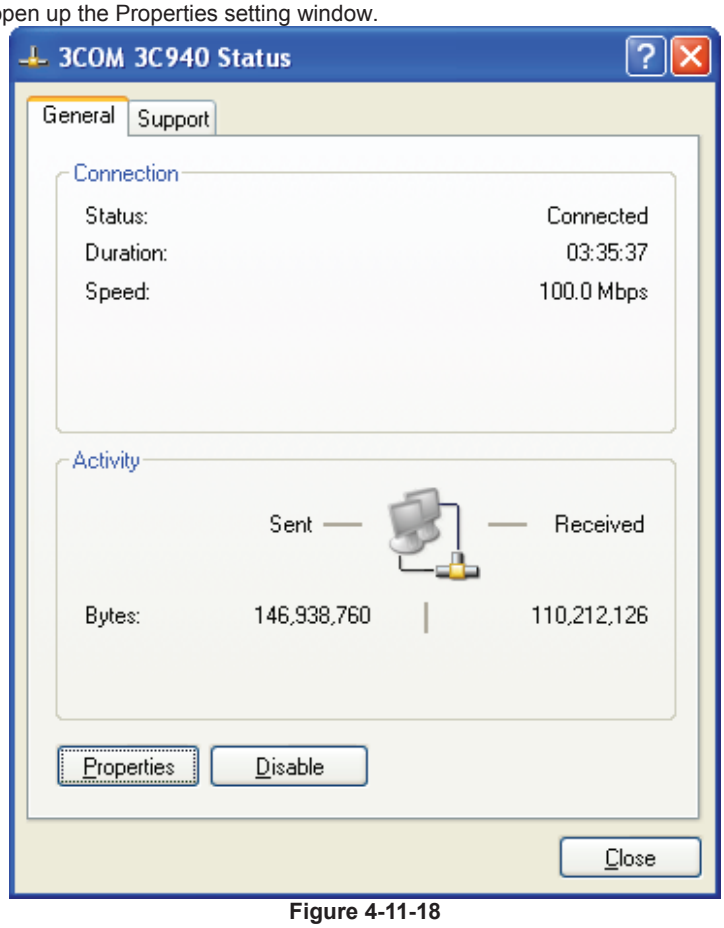


Figure 4-11-18

4. Select “**Authentication**” tab.
5. Select “**Enable network access control using IEEE 802.1X**” to enable 802.1x authentication.
6. Select “**MD-5 Challenge**” from the drop-down list box for EAP type.

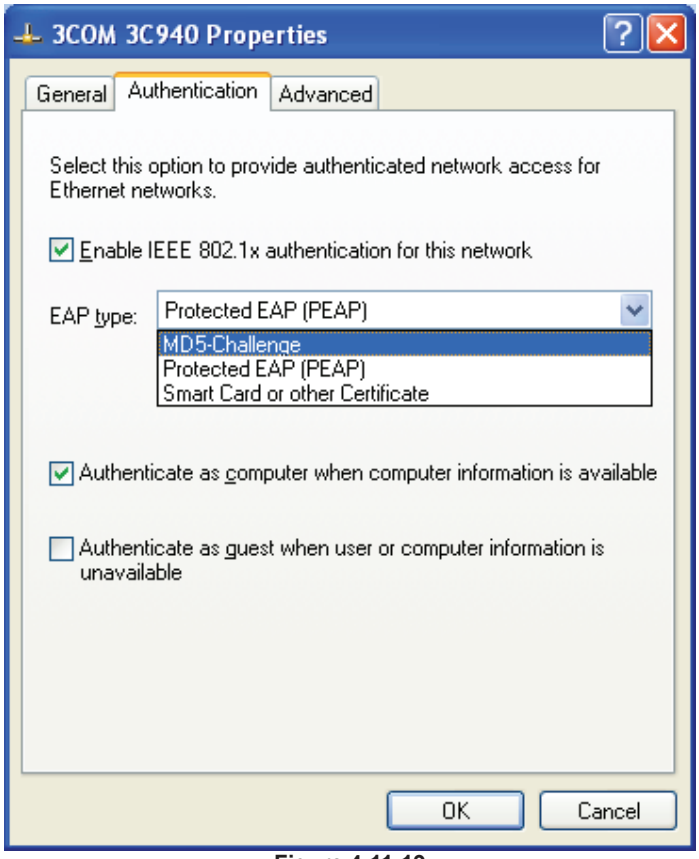


Figure 4-11-19

7. Click “**OK**”.
8. When client has associated with the Managed Switch, a user authentication notice appears in system tray. Click on the notice to continue.

Figure 4-11-20: Windows Client Popup Login Request Message

9. Enter the user name, password and the logon domain that your account belongs.
10. Click “**OK**” to complete the validation process.

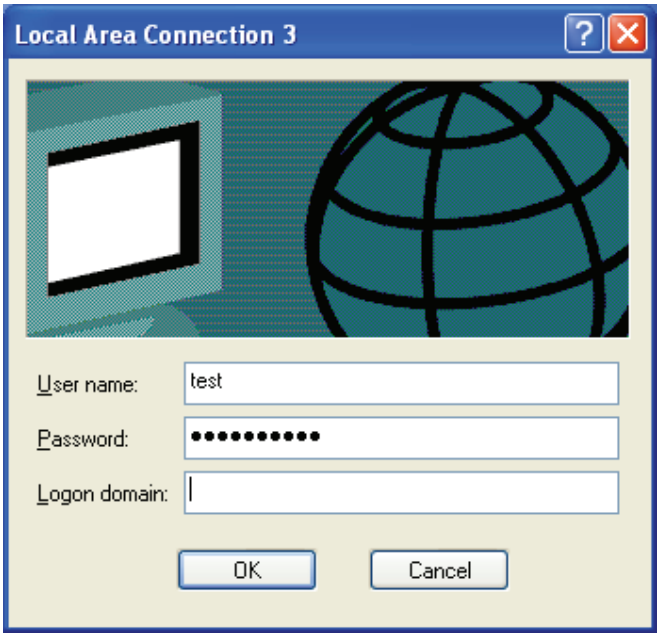


Figure 4-11-21

4.12 Security

This section is to control the access of the Industrial Managed Switch, including the user access and management control. The Security page contains links to the following main topics:

- **Port Limit Control**
- **Access Management**
- **Access Management Statistics**
- **HTTPs**
- **SSH**
- **Port Security Status**
- **Port Security Detail**
- **DHCP Snooping**
- **DHCP Snooping Statistics**
- **IP Source Guard Configuration**
- **IP Source Guard Static Table**
- **ARP Inspection**
- **ARP Inspection Static Table**

4.12.1 Port Limit Control

This page allows you to configure the Port Security Limit Control system and port settings. Limit Control allows for limiting the number of users on a given port. A user is identified by a MAC address and VLAN ID. If Limit Control is enabled on a port, the limit specifies the maximum number of users on the port. If this number is exceeded, an action is taken. The action can be one of the four different actions as described below.

The Limit Control module utilizes a lower-layer module and Port Security module, which manages MAC addresses learnt on the port. The Limit Control configuration consists of two sections, a system and a port.

The Port Limit Control Configuration screen in Figure 4-12-1 appears.

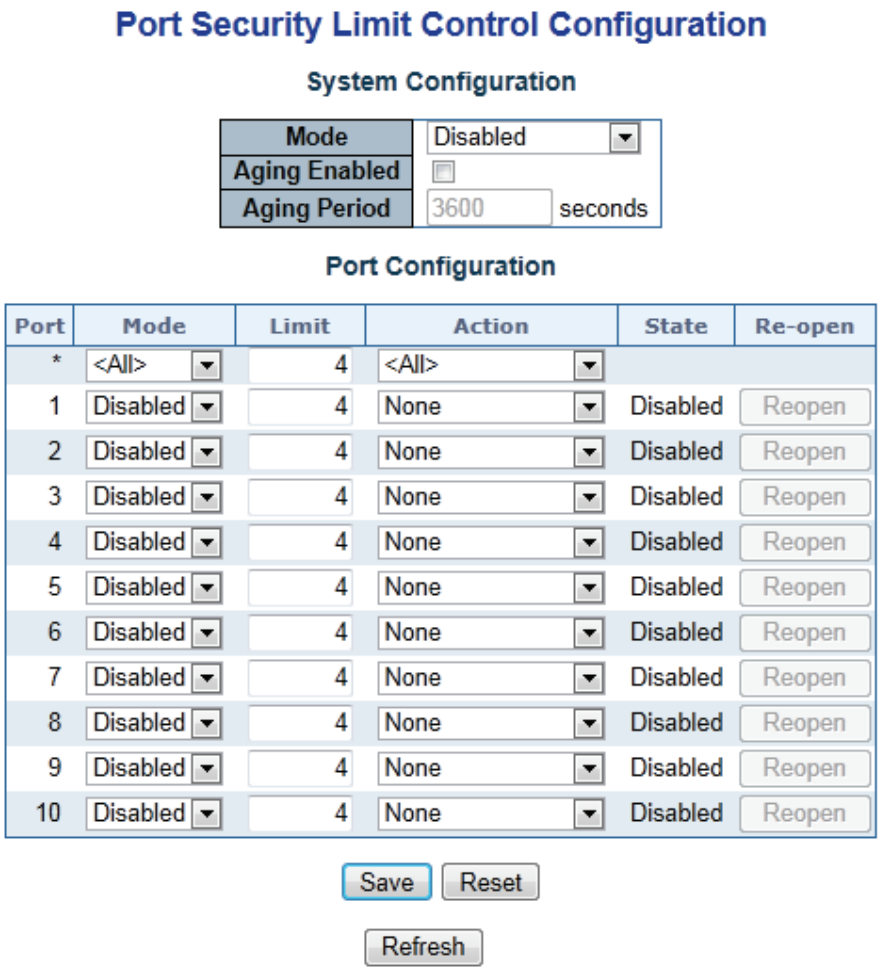


Figure 4-12-1: Port Limit Control Configuration Overview Page Screenshot

The page includes the following fields:

System Configuration

Object	Description
• **Mode**	Indicates if Limit Control is globally enabled or disabled on the switchstack. If globally disabled, other modules may still use the underlying functionality, but limit checks and corresponding actions are disabled.
• **Aging Enabled**	If checked, secured MAC addresses are subject to aging as discussed under Aging Period.
• **Aging Period**	If Aging Enabled is checked, then the aging period is controlled with this input. If other modules are using the underlying port security for securing MAC addresses, they may have other requirements to the aging period. The underlying port security will use the shorter requested aging period of all modules that use the functionality. The Aging Period can be set to a number between 10 and 10,000,000 seconds. To understand why aging may be desired, consider the following scenario: Suppose an end-host is connected to a 3rd party switch or hub, which in turn is connected to a port on this switch on which Limit Control is enabled. The end-host will be allowed to forward if the limit is not exceeded. Now suppose that the end-host logs off or powers down. If it wasn't for aging, the end-host would still take up resources on this switch and will be allowed to forward. To overcome this situation, enable aging. With aging enabled, a timer is started once the end-host gets secured. When the timer expires, the switch starts looking for frames from the end-host, and if such frames are not seen within the next Aging Period, the end-host is assumed to be disconnected, and the corresponding resources are freed on the switch.

Port Configuration

The table has one row for each port on the selected switch in the stack and a number of columns, which are:

Object	Description
• **Port**	The port number for which the configuration below applies.
• **Mode**	The Configuration All with available options will assign to whole ports. Controls whether Limit Control is enabled on this port. Both this and the Global Mode must be set to Enabled for Limit Control to be in effect. Notice that other modules may still use the underlying port security features without enabling Limit Control on a given port.
• **Limit**	The maximum number of MAC addresses that can be secured on this port. This number cannot exceed 1024. If the limit is exceeded, the corresponding action is taken. The stackswitch is "born" with a total number of MAC addresses from which all ports draw whenever a new MAC address is seen on a Port Security-enabled port. Since all ports draw from the same pool, it may happen that a configured maximum cannot be granted, if the remaining ports have already used all available MAC addresses.
• **Action**	The Configuration All with available options will assign to whole ports. If Limit is reached, the switch can take one of the following actions: **None**: Do not allow more than Limit MAC addresses on the port, but take no further action. **Trap**: If Limit + 1 MAC addresses is seen on the port, send an SNMP trap. If Aging is disabled, only one SNMP trap will be sent, but with Aging enabled, new SNMP traps will be sent everytime the limit gets exceeded. **Shutdown**: If Limit + 1 MAC addresses is seen on the port, shut down the port. This implies that all secured MAC addresses will be removed from the port, and no new will be learned. Even if the link is physically disconnected and reconnected on the port (by disconnecting the cable), the port will remain shut down. There are three ways to re-open the port: 1) Boot the stack or elect a new masterthe switch, 2) Disable and re-enable Limit Control on the port or the stackswitch, 3) Click the Reopen button. **Trap & Shutdown**: If Limit + 1 MAC addresses is seen on the port, both the "Trap" and the "Shutdown" actions described above will be taken.

• **State**	This column shows the current state of the port as seen from the Limit Control's point of view. The state takes one of four values: **Disabled**: Limit Control is either globally disabled or disabled on the port. **Ready**: The limit is not yet reached. This can be shown for all actions. **Limit Reached**: Indicates that the limit is reached on this port. This state can only be shown if Action is set to **None** or **Trap**. **Shutdown**: Indicates that the port is shut down by the Limit Control module. This state can only be shown if Action is set to **Shutdown** or **Trap & Shutdown**.
• **Reopen Button**	If a port is shutdown by this module, you may reopen it by clicking this button, which will only be enabled if this is the case. For other methods, refer to **Shutdown** in the Action section. Note, that clicking the reopen button causes the page to be refreshed, so non-committed changes will be lost.

Buttons

 : Click to save changes.

 : Click to undo any changes made locally and revert to previously saved values.

4.12.2 Access Management

Configure access management table on this page. The maximum entry number is 16. If the application's type match any one of the access management entries, it will allow access to the switch. The Access Management Configuration screen in Figure 4-12-2 appears.

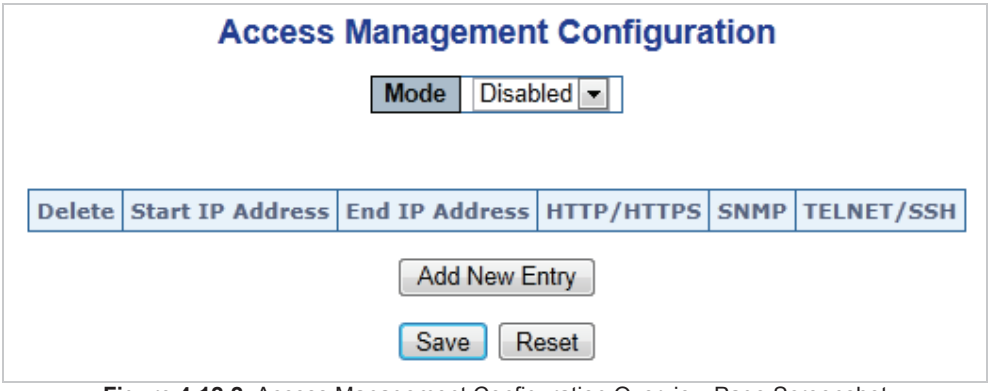


Figure 4-12-2: Access Management Configuration Overview Page Screenshot

The page includes the following fields:

Object	Description
• **Mode**	Indicates the access management mode operation. Possible modes are: ■ **Enabled**: Enable access management mode operation. ■ **Disabled**: Disable access management mode operation.
• **Delete**	Check to delete the entry. It will be deleted during the next save.
• **Start IP Address**	Indicates the start IP address for the access management entry.
• **End IP Address**	Indicates the end IP address for the access management entry.
• **HTTP/HTTPS**	Indicates the host can access the switch from HTTP/HTTPS interface that the host IP address matched the entry.
• **SNMP**	Indicates the host can access the switch from SNMP interface that the host IP address matched the entry.
• **TELNET/SSH**	Indicates the host can access the switch from TELNET/SSH interface that the host IP address matched the entry.

Buttons

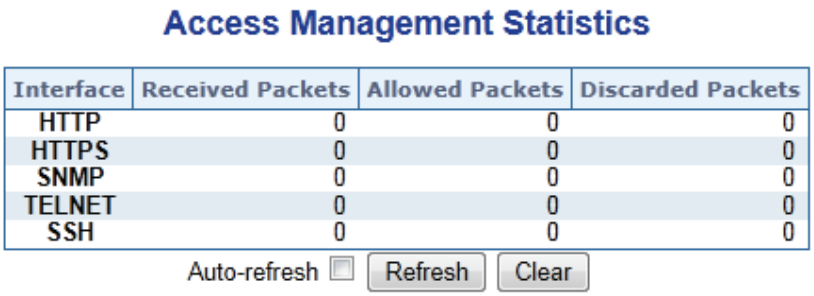


Figure 4-12-3: Access Management Statistics Overview Page Screenshot

The page includes the following fields:

Object	Description
• **Interface**	The interface that allowed remote host can access the **Industrial Managed Switch**.
• **Receive Packets**	The received packets number from the interface under access management mode is enabled.
• **Allowed Packets**	The allowed packets number from the interface under access management mode is enabled.
• **Discard Packets**	The discarded packets number from the interface under access management mode is enabled.

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

4.12.4 HTTPs

Configure HTTPS on this page. The HTTPS Configuration screen in Figure 4-12-4 appears.

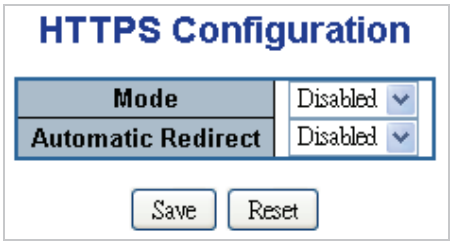


Figure 4-12-4: HTTPS Configuration Screen Page Screenshot

The page includes the following fields:

Object	Description
• **Mode**	Indicates the HTTPS mode operation. Possible modes are: ■ **Enabled**: Enable HTTPS mode operation. ■ **Disabled**: Disable HTTPS mode operation.
• **Automatic Redirect**	Indicates the HTTPS redirect mode operation. Automatic redirect web browser to HTTPS during HTTPS mode enabled. Possible modes are: ■ **Enabled**: Enable HTTPS redirect mode operation. ■ **Disabled**: Disable HTTPS redirect mode operation.

Buttons

 : Click to save changes.

 : Click to undo any changes made locally and revert to previously saved values.

4.12.5 SSH

Configure SSH on this page. This page shows the Port Security status. Port Security is a module with no direct configuration. Configuration comes indirectly from other modules - the user modules. When a user module has enabled port security on a port, the port is set-up for software-based learning. In this mode, frames from unknown MAC addresses are passed on to the port security module, which in turn asks all user modules whether to allow this new MAC address to forward or block it. For a MAC address to be set in the forwarding state, all enabled user modules must unanimously agree on allowing the MAC address to forward. If only one chooses to block it, it will be blocked until that user module decides otherwise.
The status page is divided into two sections - one with a legend of user modules and one with the actual port status. The SSH Configuration screen in Figure 4-12-5 appears.

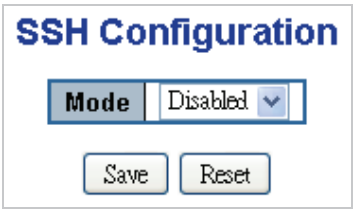


Figure 4-12-5: SSH Configuration Screen Page Screenshot

The page includes the following fields:

Object	Description
• **Mode**	Indicates the SSH mode operation. Possible modes are: ■ **Enabled**: Enable SSH mode operation. ■ **Disabled**: Disable SSH mode operation.

Buttons

 : Click to save changes.

 : Click to undo any changes made locally and revert to previously saved values.

4.12.6 Port Security Status

This page shows the Port Security status. Port Security is a module with no direct configuration. Configuration comes indirectly from other modules - the user modules. When a user module has enabled port security on a port, the port is set-up for software-based learning. In this mode, frames from unknown MAC addresses are passed on to the port security module, which in turn asks all user modules whether to allow this new MAC address to forward or block it. For a MAC address to be set in the forwarding state, all enabled user modules must unanimously agree on allowing the MAC address to forward. If only one chooses to block it, it will be blocked until that user module decides otherwise.

The status page is divided into two sections - one with a legend of user modules and the other with the actual port status. The Port Security Status screen in Figure 4-12-6 appears.

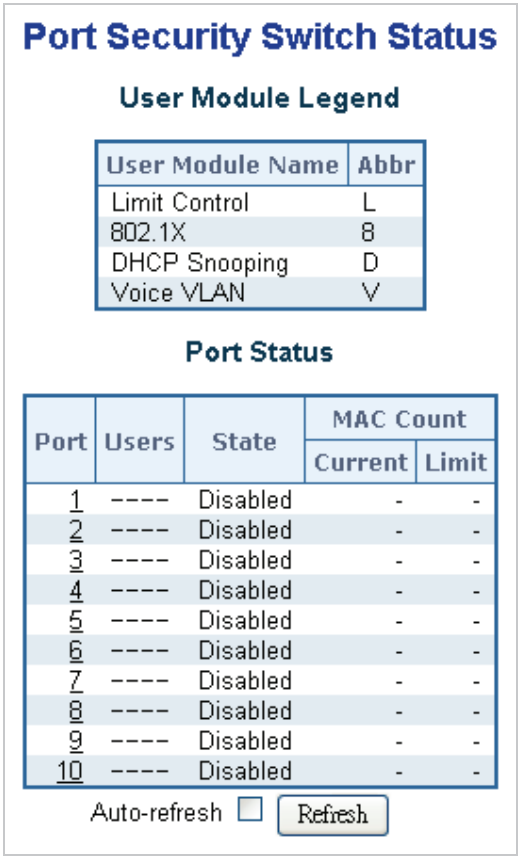


Figure 4-12-6: Port Security Status Screen Page Screenshot

The page includes the following fields:

User Module Legend

The legend shows all user modules that may request Port Security services.

Object	Description
• **User Module Name**	The full name of a module that may request Port Security services.
• **Abbr**	A one-letter abbreviation of the user module. This is used in the Users column in the port status table.

Port Status

The table has one row for each port on the selected switch in the switch and a number of columns, which are:

Object	Description
• **Port**	The port number for which the status applies. Click the port number to see the status for this particular port.
• **Users**	Each of the user modules has a column that shows whether that module has enabled Port Security or not. A '-' means that the corresponding user module is not enabled, whereas a letter indicates that the user module abbreviated by that

	letter (see Abbr) has enabled port security.
• **State**	Shows the current state of the port. It can take one of four values: ■ **Disabled**: No user modules are currently using the Port Security service. ■ **Ready**: The Port Security service is in use by at least one user module, and is awaiting frames from unknown MAC addresses to arrive. ■ **Limit Reached**: The Port Security service is enabled by at least the Limit Control user module, and that module has indicated that the limit is reached and no more MAC addresses should be taken in. ■ **Shutdown**: The Port Security service is enabled by at least the Limit Control user module, and that module has indicated that the limit is exceeded. No MAC addresses can be learned on the port until it is administratively re-opened on the Limit Control configuration Web-page.
• **MAC Count (Current, Limit)**	The two columns indicate the number of currently learned MAC addresses (forwarding as well as blocked) and the maximum number of MAC addresses that can be learned on the port, respectively. If no user modules are enabled on the port, the Current column will show a dash (-). If the Limit Control user module is not enabled on the port, the Limit column will show a dash (-).

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

4.12.7 Port Security Detail

This page shows the MAC addresses secured by the Port Security module. Port Security is a module with no direct configuration. Configuration comes indirectly from other modules - the user modules. When a user module has enabled port security on a port, the port is set-up for software-based learning. In this mode, frames from unknown MAC addresses are passed on to the port security module, which in turn asks all user modules whether to allow this new MAC address to forward or block it. For a MAC address to be set in the forwarding state, all enabled user modules must unanimously agree on allowing the MAC address to forward. If only one chooses to block it, it will be blocked until that user module decides otherwise. The Port Security Detail screen in Figure 4-12-7 appears.

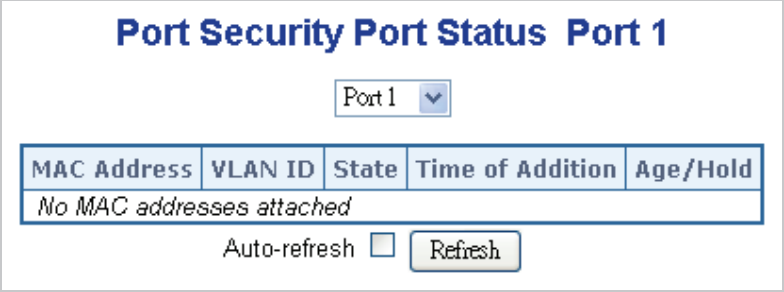


Figure 4-12-7: Port Security Detail Screen Page Screenshot

The page includes the following fields:

Object	Description
• **MAC Address & VLAN ID**	The MAC address and VLAN ID that is seen on this port. If no MAC addresses are learned, a single row stating "No MAC addresses attached" is displayed.
• **State**	Indicates whether the corresponding MAC address is blocked or forwarding. In the blocked state, it will not be allowed to transmit or receive traffic.
• **Time of Addition**	Shows the date and time when this MAC address was first seen on the port.
• **Age/Hold**	If at least one user module has decided to block this MAC address, it will stay in the blocked state until the hold time (measured in seconds) expires. If all user modules have decided to allow this MAC address to forward, and aging is enabled, the Port Security module will periodically check that this MAC address still forwards traffic. If the age period (measured in seconds) expires and no frames have been seen, the MAC address will be removed from the MAC table. Otherwise a new age period will begin. If aging is disabled or a user module has decided to hold the MAC address indefinitely, a dash (-) will be shown.

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

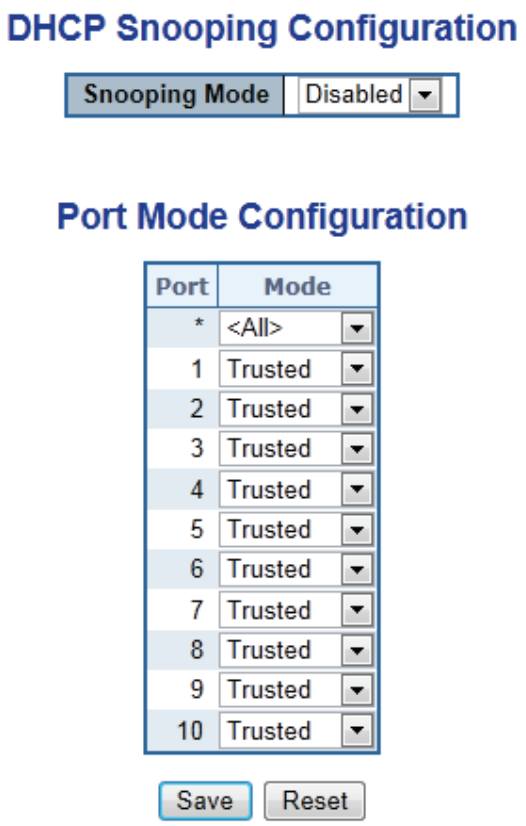


Figure 4-12-8: DHCP Snooping Configuration Screen Page Screenshot

The page includes the following fields:

Object	Description
• **Snooping Mode**	Indicates the DHCP snooping mode operation. Possible modes are: **Enabled**: Enable DHCP snooping mode operation. When enable DHCP snooping mode operation, the request DHCP messages will be forwarded to trusted ports and only allowed reply packets from trusted ports. **Disabled**: Disable DHCP snooping mode operation.
• **Port Mode**	Indicates the DHCP snooping port mode. Possible port modes are: **Trusted**: Configures the port as trusted sources of the DHCP message. **Untrusted**: Configures the port as untrusted sources of the DHCP message. **All** means all ports will have one specific setting

Buttons

: Click to save changes.

: Click to undo any changes made locally and revert to previously saved values.

4.12.9 DHCP Snooping Statistics

This page provides statistics for DHCP snooping. The statistics only counter packet under DHCP snooping mode is enabled and relay mode is disabled. And it doesn't count the DHCP packets for system DHCP client. The DHCP Snooping Port Statistics screen in Figure 4-12-9 appears.

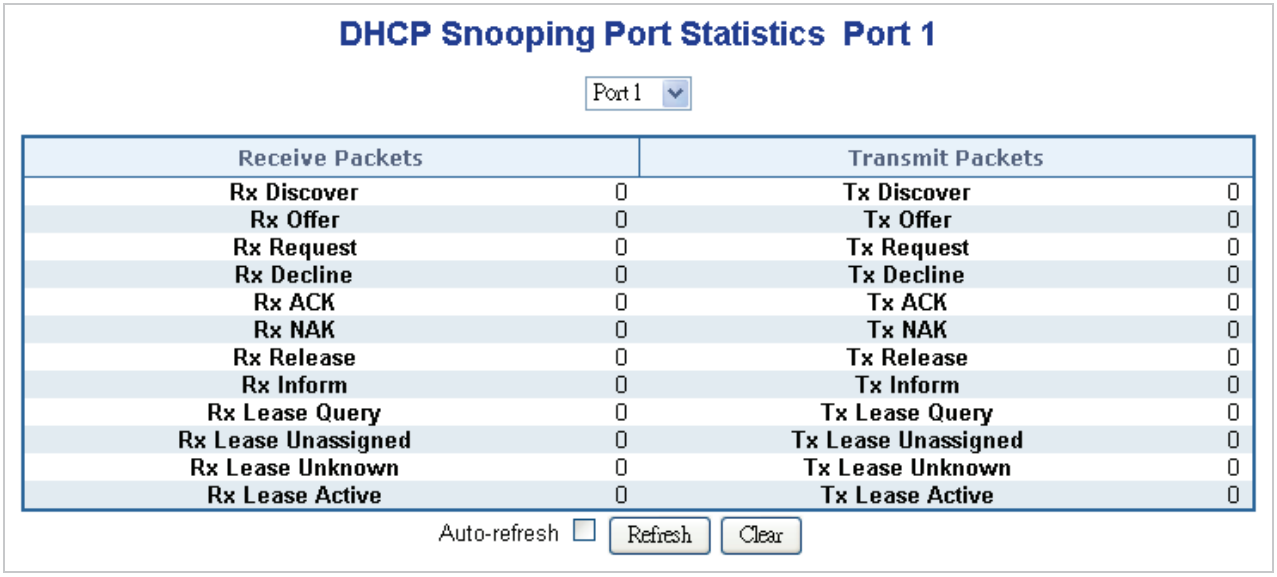


Figure 4-12-9: DHCP Snooping Port Statistics Screen Page Screenshot

The page includes the following fields:

Object	Description
• **Rx and Tx Discover**	The number of discover (option 53 with value 1) packets received and transmitted.
• **Rx and Tx Offer**	The number of offer (option 53 with value 2) packets received and transmitted.
• **Rx and Tx Request**	The number of request (option 53 with value 3) packets received and transmitted.
• **Rx and Tx Decline**	The number of decline (option 53 with value 4) packets received and transmitted.
• **Rx and Tx ACK**	The number of ACK (option 53 with value 5) packets received and transmitted.
• **Rx and Tx NAK**	The number of NAK (option 53 with value 6) packets received and transmitted.
• **Rx and Tx Release**	The number of release (option 53 with value 7) packets received and transmitted.
• **Rx and Tx Inform**	The number of inform (option 53 with value 8) packets received and transmitted.
• **Rx and Tx Lease Query**	The number of lease query (option 53 with value 10) packets received and transmitted.
• **Rx and Tx Lease Unassigned**	The number of lease unassigned (option 53 with value 11) packets received and transmitted.
• **Rx and Tx Lease Unknown**	The number of lease unknown (option 53 with value 12) packets received and transmitted.
• **Rx and Tx Lease Active**	The number of lease active (option 53 with value 13) packets received and transmitted.

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

4.12.10 IP Source Guard Configuration

IP Source Guard is a secure feature used to restrict IP traffic on DHCP snooping untrusted ports by filtering traffic based on the DHCP Snooping Table or manually configured IP Source Bindings. It helps prevent IP spoofing attacks when a host tries to spoof and use the IP address of another host. This page provides IP Source Guard related configuration. The IP Source Guard Configuration screen in Figure 4-12-10 appears.

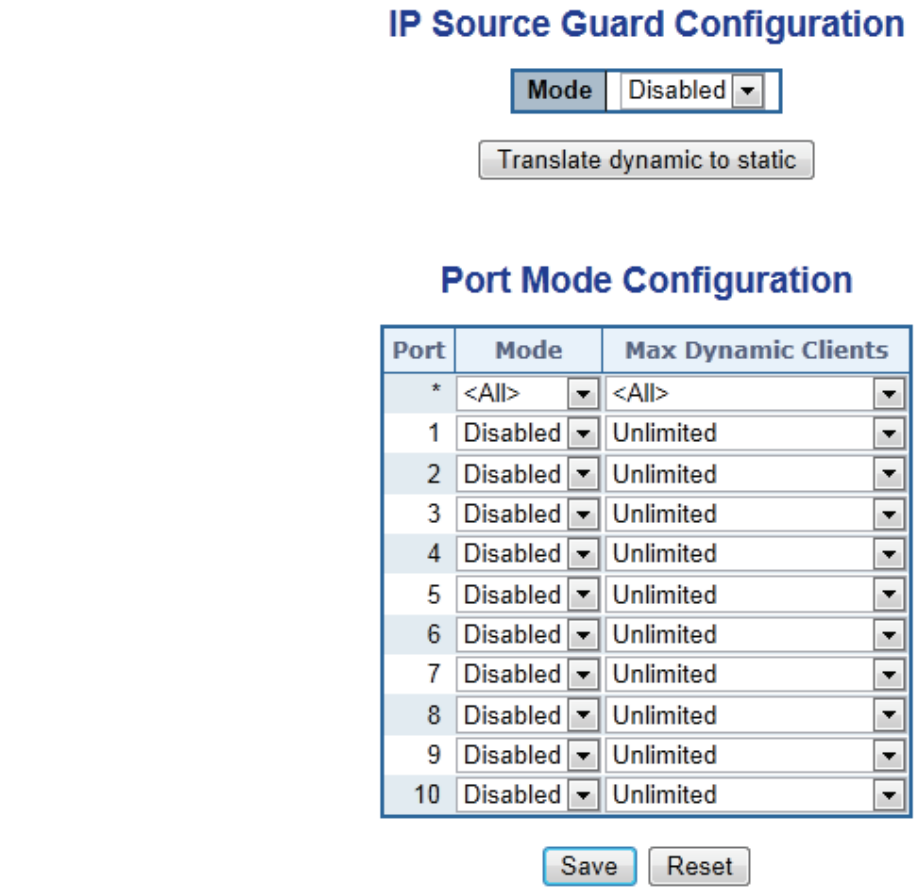


Figure 4-12-10: IP Source Guard Configuration Screen Page Screenshot

The page includes the following fields:

Object	Description
• **Mode of IP Source Guard Configuration**	Enable the Global IP Source Guard or disable the Global IP Source Guard. All configured ACEs will be lost when the mode is enabled.
• **Port Mode Configuration**	Specify IP Source Guard is enabled on which ports. Only when both Global Mode and Port Mode on a given port are enabled, IP Source Guard is enabled on this given port. **All** means all ports will have one specific setting.
• **Max Dynamic Clients**	Specify the maximum number of dynamic clients can be learned on given ports. This value can be 0, 1, 2 and unlimited. If the port mode is enabled and the value of max dynamic client is equal 0, it means only allow the IP packets forwarding that are matched in static entries on the specific port. **All** means all ports will have one specific setting.

Buttons

[redacted]: Click to translate all dynamic entries to static entries.

[redacted]: Click to save changes.

[redacted]: Click to undo any changes made locally and revert to previously saved values.

4.12.11 IP Source Guard Static Table

This page provides Static IP Source Guard Table. The Static IP Source Guard Table screen in Figure 4-12-11 appears.

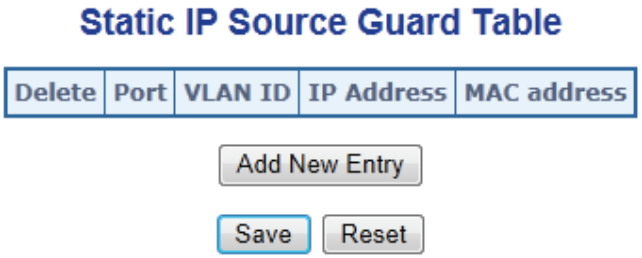


Figure 4-12-11: Static IP Source Guard Table Screen Page Screenshot

The page includes the following fields:

Object	Description
• **Delete**	Check to delete the entry. It will be deleted during the next save.
• **Port**	The logical port for the settings.
• **VLAN ID**	The VLAN ID for the settings.
• **IP Address**	Allowed Source IP address.
• **MAC address**	Allowed Source MAC address.

Buttons

4.12.12 ARP Inspection

ARP Inspection is a secure feature. Several types of attacks can be launched against a host or devices connected to Layer 2 networks by "poisoning" the ARP caches. This feature is used to block such attacks. Only valid ARP requests and responses can go through DUT. This page provides ARP Inspection related configuration. The ARP Inspection Configuration screen in Figure 4-12-12 appears.

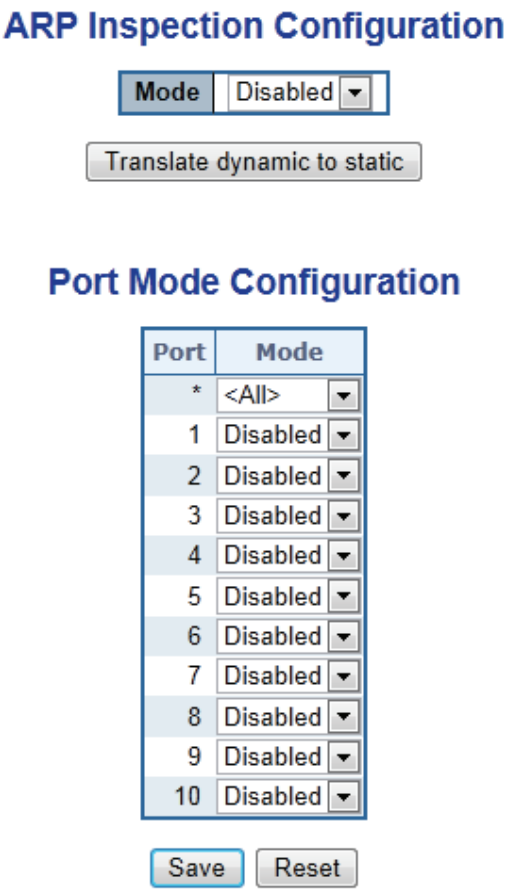


Figure 4-12-12: ARP Inspection Configuration Screen Page Screenshot

The page includes the following fields:

Object	Description
• **Mode of ARP Inspection Configuration**	Enable the Global ARP Inspection or disable the Global ARP Inspection.
• **Port Mode Configuration**	Specify ARP Inspection is enabled on which ports. Only when both Global Mode and Port Mode on a given port are enabled, ARP Inspection is enabled on this given port. **All** means all ports will have one specific setting.

Buttons

[redacted]: Click to translate all dynamic entries to static entries.

[redacted]: Click to save changes.

[redacted]: Click to undo any changes made locally and revert to previously saved values.

4.12.13 ARP Inspection Static Table

This page provides Static ARP Inspection Table. The Static ARP Inspection Table screen in Figure 4-12-13 appears.

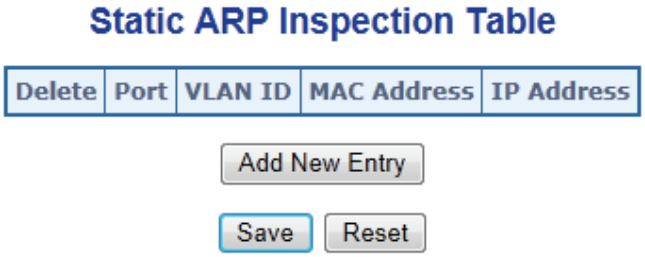


Figure 4-12-13: Static ARP Inspection Table Screen Page Screenshot

The page includes the following fields:

Object	Description
• **Delete**	Check to delete the entry. It will be deleted during the next save.
• **Port**	The logical port for the settings.
• **VLAN ID**	The VLAN ID for the settings.
• **MAC Address**	Allowed Source MAC address in ARP request packets.
• **IP Address**	Allowed Source IP address in ARP request packets.

Buttons

4.13 MAC Address Table

Switching of frames is based upon the DMAC address contained in the frame. The Managed Switch builds up a table that maps MAC addresses to switch ports for knowing which ports the frames should go to (based upon the DMAC address in the frame). This table contains both static and dynamic entries. The static entries are configured by the network administrator if the administrator wants to do a fixed mapping between the DMAC address and switch ports.

The frames also contain a MAC address (SMAC address), which shows the MAC address of the equipment sending the frame. The SMAC address is used by the switch to automatically update the MAC table with these dynamic MAC addresses. Dynamic entries are removed from the MAC table if no frame with the corresponding SMAC address have been seen after a configurable age time.

4.13.1 MAC Address Table Configuration

The MAC Address Table is configured on this page. Set timeouts for entries in the dynamic MAC Table and configure the static MAC table here. The MAC Address Table Configuration screen in Figure 4-13-1 appears.

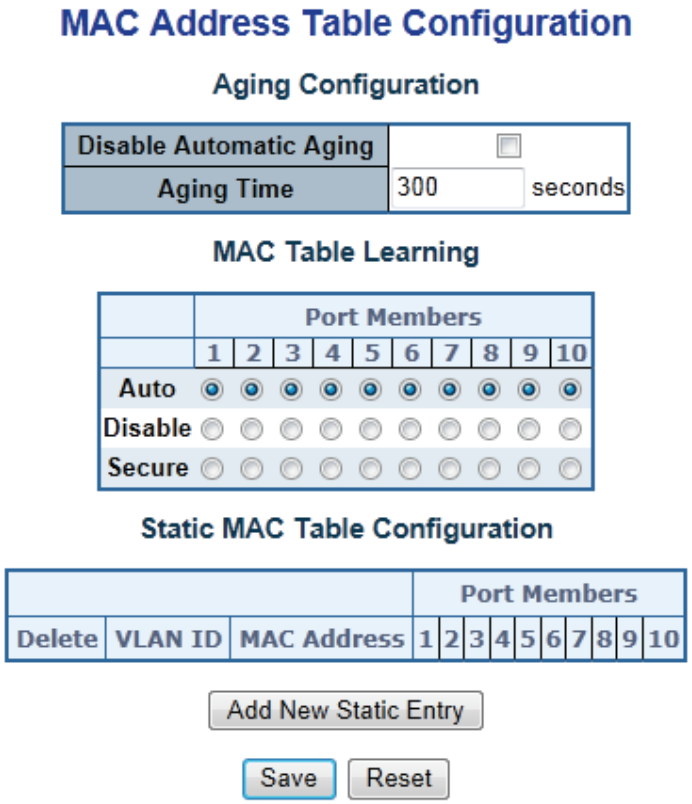


Figure 4-13-1: MAC Address Table Configuration Page Screenshot

The page includes the following fields:

Aging Configuration

By default, dynamic entries are removed from the MAC table after 300 seconds. This removal is also called aging.

Object	Description
• **Disable Automatic Aging**	Enables/disables the the automatic aging of dynamic entries
• **Aging Time**	The time after which a learned entry is discarded. By default, dynamic entries are removed from the MAC after 300 seconds. This removal is also called aging. (Range: 10-10000000 seconds; Default: 300 seconds)

MAC Table Learning

If the learning mode for a given port is greyed out, another module is in control of the mode, so that it cannot be changed by the user. An example of such a module is the MAC-Based Authentication under 802.1X.

Object	Description
• **Auto**	Learning is done automatically as soon as a frame with unknown SMAC is received.
• **Disable**	No learning is done.
• **Secure**	Only static MAC entries are learned, all other frames are dropped. **Note:** Make sure that the link used for managing the switch is added to the Static Mac Table before changing to secure learning mode, otherwise the management link is lost and can only be restored by using another non-secure port or by connecting to the switch via the serial interface.

Static MAC Table Configuration

The static entries in the MAC table are shown in this table. The static MAC table can contain 64 entries. The MAC table is sorted first by VLAN ID and then by MAC address.

Object	Description
• **Delete**	Check to delete the entry. It will be deleted during the next save.
• **VLAN ID**	The VLAN ID of the entry.
• **MAC Address**	The MAC address of the entry.
• **Port Members**	Checkmarks indicate which ports are members of the entry. Check or uncheck as needed to modify the entry.

Buttons

Add New Static Entry : Click to add a new entry.

[redacted]: Click to save changes.

[redacted]: Click to undo any changes made locally and revert to previously saved values.

4.13.2 MAC Address Table Status

Dynamic MAC Table

Entries in the MAC Table are shown on this page. The MAC Table contains up to **8192** entries, and is sorted first by VLAN ID, then by MAC address. The MAC Address Table screen in Figure 4-13-2 appears.

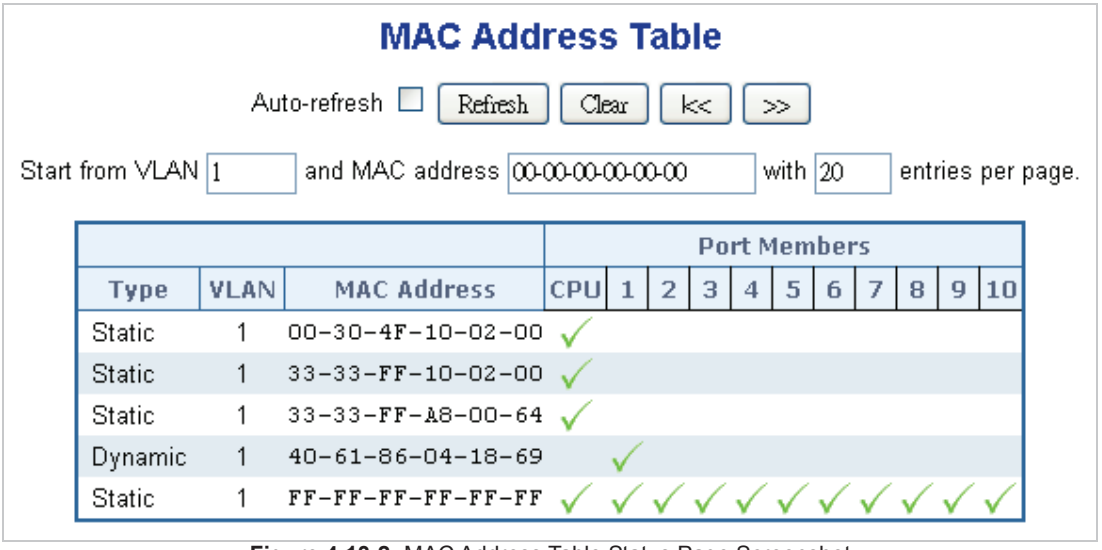


Figure 4-13-2: MAC Address Table Status Page Screenshot

Navigating the MAC Table

Each page shows up to 999 entries from the MAC table, default being 20, selected through the "**entries per page"** input field. When first visited, the web page will show the first 20 entries from the beginning of the MAC Table. The first displayed will be the one with the lowest VLAN ID and the lowest MAC address found in the MAC Table.

The "**Start from MAC address**" and "**VLAN**" input fields allow the user to select the starting point in the MAC Table. Clicking the "**Refresh**" button will update the displayed table starting from that or the closest next MAC Table match.

In addition, the two input fields will - upon a "**Refresh**" button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

The "**>>**" will use the last entry of the currently displayed VLAN/MAC address pairs as a basis for the next lookup. When the end is reached the text "no more entries" is shown in the displayed table. Use the "**|<<**" button to start over.

The page includes the following fields:

Object	Description
• **Type**	Indicates whether the entry is a static or dynamic entry.
• **VLAN**	The VLAN ID of the entry.
• **MAC Address**	The MAC address of the entry.
• **Port Members**	The ports that are members of the entry.

Buttons

Auto-refresh  : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

• **IP Address**	User IP address of the entry.

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

4.13.4 Dynamic IP Source Guard Table

Entries in the Dynamic IP Source Guard Table are shown on this page. The Dynamic IP Source Guard Table is sorted first by port, then by VLAN ID, then by IP address, and then by MAC address. The Dynamic IP Source Guard Table screen in Figure 4-13-4 appears.

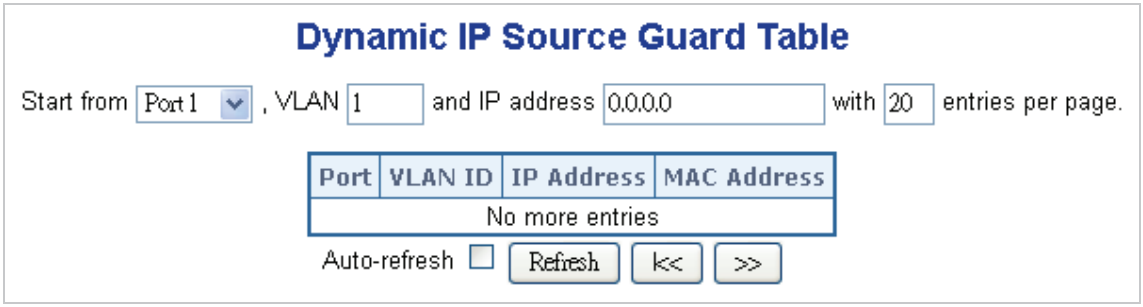


Figure 4-13-4: Dynamic IP Source Guard Table Screenshot

Navigating the ARP Inspection Table

Each page shows up to 99 entries from the Dynamic IP Source Guard table, default being 20, selected through the "**entries per page**" input field. When first visited, the web page will show the first 20 entries from the beginning of the Dynamic IP Source Guard Table. The "**Start from port address**", "**VLAN**", "**IP address**" and "**IP mask**" input fields allow the user to select the starting point in the Dynamic IP Source Guard Table. Clicking the "**Refresh**" button will update the displayed table starting from that or the closest next Dynamic IP Source Guard Table match. In addition, the two input fields will - upon a "**Refresh**" button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.
The "**>>**" will use the last entry of the currently displayed as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the "**|<<**" button to start over.
The page includes the following fields:

Object	Description
• **Port**	Switch Port Number for which the entries are displayed.
• **VLAN ID**	VLAN-ID in which the IP traffic is permitted.
• **IP Address**	User IP Address of the entry.
• **MAC Address**	Source MAC Address.

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

4.14.2 LLDP Configuration

This page allows the user to inspect and configure the current LLDP port settings. The LLDP Configuration screen in Figure 4-14-1 appears.

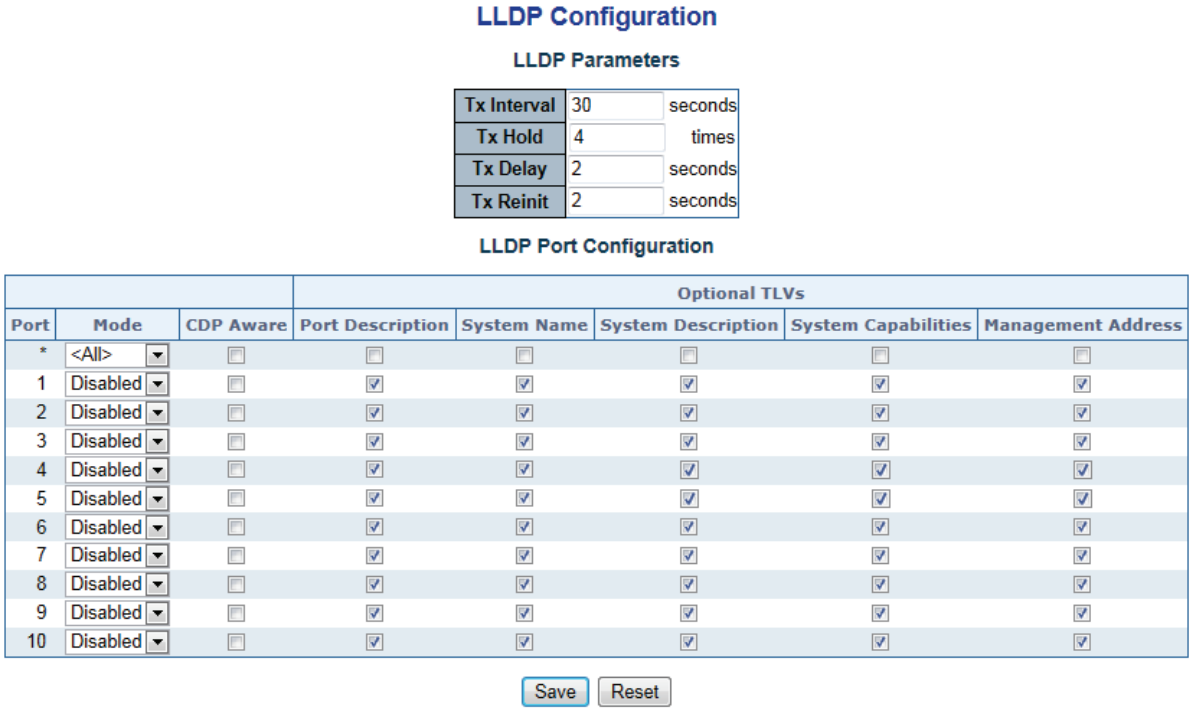


Figure 4-14-1: LLDP Configuration Page Screenshot

The page includes the following fields:

LLDP Parameters

Object	Description
• **Tx Interval**	The switch is periodically transmitting LLDP frames to its neighbors for having the network discovery information up-to-date. The interval between each LLDP frame is determined by the **Tx Interval** value. Valid values are restricted to 5 - 32768 seconds. Default: **30** seconds This attribute must comply with the following rule: (Transmission Interval * Hold Time Multiplier) ≤65536, and Transmission Interval >= (4 * Delay Interval)
• **Tx Hold**	Each LLDP frame contains information about how long the information in the LLDP frame shall be considered valid. The LLDP information valid period is set to **Tx Hold** multiplied by **Tx Interval** seconds. Valid values are restricted to 2 - 10 times. TTL in seconds is based on the following rule: (Transmission Interval * Holdtime Multiplier) ≤ 65536. Therefore, the default TTL is 4*30 = 120 seconds.
• **Tx Delay**	If some configuration is changed (e.g. the IP address) a new LLDP frame is transmitted, but the time between the LLDP frames will always be at least the value of **Tx Delay** seconds. **Tx Delay** cannot be larger than 1/4 of the **Tx Interval** value. Valid values are restricted to 1 - 8192 seconds. This attribute must comply with the rule: (4 * Delay Interval) ≤Transmission Interval
• **Tx Reinit**	When a port is disabled, LLDP is disabled or the switch is rebooted a LLDP shutdown frame is transmitted to the neighboring units, signaling that the LLDP information isn't valid anymore. **Tx Reinit** controls the amount of seconds between the shutdown frame and a new LLDP initialization. Valid values are restricted to 1 - 10 seconds.

LLDP Port Configuration

The LLDP port settings relate to the currently selected stack unit, as reflected by the page header.

Object	Description
• **Port**	The switch port number of the logical LLDP port.
• **Mode**	Select LLDP mode. **All** means all ports will have one specific setting. ■ **Rx only** The switch will not send out LLDP information, but LLDP information from neighbor units is analyzed. ■ **Tx only** The switch will drop LLDP information received from neighbors, but will send out LLDP information. ■ **Disabled** The switch will not send out LLDP information, and will drop LLDP information received from neighbors. ■ **Enabled** The switch will send out LLDP information, and will analyze LLDP information received from neighbors.
• **CDP Aware**	Select CDP awareness. The CDP operation is restricted to decoding incoming CDP frames (The switch doesn't transmit CDP frames). CDP frames are only decoded if LLDP on the port is enabled. Only CDP TLVs that can be mapped to a corresponding field in the LLDP neighbours' table are decoded. All other TLVs are discarded (Unrecognized CDP TLVs and discarded CDP frames are not shown in the LLDP statistics.). CDP TLVs are mapped onto LLDP neighbours' table as shown below. ■ CDP TLV "**Device ID**" is mapped to the LLDP "Chassis ID" field. ■ CDP TLV "**Address**" is mapped to the LLDP "Management Address" field. The CDP address TLV can contain multiple addresses, but only the first address is shown in the LLDP neighbours table. ■ CDP TLV "**Port ID**" is mapped to the LLDP "Port ID" field. ■ CDP TLV "**Version and Platform**" is mapped to the LLDP "System Description" field. Both the CDP and LLDP support "**system capabilities**", but the CDP capabilities cover capabilities that are not part of the LLDP. These capabilities are shown as "others" in the LLDP neighbours' table. If all ports have CDP awareness disabled the switch forwards CDP frames

	received from neighbour devices. If at least one port has CDP awareness enabled all CDP frames are terminated by the switch. **Note**: When CDP awareness on a port is disabled the CDP information isn't removed immediately, but gets removed when the hold time is exceeded.
• **Port Description**	Optional TLV: When checked the "port description" is included in LLDP information transmitted.
• **System Name**	Optional TLV: When checked the "system name" is included in LLDP information transmitted.
• **System Description**	Optional TLV: When checked the "system description" is included in LLDP information transmitted.
• **System Capabilities**	Optional TLV: When checked the "system capability" is included in LLDP information transmitted. The system capabilities identifies the primary function(s) of the system and whether or not these primary functions are enabled. The information advertised by this TLV is described in **IEEE 802.1AB**.
• **Management Address**	Optional TLV: When checked the "management address" is included in LLDP information transmitted. The management address protocol packet includes the IPv4 address of the switch. If no management address is available, the address should be the MAC address for the CPU or for the port sending this advertisement. The management address TLV may also include information about the specific interface associated with this address, and an object identifier indicating the type of hardware component or protocol entity associated with this address

Buttons

 : Click to save changes.

 : Click to undo any changes made locally and revert to previously saved values.

4.14.3 LLDP-MED Configuration

This page allows you to configure the LLDP-MED. The LLDP-MED Configuration screen in Figure 4-14-2 appears.

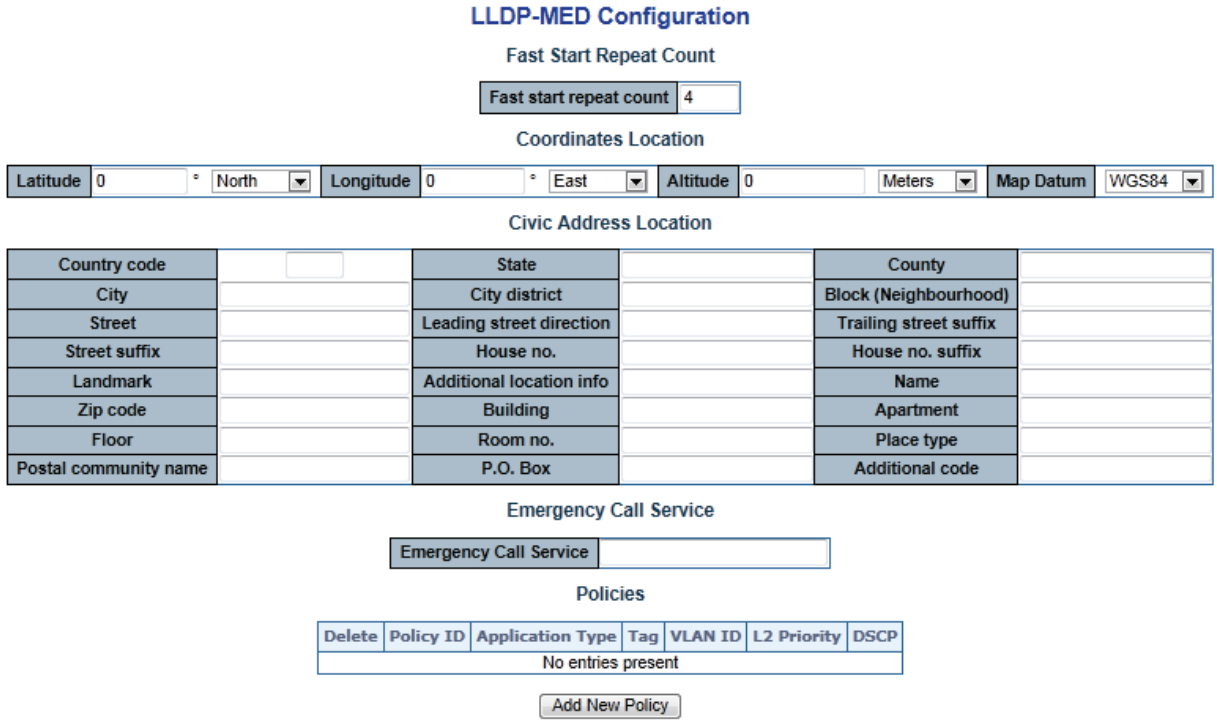


Figure 4-14-2: LLDP-MED Configuration Page Screenshot

The page includes the following fields:

Fast Start Repeat Count

Object	Description
• **Fast start repeat count**	Rapid startup and Emergency Call Service Location Identification Discovery of endpoints is a critically important aspect of VoIP systems in general.In addition, it is best to advertise only those pieces of information which are specifically relevant to particular endpoint types (for example only advertise the voice network policy to permitted voice-capable devices), both in order to conserve the limited LLDPU space and to reduce security and system integrity issues that can come with inappropriate knowledge of the network policy. With this in mind LLDP-MED defines an LLDP-MED Fast Start interaction between the protocol and the application layers on top of the protocol, in order to achieve these related properties. Initially, a Network Connectivity Device will only transmit LLDP TLVs in an LLDPDU. Only after an LLDP-MED Endpoint Device is detected, will an LLDP-MED capable Network Connectivity Device start to advertise LLDP-MED TLVs in outgoing LLDPDUs on the associated port. The LLDP-MED application will temporarily speed up the transmission of the LLDPDU to start within a second, when a new LLDP-MED neighbor has been detected in order share LLDP-MED information as fast as possible to new neighbors. Because there is a risk that a LLDP frame being lost during transmission between neighbors, it is recommended to repeat the fast start transmission multiple times to increase the possibility for that the neighbors has received the LLDP frame. With Fast start repeat count it is possible to specify the number of times the fast start transmission is repeated. The recommended value is 4 times, giving that 4 LLDP frames with a 1 second interval will be transmitted, when a LLDP frame with new information is received. It should be noted that LLDP-MED and the LLDP-MED Fast Start mechanism is only intended to run on links between LLDP-MED Network Connectivity Devices and Endpoint Devices, and as such does not apply to links between LAN infrastructure elements, including between Network Connectivity Devices, or to other types of links.

Coordinates Location

Object	Description
• **Latitude**	Latitude SHOULD be normalized to within 0-90 degrees with a maximum of 4 digits. It is possible to specify the direction to either North of the equator or South of the equator.
• **Longitude**	Longitude SHOULD be normalized to within 0-180 degrees with a maximum of 4 digits. It is possible to specify the direction to either East of the prime meridian or West of the prime meridian.
• **Altitude**	Altitude SHOULD be normalized to within -32767 to 32767 with a maximum of 4 digits. It is possible to select between two altitude types (floors or meters). **Meters**: Representing meters of Altitude defined by the vertical datum specified. **Floors**: Representing altitude in a form more relevant in buildings which have different floor-to-floor dimensions. An altitude = 0.0 is meaningful even outside a building, and represents ground level at the given latitude and longitude. Inside a building, 0.0 represents the floor level associated with ground level at the main entrance.
• **Map Datum**	The Map Datum used for the coordinates given in this Option **WGS84**: (Geographical 3D) - World Geodesic System 1984, CRS Code 4327, Prime Meridian Name: Greenwich. **NAD83/NAVD88**: North American Datum 1983, CRS Code 4269, Prime Meridian Name: Greenwich; The associated vertical datum is the North American Vertical Datum of 1988 (NAVD88). This datum pair is to be used when referencing locations on land, not near tidal water (which would use Datum = NAD83/MLLW). **NAD83/MLLW**: North American Datum 1983, CRS Code 4269, Prime Meridian Name: Greenwich; The associated vertical datum is Mean Lower Low Water (MLLW). This datum pair is to be used when referencing locations on water/sea/ocean.

Civic Address Location

IETF Geopriv Civic Address based Location Configuration Information (Civic Address LCI).

Object	Description
• **Country code**	The two-letter ISO 3166 country code in capital ASCII letters - Example: DK, DE or US.
• **State**	National subdivisions (state, canton, region, province, prefecture).
• **County**	County, parish, gun (Japan), district.
• **City**	City, township, shi (Japan) - Example: Copenhagen
• **City district**	City division, borough, city district, ward, chou (Japan)
• **Block (Neighborhood)**	Neighborhood, block
• **Street**	Street - Example: Poppelvej
• **Leading street direction**	Leading street direction - Example: N
• **Trailing street suffix**	Trailing street suffix - Example: SW
• **Street suffix**	Street suffix - Example: Ave, Platz
• **House no.**	House number - Example: 21
• **House no. suffix**	House number suffix - Example: A, 1/2
• **Landmark**	Landmark or vanity address - Example: Columbia University
• **Additional location info**	Additional location info - Example: South Wing

• **Name**	Name (residence and office occupant) - Example: Flemming Jahn
• **Zip code**	Postal/zip code - Example: 2791
• **Building**	Building (structure) - Example: Low Library
• **Apartment**	Unit (Apartment, suite) - Example: Apt 42
• **Floor**	Floor - Example: 4
• **Room no.**	Room number - Example: 450F
• **Place type**	Place type - Example: Office
• **Postal community name**	Postal community name - Example: Leonia
• **P.O. Box**	Post office box (P.O. BOX) - Example: 12345
• **Additional code**	Additional code - Example: 1320300003

Emergency Call Service

Emergency Call Service (e.g. E911 and others), such as defined by TIA or NENA.

Object	Description
• **Emergency Call Service**	Emergency Call Service ELIN identifier data format is defined to carry the ELIN identifier as used during emergency call setup to a traditional CAMA or ISDN trunk-based PSAP. This format consists of a numerical digit string, corresponding to the ELIN to be used for emergency calling.

Policies

Network Policy Discovery enables the efficient discovery and diagnosis of mismatch issues with the VLAN configuration, along with the associated Layer 2 and Layer 3 attributes, which apply for a set of specific protocol applications on that port. Improper network policy configurations are a very significant issue in VoIP environments that frequently result in voice quality degradation or loss of service.

Policies are only intended for use with applications that have specific 'real-time' network policy requirements, such as interactive voice and/or video services.

The network policy attributes advertised are:

1. Layer 2 VLAN ID (IEEE 802.1Q-2003)
2. Layer 2 priority value (IEEE 802.1D-2004)
3. Layer 3 Diffserv code point (DSCP) value (IETF RFC 2474)

This network policy is potentially advertised and associated with multiple sets of application types supported on a given port. The application types specifically addressed are:

1. Voice
2. Guest Voice
3. Softphone Voice
4. Video Conferencing
5. Streaming Video
6. Control / Signaling (conditionally support a separate network policy for the media types above)

A large network may support multiple VoIP policies across the entire organization, and different policies per application type. LLDP-MED allows multiple policies to be advertised per port, each corresponding to a different application type. Different ports on the same Network Connectivity Device may advertise different sets of policies, based on the authenticated user identity or port configuration.

It should be noted that LLDP-MED is not intended to run on links other than between Network Connectivity Devices and Endpoints, and therefore does not need to advertise the multitude of network policies that frequently run on an aggregated link interior to the LAN.

Object	Description
• **Delete**	Check to delete the policy. It will be deleted during the next save.
• **Policy ID**	ID for the policy. This is auto generated and shall be used when selecting the polices that shall be mapped to the specific ports.

• **Application Type**	Intended use of the application types: **Voice** - for use by dedicated IP Telephony handsets and other similar appliances supporting interactive voice services. These devices are typically deployed on a separate VLAN for ease of deployment and enhanced security by isolation from data applications. **Voice Signaling (conditional)** - for use in network topologies that require a different policy for the voice signaling than for the voice media. This application type should not be advertised if all the same network policies apply as those advertised in the Voice application policy. **Guest Voice** - support a separate 'limited feature-set' voice service for guest users and visitors with their own IP Telephony handsets and other similar appliances supporting interactive voice services. **Guest Voice Signaling (conditional)** - for use in network topologies that require a different policy for the guest voice signaling than for the guest voice media. This application type should not be advertised if all the same network policies apply as those advertised in the Guest Voice application policy. **Softphone Voice** - for use by softphone applications on typical data centric devices, such as PCs or laptops. This class of endpoints frequently does not support multiple VLANs, if at all, and are typically configured to use an 'untagged' VLAN or a single 'tagged' data specific VLAN. When a network policy is defined for use with an 'untagged' VLAN (see Tagged flag below), then the L2 priority field is ignored and only the DSCP value has relevance. **Video Conferencing** **Streaming Video** - for use by broadcast or multicast based video content distribution and other similar applications supporting streaming video services that require specific network policy treatment. Video applications relying on TCP with buffering would not be an intended use of this application type. **Video Signaling (conditional)** - for use in network topologies that require a separate policy for the video signaling than for the video media. This application type should not be advertised if all the same network policies apply as those advertised in the Video Conferencing application policy.
• **Tag**	Tag indicating whether the specified application type is using a 'tagged' or an 'untagged' VLAN. Untagged indicates that the device is using an untagged frame format and as such does not include a tag header as defined by IEEE 802.1Q-2003. In this case, both the VLAN ID and the Layer 2 priority fields are ignored and only the DSCP value has relevance. Tagged indicates that the device is using the IEEE 802.1Q tagged frame format, and that both the VLAN ID and the Layer 2 priority values are being used, as well as the DSCP value. The tagged format includes an additional field, known as the tag header. The tagged frame format also includes priority tagged frames as defined by IEEE 802.1Q-2003.
• **VLAN ID**	VLAN identifier (VID) for the port as defined in IEEE 802.1Q-2003
• **L2 Priority**	L2 Priority is the Layer 2 priority to be used for the specified application type. L2 Priority may specify one of eight priority levels (0 through 7), as defined by IEEE 802.1D-2004. A value of 0 represents use of the default priority as defined in IEEE 802.1D-2004.
• **DSCP**	DSCP value to be used to provide Diffserv node behavior for the specified application type as defined in IETF RFC 2474. DSCP may contain one of 64 code point values (0 through 63). A value of 0 represents use of the default DSCP value as defined in RFC 2475.

Port Policies Configuration

Every port may advertise a unique set of network policies or different attributes for the same network policies, based on the authenticated user identity or port configuration.

Object	Description
• **Port**	The port number for which the configuration applies.
• **Policy ID**	The set of policies that shall apply for a given port. The set of policies is selected by checkmarking the checkboxes that corresponds to the policies

Buttons

[redacted]: click to add new policy.

 : Click to save changes.

 : Click to undo any changes made locally and revert to previously saved values.

4.14.4 LLDP-MED Neighbor

This page provides a status overview for all LLDP-MED neighbors. The displayed table contains a row for each port on which an LLDP neighbor is detected. The LLDP-MED Neighbor Information screen in Figure 4-14-3 appears. The columns hold the following information:

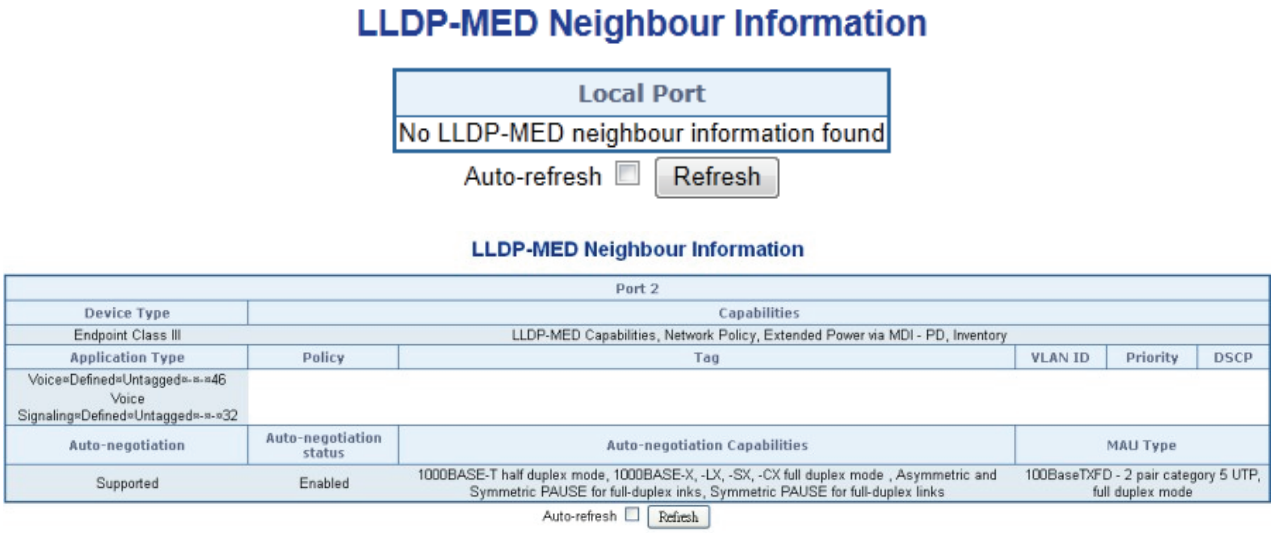


Figure 4-14-3: LLDP-MED Neighbor Information Page Screenshot

The page includes the following fields:

Fast Start Repeat Count

Object	Description
• **Port**	The port on which the LLDP frame was received.
• **Device Type**	LLDP-MED Devices are comprised of two primary Device Types: Network Connectivity Devices and Endpoint Devices. **LLDP-MED Network Connectivity Device Definition** LLDP-MED Network Connectivity Devices, as defined in TIA-1057, provide access to the IEEE 802 based LAN infrastructure for LLDP-MED Endpoint Devices. An LLDP-MED Network Connectivity Device is a LAN access device based on any of the following technologies: 1. LAN Switch/Router 2. IEEE 802.1 Bridge 3. IEEE 802.3 Repeater (included for historical reasons) 4. IEEE 802.11 Wireless Access Point 5. Any device that supports the IEEE 802.1AB and MED extensions defined by TIA-1057 and can relay IEEE 802 frames via any method. **LLDP-MED Endpoint Device Definition** Within the LLDP-MED Endpoint Device category, the LLDP-MED scheme is broken into further Endpoint Device Classes, as defined in the following. Each LLDP-MED Endpoint Device Class is defined to build upon the capabilities defined for the previous Endpoint Device Class. Fore-example will any LLDP-MED Endpoint Device claiming compliance as a Media Endpoint (Class II) also support all aspects of TIA-1057 applicable to Generic Endpoints (Class I), and any LLDP-MED Endpoint Device claiming compliance as a Communication Device (Class III) will also support all aspects of TIA-1057 applicable to both Media Endpoints (Class II) and Generic Endpoints (Class I). **LLDP-MED Generic Endpoint (Class I)** The LLDP-MED Generic Endpoint (Class I) definition is applicable to all endpoint products that require the base LLDP discovery services defined in TIA-1057, however do not support IP media or act as an end-user communication appliance. Such devices may include (but are not limited to) IP Communication Controllers, other communication related servers, or any device requiring basic services as defined in TIA-1057. Discovery services defined in this class include LAN configuration, device location, network policy, power management, and inventory management. **LLDP-MED Media Endpoint (Class II)** The LLDP-MED Media Endpoint (Class II) definition is applicable to all endpoint

	products that have IP media capabilities however may or may not be associated with a particular end user. Capabilities include all of the capabilities defined for the previous Generic Endpoint Class (Class I), and are extended to include aspects related to media streaming. Example product categories expected to adhere to this class include (but are not limited to) Voice / Media Gateways, Conference Bridges, Media Servers, and similar. Discovery services defined in this class include media-type-specific network layer policy discovery. **LLDP-MED Communication Endpoint (Class III)** The LLDP-MED Communication Endpoint (Class III) definition is applicable to all endpoint products that act as end user communication appliances supporting IP media. Capabilities include all of the capabilities defined for the previous Generic Endpoint (Class I) and Media Endpoint (Class II) classes, and are extended to include aspects related to end user devices. Example product categories expected to adhere to this class include (but are not limited to) end user communication appliances, such as IP Phones, PC-based softphones, or other communication appliances that directly support the end user. Discovery services defined in this class include provision of location identifier (including ECS / E911 information), embedded L2 switch support, inventory management
• **LLDP-MED Capabilities**	LLDP-MED Capabilities describes the neighbor unit's LLDP-MED capabilities. The possible capabilities are: 1. LLDP-MED capabilities 2. Network Policy 3. Location Identification 4. Extended Power via MDI - PSE 5. Extended Power via MDI - PD 6. Inventory 7. Reserved
• **Application Type**	Application Type indicating the primary function of the application(s) defined for this network policy, advertised by an Endpoint or Network Connectivity Device. The poosible application types are shown below. ■ **Voice** - for use by dedicated IP Telephony handsets and other similar appliances supporting interactive voice services. These devices are typically deployed on a separate VLAN for ease of deployment and enhanced security by isolation from data applications. ■ **Voice Signaling** - for use in network topologies that require a different policy for the voice signaling than for the voice media. ■ **Guest Voice** - to support a separate limited feature-set voice service for guest users and visitors with their own IP Telephony handsets and other similar appliances supporting interactive voice services. ■ **Guest Voice Signaling** - for use in network topologies that require a different policy for the guest voice signaling than for the guest voice media. ■ **Softphone Voice** - for use by softphone applications on typical data centric devices, such as PCs or laptops. ■ **Video Conferencing** - for use by dedicated Video Conferencing equipment and other similar appliances supporting real-time interactive video/audio services. ■ **Streaming Video** - for use by broadcast or multicast based video content distribution and other similar applications supporting streaming video services that require specific network policy treatment. Video applications relying on TCP with buffering would not be an intended use of this application type. ■ **Video Signaling** - for use in network topologies that require a separate policy for the video signaling than for the video media.
• **Policy**	Policy **Unknown**: The network policy for the specified application type is currently unknown. **Defined**: The network policy is defined.
• **TAG**	TAG is indicating whether the specified application type is using a tagged or an untagged VLAN. Can be Tagged ot Untagged ■ **Untagged**: The device is using an untagged frame format and as such does not include a tag header as defined by IEEE 802.1Q-2003. ■ **Tagged**: The device is using the IEEE 802.1Q tagged frame format
• **VLAN ID**	VLAN ID is the VLAN identifier (VID) for the port as defined in IEEE 802.1Q-2003. A value of 1 through 4094 is used to define a valid VLAN ID. A value of 0 (Priority Tagged) is used if the device is using priority tagged frames as defined by IEEE 802.1Q-2003, meaning that only the IEEE 802.1D priority level is significant and the default PVID of the ingress port is used instead.

• **Priority**	Priority is the Layer 2 priority to be used for the specified application type.One of eight priority levels (0 through 7)
• **DSCP**	DSCP is the DSCP value to be used to provide Diffserv node behavior for the specified application type as defined in IETF RFC 2474. Contain one of 64 code point values (0 through 63).
• **Auto-negotiation**	**Auto-negotiation** identifies if MAC/PHY auto-negotiation is supported by the link partner.
• **Auto-negotiation status**	**Auto-negotiation status** identifies if auto-negotiation is currently enabled at the link partner. If **Auto-negotiation** is supported and **Auto-negotiation status** is disabled, the 802.3 PMD operating mode will be determined the operational MAU type field value rather than by auto-negotiation.
• **Auto-negotiation Capabilities**	**Auto-negotiation Capabilities** shows the link partners MAC/PHY capabilities.

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

4.14.6 Port Statistics

This page provides an overview of all LLDP traffic. Two types of counters are shown. Global counters are counters that refer to the whole stack, switch, while local counters refer to counters for the currently selected switch. The LLDP Statistics screen in Figure 4-14-5 appears.

LLDP Global Counters

Global Counters	
Neighbour entries were last changed	- (29158 sec. ago)
Total Neighbours Entries Added	0
Total Neighbours Entries Deleted	0
Total Neighbours Entries Dropped	0
Total Neighbours Entries Aged Out	0

LLDP Statistics Local Counters

Local Port	Tx Frames	Rx Frames	Rx Errors	Frames Discarded	TLVs Discarded	TLVs Unrecognized	Org. Discarded	Age-Outs
1	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0

Auto-refresh Refresh Clear

Figure 4-14-5: LLDP Statistics Page Screenshot

The page includes the following fields:

Global Counters

Object	Description
• **Neighbor entries were last changed at**	It also shows the time when the last entry was last deleted or added. It also shows the time elapsed since the last change was detected.
• **Total Neighbors Entries Added**	Shows the number of new entries added since switch reboot.
• **Total Neighbors Entries Deleted**	Shows the number of new entries deleted since switch reboot.
• **Total Neighbors Entries Dropped**	Shows the number of LLDP frames dropped due to that the entry table was full.
• **Total Neighbors Entries Aged Out**	Shows the number of entries deleted due to Time-To-Live expiring.

Local Counters

The displayed table contains a row for each port. The columns hold the following information:

Object	Description
• **Local Port**	The port on which LLDP frames are received or transmitted.
• **Tx Frames**	The number of LLDP frames transmitted on the port.
• **Rx Frames**	The number of LLDP frames received on the port.
• **Rx Errors**	The number of received LLDP frames containing some kind of error.
• **Frames Discarded**	If an LLDP frame is received on a port, and the switch's internal table has run full, the LLDP frame is counted and discarded. This situation is known as "Too Many Neighbors" in the LLDP standard. LLDP frames require a new entry in the table when the Chassis ID or Remote Port ID is not already contained within the table. Entries are removed from the table when a given port links down, an LLDP shutdown frame is received, or when the entry ages out.
• **TLVs Discarded**	Each LLDP frame can contain multiple pieces of information, known as TLVs (TLV is short for "Type Length Value"). If a TLV is malformed, it is counted and discarded.
• **TLVs Unrecognized**	The number of well-formed TLVs, but with an unknown type value.
• **Org. Discarded**	The number of organizationally TLVs received.
• **Age-Outs**	Each LLDP frame contains information about how long time the LLDP information is valid (age-out time). If no new LLDP frame is received within the age out time, the LLDP information is removed, and the **Age-Out** counter is incremented.

Buttons

Auto-refresh  : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

4.14.7 LLDP Neighbours EEE Information

By using EEE power savings can be achieved at the expense of traffic latency. This latency occurs due to that the circuits EEE turn off to save power, need time to boot up before sending traffic over the link. This time is called "wakeup time". To achieve minimal latency, devices can use LLDP to exchange information about their respective tx and rx "wakeup time ", as a way to agree upon the minimum wakeup time they need.

This page provides an overview of EEE information exchanged by LLDP. The LLDP Neighbors EEE Information screen in Figure 4-14-6 appears.

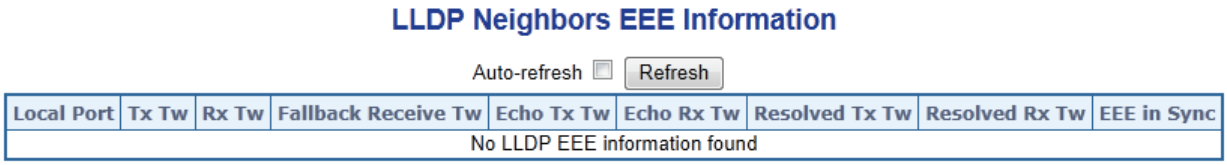


Figure 4-14-6: LLDP Neighbors EEE Information Page Screenshot

The page includes the following fields:

Object	Description
• **Local Port**	The port on which LLDP frames are received or transmitted.
• **Tx Tw**	The link parther's maximum time that transmit path can holdoff sending data after deassertion of LPI.
• **Rx Tw**	The link parther's time that receiver would like the transmitter to holdoff to allow time for the receiver to wake from sleep.
• **Fallback Receive Tw**	The link parther's fallback receive Tw. A receiving link partner may inform the transmitter of an alternate desired Tw_sys_tx. Since a receiving link partner is likely to have discrete levels for savings, this provides the transmitter with additional information that it may use for a more efficient allocation. Systems that do not implement this option default the value to be the same as that of the Receive Tw_sys_tx.
• **Echo Tx Tw**	The link partner's Echo Tx Tw value. The respective echo values shall be defined as the local link partners reflection (echo) of the remote link partners respective values. When a local link partner receives its echoed values from the remote link partner it can determine whether or not the remote link partner has received, registered and processed its most recent values. For example, if the local link partner receives echoed parameters that do not match the values in its local MIB, then the local link partner infers that the remote link partners request was based on stale information.
• **Echo Rx Tw**	The link partner's Echo Rx Tw value.
• **Resolved Tx Tw**	The resolved Tx Tw for this link. Note : NOT the link parther The resolved value that is the actual "tx wakeup time " used for this link (based on EEE information exchanged via LLDP).
• **Resolved Rx Tw**	The resolved Rx Tw for this link. Note : NOT the link parther The resolved value that is the actual "tx wakeup time " used for this link (based on EEE information exchanged via LLDP).
• **EEE in Sync**	Shows whether the switch and the link partner have agreed on wake times. Red - Switch and link partner have not agreed on wakeup times. Green - Switch and link partner have agreed on wakeup times.

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

4.15 Diagnostics

This section provide the Physical layer and IP layer network diagnostics tools for troubleshoot. The diagnostic tools are designed for network manager to help them quickly diagnose problems between point to point and better service customers.

Use the Diagnastics menu items to display and configure basic administrative details of the Managed Switch. Under System the following topics are provided to configure and view the system information:
This section has the following items:

- **Ping**
- **IPv6 Ping**
- **Remote IP Ping**
- **Cable Diagnostics**

PING

The ping and IPv6 ping allow you to issue ICMP PING packets to troubleshoot IP connectivity issues. The Managed Switch transmit ICMP packets, and the sequence number and roundtrip time are displayed upon reception of a reply.

Cable Diagnostics

The Cable Diagnostics performing tests on copper cables. These functions have the ability to identify the cable length and operating conditions, and to isolate a variety of common faults that can occur on the Cat5 twisted-pair cabling. There might be two statuses as follow:

- If the link is established on the twisted-pair interface in 1000Base-T mode, the Cable Diagnostics can run without disruption of the link or of any data transfer.
- If the link is established in 100Base-TX or 10Base-T, the Cable Diagnostics cause the link to drop while the diagnostics are running.

After the diagnostics are finished, the link is reestablished. And the following functions are available.

- Coupling between cable pairs.
- Cable pair termination
- Cable Length

4.15.1 Ping

This page allows you to issue ICMP PING packets to troubleshoot IP connectivity issues.

After you press "**Start**", 5 ICMP packets are transmitted, and the sequence number and roundtrip time are displayed upon reception of a reply. The page refreshes automatically until responses to all packets are received, or until a timeout occurs. The ICMP Ping screen in Figure 4-15-1 appears.

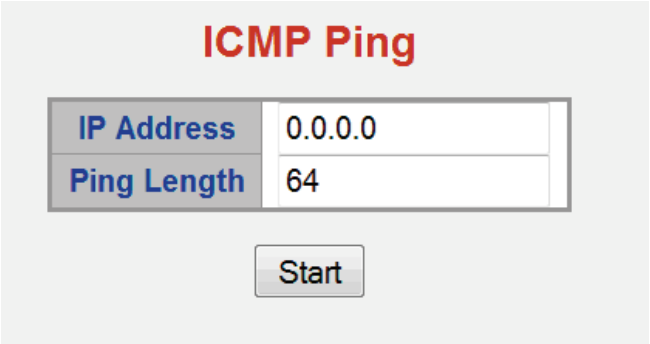


Figure 4-15-1: ICMP Ping Page Screenshot

The page includes the following fields:

Object	Description
• **IP Address**	The destination IP Address.
• **Ping Length**	The payload size of the ICMP packet. Values range from 2 bytes to 1452 bytes.
• **Ping Count**	The count of the ICMP packet. Values range from 1 time to 60 times.
• **Ping Interval**	The interval of the ICMP packet. Values range from 0 second to 30 seconds.

Note

Be sure the target IP Address is within the same network subnet of the switch, or you had setup the correct gateway IP address.

Button

[redacted]: Click to start transmitting ICMP packets.

[redacted]: Click to re-start diagnostics with PING.

4.15.2 IPv6 Ping

This page allows you to issue ICMPv6 PING packets to troubleshoot IPv6 connectivity issues.
After you press "**Start**", 5 ICMPv6 packets are transmitted, and the sequence number and roundtrip time are displayed upon reception of a reply. The page refreshes automatically until responses to all packets are received, or until a timeout occurs. The ICMPv6 Ping screen in Figure 4-15-2 appears.

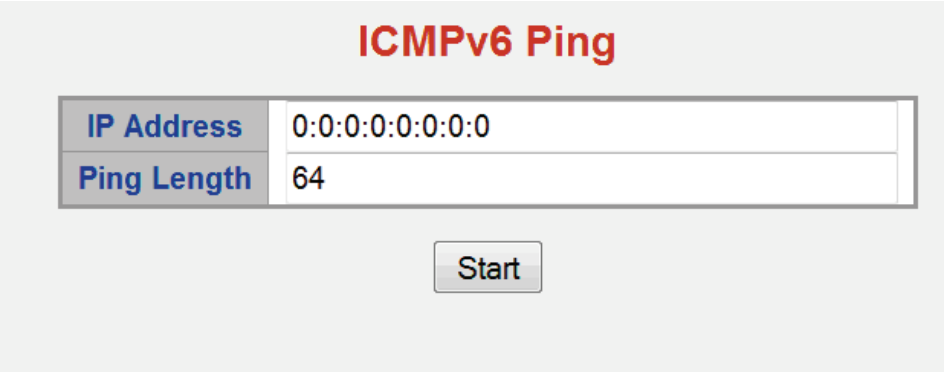


Figure 4-15-2: ICMPv6 Ping Page Screenshot

The page includes the following fields:

Object	Description
• **IP Address**	The destination IP Address.
• **Ping Length**	The payload size of the ICMP packet. Values range from 2 bytes to 1452 bytes.
• **Ping Count**	The count of the ICMP packet. Values range from 1 time to 60 times.
• **Ping Interval**	The interval of the ICMP packet. Values range from 0 second to 30 seconds.

Button

[redacted]: Click to start transmitting ICMP packets.

[redacted]: Click to re-start diagnostics with PING.

4.15.3 Remote IP Ping Test

This page allows you to issue ICMP PING packets to troubleshoot IP connectivity issues on special port.

After you press "**Test**", 5 ICMP packets are transmitted, and the sequence number and roundtrip time are displayed upon reception of a reply. The page refreshes automatically until responses to all packets are received, or until a timeout occurs. The ICMP Ping screen in Figure 4-15-3 appears.

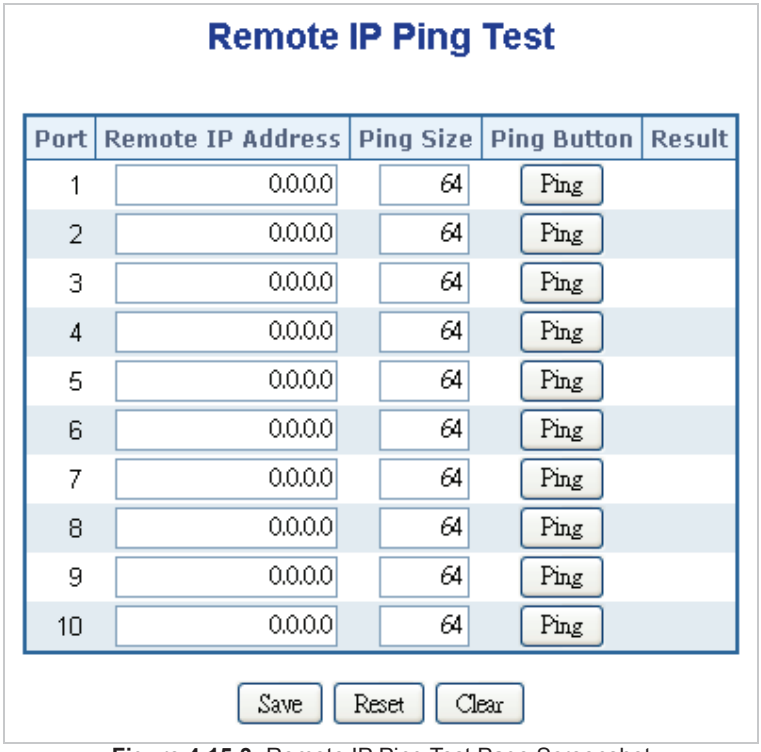


Figure 4-15-3: Remote IP Ping Test Page Screenshot

The page includes the following fields:

Object	Description
• **Port**	The logical port for the settings.
• **Remote IP Address**	The destination IP Address.
• **Ping Size**	The payload size of the ICMP packet. Values range from 8 bytes to 1400 bytes.
• **Result**	Display the ping result.

Buttons

[redacted]: Click to start ping process.

[redacted]: Click to save changes.

[redacted]: Click to undo any changes made locally and revert to previously saved values.

[redacted]: Clears the local counters. All counters (including global counters) are cleared upon reboot.

4.15.4 Cable Diagnostics

This page is used for running the Cable Diagnostics.

Press to run the diagnostics. This will take approximately 5 seconds. If all ports are selected, this can take approximately 15 seconds. When completed, the page refreshes automatically, and you can view the cable diagnostics results in the cable status table. Note that Cable Diagnostics is only accurate for cables of length 7 - 140 meters.

10 and 100 Mbps ports will be linked down while running cable diagnostic. Therefore, running cable diagnastic on a 10 or 100 Mbps management port will cause the switch to stop responding until VeriPHY is complete. The ports belong to the currently selected stack unit, as reflected by the page header. The VeriPHY Cable Diagnostics screen in Figure 4-15-4 appears.

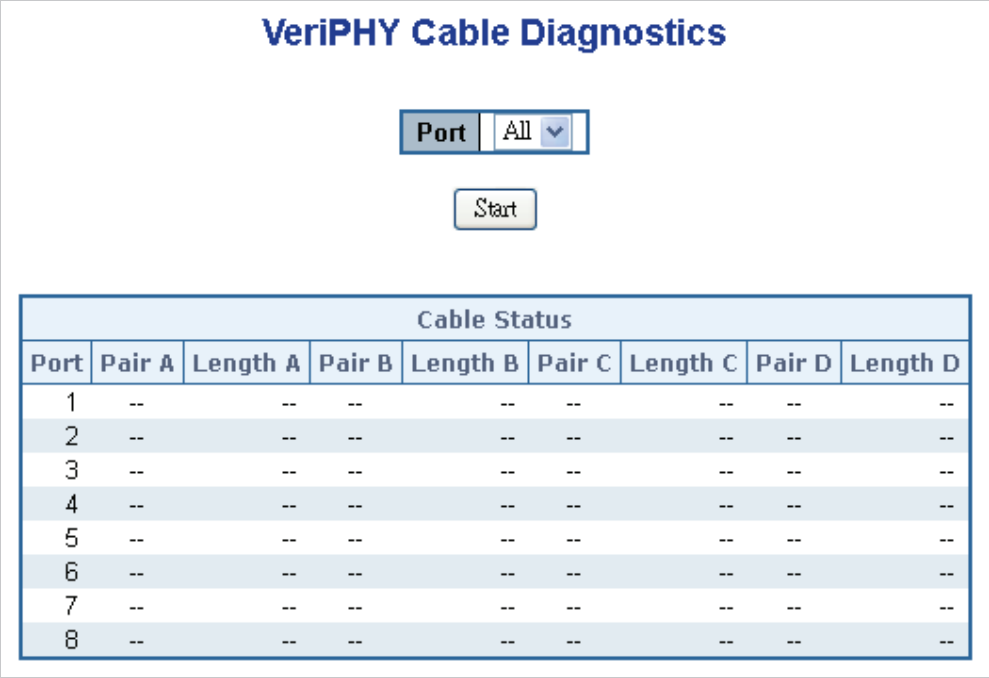


Figure 4-15-4: VeriPHY Cable Diagnostics Page Screenshot

The page includes the following fields:

Object	Description
• **Port**	The port where you are requesting Cable Diagnostics.
• **Cable Status**	■ **Port**: Port number. ■ **Pair**: The status of the cable pair. ■ **Length**: The length (in meters) of the cable pair.

Buttons

: Click to run the diagnostics.

4.16 Loop Protection

This page allows the user to inspect the current Loop Protection configurations, and possibly change them as well.

4.16.1 Configuration

This page allows the user to inspect the current Loop Protection configurations,

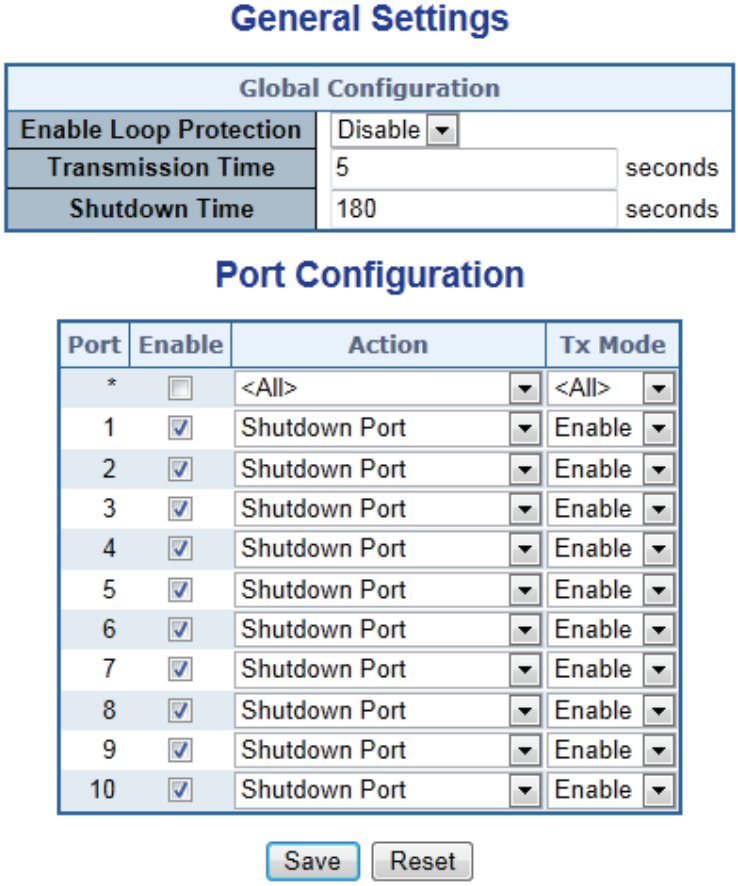


Figure 4-16-1: Loop Protection Configuration Page Screenshot

The page includes the following fields:

General Settings:

Object	Description
• **Enable Loop Protection**	Controls whether loop protections is enabled (as a whole).
• **Transmission Time**	The interval between each loop protection PDU sent on each port. valid values are 1 to 10 seconds.
• **Shutdown Time**	The period (in seconds) for which a port will be kept disabled in the event of a loop is detected (and the port action shuts down the port). Valid values are 0 to 604800 seconds (7 days). A value of zero will keep a port disabled (until next device restart).

Port Configuration:

Object	Description
• **Port**	The switch port number of the port.
• **Enable**	Controls whether loop protection is enabled on this switch port.
• **Action**	Configures the action performed when a loop is detected on a port. Valid values are **Shutdown Port**, **Shutdown Port and Log** or **Log Only**.

• **Tx Mode**	Controls whether or not the port is actively generating loop protection PDU's, or whether or not it is just passively looking for looped PDU's.

Buttons

[redacted]: Click to save changes.

[redacted]: Click to undo any changes made locally and revert to previously saved values.

4.16.2 Status

This page displays the loop protection port status the ports from the Industrial Managed Switch.

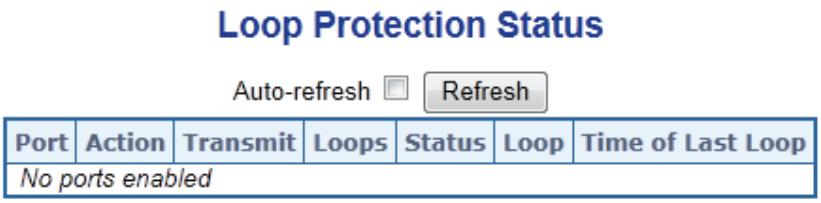


Figure 4-16-2: Loop Protection Status Page Screenshot

The page includes the following fields:

Object	Description
• **Port**	The switch port number of the logical port.
• **Action**	The currently configured port action.
• **Transmit**	The currently configured port transmit mode.
• **Loops**	The number of loops detected on this port.
• **Status**	The current loop protection status of the port.
• **Loop**	Whether a loop is currently detected on the port.
• **Time of Last Loop**	The time of the last loop event detected.

4.17 RMON

RMON is the most important expansion of the standard SNMP. RMON is a set of MIB definitions, used to define standard network monitor functions and interfaces, enabling the communication between SNMP management terminals and remote monitors. RMON provides a highly efficient method to monitor actions inside the subnets.

MID of RMON consists of 10 groups. The switch supports the most frequently used group 1, 2, 3 and 9:

- **Statistics:** Maintain basic usage and error statistics for each subnet monitored by the Agent.
- **History:** Record periodical statistic samples available from Statistics.
- **Alarm:** Allow management console users to set any count or integer for sample intervals and alert thresholds for RMON Agent records.
- **Event:** A list of all events generated by RMON Agent.

Alarm depends on the implementation of Event. Statistics and History display some current or history subnet statistics. Alarm and Event provide a method to monitor any integer data change in the network, and provide some alerts upon abnormal events (sending Trap or record in logs).

4.17.1 RMON Alarm Configuration

Configure RMON Alarm table on this page. The entry index key is **ID**.; screen in Figure 4-17-1 appears.

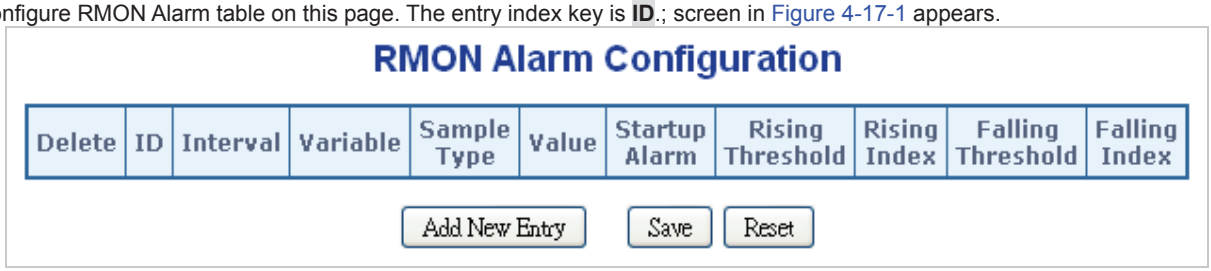


Figure 4-17-1: RMON Alarm configuration page screenshot

The page includes the following fields:

Object	Description
• **Delete**	Check to delete the entry. It will be deleted during the next save.
• **ID**	Indicates the index of the entry. The range is from 1 to 65535.
• **Interval**	Indicates the interval in seconds for sampling and comparing the rising and falling threshold. The range is from 1 to 2^31-1.
52. Variable	Indicates the particular variable to be sampled, the possible variables are: ■ **InOctets**: The total number of octets received on the interface, including framing characters. ■ **InUcastPkts**: The number of uni-cast packets delivered to a higher-layer protocol. ■ **InNUcastPkts**: The number of broad-cast and multi-cast packets delivered to a higher-layer protocol. ■ **InDiscards**: The number of inbound packets that are discarded even the packets are normal. ■ **InErrors**: The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol. ■ **InUnknownProtos**: the number of the inbound packets that were discarded because of the unknown or un-support protocol. ■ **OutOctets**: The number of octets transmitted out of the interface , including framing characters. ■ **OutUcastPkts**: The number of uni-cast packets that request to transmit. ■ **OutNUcastPkts**: The number of broad-cast and multi-cast packets that request to transmit. ■ **OutDiscards**: The number of outbound packets that are discarded event the packet is normal. ■ **OutErrors**: The The number of outbound packets that could not be transmitted because of errors.

	■ **OutQLen**: The length of the output packet queue (in packets).
53. Sample Type	The method of sampling the selected variable and calculating the value to be compared against the thresholds, possible sample types are: ■ **Absolute**: Get the sample directly. ■ **Delta**: Calculate the difference between samples (default).
54. Value	The value of the statistic during the last sampling period.
55. Startup Alarm	The method of sampling the selected variable and calculating the value to be compared against the thresholds, possible sample types are: ■ **Rising**Trigger alarm when the first value is larger than the rising threshold. ■ **Falling**Trigger alarm when the first value is less than the falling threshold. ■ **RisingOrFalling**Trigger alarm when the first value is larger than the rising threshold or less than the falling threshold (default).
• **Rising Threshold**	Rising threshold value (-2147483648-2147483647).
• **Rising Index**	Rising event index (1-65535).
• **Falling Threshold**	Falling threshold value (-2147483648-2147483647)
• **Falling Index**	Falling event index (1-65535).

Buttons

[redacted]: Click to add a new community entry.

[redacted]: Click to save changes.

[redacted]: Click to undo any changes made locally and revert to previously saved values.

4.17.2 RMON Alarm Details

This page provides details of a specific RMON statistics entry; screen in Figure 4-17-2 appears.

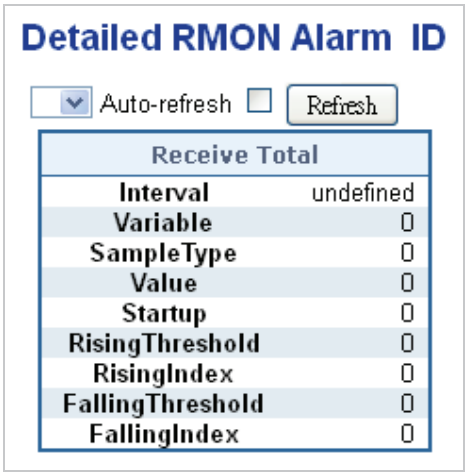


Figure 4-17-2: Detailed RMON Alarm ID page screenshot

The page includes the following fields:

Object	Description
• **Interval**	Indicates the interval in seconds for sampling and comparing the rising and falling threshold.
• **Variable**	Indicates the particular variable to be sampled
• **Sample Type**	The method of sampling the selected variable and calculating the value to be compared against the thresholds.

• **Value**	The value of the statistic during the last sampling period.
• **Startup**	The alarm that may be sent when this entry is first set to valid.
• **Rising Threshold**	Rising threshold value.
• **Rising Index**	Rising event index.
• **Falling Threshold**	Falling threshold value.
• **Falling Index**	Falling event index.

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

: Click to save changes.

 : Click to undo any changes made locally and revert to previously saved values.

4.17.5 RMON Event Details

This page provides an overview of RMON event entries; screen in Figure 4-17-5 appears.

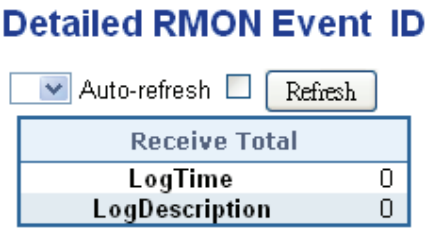


Figure 4-17-5: Detailed RMON Event ID page screenshot

The page includes the following fields:

Object	Description
• **Event Index**	Indicates the index of the event entry.
• **Log Index**	Indicates the index of the log entry.
• **LogTime**	Indicates Event log time
• **LogDescription**	Indicates the Event description.

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

4.17.6 RMON Event Status

This page provides an overview of RMON Event table entries.Each page shows up to 99 entries from the Event table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Event table. The first displayed will be the one with the lowest Event Index and Log Index found in the Event table table; screen in Figure 4-17-6 appears.

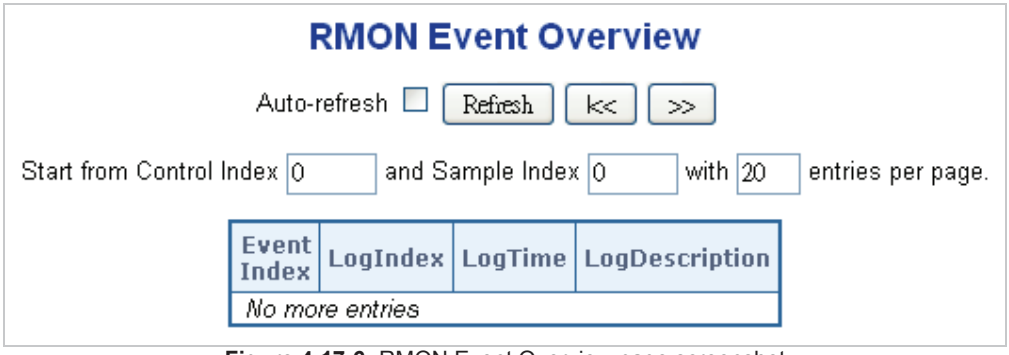


Figure 4-17-6: RMON Event Overview page screenshot

The page includes the following fields:

Object	Description
• **Event Index**	Indicates the index of the event entry.
• **Log Index**	Indicates the index of the log entry.
• **LogTime**	Indicates Event log time
• **LogDescription**	Indicates the Event description.

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

4.17.7 RMON History Configuration

Configure RMON History table on this page. The entry index key is **ID**; screen in Figure 4-17-7 appears.

Figure 4-17-7: RMON history configuration page screenshot

The page includes the following fields:

Object	Description
• **Delete**	Check to delete the entry. It will be deleted during the next save.
• **ID**	Indicates the index of the entry. The range is from 1 to 65535.
• **Data Source**	Indicates the port ID which wants to be monitored. If in stacking switch, the value must add 1000*(switch ID-1), for example, if the port is switch 3 port 5, the value is 2005.
• **Interval**	Indicates the interval in seconds for sampling the history statistics data. The range is from 1 to 3600, default value is 1800 seconds.
• **Buckets**	Indicates the maximum data entries associated this History control entry stored in RMON. The range is from 1 to 3600, default value is 50.
• **Buckets Granted**	The number of data will be saved in the RMON.

Buttons

[redacted]: Click to add a new community entry.

[redacted]: Click to save changes.

[redacted]: Click to undo any changes made locally and revert to previously saved values.

4.17.8 RMON History Details

This page provides details of RMON history entries; screen in Figure 4-17-8 appears.

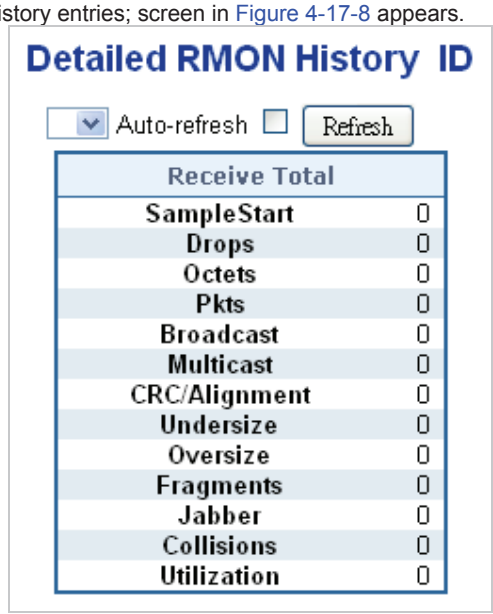


Figure 4-17-8: RMON history detailed page screenshot

The page includes the following fields:

Object	Description
• **History Index**	Indicates the index of History control entry.
• **Sample Index**	Indicates the index of the data entry associated with the control entry
• **Sample Start**	The total number of events in which packets were dropped by the probe due to lack of resources.
• **Drops**	The total number of events in which packets were dropped by the probe due to lack of resources.
• **Octets**	The total number of octets of data (including those in bad packets) received on the network.
• **Pkts**	The total number of packets (including bad packets, broadcast packets, and multicast packets) received.
• **Broadcast**	The total number of good packets received that were directed to the broadcast address.
• **Multicast**	The total number of good packets received that were directed to a multicast address.
• **CRC / Alignment**	The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets.
• **Undersize**	The total number of packets received that were less than 64 octets.
• **Oversize**	The total number of packets received that were longer than 1518 octets.
• **Fragments**	The number of frames which size is less than 64 octets received with invalid CRC.
• **Jabber**	The number of frames which size is larger than 64 octets received with invalid CRC.
• **Collisions**	The best estimate of the total number of collisions on this Ethernet segment.
• **Utilization**	The best estimate of the mean physical layer network utilization on this interface during this sampling interval, in hundredths of a percent.

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

4.17.10 RMON Statistics Configuration

Configure RMON Statistics table on this page. The entry index key is **ID**; screen in Figure 4-17-10 appears.

Figure 4-17-10: RMON Statistics Configuration Page screenshot

The page includes the following fields:

Object	Description
• **Delete**	Check to delete the entry. It will be deleted during the next save.
• **ID**	Indicates the index of the entry. The range is from 1 to 65535.
• **Data Source**	Indicates the port ID which wants to be monitored. If in stacking switch, the value must add 1000*(switch ID-1), for example, if the port is switch 3 port 5, the value is 2005

Buttons

[redacted]: Click to add a new community entry.

[redacted]: Click to save changes.

[redacted]: Click to undo any changes made locally and revert to previously saved values.

4.17.11 RMON Statistics Details

This page provides details of a specific RMON statistics entry; screen in Figure 4-17-11 appears.

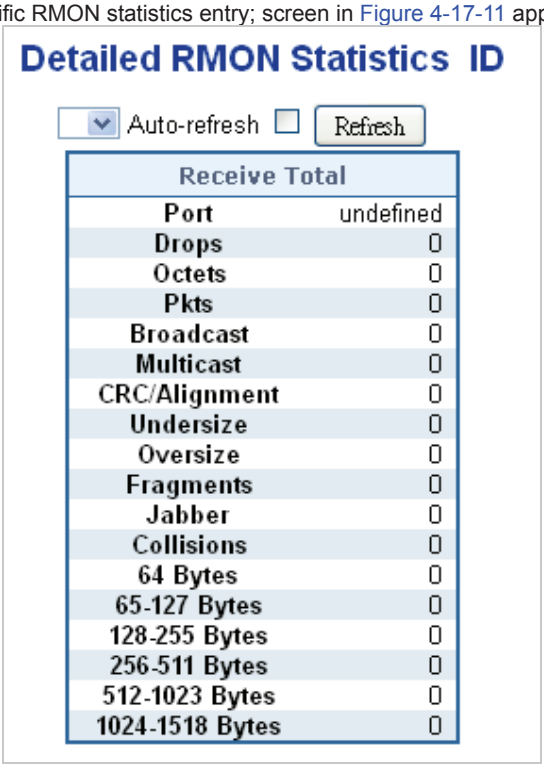


Figure 4-17-11: Loop protection configuration page screenshot

The page includes the following fields:

Object	Description
• **Data Source**	The port ID which wants to be monitored.
• **Drop**	The total number of events in which packets were dropped by the probe due to lack of resources.
• **Octets**	The total number of octets of data (including those in bad packets) received on the network.
• **Pkts**	The total number of packets (including bad packets, broadcast packets, and multicast packets) received.
• **Broad-cast**	The total number of good packets received that were directed to the broadcast address.
• **Multi-cast**	The total number of good packets received that were directed to a multicast address.
• **CRC / Alignment**	The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets.
• **Under-size**	The total number of packets received that were less than 64 octets.
• **Over-size**	The total number of packets received that were longer than 1518 octets.
• **Frag.**	The number of frames which size is less than 64 octets received with invalid CRC.
• **Jabb.**	The number of frames which size is larger than 64 octets received with invalid CRC.
• **Coll.**	The best estimate of the total number of collisions on this Ethernet segment.
• **64**	The total number of packets (including bad packets) received that were 64 octets in length.

• **65~127**	The total number of packets (including bad packets) received that were between 65 to 127 octets in length.
• **128~255**	The total number of packets (including bad packets) received that were between 128 to 255 octets in length.
• **256~511**	The total number of packets (including bad packets) received that were between 256 to 511 octets in length.
• **512~1023**	The total number of packets (including bad packets) received that were between 512 to 1023 octets in length.
• **1024~1588**	The total number of packets (including bad packets) received that were between 1024 to 1588 octets in length.

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

4.18 Precision Time Protocol

4.18.1 PTP Configuration

This section allows the user to configure and inspect the current Precision Time Protocol (PTP) clock settings.

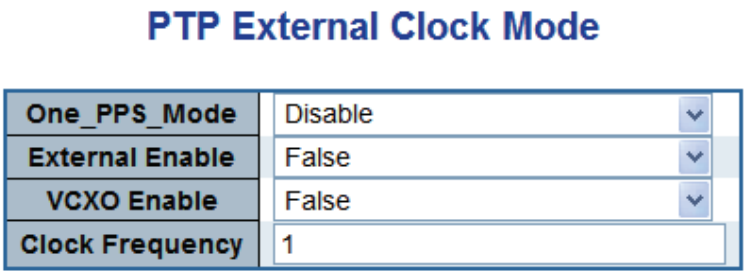


Figure 4-18-1: PTP Clock configuration page screenshot

The page includes the following fields:

Object	Description
• **One_PPS_Mode**	This Selection box will allow you to select the One_pps_mode configuration. The following values are possible: 1. Output : Enable the 1 pps clock output 2. Input : Enable the 1 pps clock input 3. Disable : Disable the 1 pps clock in/out-put
• **External Enable**	This Selection box will allow you to configure the External Clock output. The following values are possible: 1. True : Enable the external clock output 2. False : Disable the external clock output
• **VCXO_Enable**	This Selection box will allow you to configure the External VCXO rate adjustment. The following values are possible: 1. True : Enable the external VCXO rate adjustment 2. False : Disable the external VCXO rate adjustment
• **Clock Frequency**	This will allow setting the Clock Frequency. The possible range of values are 1 - 25000000 (1 - 25MHz)

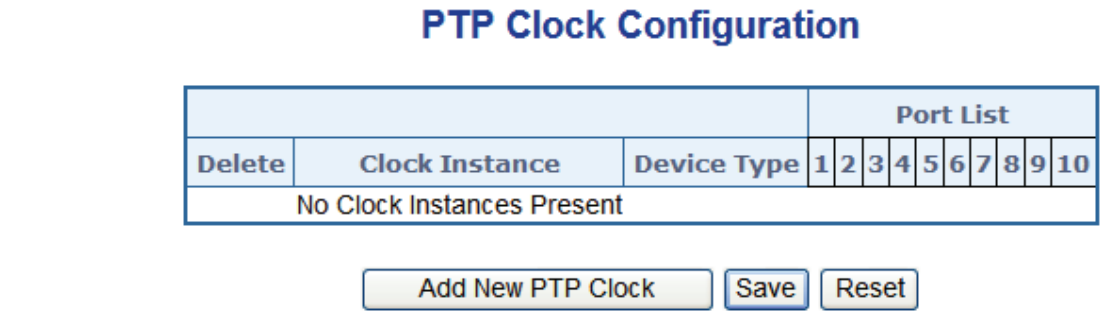


Figure 4-18-2: PTP Clock configuration page screenshot

The page includes the following fields:

Object	Description
• **Delete**	Check this box and click on 'Save' to delete the clock instance.
• **Clock Instance**	Indicates the Instance of a particular Clock Instance [0..3]. Click on the Clock Instance number to edit the Clock details.
• **Device Type**	Indicates the Type of the Clock Instance. There are five Device Types. 1. Ord-Bound - clock's Device Type is Ordinary-Boundary Clock. 2. P2p Transp - clock's Device Type is Peer to Peer Transparent Clock. 3. E2e Transp - clock's Device Type is End to End Transparent Clock. 4. Master Only - clock's Device Type is Master Only. 5. Slave Only - clock's Device Type is Slave Only.
• **Port List**	Set check mark for each port configured for this Clock Instance.

Buttons

Add New PTP Clock: Click to create a new clock instance.

[redacted]: Click to save the page immediately.

[redacted]: Click to reset the the page immediately.

4.18.2 PTP Status

This section allows the user to inspect the current Precision Time Protocol (PTP) clock settings.

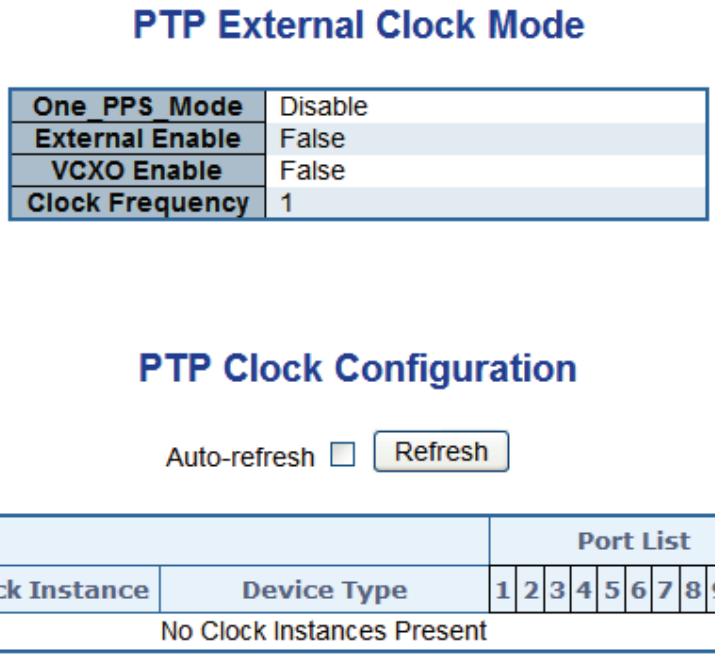


Figure 4-18-3: PTP Clock Status page screenshot

The page includes the following fields:

Object	Description
• **One_pps_mode**	Shows the current One_pps_mode configured. 1. Output : Enable the 1 pps clock output 2. Input : Enable the 1 pps clock input 3. Disable : Disable the 1 pps clock in/out-put
• **External Enable**	Shows the current External clock output configuration. 1. True : Enable the external clock output 2. False : Disable the external clock output
• **VCXO_Enable**	Shows the current VCXO rate adjustment configuration. 1. True : Enable the external VCXO rate adjustment 2. False : Disable the external VCXO rate adjustment
• **Clock Frequency**	Shows the current clock frequency used by the External Clock. The possible range of values are 1 - 25000000 (1 - 25MHz)
• **Clock Instance**	Indicates the Instance of a particular Clock Instance [0..3]. Click on the Clock Instance number to monitor the Clock details
• **Device Type**	Indicates the Type of the Clock Instance. There are five Device Types. 1. Ord-Bound - Clock's Device Type is Ordinary-Boundary Clock. 2. P2p Transp - Clock's Device Type is Peer to Peer Transparent Clock. 3. E2e Transp - Clock's Device Type is End to End Transparent Clock. 4. Master Only - Clock's Device Type is Master Only. 5. Slave Only - Clock's Device Type is Slave Only.
• **Port List**	Shows the ports configured for that Clock Instance.

Buttons

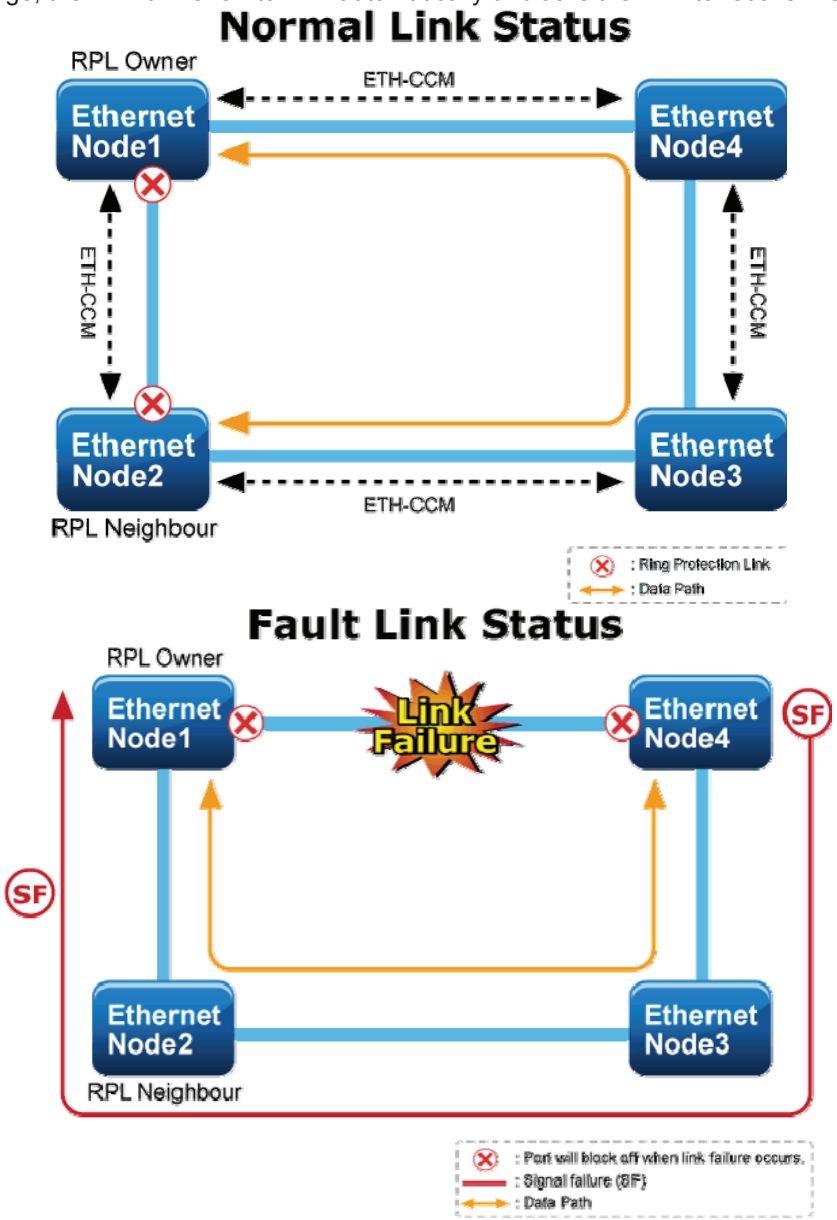
Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 6 seconds.

[redacted]: Click to refresh the page immediately.

4.19 Ring

ITU-T G.8032 **Ethernet Ring protection switching** (**ERPS**) is a link layer protocol applied on Ethernet loop protection to provide sub-50ms protection and recovery switching for Ethernet traffic in a ring topology.

ERPS provides a faster redundant recovery than Spanning Tree topology. The action is similar to STP or RSTP, but the algorithms between them are not the same. In the Ring topology, every switch should be enabled with Ring function and two ports should be assigned as the member ports in the ERPS. Only one switch in the Ring group would be set as the RPL owner switch that one port would be blocked, called **owner port**, and PRL neighbour switch has one port that one port would be blocked, called **neighbour port** that connect to owner port directly and this link is called the **Ring Protection Link** or **RPL**. Each switch will sends ETH-CCM message to check the link status in the ring group. When the failure of network connection occurs, the nodes block the failed link and report the signal failure message, the RPL owner switch will automatically unblocks the PRL to recover from the failure.



4.19.1 MEP Configuration

The Maintenance Entity Point instances are configured here; screen in Figure 4-19-1 appears.

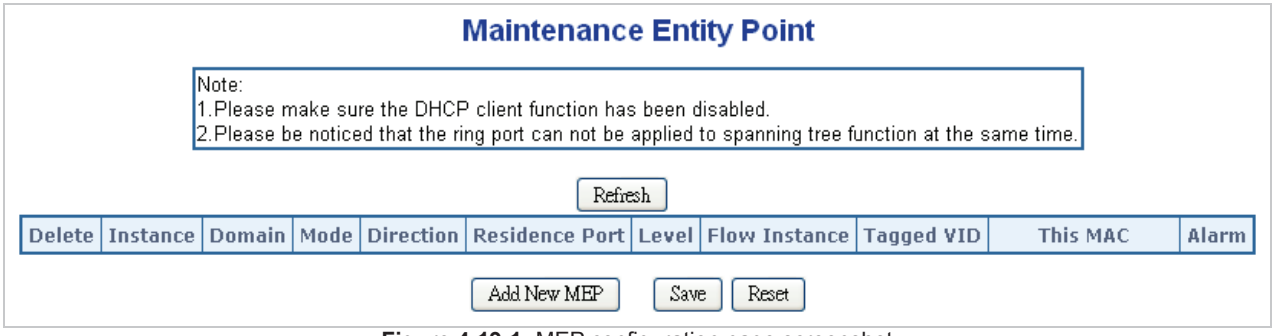


Figure 4-19-1: MEP configuration page screenshot

The page includes the following fields:

Object	Description
• **Delete**	This box is used to mark a MEP for deletion in next Save operation.
• **Instance**	The ID of the MEP. Click on the ID of a MEP to enter the configuration page.
• **Domain**	■ **Port**: This is a MEP in the Port Domain. 'Flow Instance' is a Port. ■ **Esp**: Future use ■ **Evc**: This is a MEP in the EVC Domain. 'Flow Instance' is a EVC ■ **Mpls**: Future use
• **Mode**	■ **MEP**: This is a Maintenance Entity End Point. ■ **MIP**: This is a Maintenance Entity Intermediate Point.
• **Direction**	■ **Ingress**: This is a Ingress (down) MEP - monitoring ingress traffic on 'Residence Port'. ■ **Egress**: This is a Egress (up) MEP - monitoring egress traffic on 'Residence Port'.
• **Residence Port**	The port where MEP is monitoring - see 'Direction'.
• **Level**	The MEG level of this MEP.
• **Flow Instance**	The MEP is related to this flow - See 'Domain'.
• **Tagged VID**	**Port MEP**: An outer C/S-tag (depending on VLAN Port Type) is added with this VID. Entering '0' means no TAG added.
• **This MAC**	The MAC of this MEP - can be used by other MEP when unicast is selected (Info only).
• **Alarm**	There is an active alarm on the MEP.

Buttons

 : Click to add a new MEP entry

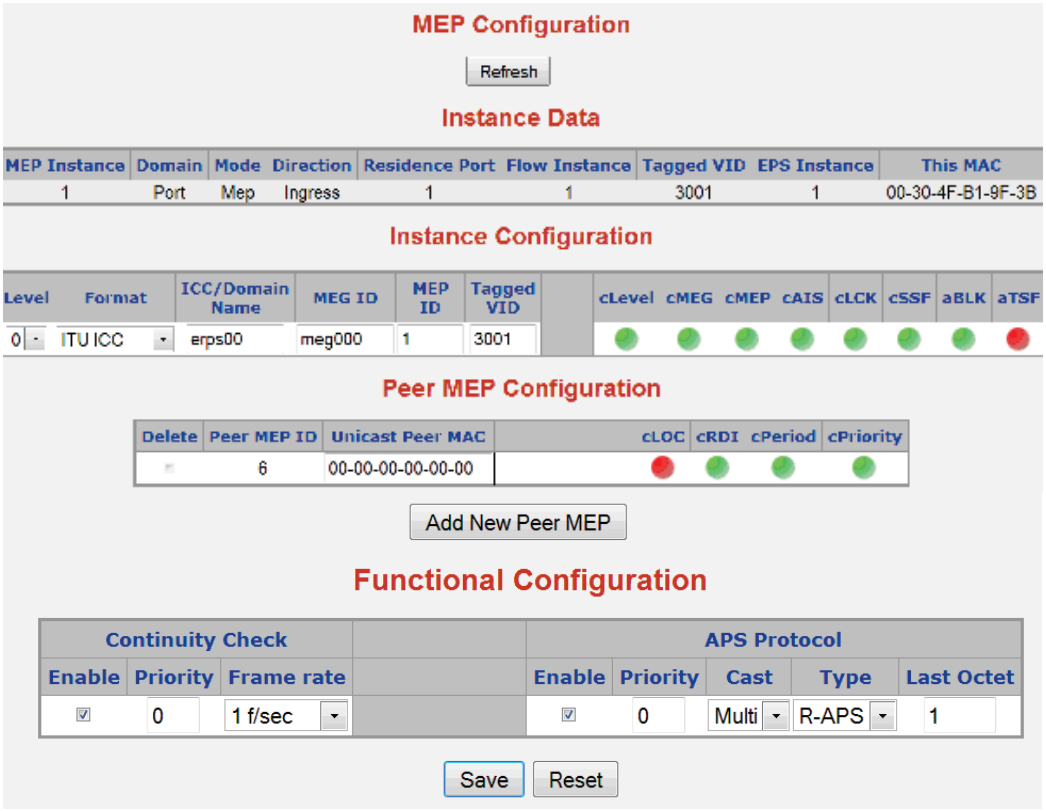


Figure 4-19-2: Detail MEP configuration page screenshot

The page includes the following fields:

Instance Data:

Object	Description
• **MEP Instance**	The ID of the MEP.
• **Domain**	See help on MEP create WEB.
• **Mode**	See help on MEP create WEB.
• **Direction**	See help on MEP create WEB.
• **Residence Port**	See help on MEP create WEB.
• **Flow Instance**	See help on MEP create WEB.
• **Tagged VID**	See help on MEP create WEB.
• **This MAC**	See help on MEP create WEB.

Instance Configuration:

Object	Description
• **Level**	See help on MEP create WEB.
• **Format**	This is the configuration of the two possible Maintenance Association Identifier formats. **ITU ICC**: This is defined by ITU. 'ICC' can be max. 6 char. 'MEG id' can be max. 7 char.

	IEEE String: This is defined by IEEE. 'Domain Name' can be max. 8 char. 'MEG id' can be max. 8 char.
• **ICC/Domain Name**	This is either ITU ICC (MEG ID value[1-6]) or IEEE Maintenance Domain Name - depending on 'Format'. See 'Format'.
• **MEG Id**	This is either ITU UMC (MEG ID value[7-13]) or IEEE Short MA Name - depending on 'Format'. See 'Format'. In case of ITU ICC format this can be max. 7 char. If only 6 char. is entered the MEG ID value[13] will become NULL.
• **MEP Id**	This value will become the transmitted two byte CCM MEP ID.
• **cLevel**	Fault Cause indicating that a CCM is received with a lower level than the configured for this MEP.
• **cMEG**	Fault Cause indicating that a CCM is received with a MEG ID different from configured for this MEP.
• **cMEP**	Fault Cause indicating that a CCM is received with a MEP ID different from all 'Peer MEP ID' configured for this MEP.
• **cAIS**	Fault Cause indicating that AIS PDU is received.
• **cLCK**	Fault Cause indicating that LCK PDU is received.
• **cSSF**	Fault Cause indicating that server layer is indicating Signal Fail.
• **aBLK**	The consequent action of blocking service frames in this flow is active.
• **aTSF**	The consequent action of indicating Trail Signal Fail to-wards protection is active.
• **Delete**	This box is used to mark a Peer MEP for deletion in next Save operation.
• **Peer MEP ID**	This value will become an expected MEP ID in a received CCM - see 'cMEP'.
• **Unicast Peer MAC**	This MAC will be used when unicast is selected with this peer MEP. Also this MAC is used to create HW checking of receiving CCM PDU (LOC detection) from this MEP.
• **cLOC**	Fault Cause indicating that no CCM has been received (in 3,5 periods) - from this peer MEP.
• **cRDI**	Fault Cause indicating that a CCM is received with Remote Defect Indication - from this peer MEP.
• **cPeriod**	Fault Cause indicating that a CCM is received with a period different what is configured for this MEP - from this peer MEP.
• **cPriority**	Fault Cause indicating that a CCM is received with a priority different what is configured for this MEP - from this peer MEP.

Buttons

[redacted]: Click to add a new peer MEP.

Functional Configuration
Instance Data:

Object	Description
• **Enable**	Continuity Check based on transmitting/receiving CCM PDU can be enabled/disabled. The CCM PDU is always transmitted as Multi-cast Class 1.
• **Priority**	The priority to be inserted as PCP bits in TAG (if any). In case of enable of Continuity Check and Loss Measurement both implemented on SW based CCM, 'Priority' has to be the same.
• **Frame rate**	Selecting the frame rate of CCM PDU. This is the inverse of transmission period as described in Y.1731. This value has the following uses: * The transmission rate of the CCM PDU. * Fault Cause cLOC is declared if no CCM PDU has been received within 3.5

	periods - see 'cLOC'. * Fault Cause cPeriod is declared if a CCM PDU has been received with different period - see 'cPeriod'. Selecting 300f/sec or 100f/sec will configure HW based CCM (if possible). Selecting other frame rates will configure SW based CCM. In case of enable of Continuity Check and Loss Measurement both implemented on SW based CCM, 'Frame Rate' has to be the same.

APS Protocol:

Object	Description
• **Enable**	Automatic Protection Switching protocol information transportation based on transmitting/receiving R-APS/L-APS PDU can be enabled/disabled. Must be enabled to support ERPS/ELPS implementing APS. This is only valid with one Peer MEP configured.
• **Priority**	The priority to be inserted as PCP bits in TAG (if any).
• **Cast**	Selection of APS PDU transmitted unicast or multi-cast. The unicast MAC will be taken from the 'Unicast Peer MAC' configuration. Unicast is only valid for L-APS - see 'Type'. The R-APS PDU is always transmitted with multi-cast MAC described in G.8032.
• **Type**	**R-APS**: APS PDU is transmitted as R-APS - this is for ERPS. **L-APS**: APS PDU is transmitted as L-APS - this is for ELPS.
• **Last Octet**	This is the last octet of the transmitted and expected RAPS multi-cast MAC. In G.8031 (03/2010) a RAPS multi-cast MAC is defined as 01-19-A7-00-00-XX. In current standard the value for this last octet is '01' and the usage of other values is for further study.

Buttons

[redacted]: Click to go to Fault Management page.

[redacted]: Click to go to Performance Monitor page.

• **Delete**	This box is used to mark an ERPS for deletion in next Save operation.
• **Port 0**	This will create a Port 0 of the switch in the ring.
• **Port 1**	This will create "Port 1" of the switch in the Ring. As interconnected sub-ring will have only one ring port, "Port 1" is configured as "0" for interconnected sub-ring. "0" in this field indicates that no "Port 1" is associated with this instance
• **Port 0 SF MEP**	The Port 0 Signal Fail reporting MEP.
• **Port 1 SF MEP**	The Port 1 Signal Fail reporting MEP. As only one SF MEP is associated with interconnected sub-ring without virtual channel, it is configured as "0" for such ring instances. "0" in this field indicates that no Port 1 SF MEP is associated with this instance.
• **Port 0 APS MEP**	The Port 0 APS PDU handling MEP.
• **Port 1 APS MEP**	The Port 1 APS PDU handling MEP. As only one APS MEP is associated with interconnected sub-ring without virtual channel, it is configured as "0" for such ring instances. "0" in this field indicates that no Port 1 APS MEP is associated with this instance.
• **Ring Type**	Type of Protecting ring. It can be either major ring or sub-ring.
• **Major Ring ID**	Major ring group ID for the interconnected sub-ring. It is used to send topology change updates on major ring. If ring is major, this value is same as the protection group ID of this ring.
• **Alarm**	There is an active alarm on the ERPS.

Buttons

 : Click to add a new Protection group entry.

4.19.4 Ethernet Ring Protocol Switch Configuration

This page allows the user to inspect and configure the current ERPS Instance; screen in Figure 4-19-4 appears.

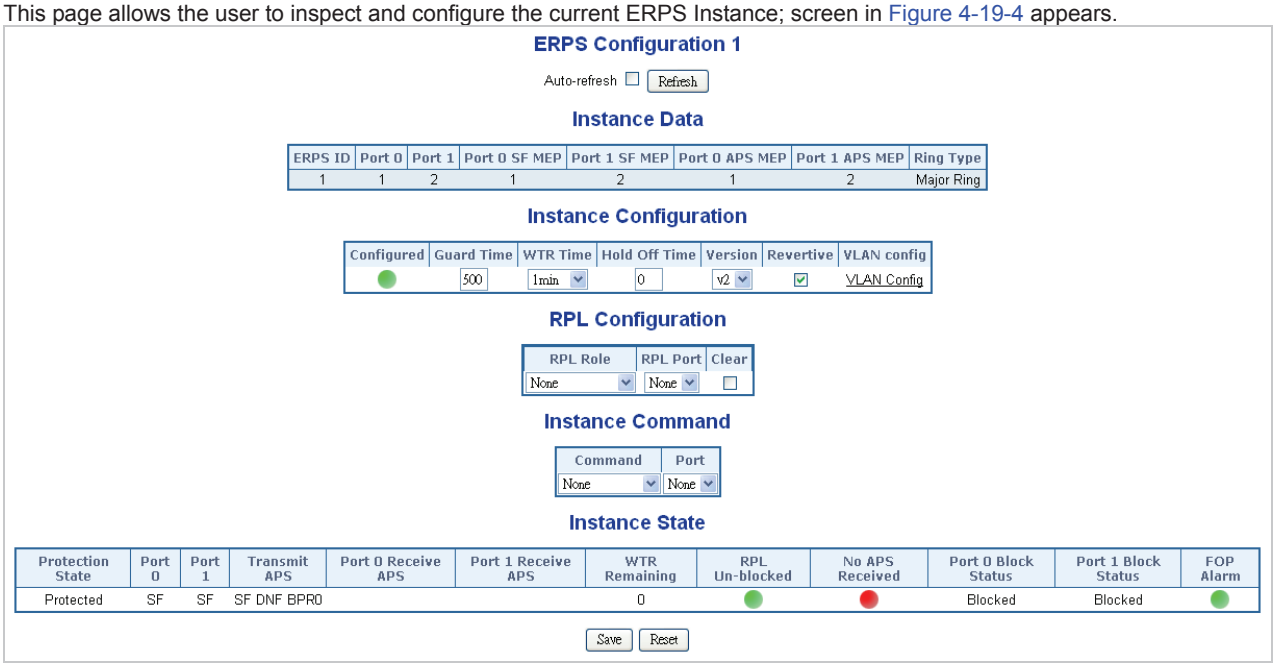


Figure 4-19-4: Ethernet Ring Protocol Switch Configuration page screenshot

The page includes the following fields:

Instance Data:

Object	Description
• **ERPS ID**	The ID of the Protection group.
• **Port 0**	See help on ERPS create WEB.
• **Port 1**	See help on ERPS create WEB.
• **Port 0 SF MEP**	See help on ERPS create WEB.
• **Port 1 SF MEP**	See help on ERPS create WEB.
• **Port 0 APS MEP**	See help on ERPS create WEB.
• **Port 1 APS MEP**	See help on ERPS create WEB.
• **Ring Type**	Type of Protecting ring. It can be either major ring or sub-ring.

Instance Configuration:

Object	Description
• **Configuration**	**Red**: This ERPS is only created and has not yet been configured - is not active. **Green**: This ERPS is configured - is active.
• **Guard Time**	Guard timeout value to be used to prevent ring nodes from receiving outdated R-APS messages. The period of the guard timer can be configured in 10 ms steps between 10 ms and 2 seconds, with a default value of 500 ms
• **WTR Time**	The Wait To Restore timing value to be used in revertive switching. The period of the WTR time can be configured by the operator in 1 minute steps between 5 and 12 minutes with a default value of 5 minutes.

• **Hold Off Time**	The timing value to be used to make persistent check on Signal Fail before switching. The range of the hold off timer is 0 to 10 seconds in steps of 100 ms
• **Version**	ERPS Protocol Version - v1 or v2
• **Revertive**	In Revertive mode, after the conditions causing a protection switch has cleared, the traffic channel is restored to the working transport entity, i.e., blocked on the RPL. In Non-Revertive mode, the traffic channel continues to use the RPL, if it is not failed, after a protection switch condition has cleared.
• **VLAN Config**	VLAN configuration of the Protection Group. Click on the "VLAN Config" link to confure VLANs for this protection group.

PRL Configuration:

Object	Description
• **PRL Role**	It can be either RPL owner or RPL Neighbour.
• **PRL Port**	This allows to select the east port or west port as the RPL block.
• **Clear**	If the owner has to be changed, then the clear check box allows to clear the RPL owner for that ERPS ring.

Instance Command:

Object	Description
• **Command**	Administrative command. A port can be administratively configured to be in either manual switch or forced switch state.
• **Port**	Port selection - Port0 or Port1 of the protection Group on which the command is applied.

Instance State:

Object	Description
• **Protection State**	ERPS state according to State Transition Tables in G.8032.
• **Port 0**	**OK**: State of East port is ok **SF**: State of East port is Signal Fail
• **Port 1**	**OK**: State of West port is ok **SF**: State of West port is Signal Fail
• **Transmit APS**	The transmitted APS according to State Transition Tables in G.8032.
• **Port 0 Receive APS**	The received APS on Port 0 according to State Transition Tables in G.8032.
• **Port 1 Receive APS**	The received APS on Port 1 according to State Transition Tables in G.8032.
• **WTR Remaining**	Remaining WTR timeout in milliseconds.
• **RPL Un-blocked**	APS is received on the working flow.
• **No APS Received**	RAPS PDU is not received from the other end.
• **Port 0 Block Status**	Block status for Port 0 (Both traffic and R-APS block status). R-APS channel is never blocked on sub-rings without virtual channel.
• **Port 1 Block Status**	Block status for Port 1 (Both traffic and R-APS block status). R-APS channel is never blocked on sub-rings without virtual channel.
• **FOP Alarm**	Failure of Protocol Defect(FOP) status. If FOP is detected, red LED glows; else green LED glows.

Buttons

 : Click to save changes.

Auto-refresh  : Check this box to refresh the page automatically. Automatic refresh occurs every 6 seconds.

4.19.5 Ring Wizard

This page allows the user to configure the ERPS by wizard; screen in Figure 4-19-4 appears.

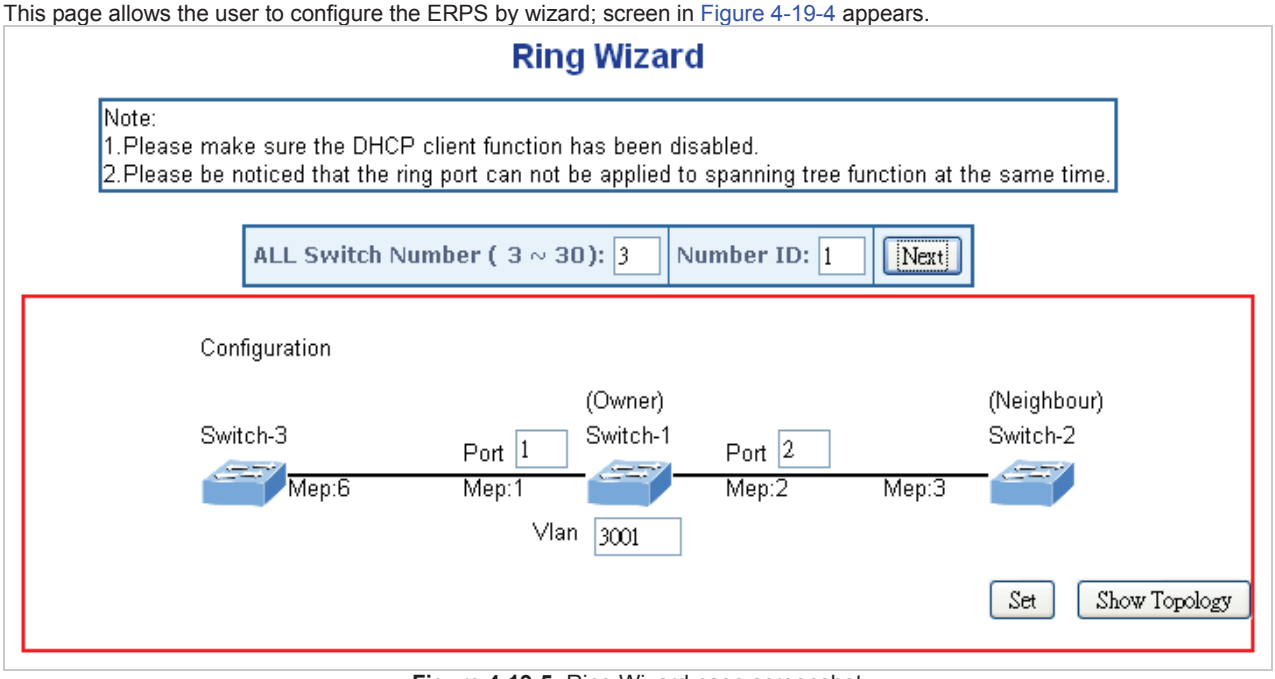


Figure 4-19-5: Ring Wizard page screenshot

The page includes the following fields:

Object	Description
• **All Switch Numbers**	Set all the switch numbers for the ring group. The default number is 3 and maximum number is 30.
• **Number ID**	The switch where you are requesting ERPS.
• **Port**	Configures the port number for the MEP.
• **VLAN**	Set the ERPS VLAN.

Buttons

[redacted]: Click to configure ERPS.

[redacted]: Click to save changes.

[redacted]: Click to show the ring topology.

4.19.6 Ring Wizard Example:

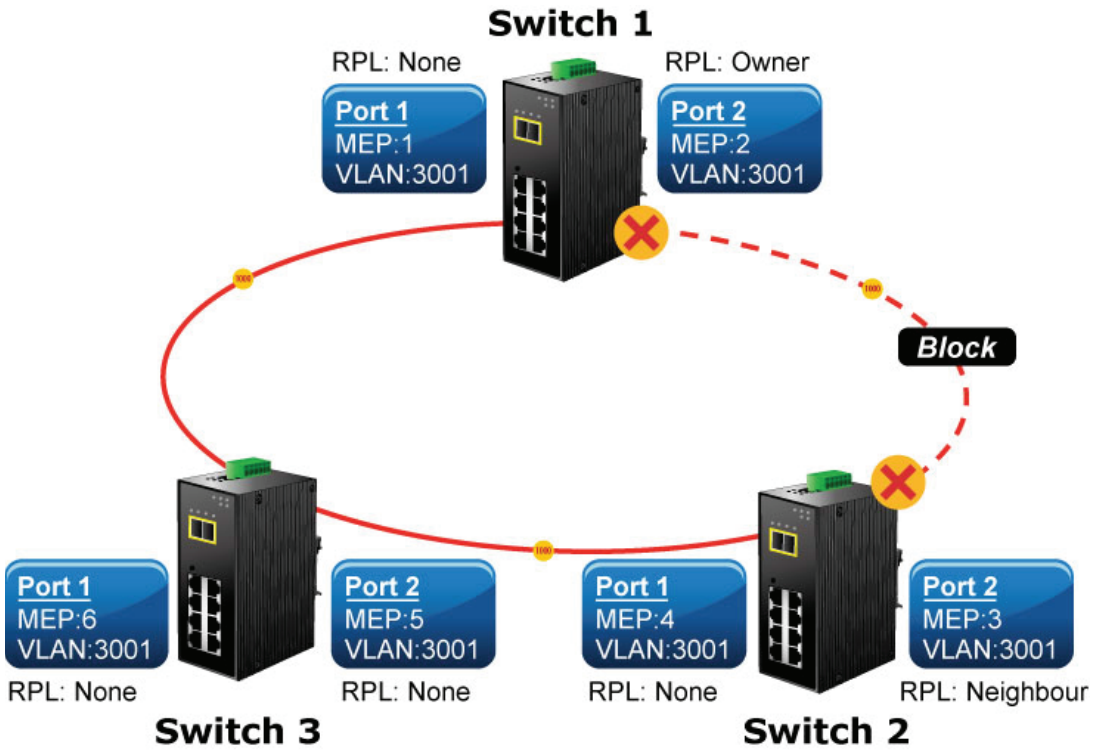


Figure 4-19-6: Ring Example Diagram

The above topology often occurs on using ERPS protocol. The multi switch constitutes a single ERPS ring; all of the switches only are configured as an ERPS in VLAN 3001, thereby constituting a single MRPP ring.

Switch ID	Port	MEP ID	RPL Type	VLAN Group
Switch 1	Port 1	1	None	3001
	Port 2	2	**Owner**	3001
Switch 2	Port 1	4	None	3001
	Port 2	3	**Neighbour**	3001
Switch 3	Port 1	6	None	3001
	Port 2	5	None	3001

Table 4-2: ERPS Configuration Table

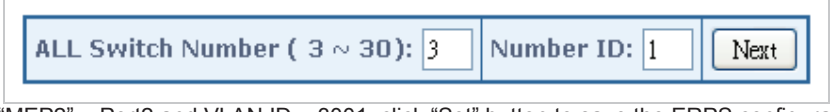
The scenario described as follows:

1. Disable DHCP client and set proper static IP for Switch 1, 2 & 3. In this example, switch 1 is 192.168.0.101; switch 2 is 192.168.0.102 and switch 3 is 192.168.0.103.
2. On switch 1, 2 & 3, disable spanning tree protocol to avoid confliction with ERPS.

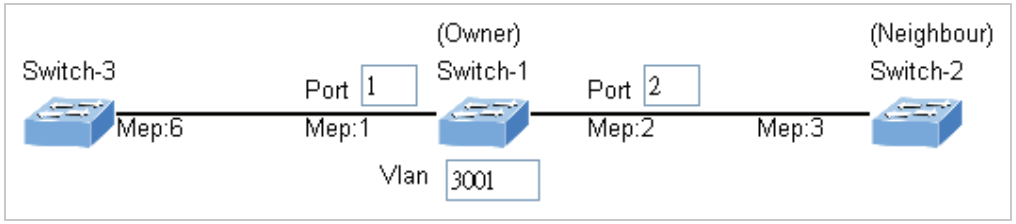
Setup steps

Set ERPS Configuration on Switch 1

Connect PC to switch 1 directly; don't connect to port 1 & 2
Logging on the Switch 1 and click "Ring > Ring Wizard"
Set "All Switch Number" = 3 and "Number ID" = 1; click "Next" button to set the ERPS configuration for Switch 1.



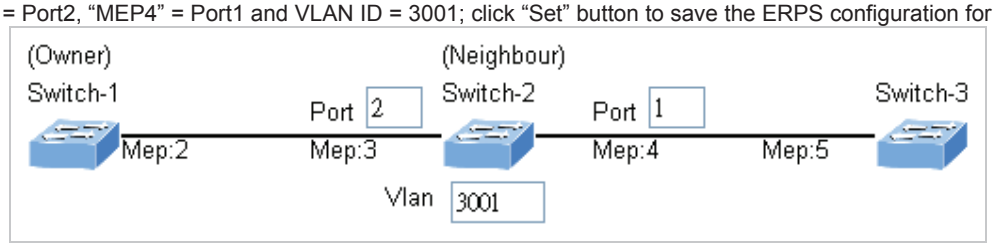
Set "MEP1" = Port1, "MEP2" = Port2 and VLAN ID = 3001; click "Set" button to save the ERPS configuration for Switch 1.



Set ERPS Configuration on Switch 2

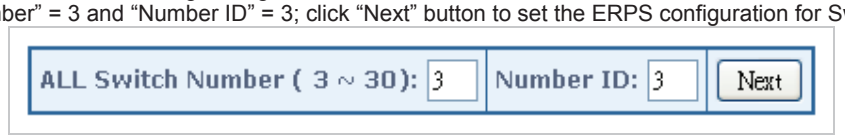
Connect PC to switch 2 directly; don't connect to port 1 & 2
Logging on the Switch 2 and click "Ring > Ring Wizard"
Set "All Switch Number" = 3 and "Number ID" = 2; click "Next" button to set the ERPS configuration for Switch 2.

Set "MEP3" = Port2, "MEP4" = Port1 and VLAN ID = 3001; click "Set" button to save the ERPS configuration for Switch 2.

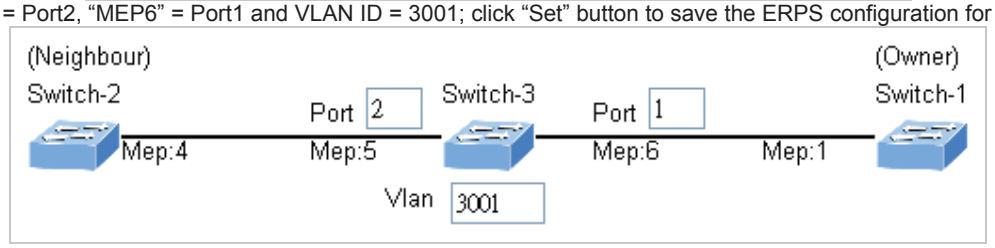


Set ERPS Configuration on Switch 3

Connect PC to switch 3 directly; don't connect to port 1 & 2
Logging on the Switch 3 and click "Ring > Ring Wizard"
Set "All Switch Number" = 3 and "Number ID" = 3; click "Next" button to set the ERPS configuration for Switch 3.



Set "MEP5" = Port2, "MEP6" = Port1 and VLAN ID = 3001; click "Set" button to save the ERPS configuration for Switch 3.



To avoid loop, please don't connect switch 1, 2 & 3 together in the ring topology before configuring the end of ERPS .

Follow the configuration or ERPS wizard to connect the Switch 1, 2 & 3 together to establish ERPS application:

MEP2 ⟷ MEP3 = Switch1 / Port2 ⟷ Switch2 / Port2

MEP4 ⟷ MEP5 = Switch2 / Port1 ⟷ Switch3 / Port2

MEP1 ⟷ MEP6 = Switch1 / Port1 ⟷ Switch3 / Port1

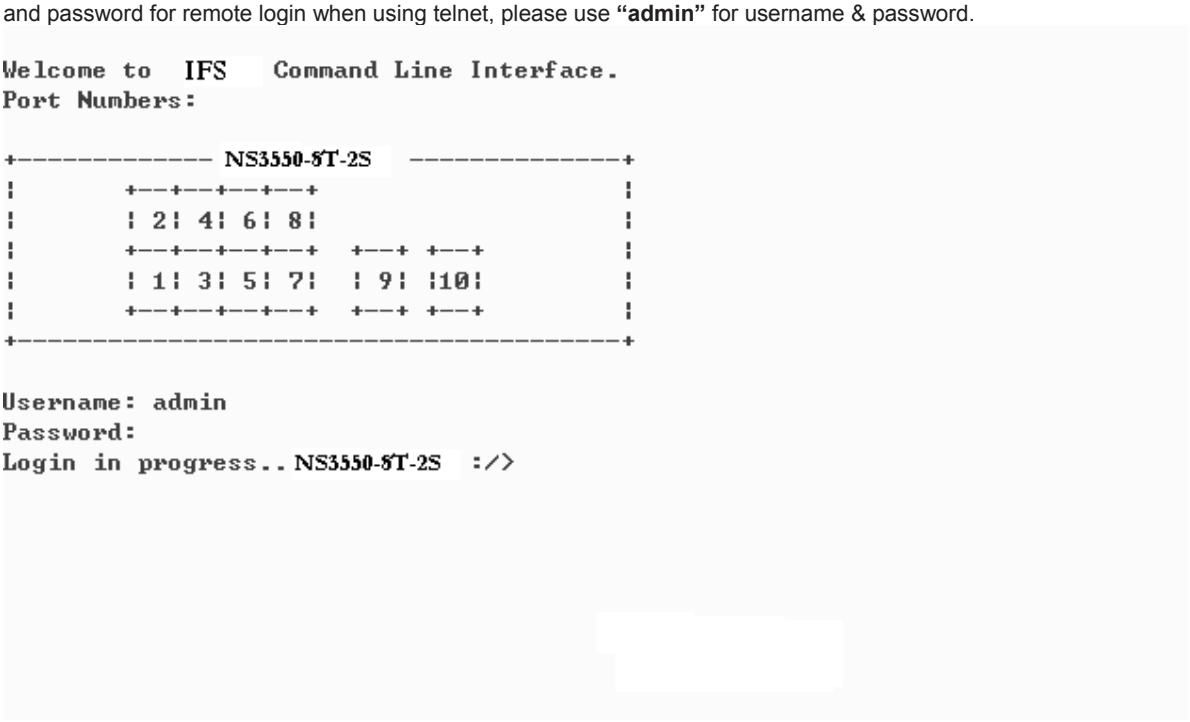
5. COMMAND LINE INTERFACE

5.1 Accessing the CLI

When accessing the management interface for the **Industrial Managed Switch** via a Telnet connection, the **Industrial Managed Switch** can be managed by entering command keywords and parameters at the prompt. Using the **Industrial Managed Switch**'s command-line interface (CLI) is very similar to entering commands on a UNIX system.
This chapter describes how to use the Command Line Interface (CLI).

5.2 Telnet Login

The **Industrial Managed Switch** supports telnet for remote management. The **Industrial Managed Switch** asks for user name and password for remote login when using telnet, please use **"admin"** for username & password.



6. COMMAND LINE MODE

The CLI groups all the commands in appropriate modes according to the nature of the command. A sample of the CLI command modes are described below. Each of the command modes supports specific software commands.

Command Groups:

System	System settings and reset options
IP	IP configuration and Ping
Port	Port management
MAC	MAC address table
VLAN	Virtual LAN
PVLAN	Private VLAN
Security	Security management
STP	Spanning Tree Protocol
Aggr	Link Aggregation
LACP	Link Aggregation Control Protocol
LLDP	Link Layer Discovery Protocol
LLDPMED	Link Layer Discovery Protocol Media
EEE	Energy Efficient Ethernet
Thermal	Thermal Protection
QoS	Quality of Service
Mirror	Port mirroring
Config	Load/Save of configuration via TFTP
Firmware	Download of firmware via TFTP
UPnP	Universal Plug and Play
MVR	Multicast VLAN Registration
Voice VLAN	Specific VLAN for voice traffic
Loop Protect	Loop Protection
IPMC	MLD/IGMP Snooping
VCL	VLAN Control List
SMTP	SMTP Control Configure

6.1 System Command

System Configuration

Description:
Show system configuration.

Syntax:
System Configuration [all] [<port_list>]

Parameters:
all : Show all switch configuration, default: Show system configuration
port : Show switch port configuration
<port_list>: Port list or 'all', default: All ports

Example:
To display system information:

```
NS3550-8T-2S:/>System configuration
System Contact    :
System Name       : NS3550-8T-2S
System Location :
Timezone Offset : 0
MAC Address       : 00-30-4F-00-a0-01
System Time       : 1970-01-01 Thu 02:50:01+00:00
System Uptime     : 00:10:55
Software Version: 1.5b131219
Software Date     : 2013-12-19T10:43:11+0800
Previous Restart: Cold
NS3550-8T-2S:/>
```

System Log Configuration

Description:
Show system log configuration.

Syntax:
System Log Configuration

Example:

To display system log information:

```
NS3550-8T-2S:/>System log configuration
System Log Configuration:
=========================

System Log Server Mode       : Disabled
System Log Server Address    :
System Log Level             : Info
NS3550-8T-2S:/>
```

System Version

Description:

Show system version information.

Syntax:

System Version

Example:

To display system version:

```
NS3550-8T-2S:/>System version
Version          : 1.5b131219
Build Date       : 2013-12-19T10:43:11+0800
NS3550-8T-2S:/>
```

System Log Server Mode

Description:

Show or set the system log server mode.

Syntax:

System Log Server Mode [enable|disable]

Parameters:

enable : Enable system log server mode
disable: Disable system log server mode
(default: Show system Log server mode)

Default Setting:

disable

Example:

To show the log server mode:

```
NS3550-8T-2S:/>System log server mode
System Log Server Mode       : Disabled
```

System Name

Description:

Set or show the system name.

Syntax:

System Name [<name>] [clear]

Parameters:

<name>: System name string. (1-255)
Use 'clear' or "" to clear the string
System name is a text string drawn from the alphabet (A-Za-z), digits (0-9), minus sign (-).
In CLI, no blank or space characters are permitted as part of a name.
The first character must be an alpha character, and the first or last character must not be a minus sign.
clear : Clear system name

Example:

To set device title:

```
NS3550-8T-2S:/>System name        : NS3550-8T-2S
```

System Contact

Description:
Set or show the system contact.

Syntax:
System Contact [<contact>] [clear]

Parameters:
<contact>: System contact string. (1-255)
Use 'clear' or "" to clear the string
In CLI, No blank or space characters are permitted as part of a contact.
clear : Clear system contact

Default Setting:
empty

Example:
To set device contact:

```
NS3550-8T-2S:/>System contact        :
```

System Log Server Address

Description:
Show or set the system log server address.

Syntax:
System Log Server Address [<ip_addr_string>]

Parameters:
<ip_addr_string>: IP host address (a.b.c.d) or a host name string

Default Setting:
empty

Example:
To set log server address:

```
NS3550-8T-2S:/> log server address 192.168.0.21
```

System Location

Description:
Set or show the system location.

Syntax:
System Location [<location>] [clear]

Parameters:
<location>: System location string. (1-255)
Use 'clear' or "" to clear the string
In CLI, no blank or space characters are permitted as part of a location.
clear : Clear system location

Default Setting:
empty

Example:
To set device location:

```
NS3550-8T-2S:/>System location 9F-LAB
```

System Log Level

Description:

Show or set the system log level.
It uses to determine what kind of message will send to syslog server.

Syntax:

System Log Level [info|warning|error]

Parameters:

info : Send informations, warnings and errors
warning : Send warnings and errors
error : Send errors

Default Setting:

info

Example:

To set log level:

```
NS3550-8T-2S:/> log level warning
```

System Timezone

Description:
Set or show the system timezone offset.

Syntax:
System Timezone [<offset>]

Parameters:
<offset>: Time zone offset in minutes (-720 to 720) relative to UTC

Default Setting:
0

Example:
To set timezone:

```
NS3550-8T-2S:/>system timezone 0
```

System Log Lookup

Description:
Show or clear the system log.

Syntax:
System Log Lookup [<log_id>] [all|info|warning|error] [clear]

Parameters:
<log_id>: System log ID or range (default: All entries)
all : Show all levels (default)
info : Show informations
warning : Show warnings
error : Show errors
clear : Clear log

Example:

To show system log:

```
NS3550-8T-2S:/>system log lookup
Number of entries:
Info     : 2
Warning: 0
Error    : 0
All      : 2

ID      Level     Time                            Message
----   ------   -------------------------   -------
    1   Info      -   Switch just made a cold boot.
    2   Info      1970-01-01T00:00:05+00:00   Link up on port 8
NS3550-8T-2S:/>
```

System Reboot

Description:

Reboot the system.

Syntax:

System Reboot

Example:

To reboot device without changing any of the settings:

```
NS3550-8T-2S:/>system reboot
```

System Restore Default

Description:

Restore factory default configuration.

Syntax:

System Restore Default [keep_ip]

Parameters:

keep_ip: Keep IP configuration, default: Restore full configuration

Example:

To restore default value but not reset IP address:

```
NS3550-8T-2S:/>system restore default keep_ip
```

System Load

Description:

Show current CPU load: 100ms, 1s and 10s running average (in percent, zero is idle).

Syntax:

System Load

Example:

To show current CPU load:

```
NS3550-8T-2S:/>system load
Load average(100ms, 1s, 10s):     1%,     1%,     1%
```

6.2 IP Command

IP Configuration

Description:

Show IP configuration.

Syntax:
IP Configuration

Example:
Show IP configuration:

```
NS3550-8T-2S:/>ip configuration

IP Configuration:
=================

DHCP Client          : Disabled
IP Address           : 192.168.0.101
IP Mask              : 255.255.255.0
IP Router            : 192.168.0.253
DNS Server           : 0.0.0.0
VLAN ID              : 1
DNS Proxy            : Disabled

IPv6 AUTOCONFIG mode     : Disabled
IPv6 Link-Local Address: fe80::6082:cdb9:19ab:c0e2
IPv6 Address             : ::192.168.0.100
IPv6 Prefix              : 96
IPv6 Router              : ::
```

IP DHCP

Description:
Set or show the DHCP client mode.

Syntax:
IP DHCP [enable|disable]

Parameters:
enable : Enable or renew DHCP client
disable: Disable DHCP client

Default Setting:
Disable

Example:
Disable DHCP sever:

```
NS3550-8T-2S:/>ip dhcp disable
```

IP Setup

Description:
Set or show the IP setup.

Syntax:
IP Setup [<ip_addr>] [<ip_mask>] [<ip_router>] [<vid>]

Parameters:

<ip_addr> : IP address (a.b.c.d), default: Show IP address
<ip_mask> : IP subnet mask (a.b.c.d), default: Show IP mask
<ip_router>: IP router (a.b.c.d), default: Show IP router
<vid> : VLAN ID (1-4095), default: Show VLAN ID

Default Setting:

IP Address : 192.168.0.100
IP Mask : 255.255.255.0
IP Router : 192.168.0.1
DNS Server : 0.0.0.0
VLAN ID : 1

Example:

Set IP address:

```
NS3550-8T-2S:/>ip setup 192.168.0.100 255.255.255.0
```

IP Ping

Description:

Ping IP address (ICMP echo).

Syntax:

IP Ping <ip_addr_string> [<ping_length>]

Parameters:

<ip_addr_string>: IP host address (a.b.c.d) or a host name string
<ping_length> : Ping data length (8-1400), excluding MAC, IP and ICMP headers

Example:

```
NS3550-8T-2S:/>ip ping 192.168.0.21
PING server 192.168.0.21
60 bytes from 192.168.0.21: icmp_seq=0, time=0ms
60 bytes from 192.168.0.21: icmp_seq=1, time=0ms
60 bytes from 192.168.0.21: icmp_seq=2, time=0ms
60 bytes from 192.168.0.21: icmp_seq=3, time=10ms
60 bytes from 192.168.0.21: icmp_seq=4, time=0ms
Sent 5 packets, received 5 OK, 0 bad
```

IP DNS

Description:

Set or show the DNS server address.

Syntax:

IP DNS [<ip_addr>]

Parameters:

<ip_addr>: IP address (a.b.c.d), default: Showdne IP address

Default Setting:

0.0.0.0

Example:

Set DNS IP address:

```
NS3550-8T-2S:/>ip dns 168.95.1.1
```

IP DNS Proxy

Description:

Set or show the IP DNS Proxy mode.

Syntax:
IP DNS_Proxy [enable|disable]

Parameters:
enable : Enable DNS Proxy
disable: Disable DNS Proxy

Default Setting:
disable

Example:
Enable DNS proxy function:

```
NS3550-8T-2S:/>ip dns_proxy enable
```

IPv6 AUTOCINFIG

Description:
Set or show the IPv6 AUTOCONFIG mode.

Syntax:
IP IPv6 AUTOCONFIG [enable|disable]

Parameters:
enable : Enable IPv6 AUTOCONFIG mode
disable: Disable IPv6 AUTOCONFIG mode

Default Setting:
disable

Example:
Enable IPv6 autoconfig function:

```
NS3550-8T-2S:/>ip ipv6 autoconfig enable
```

IPv6 Setup

Description:
Set or show the IPv6 setup.

Syntax:
IP IPv6 Setup [<ipv6_addr>] [<ipv6_prefix>] [<ipv6_router>]

Parameters:
<ipv6_addr> : IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separates each field (:). For example, four hexadecimal digits with a colon separates each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can only appear once. It also used a following legally IPv4 address. For example,'::192.1.2.34'.
<ipv6_prefix>: IPv6 subnet mask , default: Show IPv6 prefix
<ipv6_router>: IPv6 router , default: Show IPv6 router. IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separates each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can only appear once. It also used a following legally IPv4 address. For example,'::192.1.2.34'.

Default Setting:
IPv6 AUTOCONFIG mode : Disabled
IPv6 Link-Local Address: fe80::6082:cdb9:19ab:c0e2
IPv6 Address : ::192.168.0.100
IPv6 Prefix : 96
IPv6 Router : ::

Example:
Set IPv6 address:

```
NS3550-8T-2S:/>ip ipv6 setup 2001::0002 64 2100::0001
```

IPv6 Ping

Description:
Ping IPv6 address (ICMPv6 echo).

Syntax:
IP IPv6 Ping6 <ipv6_addr> [<ping_length>]

Parameters:
<ipv6_addr> : IPv6 host address.
IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separates each field (:). For example, four hexadecimal digits with a colon separates each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can only appear once. It also used a following legally IPv4 address. For example,'::192.1.2.34'.
<ping_length>: Ping data length (8-1400), excluding MAC, IP and ICMP headers

Example:

```
NS3550-8T-2S:/>ip ipv6 ping 2001::0002
PING6 server 2001::2
68 bytes from 2001::2: icmp_seq=0, time=0ms
68 bytes from 2001::2: icmp_seq=1, time=0ms
68 bytes from 2001::2: icmp_seq=2, time=0ms
68 bytes from 2001::2: icmp_seq=3, time=0ms
68 bytes from 2001::2: icmp_seq=4, time=0ms
Sent 5 packets, received 5 OK, 0 bad
```

IP NTP Configuration

Description:
Show NTP configuration.

Syntax:
IP NTP Configuration

Default Setting:

```
IP NTP Configuration:
=====================

NTP Mode : Disabled
Idx     Server IP host address (a.b.c.d) or a host name string
---     --------------------------------------------------------
1       pool.ntp.org
2       europe.pool.ntp.org
3       north-america.pool.ntp.org
4       asia.pool.ntp.org
5       oceania.pool.ntp.org
```

IP NTP Mode

Description:
Set or show the NTP mode.

Syntax:
IP NTP Mode [enable|disable]

Parameters:
enable : Enable NTP mode
disable : Disable NTP mode
(default: Show NTP mode)

Default Setting:
disable

Example:

Enable NTP mode:

```
NS3550-8T-2S:/>ip ntp mode enable
```

IP NTP Server Add

Description:

Add NTP server entry.

Syntax:

IP NTP Server Add <server_index> <ip_addr_string>

Parameters:

<server_index> : The server index (1-5)
<ip_addr_string>: IP host address (a.b.c.d) or a host name string

Example:

To add NTP server:

```
NS3550-8T-2S:/>ip ntp server add 1 60.249.136.151
```

IP NTP Server IPv6 Add

Description:

Add NTP server IPv6 entry.

Syntax:

IP NTP Server Ipv6 Add <server_index> <server_ipv6>

Parameters:

<server_index>: The server index (1-5)
<server_ipv6> : IPv6 server address. IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separates each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can only appear once. It also used a following legally IPv4 address. For example,'::192.1.2.34'.

Example:

To add IPv6 NTP server:

```
NS3550-8T-2S:/>ip ntp server ipv6 add 1 2001:7b8:3:2c::123
```

IP NTP Server Delete

Description:

Delete NTP server entry.

Syntax:

IP NTP Server Delete <server_index>

Parameters:

<server_index>: The server index (1-5)

Example:

To delete NTP server:

```
NS3550-8T-2S:/>ip ntp server delete 1
```

6.3 Port Management Command

Port Configuration

Description:
Show port configuration.

Syntax:
Port Configuration [<port_list>] [up|down]

Parameters:
<port_list>: Port list or 'all', default: All ports
up : Show ports, which are up
down : Show ports, which are down
(default: Show all ports)

Example:
Display port1~4 status

```
NS3550-8T-2S:/>port configuration 1-4

Port Configuration:
====================


Port   State       Mode      Flow Control   MaxFrame   Power       Excessive   Link
----   --------   ------   -------------   --------   --------   ----------   ----
1      Enabled    Auto      Disabled          9600      Disabled   Discard      Down
2      Enabled    Auto      Disabled          9600      Disabled   Discard      Down
3      Enabled    Auto      Disabled          9600      Disabled   Discard      Down
4      Enabled    Auto      Disabled          9600      Disabled   Discard      Down
```

Port Mode

Description:
Set or show the port speed and duplex mode.

Syntax:
Port Mode [<port_list>] [auto|10hdx|10fdx|100hdx|100fdx|1000fdx]

Parameters:
<port_list>: Port list or 'all', default: All ports
auto : Auto negotiation of speed and duplex
10hdx : 10 Mbps, half duplex
10fdx : 10 Mbps, full duplex
100hdx : 100 Mbps, half duplex
100fdx : 100 Mbps, full duplex
1000fdx : 1 Gbps, full duplex
(default: Show configured and current mode)

Default Setting:
Auto

Example:
Set 10Mbps (half duplex) speed for port1

```
NS3550-8T-2S:/>port mode 1 10hdx
```

Port Flow Control

Description:
Set or show the port flow control mode.

Syntax:
Port Flow Control [<port_list>] [enable|disable]

Parameters:
<port_list>: Port list or 'all', default: All ports
enable : Enable flow control
disable : Disable flow control
(default: Show flow control mode)

Default Setting:
Disable

Example:
Enable flow control function for port1

```
NS3550-8T-2S:/>port flow control 1 enable
```

Port State

Description:
Set or show the port administrative state.

Syntax:
Port State [<port_list>] [enable|disable]

Parameters:
<port_list>: Port list or 'all', default: All ports
enable : Enable port
disable : Disable port
(default: Show administrative mode)

Default Setting:
Enable

Example:
Disable port1

```
NS3550-8T-2S:/>port state 1 disable
```

Port Maximum Frame

Description:
Set or show the port maximum frame size.

Syntax:
Port MaxFrame [<port_list>] [<max_frame>]

Parameters:
<port_list>: Port list or 'all', default: All ports
<max_frame>: Port maximum frame size (1518-9600), default: Show maximum frame size

Default Setting:
9600

Example:
Set 2048 frame size for port1

```
NS3550-8T-2S:/>port maxframe 1 2048
```

Port Power

Description:
Set or show the port PHY power mode.

Syntax:
Port Power [<port_list>] [enable|disable|actiphy|dynamic]

Parameters:
<port_list>: Port list or 'all', default: All ports
enable : Enable all power control

disable: Disable all power control
actiphy: Enable ActiPHY power control
dynamic: Enable Dynamic power control

Default Setting:
disable

Example:
Disable port power function for port1-4

```
NS3550-8T-2S:/>port power 1-4 enable
```

Port Excessive

Description:
Set or show the port excessive collision mode.

Syntax:
Port Excessive [<port_list>] [discard|restart]

Parameters:
<port_list>: Port list or 'all', default: All ports
discard : Discard frame after 16 collisions
restart : Restart backoff algorithm after 16 collisions
(default: Show mode)

Default Setting:
Discard

Example:

```
NS3550-8T-2S:/>port excessive 1 restart
```

Port Statistics

Description:
Show port statistics.

Syntax:
Port Statistics [<port_list>] [<command>] [up|down]

Parameters:
<port_list>: Port list or 'all', default: All ports
<command> : The command parameter takes the following values:
clear : Clear port statistics
packets : Show packet statistics
bytes : Show byte statistics
errors : Show error statistics
discards : Show discard statistics
filtered : Show filtered statistics
0..7 : Show priority statistics
(default: Show all port statistics)
up : Show ports, which are up
down : Show ports, which are down
(default: Show all ports)

Port VeriPHY

Description:
Run cable diagnostics.

Syntax:
Port VeriPHY [<port_list>]

Parameters:

<port_list>: Port list or 'all', default: All ports

Port SFP

Description:
Show SFP port information.

Syntax:
Port SFP [<port_list>]

Parameters:
<port_list>: Port list or 'all', default: All ports

Example:
Show SFP information for port21-24

```
NS3550-8T-2S:/>port sfp

Port   Type              Speed        Wave Length(nm)   Distance(m)
----   --------------     --------      ---------------   -----------
9      1000Base-LX       1000-Base     1310               10000
10      1000Base-LX       1000-Base     1310               10000
```

6.4 MAC Address Table Command

MAC Configuration

Description:
Show MAC address table configuration.

Syntax:
MAC Configuration [<port_list>]

Parameters:
<port_list>: Port list or 'all', default: All ports

Example:
Show Mac address state

```
NS3550-8T-2S:/>mac configuration

MAC Configuration:
==================

MAC Address       : 00-30-4f-24-04-d1
MAC Age Time: 300

Port   Learning
----   --------
1       Auto
2       Auto
3       Auto
4       Auto
5       Auto
6       Auto
7       Auto
8       Auto
9       Auto
10      Auto
```

MAC Add

Description:
Add MAC address table entry.
Syntax:
MAC Add <mac_addr> <port_list> [<vid>]

Parameters:
<mac_addr> : MAC address (xx-xx-xx-xx-xx-xx)
<port_list>: Port list or 'all' or 'none'
<vid> : VLAN ID (1-4095), default: 1

Example:
Add Mac address 00-30-4F-01-01-02 in port1 and vid1

```
NS3550-8T-2S:/>mac add 00-30-4f-01-01-02 1 1
```

MAC Delete

Description:
Delete MAC address entry.

Syntax:
MAC Delete <mac_addr> [<vid>]

Parameters:
<mac_addr>: MAC address (xx-xx-xx-xx-xx-xx)
<vid> : VLAN ID (1-4095), default: 1

Example:

Delete Mac address 00-30-4F-01-01-02 in vid1

```
NS3550-8T-2S:/>mac delete 00-30-4f-01-01-02 1
```

MAC Lookup

Description:

Lookup MAC address entry.

Syntax:

MAC Lookup <mac_addr> [<vid>]

Parameters:

<mac_addr>: MAC address (xx-xx-xx-xx-xx-xx)
<vid> : VLAN ID (1-4095), default: 1

Example:

Lookup state of Mac address 00-30-4F-01-01-02

```
NS3550-8T-2S:/>mac lookup 00-30-4f-01-01-02
```

MAC Age Time

Description:

Set or show the MAC address age timer.

Syntax:

MAC Agetime [<age_time>]

Parameters:

<age_time>: MAC address age time (0,10-1000000) 0=disable,
(default: Show age time)

Default Setting:

300

Example:

Set agetime value in 30

```
NS3550-8T-2S:/>mac agetime 30
```

MAC Learning

Description:

Set or show the port learn mode.

Syntax:

MAC Learning [<port_list>] [auto|disable|secure]

Parameters:

<port_list>: Port list or 'all', default: All ports
auto : Automatic learning
disable: Disable learning
secure : Secure learning
(default: Show learn mode)

Default Setting:

Auto

Example:

Set secure learning mode in port1

```
NS3550-8T-2S:/>mac learning 1 secure
```

MAC Dump

Description:
Show sorted list of MAC address entries.

Syntax:
MAC Dump [<mac_max>] [<mac_addr>] [<vid>]

Parameters:
<mac_max> : Maximum number of MAC addresses 1-8192, default: Show all addresses
<mac_addr>: First MAC address (xx-xx-xx-xx-xx-xx), default: MAC address zero
<vid> : First VLAN ID (1-4095), default: 1

Example:
Show all of MAC table

```
NS3550-8T-2S:/>mac dump
Type      VID    MAC Address          Ports
------    ---    -----------------    -----
Static     1     00-30-00-33-22-55    1
Static     1     00-30-4f-24-04-d1    None,CPU
Static     1     33-33-ff-24-04-d1    None,CPU
Static     1     33-33-ff-a8-00-64    None,CPU
Dynamic    1     40-61-86-04-18-69    10
Static     1     ff-ff-ff-ff-ff-ff    1-24,CPU
```

MAC Statistics

Description:
Show MAC address table statistics.

Syntax:
MAC Statistics [<port_list>]

Parameters:
<port_list>: Port list or 'all',
(default: All ports)

Example:
Set all of MAC statistics

```
NS3550-8T-2S:/>mac statistics
Port   Dynamic Addresses
----   -----------------
1      0
2      0
3      0
4      0
5      0
6      0
7      0
8      0
9      0
10     0

Total Dynamic Addresses: 0
Total Static Addresses : 4
```

MAC Flush

Description:
Flush all learned entries.

Syntax:
MAC Flush

6.5 VLAN Configuration Command

VLAN Configuration

Description:
Show VLAN configuration.

Syntax:
VLAN Configuration [<port_list>]

Parameters:
<port_list>: Port list or 'all',
(default: All ports)

Example:
Show VLAN status of port1

```
NS3550-8T-2S:/>vlan configuration 1

VLAN Configuration:
====================


Mode : IEEE 802.1Q
Port   PVID   IngrFilter   FrameType     LinkType   Q-in-Q Mode   Eth type
----   ----   ----------   ----------   --------   -----------   --------
1      1      Disabled     All          UnTag      Disable       N/A

VID    VLAN Name                              Ports
----   --------------------------------   -----
1      default                            1-10

VID    VLAN Name                              Ports
----   --------------------------------   -----
VLAN forbidden table is empty
```

VLAV PVID

Description:
Set or show the port VLAN ID.
Syntax:
VLAN PVID [<port_list>] [<vid>|none]

Parameters:
<port_list>: Port list or 'all', default: All ports
<vid>|none : Port VLAN ID (1-4095) or 'none',
(default: Show port VLAN ID)

Default Setting:
1

Example:
Set PVID2 for port10

```
NS3550-8T-2S:/>vlan pvid 10 2
```

VLAN Frame Type

Description:
Set or show the port VLAN frame type.

Syntax:
VLAN FrameType [<port_list>] [all|tagged]

Parameters:
<port_list>: Port list or 'all', default: All ports

all : Allow tagged and untagged frames
tagged : Allow tagged frames only
(default: Show accepted frame types)

Default Setting:
All

Example:
Set port10 that allow tagged frames only

```
NS3550-8T-2S:/>vlan frametype 10 tagged
```

VLAN Ingress Filter

Description:
Set or show the port VLAN ingress filter.

Syntax:
VLAN IngressFilter [<port_list>] [enable|disable]

Parameters:
<port_list>: Port list or 'all', default: All ports
enable : Enable VLAN ingress filtering
disable : Disable VLAN ingress filtering
(default: Show VLAN ingress filtering)

Default Setting:
Disable

Example:
Enable VLAN ingress filtering for port10

```
NS3550-8T-2S:/>vlan ingressfilter 10 enable
```

VLAN Mode

Description:
Set or show the VLAN Mode.

Syntax:
VLAN Mode [portbased|dot1q]

Parameters:
portbased : Port-Based VLAN Mode
dot1q : 802.1Q VLAN Mode
(default: Show VLAN Mode)

Default Setting:
IEEE 802.1Q

Example:

Set VLAN mode in port base

```
NS3550-8T-2S:/>vlan mode portbased
```

VLAN Link Type

Description:

Set or show the port VLAN link type.

Syntax:

VLAN LinkType [<port_list>] [untagged|tagged]

Parameters:

<port_list>: Port list or 'all', default: All ports
untagged : VLAN Link Type Tagged
tagged : VLAN Link Type Untagged
(default: Show VLAN link type)

Default Setting:

Un-tagged

Example:

Enable tagged frame for port2

```
NS3550-8T-2S:/>vlan linktype 2 tagged
```

VLAN Q-in-Q Mode

Description:

Set or show the port Q-in-Q mode.

Syntax:

VLAN QinQ [<port_list>] [disable|man|customer]

Parameters:

<port_list>: Port list or 'all', default: All ports
disable : Disable Q-in-Q VLAN Mode
man : Q-in-Q MAN Port Mode
customer : Q-in-Q Customer Port Mode
(default: Show VLAN QinQ Mode)

Example:

Set port2 in man port

```
NS3550-8T-2S:/>vlan qinq 2 man
```

VLAN Ethernet Type

Description:

Set or show out layer VLAN tag ether type in Q-in-Q VLAN mode.

Syntax:

VLAN Ethtype [<port_list>] [man|dot1q]

Parameters:

<port_list>: Port list or 'all', default: All ports
man : Set out layer VLAN tag ether type : MAN
dot1q : Set out layer VLAN tag ether type : 802.1Q
(default: Show VLAN out layer VLAN tag ether type)

Default Setting:

N/A

Example:

Set out layer VLAN tag Ethernet type for port 10 in man Ethernet type

```
NS3550-8T-2S:/>vlan ethtype 10 man
```

VLAN Add

Description:

Add or modify VLAN entry.

Syntax:
VLAN Add <vid>|<name> [<port_list>]

Parameters:
<vid>|<name>: VLAN ID (1-4095) or VLAN Name
<port_list> : Port list or 'all', default: All ports

Default Setting:
1

Example:
Add port1 to port4 in VLAN10

```
NS3550-8T-2S:/>vlan add 10 1-4
```

VLAN Forbidden Add

Description:
Add or modify VLAN entry in forbidden table.

Syntax:
VLAN Forbidden Add <vid>|<name> [<port_list>]

Parameters:
<vid>|<name>: VLAN ID (1-4095) or VLAN Name
<port_list> : Port list or 'all', default: All ports

Example:
Frobidden add port1 to port4 in VLAN10

```
NS3550-8T-2S:/>vlan forbidden add 10 1-4
```

VLAN Delete

Description:
Delete VLAN entry.

Syntax:
VLAN Delete <vid>|<name>
Parameters:
<vid>|<name>: VLAN ID (1-4095) or VLAN Name

Example:
Delete VLAN10

```
NS3550-8T-2S:/>vlan delete 10
```

VLAN Forbidden Delete

Description:
Delete VLAN entry.

Syntax:
LAN Forbidden Delete <vid>|<name>

Parameters:
<vid>|<name>: VLAN ID (1-4095) or VLAN Name

Example:
Forbidden delete VLAN10

```
NS3550-8T-2S:/>vlan forbidden delete 10
```

VLAN Forbidden Lookup

Description:
Lookup VLAN Forbidden port entry.

Syntax:
VLAN Forbidden Lookup [<vid>] [(name <name>)]

Parameters:
<vid> : VLAN ID (1-4095), default: Show all VLANs
name : VLAN name string
<name>: VLAN name - Maximum of 32 characters. VLAN Name can only contain alphabets or numbers. VLAN name should contain atleast one alphabet.

VLAN Lookup

Description:
Lookup VLAN entry.

Syntax:
VLAN Lookup [<vid>] [(name <name>)] [combined|static|nas|mvr|voice_vlan|all]

Parameters:
<vid> : VLAN ID (1-4095), default: Show all VLANs
name : VLAN name string
<name>: VLAN name - Maximum of 32 characters. VLAN Name can only contain alphabets or numbers. VLAN name should contain atleast one alphabet.
combined : Shows All the Combined VLAN database
static : Shows the VLAN entries configured by the administrator
nas : Shows the VLANs configured by NAS
mvr : Shows the VLANs configured by MVR
voice_vlan : Shows the VLANs configured by Voice VLAN
all : Shows all VLANs configuration
(default: combined VLAN Users configuration)

Example:
Show VLAN status

```
NS3550-8T-2S:/>vlan lookup

VID    VLAN Name                        Ports
----   --------------------------------  -----
1      default                          1-10
```

VLAN Name Add

Description:
Add VLAN Name to a VLAN ID Mapping.

Syntax:
VLAN Name Add <name> <vid>

Parameters:

<name>: VLAN name - Maximum of 32 characters. VLAN Name can only contain alphabets or numbers. VLAN name should contain atleast one alphabet.
<vid> : VLAN ID (1-4095)

Example:

Add VLAN name for VLAN 1

```
NS3550-8T-2S:/>vlan name add test 1
```

VLAN Name Delete

Description:

Delete VLAN Name to VLAN ID Mapping.

Syntax:

VLAN Name Delete <name>

Parameters:

<name>: VLAN name - Maximum of 32 characters. VLAN Name can only contain alphabets or numbers. VLAN name should contain atleast one alphabet.

Example:

Delete VLAN name

```
NS3550-8T-2S:/>vlan name delete test
```

VLAN Name Lookup

Description:

Show VLAN Name table.

Syntax:

VLAN Name Lookup [<name>]

Parameters:

<name>: VLAN name - Maximum of 32 characters. VLAN Name can only contain alphabets or numbers. VLAN name should contain atleast one alphabet.

Example:

To show VLAN Name table

```
NS3550-8T-2S:/>vlan name lookup
VLAN NAME                              vid
-------------------------------   ---
test                                   1
```

VLAN Status

Description:

VLAN Port Configuration Status.

Syntax:

VLAN Status [<port_list>] [combined|static|nas|mvr|voice_vlan|mstp|all|conflicts]

Parameters:

<port_list>: Port list or 'all', default: All ports
combined : combined VLAN Users configuration
static : static port configuration
nas : NAS port configuration
mvr : MVR port configuration
voice_vlan : Voice VLAN port configuration
mstp : MSTP port configuration
all : All VLAN Users configuration
(default: combined VLAN Users configuration)

Default Setting:

Promiscous

Example:

Show VLAN configuration of port10

```
NS3550-8T-2S:/>status 1

Port   VLAN User      PortType          PVID   Frame Type   Ing Filter     Tx Tag          UVID
Conflicts
----   ----------   -------------   ----   ----------   ----------   -----   ---------
1      Static         Unaware          1      All            Disabled      Untag This    1
       NAS
No
       MVR
No
       Voice VLAN
No
       MSTP
No
       Combined       Unaware          1      All            Disabled      Untag This    1
No
```

6.6 Private VLAN Configuration Command

PVLAN Configuration

Description:

Show Private VLAN configuration.

Syntax:

PVLAN Configuration [<port_list>]

Parameters:

<port_list>: Port list or 'all', default: All ports

Example:

Show private VLAN configuration

```
NS3550-8T-2S:/> pvlan configuration

Private VLAN Configuration:
===========================


Port    Isolation
----    ---------
1       Disabled
2       Disabled
3       Disabled
4       Disabled
5       Disabled
6       Disabled
7       Disabled
8       Disabled
9       Disabled
10      Disabled

PVLAN ID    Ports
--------    -----
1               1-10
```

PVLAN Add

Description:
Add or modify Private VLAN entry.

Syntax:
PVLAN Add <pvlan_id> [<port_list>]

Parameters:
<pvlan_id> : Private VLAN ID. The allowed range for a Private VLAN ID is the same as the switch port number range.
<port_list>: Port list or 'all', default: All ports

Example:
Add port1 to port4 in PVLAN10

```
NS3550-8T-2S:/>pvlan add 10 1-4
```

PVLAN Delete

Description:
Delete Private VLAN entry.

Syntax:
PVLAN Delete <pvlan_id>

Parameters:
<pvlan_id>: Private VLAN ID. The allowed range for a Private VLAN ID is the same as the switch port number range.

Example:
Delete PVLAN10

```
NS3550-8T-2S:/>pvlan delete 10
```

PVLAN Lookup

Description:
Lookup Private VLAN entry.

Syntax:
PVLAN Lookup [<pvlan_id>]

Parameters:

<pvlan_id>: Private VLAN ID, default: Show all PVLANs. The allowed range for a Private VLAN ID is the same as the switch port number range.

Example:

Lookup PVLAN

```
NS3550-8T-2S:/>pvlan lookup

PVLAN ID    Ports
--------    -----
1           1-10
```

PVLAN Isolate

Description:

Set or show the port isolation mode.

Syntax:

PVLAN Isolate [<port_list>] [enable|disable]

Parameters:

<port_list>: Port list or 'all', default: All ports
enable : Enable port isolation
disable : Disable port isolation
(default: Show port isolation port list)

Default Setting:

disable

Example:

Enable isolate for port10

```
NS3550-8T-2S:/>pvlan isolate 10 enable
```

6.7 Security Command

Security Switch User Configuration

Description:

Show users configuration.

Syntax:

Security Switch Users Configuration

Default Setting:

User Name	Privilege
admin	15

Example:

Show users configuration

```
NS3550-8T-2S:/>security switch user configuration

Users Configuration:
====================

User Name                        Privilege Level
--------------------------------  ---------------
admin                                         15
```

Security Switch User Add

Description:

Add or modify users entry.

Syntax:

Security Switch Users Add <user_name> <password> <privilege_level>

Parameters:

<user_name> : A string identifying the user name that this entry should belong to. The allowed string length is (1-32). The valid user name is a combination of letters, numbers and underscores

<password> : The password for this user name. The allowed string length is (0-32). Use 'clear' or "" as null string

<privilege_level>: User privilege level (1-15)

Example:

Add new user: username: test, password: test & privilege: 10

```
NS3550-8T-2S:/>security switch users add test test 10
```

Security Switch User Delete

Description:

Delete users entry.

Syntax:

Security Switch Users Delete <user_name>

Parameters:

<user_name>: A string identifying the user name that this entry should belong to. The allowed string length is (1-32). The valid user name is a combination of letters, numbers and underscores

Example:

Delete test account.

```
NS3550-8T-2S:/>security switch users delete user
```

Security Switch Privilege Level Configuration

Description:

Show privilege configuration.

Syntax:

Security Switch Privilege Level Configuration

Example:

Show privilege level

```
NS3550-8T-2S:/>security switch privilege level configuration

Privilege Level Configuration:
==============================

Privilege Current Level: 15
Group Name                          Priviliege Level
                                   CRO CRW SRO SRW
------------------------------- --- --- --- ---
Aggregation                         5   10    5   10
Debug                              15   15   15   15
Diagnostics                         5   10    5   10
DualCPU                             5   10    5   10
EEE                                 5   10    5   10
IP                                  5   10    5   10
LACP                                5   10    5   10
LLDP                                5   10    5   10
LLDP_MED                            5   10    5   10
MAC_Table                           5   10    5   10
MVR                                 5   10    5   10
Maintenance                        15   15   15   15
Mirroring                           5   10    5   10
Multicast                           5   10    5   10
Port_Security                       5   10    5   10
```

```
Ports                          5   10    1   10
Private_VLANs                   5   10    5   10
Protocol_based_VLAN              5   10    5   10
QoS                            5   10    5   10
SNMP                            5   10    5   10
Security                       5   10    5   10
Spanning_Tree                   5   10    5   10
System                         5   10    1   10
UPnP                           5   10    5   10
VLANs                          5   10    5   10
Voice_VLAN                      5   10    5   10
```

Security Switch Privilege Level Group

Description:
Configure a privilege level group.

Syntax:
Security Switch Privilege Level Group <group_name> [<cro>] [<crw>] [<sro>] [<srw>]

Parameters:
<group_name>: Privilege group name
<cro> : Configuration read-only privilege level (1-15)
<crw> : Configuration/Execute read-write privilege level (1-15)
<sro> : Status/Statistics read-only privilege level (1-15)
<srw> : Status/Statistics read-write privilege level (1-15)

Example:
Change privilege level of MVR group.

```
NS3550-8T-2S:/>security switch privilege level group mvr 15 15 15 15
```

Security Switch Privilege Level Current

Description:
Show the current privilege level.

Syntax:
Security Switch Privilege Level Current

Default Setting:
15

Security Switch Auth Configuration

Description:
Show Auth configuration.

Syntax:
Security Switch Auth Configuration

Example:
Show authentication configuration.

```
NS3550-8T-2S:/>security switch auth configuration

Auth Configuration:
====================

Client     Authentication Method     Local Authentication Fallback
-------    ----------------------    -----------------------------
console     local                     Disabled
telnet      local                     Disabled
ssh         local                     Disabled
web         local                     Disabled
```

Security Switch Auth Method

Description:
Set or show Auth method. (default: Show Auth method).

Syntax:
Security Switch Auth Method [console|telnet|ssh|web] [none|local|radius|tacacs+] [enable|disable]

Parameters:
console : Settings for console
telnet : Settings for telnet
ssh : Settings for ssh
web : Settings for web
(default: Set or show the specific client authentication method)
none : Authentication disabled
local : Use local authentication
radius : Use remote RADIUS authentication
tacacs+ : Use remote TACACS+ authentication
(default: Show client authentication method)
enable : Enable local authentication if remote authentication fails
disable : Disable local authentication if remote authentication fails
(The parameter is effective when it is typed)

Default Setting:
disable

Example:
Use RADIUS authentication method for telnet.

```
NS3550-8T-2S:/>security switch auth method telnet radius enable
```

Security Switch SSH Configuration

Description:
Show SSH configuration.

Syntax:
Security Switch SSH Configuration

Example:
Show SSH configuration.

```
NS3550-8T-2S:/>security switch ssh configuration

SSH Configuration:
==================

SSH Mode : Enable
```

Security Switch SSH Mode

Description:
Set or show the SSH mode.

Syntax:
Security Switch SSH Mode [enable|disable]

Parameters:
enable : Enable SSH
disable: Disable SSH
(default: Show SSH mode)

Default Setting:
enable

Example:

Enable SSH function.

```
NS3550-8T-2S:/>security switch ssh mode enable
```

Security Switch HTTPs Configuration

Description:
Show HTTPS configuration.

Syntax:
Security Switch HTTPS Configuration

Example:
Show HTTPs configuration.

```
NS3550-8T-2S:/>security switch https configuration

HTTPS Configuration:
====================

HTTPS Mode              : Enable
HTTPS Redirect Mode : Disabled
```

Security Switch HTTPs Mode

Description:
Set or show the HTTPS mode.

Syntax:
Security Switch HTTPS Mode [enable|disable]

Parameters:
enable : Enable HTTPs
disable: Disable HTTPs
(default: Show HTTPs mode)

Default Setting:
enable

Example:
Enable HTTPs function.

```
NS3550-8T-2S:/>security switch https mode enable
```

Security Switch HTTPs Redirect

Description:
Set or show the HTTPS redirect mode.
Automatic redirect web browser to HTTPS during HTTPS mode enabled.

Syntax:
Security Switch HTTPS Redirect [enable|disable]

Parameters:
enable : Enable HTTPs redirect
disable: Disable HTTPs redirect
(default: Show HTTPs redirect mode)

Default Setting:
disable

Example:
Enable HTTPs redirect function.

```
NS3550-8T-2S:/>security switch https redirect enable
```

Security Switch Access Configuration

Description:
Show access management configuration.

Syntax:
Security Switch Access Configuration

Example:
Show access management configuration.

```
NS3550-8T-2S:/>security switch access configuration

Access Mgmt Configuration:
==========================

System Access Mode : Disabled
System Access number of entries: 0
```

Security Switch Access Mode

Description:
Set or show the access management mode.

Syntax:
Security Switch Access Mode [enable|disable]

Parameters:
enable : Enable access management
disable: Disable access management
(default: Show access management mode)

Default Setting:
disable

Example:
Enable access management function.

```
NS3550-8T-2S:/>security switch access mode enable
```

Security Switch Access Configuration

Description:
Show access management configuration.

Syntax:
Security Switch Access Configuration

Example:
Show access management configuration.

```
NS3550-8T-2S:/>security switch access configuration

Access Mgmt Configuration:
==========================

System Access Mode : Disabled
W: WEB/HTTPS
S: SNMP
T: TELNET/SSH

Idx Start IP Address                End IP Address                W S T
--- ------------------------------- ------------------------------- - - -
```

Security Switch Access Mode

Description:
Set or show the access management mode.

Syntax:
Security Switch Access Mode [enable|disable]

Parameters:
enable : Enable access management
disable: Disable access management
(default: Show access management mode)

Default Setting:
disable

Example:
Enable switch access mode

```
NS3550-8T-2S:/>security switch access mode enable
```

Security Switch Access Add

Description:
Add access management entry, default: Add all supported protocols.

Syntax:
Security Switch Access Add <access_id> <start_ip_addr> <end_ip_addr> [web] [snmp] [telnet]

Parameters:
<access_id> : entry index (1-16)
<start_ip_addr>: Start IP address (a.b.c.d)
<end_ip_addr> : End IP address (a.b.c.d)
web : Indicates that the host can access the switch from HTTP/HTTPS
snmp : Indicates that the host can access the switch from SNMP
telnet : Indicates that the host can access the switch from TELNET/SSH

Example:
Add access management list from 192.168.0.1 to 192.168.0.200 via web interface.

```
NS3550-8T-2S:/>security switch access add 1 192.168.0.1 192.168.0.200 web
```

Security Switch Access IPv6 Add

Description:
Add access management IPv6 entry, default: Add all supported protocols.

Syntax:
Security Switch Access Ipv6 Add <access_id> <start_ipv6_addr> <end_ipv6_addr> [web] [snmp] [telnet]

Parameters:
<access_id> : entry index (1-16)
<start_ipv6_addr>: Start IPv6 address.
IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separates each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can only appear once. It also used a following legally IPv4 address. For example,'::192.1.2.34'.
<end_ipv6_addr> : End IPv6 address.
IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separates each field (:). For example,'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can only appear once. It also used a following legally IPv4 address. For example,'::192.1.2.34'.
web : Indicates that the host can access the switch from HTTP/HTTPS
snmp : Indicates that the host can access the switch from SNMP

telnet : Indicates that the host can access the switch from TELNET/SSH

Example:

Add access management list from 2001::0001 to 2001::0100 via web interface.

```
NS3550-8T-2S:/> security switch access add 2001::0001 2001::0100 web
```

Security Switch Access Delete

Description:

Delete access management entry.

Syntax:

Security Switch Access Delete <access_id>

Parameters:

<access_id>: entry index (1-16)

Example:

Delete access management ID 1

```
NS3550-8T-2S:/>security switch access delete 1
```

Security Switch Access Lookup

Description:

Lookup access management entry.

Syntax:

Security Switch Access Lookup [<access_id>]

Parameters:

<access_id> : entry index (1-16)

Example:

Lookup access management entry.

```
NS3550-8T-2S:/>security switch access lookup 1
```

Security Switch Access Clear

Description:

Clear access management entry.

Syntax:

Security Switch Access Clear

Example:

Clear access management entry.

```
NS3550-8T-2S:/>security switch access clear
```

Security Switch Access Statistics

Description:

Show or clear access management statistics.

Syntax:

Security Switch Access Statistics [clear]

Parameters:

clear: Clear access management statistics

Example:

Show access management statistics.

```
NS3550-8T-2S:/>security switch access statistics

Access Management Statistics:
------------------------------
HTTP      Receive:          0     Allow:          0     Discard:          0
HTTPS     Receive:          0     Allow:          0     Discard:          0
SNMP      Receive:          0     Allow:          0     Discard:          0
TELNET    Receive:          0     Allow:          0     Discard:          0
SSH       Receive:          0     Allow:          0     Discard:          0
```

Security Switch SNMP Configuration

Description:
Show SNMP configuration.

Syntax:
Security Switch SNMP Configuration

Security Switch SNMP Mode

Description:
Set or show the SNMP mode.

Syntax:
Security Switch SNMP Mode [enable|disable]

Parameters:
enable : Enable SNMP
disable: Disable SNMP
(default: Show SNMP mode)

Default Setting:
enable

Example:
Disable SNMP mode.

```
NS3550-8T-2S:/>security switch snmp mode disable
```

Security Switch SNMP Version

Description:
Set or show the SNMP protocol version.

Syntax:
Security Switch SNMP Version [1|2c|3]

Parameters:

1 : SNMP version 1
2c: SNMP version 2c
3 : SNMP version 3
(default: Show SNMP version)

Default Setting:

2c

Example:

Set SNMP in version 3.

```
NS3550-8T-2S:/>security switch snmp version 3
```

Security Switch SNMP Read Community

Description:

Set or show the community string for SNMP read access.

Syntax:

Security Switch SNMP Read Community [<community>]

Parameters:

<community>: Community string. Use 'clear' or "" to clear the string
(default: Show SNMP read community)

Default Setting:

public

Example:

Set SNMP read community private.

```
NS3550-8T-2S:/>security switch snmp read community private
```

Security Switch SNMP Write Community

Description:
Set or show the community string for SNMP write access.

Syntax:
Security Switch SNMP Write Community [<community>]

Parameters:
<community>: Community string. Use 'clear' or "" to clear the string
(default: Show SNMP write community)

Default Setting:
private

Example:

Set public value in SNMP write community.

```
NS3550-8T-2S:/>security switch snmp write community public
```

Security Switch SNMP Trap Mode

Description:
Set or show the SNMP trap mode.

Syntax:
Security Switch SNMP Trap Mode [enable|disable]

Parameters:
enable : Enable SNMP traps
disable: Disable SNMP traps
(default: Show SNMP trap mode)

Default Setting:
disable

Example:

Enable SNMP trap mode.

```
NS3550-8T-2S:/>security switch snmp trap mode enable
```

Security Switch SNMP Trap Version

Description:

Set or show the SNMP trap protocol version.

Syntax:

Security Switch SNMP Trap Version [1|2c|3]

Parameters:

1 : SNMP version 1
2c: SNMP version 2c
3 : SNMP version 3
(default: Show SNMP trap version)

Default Setting:

1

Example:

Set SNMP trap version in version 2c.

```
NS3550-8T-2S:/>security switch snmp trap version 2c
```

Security Switch SNMP Trap Community

Description:

Set or show the community string for SNMP traps.

Syntax:

Security Switch SNMP Trap Community [<community>]

Parameters:

<community>: Community string. Use 'clear' or "" to clear the string
(default: Show SNMP trap community)

Default Setting:
public

Example:
Set private value for SNMP trap community.

```
NS3550-8T-2S:/>security switch snmp trap community private
```

Security Switch SNMP Trap Destination

Description:
Set or Show the SNMP trap destination address.

Syntax:
Security Switch SNMP Trap Destination [<ip_addr_string>]

Parameters:
<ip_addr_string>: IP host address (a.b.c.d) or a host name string

Example:
Set SNMP trap destination address for 192.168.0.20

```
NS3550-8T-2S:/>security switch snmp trap destination 192.168.0.20
```

Security Switch SNMP Trap IPv6 Destination

Description:
Set or Show the SNMP trap destination IPv6 address.

Syntax:
Security Switch SNMP Trap IPv6 Destination [<ipv6_addr>]

Parameters:
<ipv6_addr>: IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separates each field (:). For example, four hexadecimal digits with a colon separates each field (:). For example, fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can only appear once. It also used a following legally IPv4 address. For example,'::192.1.2.34'.

Example:
Set SNMP trap IPv6 destination address for 2001::0001

```
NS3550-8T-2S:/>security switch snmp trap ipv6 destination 2001::0001
```

Security Switch SNMP Trap Authentication Failure

Description:
Set or show the SNMP authentication failure trap mode.

Syntax:
Security Switch SNMP Trap Authentication Failure [enable|disable]

Parameters:
enable : Enable SNMP trap authentication failure
disable: Disable SNMP trap authentication failure
(default: Show SNMP trap authentication failure mode)

Default Setting:
enable

Example:
Disable SNMP trap authentication failure

```
NS3550-8T-2S:/>security switch snmp trap authentication failure disable
```

Security Switch SNMP Trap Link-up

Description:
Set or show the port link-up and link-down trap mode.

Syntax:
Security Switch SNMP Trap Link-up [enable|disable]

Parameters:
enable : Enable SNMP trap link-up and link-down
disable: Disable SNMP trap link-up and link-down
(default: Show SNMP trap link-up and link-down mode)
Default Setting:
enable

Example:
Disable SNMP trap link-up

```
NS3550-8T-2S:/>security switch snmp trap link-up disable
```

Security Switch SNMP Trap Inform Mode

Description:
Set or show the SNMP trap inform mode.

Syntax:
Security Switch SNMP Trap Inform Mode [enable|disable]

Parameters:
enable : Enable SNMP trap inform
disable: Disable SNMP trap inform
(default: Show SNMP inform mode)

Default Setting:
enable

Example:
Disable SNMP trap inform mode.

```
NS3550-8T-2S:/>security switch snmp trap inform mode disable
```

Security Switch SNMP Trap Inform Timeout

Description:
Set or show the SNMP trap inform timeout (usecs).

Syntax:
Security Switch SNMP Trap Inform Timeout [<timeout>]

Parameters:
<timeout>: SNMP trap inform timeout (0-2147 seconds)
(default: Show SNMP trap inform timeout)
Default Setting:
1

Example:
Set SNMP trap inform timeout in 20sec.

```
NS3550-8T-2S:/>security switch snmp trap inform timeout 20
```

Security Switch SNMP Trap Inform Retry Times

Description:
Set or show the SNMP trap inform retry times.

Syntax:
Security Switch SNMP Trap Inform Retry Times [<retries>]

Parameters:
<retries>: SNMP trap inform retransmited times (0-255)
(default: Show SNMP trap inform retry times)

Default Setting:
5

Example:
Set SNMP trap inform retry times in 10.

```
NS3550-8T-2S:/>security switch snmp trap inform retry times 10
```

Security Switch SNMP Trap Probe Security Engine ID

Description:
Show SNMP trap security engine ID probe mode.

Syntax:
Security Switch SNMP Trap Probe Security Engine ID [enable|disable]

Parameters:
enable : Enable SNMP trap security engine ID probe
disable: Disable SNMP trap security engine ID probe
(default: Show SNMP trap security engine ID probe mode)
Default Setting:
enable

Example:
Disable SNMP trap probe security engine ID

```
NS3550-8T-2S:/>security switch snmp trap probe security engine id disable
```

Security Switch SNMP Trap Security Engine ID

Description:
Set or show SNMP trap security engine ID.

Syntax:
Security Switch SNMP Trap Security Engine ID [<engineid>]

Parameters:
<engineid>: Engine ID, the format may not be all zeros or all 'ff'H and is restricted to 5 - 32 octet string

Example:
Set the SNMP trap security engine ID

```
NS3550-8T-2S:/>security switch snmp trap security engine id 800007e5017f000011
```

Security Switch SNMP Trap Security Name

Description:
Set or show SNMP trap security name.

Syntax:
Security Switch SNMP Trap Security Name [<security_name>]

Parameters:

<security_name>: A string representing the security name for a principal (default: Show SNMP trap security name). The allowed string length is (1-32), and the allowed content is ASCII characters from 33 to 126

Example:

Set the SNMP trap security name

```
NS3550-8T-2S:/>security switch snmp trap security name 12345678
```

Security Switch SNMP Engine ID

Description:

Set or show SNMPv3 local engine ID.

Syntax:

Security Switch SNMP Engine ID [<engineid>]

Parameters:

<engineid>: Engine ID, the format may not be all zeros or all 'ff'H and is restricted to 5 - 32 octet string

Default Setting:

800007e5017f000001

Example:

Set 800007e5017f000002 for SNMPv3 local engine ID

```
NS3550-8T-2S:/>security switch snmp engine id 800007e5017f000002
```

Security Switch SNMP Community Add

Description:

Add or modify SNMPv3 community entry.
The entry index key is <community>.

Syntax:

Security Switch SNMP Community Add <community> [<ip_addr>] [<ip_mask>]

Parameters:

<community>: Community string
<ip_addr> : IP address (a.b.c.d), default: Show IP address
<ip_mask> : IP subnet mask (a.b.c.d), default: Show IP mask

Example:

Add SNMPv3 community entry.

```
NS3550-8T-2S:/>security switch snmp community add public 192.168.0.20 255.255.255.0
```

Security Switch SNMP Community Delete

Description:

Delete SNMPv3 community entry.

Syntax:

Security Switch SNMP Community Delete <index>

Parameters:

<index>: entry index (1-64)

Example:

Delete SNMPv3 community entry

```
NS3550-8T-2S:/>security switch snmp community delete 3
```

Security Switch SNMP Community Lookup

Description:

Lookup SNMPv3 community entry.

Syntax:

Security Switch SNMP Community Lookup [<index>]

Parameters:

<index>: entry index (1-64)

Example:

Lookup SNMPv3 community entry

```
NS3550-8T-2S:/>security switch snmp community lookup
Idx Community                        Source IP          Source Mask
--- -------------------------------- ---------------    ---------------
1   public                           192.168.0.20       255.255.255.0
2   private                          0.0.0.0            0.0.0.0

Number of entries: 2
```

Security Switch SNMP User Add

Description:

Add SNMPv3 user entry.
The entry index key are <engineid> and <user_name> and it doesn't allow modify.

Syntax:

Security Switch SNMP User Add <engineid> <user_name> [MD5|SHA] [<auth_password>] [DES] [<priv_password>]

Parameters:

<engineid> : Engine ID, the format may not be all zeros or all 'ff'H and is restricted to 5 - 32 octet string
<user_name> : A string identifying the user name that this entry should belong to. The name of "None" is reserved. The allowed string length is (1-32), and the allowed content is ASCII characters from 33 to 126
md5 : An optional flag to indicate that this user using MD5 authentication protocol. The allowed length is (8-32), and the allowed content is ASCII characters from 33 to 126
sha : An optional flag to indicate that this user using SHA authentication protocol. The allowed length is (8-40), and the allowed content is ASCII characters from 33 to 126
<auth_password>: A string identifying the authentication pass phrase
des : An optional flag to indicate that this user using DES privacy protocol privacy protocol should belong to. The allowed string length is (8-32), and the allowed content is ASCII characters from 33 to 126
<priv_password>: A string identifying the privacy pass phrase.

The allowed string length is (8-40), and the allowed content is ASCII characters from 33 to 126

Example:

Add SNMPv3 user entry

```
NS3550-8T-2S:/>security switch snmp user add 800007e5017f000003 admin_snmpv3 md5
12345678 des abcdefgh
```

Security Switch SNMP User Delete

Description:

Delete SNMPv3 user entry.

Syntax:
Security Switch SNMP User Delete <index>

Parameters:
<index>: entry index (1-64)

Example:
Delete SNMPv3 user entry

```
NS3550-8T-2S:/>security switch snmp user delete 1
```

Security Switch SNMP User Changekey

Description:
Change SNMPv3 user password.

Syntax:
Security Switch SNMP User Changekey <engineid> <user_name> <auth_password> [<priv_password>]

Parameters:
<engineid> : Engine ID, the format may not be all zeros or all 'ff'H and is restricted to 5 - 32 octet string
<user_name> : A string identifying the user name that this entry should belong to. The name of "None" is reserved.
The allowed string length is (1-32), and the allowed content is ASCII characters from 33 to 126
<auth_password>: A string identifying the authentication pass phrase
<priv_password>: A string identifying the privacy pass phrase.
The allowed string length is (8-40), and the allowed content is ASCII characters from 33 to 126

Example:
Delete SNMPv3 user entry

```
NS3550-8T-2S:/>security switch snmp user changekey 800007e5017f000003 admin_snmpv3
87654321 12345678
```

Security Switch SNMP User Lookup

Description:
Lookup SNMPv3 user entry.

Syntax:
Security Switch SNMP User Lookup [<index>]
Parameters:
<index>: entry index (1-64)

Example:
Lookup SNMPv3 user entry

```
NS3550-8T-2S:/>security switch snmp user lookup
Idx Engine ID    User Name                        Level          Auth   Priv
---  ---------    --------------------------------  --------------  ----   ----
1    Remote       admin_snmpv3                      Auth, Priv     MD5    DES

Number of entries: 1
```

Security Switch SNMP Group Add

Description:
Add or modify SNMPv3 group entry.
The entry index key are <security_model> and <security_name>.

Syntax:
Security Switch SNMP Group Add <security_model> <security_name> <group_name>

Parameters:
<security_model>: v1 - Reserved for SNMPv1
v2c - Reserved for SNMPv2c
usm - User-based Security Model (USM)
<security_name> : A string identifying the security name that this entry should belong to. The allowed string length is

(1-32), and the allowed content is ASCII characters from 33 to 126

<group_name> : A string identifying the group name that this entry should belong to. The allowed string length is (1-32), and the allowed content is ASCII characters from 33 to 126

Example:

Add SNMPv3 group entry

```
NS3550-8T-2S:/>security switch snmp group add usm admin_snmpv3 group_snmpv3
```

Security Switch SNMP Group Delete

Description:
Delete SNMPv3 group entry.

Syntax:
Security Switch SNMP Group Delete <index>

Parameters:
<index>: entry index (1-64)

Example:
Delete SNMPv3 group entry

```
NS3550-8T-2S:/>security switch snmp group delete 1
```

Security Switch SNMP Group Lookup

Description:
Lookup SNMPv3 group entry.

Syntax:
Security Switch SNMP Group Lookup [<index>]

Parameters:
<index>: entry index (1-64)

Example:
Lookup SNMPv3 group entry

```
NS3550-8T-2S:/>security switch snmp group lookup
Idx Model Security Name                    Group Name
--- ----- ---------------------------------- ----------------------------------
1   v1    public                           default_ro_group
2   v1    private                          default_rw_group
3   v2c   public                           default_ro_group
4   v2c   private                          default_rw_group
5   usm   default_user                     default_rw_group

Number of entries: 5
```

Security Switch SNMP View Add

Description:
Add or modify SNMPv3 view entry.
The entry index key are <view_name> and <oid_subtree>.

Syntax:
Security Switch SNMP View Add <view_name> [included|excluded] <oid_subtree>

Parameters:
<view_name> : A string identifying the view name that this entry should belong to. The allowed string length is (1-32), and the allowed content is ASCII characters from 33 to 126
included : An optional flag to indicate that this view subtree should included
excluded : An optional flag to indicate that this view subtree should excluded
<oid_subtree>: The OID defining the root of the subtree to add to the named view

Example:
Add SNMPv3 view entry

```
NS3550-8T-2S:/>security switch snmp view add snmpv3_view include .1
```

Security Switch SNMP View Delete

Description:
Delete SNMPv3 view entry.

Syntax:
Security Switch SNMP View Delete <index>

Parameters:
<index>: entry index (1-64)

Example:
Delete SNMPv3 view entry

```
NS3550-8T-2S:/>security switch snmp view delete 3
```

Security Switch SNMP View Lookup

Description:
Lookup SNMPv3 view entry.

Syntax:
Security Switch SNMP View Lookup [<index>]

Parameters:
<index>: entry index (1-64)

Example:
Lookup SNMPv3 view entry

```
NS3550-8T-2S:/>security switch snmp view lookup
Idx   View Name                        View Type   OID Subtree
---   ------------------------------   ---------   --------------------------------
1     default_view                     included    .1
2     snmpv3_viwe                      included    .1

Number of entries: 2
```

Security Switch SNMP Access Add

Description:
Add or modify SNMPv3 access entry.
The entry index key are <group_name>, <security_model> and <security_level>.

Syntax:
Security Switch SNMP Access Add <group_name> <security_model> <security_level> [<read_view_name>] [<write_view_name>]

Parameters:
<group_name> : A string identifying the group name that this entry should belong to. The allowed string length is (1-32), and the allowed content is ASCII characters from 33 to 126
<security_model> : any - Accepted any security model (v1|v2c|usm)
v1 - Reserved for SNMPv1
v2c - Reserved for SNMPv2c
usm - User-based Security Model (USM)
<security_level> : noAuthNoPriv - None authentication and none privacy
AuthNoPriv - Authentication and none privacy
AuthPriv - Authentication and privacy
<read_view_name> : The name of the MIB view defining the MIB objects for which this request may request the current values.
The name of "None" is reserved.
The allowed string length is (1-32), and the allowed content is ASCII characters from 33 to 126
<write_view_name>: The name of the MIB view defining the MIB objects for which this request may potentially SET new values.
The name of "None" is reserved.
The allowed string length is (1-32), and the allowed content is ASCII characters from 33 to 126

Example:
Add SNMPv3 access entry

```
NS3550-8T-2S:/>security switch snmp access add group_snmpv3 usm authpriv
snmpv3_view snmpv3_view
```

Security Switch SNMP Access Delete

Description:
Delete SNMPv3 access entry.

Syntax:
Security Switch SNMP Access Delete <index>

Parameters:
<index>: entry index (1-64)

Example:
Delete SNMPv3 access entry

```
NS3550-8T-2S:/>security switch snmp access delete 3
```

Security Switch SNMP Access Lookup

Description:
Lookup SNMPv3 access entry.

Syntax:
Security Switch SNMP Access Lookup [<index>]

Parameters:
<index>: entry index (1-64)

Example:
Lookup SNMPv3 access entry

```
NS3550-8T-2S:/>security switch snmp access lookup
Idx Group Name                       Model Level
--- -------------------------------- ----- --------------
1   default_ro_group                 any   NoAuth, NoPriv
2   default_rw_group                 any   NoAuth, NoPriv

Number of entries: 2
```

Security Network Psec Switch

Description:
Show Port Security status.

Syntax:
Security Network Psec Switch [<port_list>]

Parameters:
<port_list>: Port list or 'all', default: All ports

Example:
Show port security status.

```
NS3550-8T-2S:/>security network psec switch
Users:
L = Limit Control
8 = 802.1X
D = DHCP Snooping
V = Voice VLAN

Port   Users   State                MAC Cnt
----   -----   -------------        -------
1      ----    No users                   0
2      ----    No users                   0
3      ----    No users                   0
4      ----    No users                   0
5      ----    No users                   0
```

```
6       ----      No users                0
7       ----      No users                0
8       ----      No users                0
9       ----      No users                0
10      ----      No users                0
```

Security Network Psec Port

Description:
Show MAC Addresses learned by Port Security.

Syntax:
Security Network Psec Port [<port_list>]

Parameters:
<port_list>: Port list or 'all', default: All ports

Example:
Show MAC address learned on port 1

```
NS3550-8T-2S:/>security network psec port 1

Port 1:
-------

MAC Address          VID    State         Added                        Age/Hold Time
-----------------    ----   ----------    --------------------------   -------------
<none>
```

Security Network Limit Configuration

Description:
Show Limit Control configuration.

Syntax:
Security Network Limit Configuration [<port_list>]
Parameters:
<port_list>: Port list or 'all', default: All ports

Example:
Show Limit Control configuration.

```
NS3550-8T-2S:/>security network limit configuration

Port Security Limit Control Configuration:
==========================================

Mode         : Disabled
Aging        : Disabled
Age Period: 3600

Port   Mode          Limit   Action
----   --------       -----   ---------------
1      Disabled        4     None
2      Disabled        4     None
3      Disabled        4     None
4      Disabled        4     None
5      Disabled        4     None
6      Disabled        4     None
7      Disabled        4     None
8      Disabled        4     None
9      Disabled        4     None
10     Disabled        4     None
```

Security Network Limit Mode

Description:
Set or show global enabledness.

Syntax:
Security Network Limit Mode [enable|disable]

Parameters:
enable : Globally enable port security
disable : Globally disable port security
(default: Show current global enabledness of port security limit control)
Default Setting:
disable

Example:
Enable the limit mode

```
NS3550-8T-2S:/>security network limit mode enable
```

Security Network Limit Aging

Description:
Set or show aging enabledness.

Syntax:
Security Network Limit Aging [enable|disable]

Parameters:
enable : Enable aging
disable : Disable aging
(default: Show current enabledness of aging)

Default Setting:
disable

Example:
Enable limit aging

```
NS3550-8T-2S:/>security network limit aging enable
```

Security Network Limit Agetime

Description:
Time in seconds between check for activity on learned MAC addresses.

Syntax:
Security Network Limit Agetime [<age_time>]

Parameters:
<age_time>: Time in seconds between checks for activity on a MAC address (10-10000000 seconds)
(default: Show current age time)
Default Setting:
3600

Example:
Set age time in 100sec.

```
NS3550-8T-2S:/>security network limit agetime 100
```

Security Network Limit Port

Description:
Set or show per-port enabledness.
Syntax:

Security Network Limit Port [<port_list>] [enable|disable]

Parameters:
<port_list>: Port list or 'all', default: All ports
enable : Enable port security on this port
disable : Disable port security on this port
(default: Show current port enabledness of port security limit control)

Default Setting:
disable

Example:
Enable port limit for port 1

```
NS3550-8T-2S:/>security network limit port 1 enable
```

Security Network Limit Limit

Description:
Set or show the max. number of MAC addresses that can be learned on this set of ports.

Syntax:
Security Network Limit Limit [<port_list>] [<limit>]

Parameters:
<port_list>: Port list or 'all', default: All ports
<limit> : Max. number of MAC addresses on this port
(default: Show current limit)
Default Setting:
4

Example:
Set limit in 5

```
NS3550-8T-2S:/>security network limit limit 1-10 5
```

Security Network Limit Action

Description:
Set or show the action involved with exceeding the limit.

Syntax:
Security Network Limit Action [<port_list>] [none|trap|shut|trap_shut]

Parameters:
<port_list> : Port list or 'all', default: All ports
none|trap|shut|trap_shut: Action to be taken in case the number of MAC addresses exceeds the limit
none : Don't do anything
trap : Send an SNMP trap
shut : Shutdown the port
trap_shut: Send an SNMP trap and shutdown the port
(default: Show current action)

Default Setting:
none

Example:
Set trap mode for limit action for port 1

```
NS3550-8T-2S:/>security network limit action 1 trap
```

Security Network Limit Reopen

Description:

Reopen one or more ports whose limit is exceeded and shut down.

Syntax:
Security Network Limit Reopen [<port_list>]

Parameters:
<port_list>: Port list or 'all', default: All ports

Example:
Reopen port 1

```
NS3550-8T-2S:/>security network limit reopen 1
```

Security Network NAS Configuration

Description:
Show 802.1X configuration.

Syntax:
Security Network NAS Configuration [<port_list>]

Parameters:
<port_list>: Port list or 'all', default: All ports

Example:
Show 802.1X configuration of port 1

```
NS3550-8T-2S:/>security network nas configuration 1

802.1X Configuration:
=====================

Mode                  : Disabled
Reauth.               : Disabled
Reauth. Period        : 3600
EAPOL Timeout         : 30
Age Period            : 300
Hold Time             : 10
RADIUS QoS            : Disabled
RADIUS VLAN           : Disabled
Guest VLAN            : Disabled
Guest VLAN ID         : 1
Max. Reauth Count: 2
Allow Guest VLAN if EAPOL Frame Seen: Disabled

Port    Admin State             Port State              Last Source           Last ID
----    -------------------   ----------------------   -------------------   -------------------
1       Force Authorized      Globally Disabled         -                     -
```

Security Network NAS Mode

Description:
Set or show the global NAS enabledness.

Syntax:
Security Network NAS Mode [enable|disable]

Parameters:
enable : Globally enable 802.1X
disable: Globally disable 802.1X
(default: Show current 802.1X global enabledness)

Default Setting:
disable

Example:
Enable IEEE802.1X function

```
NS3550-8T-2S:/>security network nas mode enable
```

Security Network NAS State

Description:
Set or show the port security state.

Syntax:
Security Network NAS State [<port_list>] [auto|authorized|unauthorized|single|multi|macbased]

Parameters:
<port_list>: Port list or 'all', default: All ports
auto : Port-based 802.1X Authentication
authorized : Port access is allowed
unauthorized: Port access is not allowed
single : Single Host 802.1X Authentication
multi : Multiple Host 802.1X Authentication
macbased : Switch authenticates on behalf of the client
(default: Show 802.1X state)

Default Setting:
none

Example:
Show the port 1 security state.

```
NS3550-8T-2S:/>security network nas state 1

Port   Admin State          Port State            Last Source          Last ID
----   -----------------   ------------------    -----------------    ----------
1      Force Authorized    Globally Disabled      -                    -
```

Security Network NAS Reauthentication

Description:
Set or show Reauthentication enabledness.

Syntax:
Security Network NAS Reauthentication [enable|disable]

Parameters:
enable : Enable reauthentication
disable: Disable reauthentication
(default: Show current reauthentication mode)

Default Setting:
disable

Example:
Enable reauthentication function.

```
NS3550-8T-2S:/>security network nas reauthentication enable
```

Security Network NAS ReauthPeriod

Description:
Set or show either global enabledness (use the global keyword) or per-port enabledness of RADIUS-assigned VLAN.

Syntax:
Security Network NAS RADIUS_VLAN [global|<port_list>] [enable|disable]

Parameters:
global : Select the global RADIUS-assigned VLAN setting
<port_list>: Select the per-port RADIUS-assigned VLAN setting
(default: Show current per-port RADIUS-assigned VLAN enabledness)
enable : Enable RADIUS-assigned VLAN either globally or on one or more ports

disable: Disable RADIUS-assigned VLAN either globally or on one or more ports
(default: Show current RADIUS-assigned VLAN enabledness)

Default Setting:
disable

Example:
Enable RADIUS-assigned VLAN.

```
NS3550-8T-2S:/>security network nas radius_vlan enable
```

Security Network NAS EapolTimeout

Description:
Set or show the time between EAPOL retransmissions.

Syntax:
Security Network NAS EapolTimeout [<eapol_timeout>]

Parameters:
<eapol_timeout>: Time between EAPOL retransmissions (1-65535 seconds)
(default: Show current EAPOL retransmission timeout)

Default Setting:
30

Example:

Set the time between EAPOL retransmissions for 100sec.

```
NS3550-8T-2S:/>security network nas eapoltimeout 100
```

Security Network NAS Agetime

Description:

Time in seconds between check for activity on successfully authenticated MAC addresses.

Syntax:

Security Network NAS Agetime [<age_time>]

Parameters:

<age_time>: Time between checks for activitiy on a MAC address that succeeded autentication
(default: Show current age time)

Default Setting:

300

Example:

Set NAS age time in 1000sec

```
NS3550-8T-2S:/>security network nas agetime 1000
```

Security Network NAS Holdtime

Description:

Time in seconds before a MAC-address that failed authentication gets a new authentication chance.

Syntax:

Security Network NAS Holdtime [<hold_time>]

Parameters:

<hold_time>: Hold time before MAC addresses that failed authentication expire
(default: Show current hold time)

Default Setting:

10

Example:

Set NAS hold time in 100sec

```
NS3550-8T-2S:/>security network nas holdtime 100
```

Security Network NAS RADIUS_QoS

Description:

Set or show either global enabledness (use the global keyword) or per-port enabledness of RADIUS-assigned QoS.

Syntax:

Security Network NAS RADIUS_QoS [global|<port_list>] [enable|disable]

Parameters:

global : Select the global RADIUS-assigned QoS setting
<port_list>: Select the per-port RADIUS-assigned QoS setting
(default: Show current per-port RADIUS-assigned QoS enabledness)
enable : Enable RADIUS-assigned QoS either globally or on one or more ports
disable: Disable RADIUS-assigned QoS either globally or on one or more ports
(default: Show current RADIUS-assigned QoS enabledness)

Default Setting:

disable

Example:

Enable NAS RADIUS QoS

```
NS3550-8T-2S:/>security network nas radius_qos enable
```

Security Network NAS RADIUS_VLAN

Description:

Set or show either global enabledness (use the global keyword) or per-port enabledness of RADIUS-assigned VLAN.

Syntax:

Security Network NAS RADIUS_VLAN [global|<port_list>] [enable|disable]

Parameters:

global : Select the global RADIUS-assigned VLAN setting
<port_list>: Select the per-port RADIUS-assigned VLAN setting
(default: Show current per-port RADIUS-assigned VLAN enabledness)
enable : Enable RADIUS-assigned VLAN either globally or on one or more ports
disable: Disable RADIUS-assigned VLAN either globally or on one or more ports
(default: Show current RADIUS-assigned VLAN enabledness)

Default Setting:

disable

Example:

Enable NAS RADIUS VLAN

```
NS3550-8T-2S:/>security network nas radius_vlan enable
```

Security Network NAS Guest_VLAN

Description:

Set or show either global enabledness and parameters (use the global keyword) or per-port enabledness of Guest VLAN
Unless the 'global' keyword is used, the <reauth_max> and <allow_if_eapol_seen> parameters will not be unused..

Syntax:

Security Network NAS Guest_VLAN [global|<port_list>] [enable|disable] [<vid>] [<reauth_max>] [<allow_if_eapol_seen>]

Parameters:

global: Select the global Guest VLAN setting
<port_list>: Select the per-port Guest VLAN setting
(default: Show current per-port Guest VLAN enabledness)
enable|disable: enable : Enable Guest VLAN either globally or on one or more ports
disable: Disable Guest VLAN either globally or on one or more ports
(default: Show current Guest VLAN enabledness)
<vid>: Guest VLAN ID used when entering the Guest VLAN. Use the 'global' keyword to change it
(default: Show current Guest VLAN ID)
<reauth_max>: The value can only be set if you use the 'global' keyword in the beginning of the command. The number of times a Request Identity EAPOL frame is sent without reasponse before considering entering the Guest VLAN
(default: Show current Maximum Reauth Count value)
<allow_if_eapol_seen>: The value can only be set if you use the 'global' keyword in the beginning of the command.
disable:The Guest VLAN can only be entered if no EAPOL frames have been received on a port for the lifetime of the port
enable :The Guest VLAN can be entered even if an EAPOL frame has been received during the lifetime of the port
(default: Show current setting)

Default Setting:

disable

Example:

Enable NAS guest VLAN

```
NS3550-8T-2S:/>security network nas guest_vlan enable
```

Security Network NAS Authenticate

Description:

Refresh (restart) 802.1X authentication process.

Syntax:
Security Network NAS Authenticate [<port_list>] [now]

Parameters:
<port_list>: Port list or 'all', default: All ports
now: Force reauthentication immediately

Example:
Start NAS authentication now for port 1.

```
NS3550-8T-2S:/>security network nas authenticate 1 now
```

Security Network NAS Statistics

Description:
Show or clear 802.1X statistics.

Syntax:
Security Network NAS Statistics [<port_list>] [clear|eapol|radius]

Parameters:
<port_list>: Port list or 'all', default: All ports
clear : Clear statistics
eapol : Show EAPOL statistics
radius : Show Backend Server statistics
(default: Show all statistics)

Example:
Show 802.1X statistics in port 1

```
NS3550-8T-2S:/>security network nas statistics 1
Port 1 EAPOL Statistics:

Rx Total:                    0    Tx Total:                    0
Rx Response/Id:              0    Tx Request/Id:               0
Rx Response:                 0    Tx Request:                  0
Rx Start:                    0
Rx Logoff:                   0
Rx Invalid Type:             0
Rx Invalid Length:           0

Port 1 Backend Server Statistics:

Rx Access Challenges:        0    Tx Responses:                0
Rx Other Requests:           0
Rx Auth. Successes:          0
Rx Auth. Failures:           0
```

Security Network ACL Configuration

Description:
Show ACL Configuration.

Syntax:
Security Network ACL Configuration [<port_list>]

Parameters:
<port_list>: Port list or 'all', default: All ports

Security Network ACL Action

Description:
Set or show the ACL port default action.

Syntax:
Security Network ACL Action [<port_list>] [permit|deny] [<rate_limiter>] [<port_copy>] [<logging>] [<shutdown>]

Parameters:

<port_list> : Port list or 'all', default: All ports
permit : Permit forwarding (default)
deny : Deny forwarding
<rate_limiter>: Rate limiter number (1-15) or 'disable'
<port_copy> : Port number for copy of frames or 'disable'
<logging> : System logging of frames: log|log_disable
<shutdown> : Shut down ingress port: shut|shut_disable

Example:

Show ACL action in port 1

```
NS3550-8T-2S:/>security network acl action 1

Port   Action   Rate Limiter   Port Copy   Mirror      Logging     Shutdown   Counter
----   ------   ------------   ---------   ---------   ---------   --------
1      Permit   Disabled       Disabled    Disabled    Disabled    Disabled   0
```

Security Network ACL Policy

Description:

Set or show the ACL port policy.

Syntax:

Security Network ACL Policy [<port_list>] [<policy>]

Parameters:

<port_list>: Port list or 'all', default: All ports
<policy> : Policy number (1-8)

Default Setting:

1

Example:

Set ACL policy 2 for port 1

```
NS3550-8T-2S:/>security network acl policy 1 2
```

Security Network ACL Rate

Description:

Set or show the ACL rate limiter.

Syntax:

Security Network ACL Rate [<rate_limiter_list>] [<rate_unit>] [<rate>]

Parameters:

<rate_limiter_list>: Rate limiter list (1-16), default: All rate limiters
<rate_unit> : IP flags: pps|kbps, default: pss
<rate> : Rate in pps (0-100) or kbps (0, 100, 2*100, 3*100, ..., 1000000)

Default Setting:

1

Example:

Set rate limit value in 100 for port 1

```
NS3550-8T-2S:/>security network acl rate 1 100
```

Security Network ACL Add

Description:

Add or modify Access Control Entry (ACE).

If the ACE ID parameter <ace_id> is specified and an entry with this ACE ID already exists, the ACE will be modified. Otherwise, a new ACE will be added. If the ACE ID is not specified, the next available ACE ID will be used.

If the next ACE ID parameter <ace_id_next> is specified, the ACE will be placed before this ACE in the list. If the next ACE ID is not specified, the ACE will be placed last in the list.

If the Switch keyword is used, the rule applies to all ports.
If the Port keyword is used, the rule applies to the specified port only. If the Policy keyword is used, the rule applies to all ports configured with the specified policy. The default is that the rule applies to all ports.

Syntax:

Security Network ACL Add [<ace_id>] [<ace_id_next>] [switch | (port <port_list>) | (policy <policy>)] [<tagged>] [<vid>] [<tag_prio>] [<dmac_type>] [(etype [<etype>] [<smac>] [<dmac>]) | (arp [<sip>] [<dip>] [<smac>] [<arp_opcode>] [<arp_flags>]) | (ip [<sip>] [<dip>] [<protocol>] [<ip_flags>]) | (icmp [<sip>] [<dip>] [<icmp_type>] [<icmp_code>] [<ip_flags>]) | (udp [<sip>] [<dip>] [<sport>] [<dport>] [<ip_flags>]) | (tcp [<sip>] [<dip>] [<sport>] [<dport>] [<ip_flags>] [<tcp_flags>])] [permit|deny] [<rate_limiter>] [<port_copy>] [<mirror>] [<logging>] [<shutdown>]

Parameters:

<ace_id> : ACE ID (1-256), default: Next available ID
<ace_id_next> : Next ACE ID (1-256), default: Add ACE last
switch : Switch ACE keyword
port : Port ACE keyword
<port_list> : Port list or 'all', default: All ports
policy : Policy ACE keyword
<policy> : Policy number (1-8)
<tagged> : Tagged of frames: any|enable|disable
<vid> : VLAN ID (1-4095) or 'any'
<tag_prio> : VLAN tag priority (0-7) or 'any'
<dmac_type> : DMAC type: any|unicast|multicast|broadcast
etype : Ethernet Type keyword
<etype> : Ethernet Type: 0x600 - 0xFFFF or 'any' but excluding, 0x800(IPv4) 0x806(ARP) and 0x86DD(IPv6)
<smac> : Source MAC address (xx-xx-xx-xx-xx-xx) or 'any'
<dmac> : Destination MAC address (xx-xx-xx-xx-xx-xx) or 'any'
arp : ARP keyword
<sip> : Source IP address (a.b.c.d/n) or 'any'
<dip> : Destination IP address (a.b.c.d/n) or 'any'
<arp_opcode> : ARP operation code: any|arp|rarp|other
<arp_flags> : ARP flags: request|smac|tmac|len|ip|ether [0|1|any]
ip : IP keyword
<protocol> : IP protocol number (0-255) or 'any'
<ip_flags> : IP flags: ttl|options|fragment [0|1|any]
icmp : ICMP keyword
<icmp_type> : ICMP type number (0-255) or 'any'
<icmp_code> : ICMP code number (0-255) or 'any'
udp : UDP keyword
<sport> : Source UDP/TCP port range (0-65535) or 'any'
<dport> : Destination UDP/TCP port range (0-65535) or 'any'
tcp : TCP keyword
<tcp_flags> : TCP flags: fin|syn|rst|psh|ack|urg [0|1|any]
permit : Permit forwarding (default)
deny : Deny forwarding
<rate_limiter>: Rate limiter number (1-15) or 'disable'
<port_copy> : Port list for copy of frames or 'disable'
<mirror> : Mirror of frames: enable|disable
<logging> : System logging of frames: log|log_disable
<shutdown> : Shut down ingress port: shut|shut_disable

Security Network ACL Delete

Description:

Delete ACE.

Syntax:

Security Network ACL Delete <ace_id>

Parameters:

<ace_id>: ACE ID (1-256)

Example:

Delete ACE 1

```
NS3550-8T-2S:/>security network acl delete 1
```

Security Network ACL Lookup

Description:

Show ACE, default: All ACEs.

Syntax:

Security Network ACL Lookup [<ace_id>]

Parameters:

<ace_id>: ACE ID (1-256)

Example:

Lookup ACE 1

```
NS3550-8T-2S:/>security network acl lookup 1
```

Security Network ACL Clear

Description:

Clear all ACL counters.

Syntax:

Security Network ACL Clear

Example:

Clear all ACL counters.

```
NS3550-8T-2S:/>security network acl clear
```

Security Network ACL Status

Description:

Show ACL status.

Syntax:

Security Network ACL Status [combined|static|dhcp|upnp|arp_inspection|ipmc|ip_source_guard|conflicts]

Parameters:

combined : Shows the combined status
static : Shows the static user configured status
dhcp : Shows the status by DHCP
upnp : Shows the status by UPnP
arp_inspection : Shows the status by ARP Inspection
ip_source_guard : Shows the status by IP Source Guard
conflicts : Shows all conflict status
(default : Shows the combined status)

Example:

Show ACL status.

```
NS3550-8T-2S:/>security network acl status
```

Security Network DHCP Relay Configuration

Description:

Show DHCP relay configuration.

Syntax:

Security Network DHCP Relay Configuration

Example:

Show DHCP relay configuration.

```
NS3550-8T-2S:/>security network dhcp relay configuration

DHCP Relay Configuration:
=========================

DHCP Relay Mode                  : Disabled
DHCP Relay Server                : NULL
DHCP Relay Information Mode      : Disabled
DHCP Relay Information Policy : replace
```

Security Network DHCP Relay Mode

Description:

Set or show the DHCP relay mode.

Syntax:

Security Network DHCP Relay Mode [enable|disable]

Parameters:

enable : Enable DHCP relaly mode.
When enable DHCP relay mode operation, the agent forward and to transfer DHCP messages between the clients and the server when they are not on the same subnet domain. And the DHCP broadcast message won't flood for security considered.
disable: Disable DHCP relaly mode
(default: Show flow DHCP relaly mode)

Default Setting:

disable

Example:

Enable DHCP relay mode

```
NS3550-8T-2S:/>security network dhcp relay mode enable
```

Security Network DHCP Relay Server

Description:

Show or set DHCP relay server.

Syntax:

Security Network DHCP Relay Server [<ip_addr>]

Parameters:

<ip_addr>: IP address (a.b.c.d), default: Show IP address

Default Setting:

null

Example:

Set DHCP relay server in 192.168.0.20

```
NS3550-8T-2S:/>security network dhcp relay server 192.168.0.20
```

Security Network DHCP Relay Information Mode

Description:

Set or show DHCP relay agent information option mode.
When enable DHCP relay information mode operation, the agent insert specific information (option 82) into a DHCP message when forwarding to DHCP server and remote it from a DHCP message when transferring to DHCP client. It only works under DHCP relay operation mode enabled.

Syntax:

Security Network DHCP Relay Information Mode [enable|disable]

Parameters:

enable : Enable DHCP relay agent information option mode
disable: Disable DHCP relay agent information option mode
(default: Show DHCP relay agent information option mode)

Default Setting:

disable

Example:

Enable DHCP relay agent information option mode.

```
NS3550-8T-2S:/>security network dhcp relay information mode enable
```

Security Network DHCP Relay Information Policy

Description:

Set or show the DHCP relay mode.
When enable DHCP relay information mode operation, if agent receive a DHCP message that already contains relay agent information. It will enforce the policy.

Syntax:

Security Network DHCP Relay Information Policy [replace|keep|drop]

Parameters:

replace : Replace the original relay information when receive a DHCP message that already contains it
keep : Keep the original relay information when receive a DHCP message that already contains it
drop : Drop the package when receive a DHCP message that already contains relay information
(default: Show DHCP relay information policy)

Default Setting:

replace

Example:

Keep the original relay information when receive a DHCP message that already contains it

```
NS3550-8T-2S:/>security network dhcp relay information policy keep
```

Security Network DHCP Relay Statistics

Description:

Show or clear DHCP relay statistics.

Syntax:

Security Network DHCP Relay Statistics [clear]

Parameters:

clear: Clear DHCP relay statistics

Example:

Show DHCP relay statistics.

```
NS3550-8T-2S:/>security network dhcp relay statistics
```

Security Network DHCP Snooping Configuration

Description:

Show DHCP snooping configuration.

Syntax:

Security Network DHCP Snooping Configuration

Security Network DHCP Snooping Mode

Description:

Set or show the DHCP snooping mode.

Syntax:

Security Network DHCP Snooping Mode [enable|disable]

Parameters:

enable : Enable DHCP snooping mode.
When enable DHCP snooping mode operation, the request DHCP messages will be forwarded to trusted ports

and only allowed reply packets from trusted ports.
disable: Disable DHCP snooping mode
(default: Show flow DHCP snooping mode)

Default Setting:
disable

Example:
Enable DHCP snooping mode

```
NS3550-8T-2S:/>security network dhcp snooping mode enable
```

Security Network DHCP Snooping Port Mode

Description:
Set or show the DHCP snooping port mode.

Syntax:
Security Network DHCP Snooping Port Mode [<port_list>] [trusted|untrusted]

Parameters:
<port_list>: Port list or 'all', default: All ports
trusted : Configures the port as trusted sources of the DHCP message
untrusted: Configures the port as untrusted sources of the DHCP message
(default: Show flow DHCP snooping port mode)

Default Setting:
trusted

Example:
Set untrusted DHCP snooping port mode in port 1

```
NS3550-8T-2S:/>security network dhcp snooping port mode 1 untrusted
```

Security Network DHCP Snooping Statistics

Description:
Show or clear DHCP snooping statistics.

Syntax:
Security Network DHCP Snooping Statistics [<port_list>] [clear]

Parameters:
<port_list>: Port list or 'all', default: All ports
clear : Clear DHCP snooping statistics

Example:
Show DHCP snooping statistics of port 1.

```
NS3550-8T-2S:/>security network dhcp snooping statistics 1
Port 1 Statistics:
--------------------
Rx Discover:                0     Tx Discover:                0
Rx Offer:                   0     Tx Offer:                   0
Rx Request:                 0     Tx Request:                 0
Rx Decline:                 0     Tx Decline:                 0
Rx ACK:                     0     Tx ACK:                     0
Rx NAK:                     0     Tx NAK:                     0
Rx Release:                 0     Tx Release:                 0
Rx Inform:                  0     Tx Inform:                  0
Rx Lease Query:             0     Tx Lease Query:             0
Rx Lease Unassigned:        0     Tx Lease Unassigned:        0
Rx Lease Unknown:           0     Tx Lease Unknown:           0
Rx Lease Active:            0     Tx Lease Active:            0
```

Security Network IP Source Guard Configuration

Description:
Show IP source guard configuration.

Syntax:
Security Network IP Source Guard Configuration

Security Network IP Source Guard Mode

Description:
Set or show IP source guard mode.

Syntax:
Security Network IP Source Guard Mode [enable|disable]

Parameters:
enable : Enable IP Source Guard
disable: Disable IP Source Guard

Default Setting:
disable

Example:

Enable IP source guard mode

```
NS3550-8T-2S:/>security network ip source guard mode enable
```

Security Network IP Source Guard Port Mode

Description:

Set or show the IP Source Guard port mode.

Syntax:

Security Network IP Source Guard Port Mode [<port_list>] [enable|disable]

Parameters:

<port_list>: Port list or 'all', default: All ports
enable : Enable IP Source Guard port
disable : Disable IP Source Guard port
(default: Show IP Source Guard port mode)

Default Setting:

disable

Example:

Enable IP source guard port mode for port1~4

```
NS3550-8T-2S:/>security network ip source guard port mode 1-4 enable
```

Security Network IP Source Guard Limit

Description:

Set or show the IP Source Guard port limitation for dynamic entries.

Syntax:

Security Network IP Source Guard limit [<port_list>] [<dynamic_entry_limit>|unlimited]

Parameters:

<port_list> : Port list or 'all', default: All ports
<dynamic_entry_limit>|unlimited: dynamic entry limit (0-2) or unlimited

Default Setting:

unlimited

Example:

Set IP source guard limit

```
NS3550-8T-2S:/>security network ip source guard 1 1
```

Security Network IP Source Guard Entry

Description:

Add or delete IP source guard static entry.

Syntax:

Security Network IP Source Guard Entry [<port_list>] add|delete <vid> <allowed_ip> <allowed_mac>

Parameters:

<port_list> : Port list or 'all', default: All ports
add : Add new port IP source guard static entry
delete : Delete existing port IP source guard static entry
<vid> : VLAN ID (1-4095)
<allowed_ip> : IP address (a.b.c.d), IP address allowed for doing IP source guard
<allowed_mac>: MAC address (xx-xx-xx-xx-xx-xx), MAC address allowed for doing IP source guard

Example:

Add IP source guard static entry.

```
NS3550-8T-2S:/>security network ip source guard entry 1 add 1 192.168.0.20
```

Security Network IP Source Guard Status

Description:
Show IP source guard static and dynamic entries.

Syntax:
Security Network IP Source Guard Status [<port_list>]

Parameters:
<port_list>: Port list or 'all', default: All ports

Example:
Show IP source guard static and dynamic entries.

```
NS3550-8T-2S:/>security network ip source guard status
```

Security Network ARP Inspection Configuration

Description:
Show ARP inspection configuration.

Syntax:
Security Network ARP Inspection Configuration

Example:
Show ARP inspection configuration.

```
NS3550-8T-2S:/>security network arp inspection configuration
```

Security Network ARP Inspection Mode

Description:
Set or show ARP inspection mode.

Syntax:
Security Network ARP Inspection Mode [enable|disable]

Parameters:
enable : Enable ARP Inspection
disable: Disable ARP Inspection

Default Setting:
disable

Example:
Enable ARP inspection mode

```
NS3550-8T-2S:/>security network arp inspection mode enable
```

Security Network ARP Inspection Port Mode

Description:
Set or show the ARP Inspection port mode.

Syntax:
Security Network ARP Inspection Port Mode [<port_list>] [enable|disable]

Parameters:
<port_list>: Port list or 'all', default: All ports
enable : Enable ARP Inspection port

disable : Disable ARP Inspection port
(default: Show ARP Inspection port mode)

Default Setting:
Disable

Example:
Enable the ARP inspection mode of port 1

```
NS3550-8T-2S:/>security network arp inspection port mode 1
```

Security Network ARP Inspection Entry

Description:
Add or delete ARP inspection static entry.

Syntax:
Security Network ARP Inspection Entry [<port_list>] add|delete <vid> <allowed_mac> <allowed_ip>

Parameters:
<port_list> : Port list or 'all', default: All ports
add : Add new port ARP inspection static entry
delete : Delete existing port ARP inspection static entry
<vid> : VLAN ID (1-4095)
<allowed_mac>: MAC address (xx-xx-xx-xx-xx-xx), MAC address allowed for doing ARP request
<allowed_ip> : IP address (a.b.c.d), IP address allowed for doing ARP request

Example:
Add ARP inspection static entry.

```
NS3550-8T-2S:/>security network arp inspection entry 1 add 1 00-30-4f-00-00-11 192.168.0.11
```

Security Network ARP Inspection Status

Description:
Show ARP inspection static and dynamic entries.

Syntax:
Security Network ARP Inspection Status [<port_list>]

Parameters:
<port_list>: Port list or 'all', default: All ports

Example:
Show ARP inspection static and dynamic entries.

```
NS3550-8T-2S:/>security network arp inspection status
```

Security AAA Configuration

Description:
Show Auth configuration.

Syntax:
Security AAA Configuration

Example:
Show Auth configuration.

```
NS3550-8T-2S:/>security aaa configuration

AAA Configuration:
==================
```

```
Server Timeout     : 15 seconds

Server Dead Time : 300 seconds

RADIUS Authentication Server Configuration:
===========================================
Server   Mode        IP Address          Secret                          Port
------   --------    ---------------     ------------------------------  -----
1        Disabled                                                        1812
2        Disabled                                                        1812
3        Disabled                                                        1812
4        Disabled                                                        1812
5        Disabled                                                        1812

RADIUS Accounting Server Configuration:
=======================================
Server   Mode        IP Address          Secret                          Port
------   --------    ---------------     ------------------------------  -----
1        Disabled                                                        1813
2        Disabled                                                        1813
3        Disabled                                                        1813
4        Disabled                                                        1813
5        Disabled                                                        1813

TACACS+ Authentication Server Configuration:
============================================
Server   Mode        IP Address          Secret                          Port
------   --------    ---------------     ------------------------------  -----
1        Disabled                                                          49
2        Disabled                                                          49
3        Disabled                                                          49
4        Disabled                                                          49
5        Disabled                                                          49
```

Security AAA Timeout

Description:

Set or show server timeout.

Syntax:

Security AAA Timeout [<timeout>]

Parameters:

<timeout>: Server response timeout (3-3600 seconds)
(default: Show server timeout configuration)

Default Setting:

15

Example:

Set 30sec for server timeout

```
NS3550-8T-2S:/>security aaa timeout 30
```

Security AAA Deadtime

Description:

Set or show server dead time.

Syntax:

Security AAA Deadtime [<dead_time>]

Parameters:

<dead_time>: Time that a server is considered dead if it doesn't answer a request (0-3600 seconds)
(default: Show server dead time configuration)

Default Setting:

300

Example:

Set 1000sec for server dead time

```
NS3550-8T-2S:/>security aaa deadtime 1000
```

Security AAA RADIUS

Description:

Set or show RADIUS authentication server setup.

Syntax:

Security AAA RADIUS [<server_index>] [enable|disable] [<ip_addr_string>] [<secret>] [<server_port>]

Parameters:

The server index (1-5)
(default: Show RADIUS authentication server configuration)
enable : Enable RADIUS authentication server
disable : Disable RADIUS authentication server
(default: Show RADIUS server mode)
<ip_addr_string>: IP host address (a.b.c.d) or a host name string
<secret> : Secret shared with external authentication server.
To set an empty secret, use two quotes ("").
To use spaces in secret, enquote the secret.
Quotes in the secret are not allowed.
<server_port> : Server UDP port. Use 0 to use the default RADIUS port (1812)

Example:

Set RADIUS authentication server configuration.

```
NS3550-8T-2S:/>security aaa radius 1 enable 192.168.0.20 12345678 1812
```

Security AAA ACCT_RADIUS

Description:

Set or show RADIUS accounting server setup.

Syntax:

Security AAA ACCT_RADIUS [<server_index>] [enable|disable] [<ip_addr_string>] [<secret>] [<server_port>]

Parameters:

The server index (1-5)
(default: Show RADIUS accounting server configuration)
enable : Enable RADIUS accounting server
disable : Disable RADIUS accounting server
(default: Show RADIUS server mode)
<ip_addr_string>: IP host address (a.b.c.d) or a host name string
<secret> : Secret shared with external accounting server.
To set an empty secret, use two quotes ("").
To use spaces in secret, enquote the secret.
Quotes in the secret are not allowed.
<server_port> : Server UDP port. Use 0 to use the default RADIUS port (1813)

Example:

Set RADIUS accounting server configuration.

```
NS3550-8T-2S:/>security acct_radius 1 enable 192.168.0.20 12345678 1813
```

Security AAA TACACS+

Description:

Set or show TACACS+ authentication server setup.

Syntax:

Security AAA TACACS+ [<server_index>] [enable|disable] [<ip_addr_string>] [<secret>] [<server_port>]

Parameters:

The server index (1-5)
(default: Show TACACS+ authentication server configuration)
enable : Enable TACACS+ authentication server
disable : Disable TACACS+ authentication server
(default: Show TACACS+ server mode)
<ip_addr_string>: IP host address (a.b.c.d) or a host name string
<secret> : Secret shared with external authentication server.
To set an empty secret, use two quotes ("").
To use spaces in secret, enquote the secret.
Quotes in the secret are not allowed.
<server_port> : Server TCP port. Use 0 to use the default TACACS+ port (49)

Example:

Set TACACS+ authentication server configuration.

```
NS3550-8T-2S:/>security aaa tacacs+ 1 enable 192.168.0.20 12345678 49
```

Security AAA Statistics

Description:

Show RADIUS statistics.

Syntax:

Security AAA Statistics [<server_index>]

Parameters:

The server index (1-5)
(default: Show statistics for all servers)

Example:

Show RADIUS statistics.

```
NS3550-8T-2S:/>security aaa statistics
```

6.8 Spanning Tree Protocol Command

STP Configuration

Description:

Show STP configuration.

Syntax:

STP Configuration

Example:

Show STP configuration.

```
NS3550-8T-2S:/>stp cofiguration
```

```
STP Configuration:
==================

Protocol Version: MSTP
Max Age             : 20
Forward Delay       : 15
Tx Hold Count       : 6
Max Hop Count       : 20
BPDU Filtering      : Disabled
BPDU Guard          : Disabled
Error Recovery      : Disabled
```

STP Version

Description:
Set or show the STP Bridge protocol version.
Syntax:
STP Version [<stp_version>]

Parameters:
<stp_version>: mstp|rstp|stp

Default Setting:
MSTP
Example:
Set the STP Bridge protocol version.

```
NS3550-8T-2S:/> stp version rstp
```

STP Tx Hold

Description:
Set or show the STP Bridge Transmit Hold Count parameter.

Syntax:
STP Txhold [<holdcount>]

Parameters:
<holdcount>: STP Transmit Hold Count (1-10)

Default Setting:
6

Example:
Set STP Tx hold in 10

```
NS3550-8T-2S:/>stp txhold 10
```

STP MaxHops

Description:
Set or show the MSTP Bridge Max Hop Count parameter.
Syntax:
STP MaxHops [<maxhops>]

Parameters:
<maxhops>: STP BPDU MaxHops (6-40))
Default Setting:
20

Example:
Set STP maximum hops in 25

```
NS3550-8T-2S:/>stp maxhops 25
```

STP MaxAge

Description:
Set or show the bridge instance maximum age.

Syntax:
STP MaxAge [<max_age>]

Parameters:
<max_age>: STP maximum age time (6-40, and max_age <= (forward_delay-1)*2)

Default Setting:
20

Example:
Set STP maximum age time in 10

```
NS3550-8T-2S:/>stp maxage 10
```

STP FwdDelay

Description:
Set or show the CIST/MSTI bridge forward delay.

Syntax:
STP FwdDelay [<delay>]

Parameters:
<delay>: MSTP forward delay (4-30, and max_age <= (forward_delay-1)*2))

Default Setting:
15

Example:
Set STP forward delay value in 25

```
NS3550-8T-2S:/>stp fwddelay 25
```

STP CName

Description:
Set or Show MSTP configuration name and revision.

Syntax:
STP CName [<config-name>] [<integer>]

Parameters:
<config-name>: MSTP Configuration name. A text string up to 32 characters long.
Use quotes (") to embed spaces in name.
<integer> : Integer value

Default Setting:
Configuration name: MAC address
Configuration rev.: 0

Example:
Set MSTP configuration name and revision.

```
NS3550-8T-2S:/>stp cname 9f_NS3550-8T-2S 1
```

STP BPDU Filter

Description:
Set or show edge port BPDU Filtering.

Syntax:

STP bpduFilter [enable|disable]

Parameters:

enable|disable: enable or disable BPDU Filtering for Edge ports

Default Setting:
Disable

Example:
Set edge port BPDU filtering

```
NS3550-8T-2S:/>stp bpdufilter enable
```

STP BPDU Guard

Description:
Set or show edge port BPDU Guard.

Syntax:
STP bpduGuard [enable|disable]

Parameters:
enable|disable: enable or disable BPDU Guard for Edge ports

Default Setting:
Disable

Example:
Set edge port BPDU guard

```
NS3550-8T-2S:/>stp bpduguard enable
```

STP Recovery

Description:
Set or show edge port error recovery timeout.

Syntax:
STP recovery [<timeout>]

Parameters:
<timeout>: Time before error-disabled ports are reenabled (30-86400 seconds, 0 disables)
(default: Show recovery timeout)

Default Setting:
Disable

Example:
Set STP recovery value in 30 sec.

```
NS3550-8T-2S:/>stp recovery 30
```

STP Status

Description:
Show STP Bridge status.

Syntax:
STP Status [<msti>] [<port_list>]

Parameters:
<msti> : STP bridge instance no (0-7, CIST=0, MSTI1=1, ...)
<port_list>: Port list or 'all', default: All ports

Default Setting:
Disable

Example:
Show STP Bridge status.

```
NS3550-8T-2S:/>stp status
CIST Bridge STP Status
Bridge ID      : 80:00-00:30:4F:24:04:D1
Root ID        : 80:00-00:30:4F:24:04:D1
Root Port      : -
Root PathCost: 0
Regional Root: 80:00-00:30:4F:24:04:D1
Int. PathCost: 0
Max Hops       : 20
TC Flag        : Steady
TC Count       : 0
TC Last        : -
Port        Port Role         State         Pri   PathCost   Edge   P2P   Uptime
---------   --------------    ----------    ---   --------   ----   ---   -------------
10          DesignatedPort    Forwarding    128   20000       Yes    Yes   0d 00:10:32
```

STP MSTI Priority

Description:
Set or show the bridge instance priority.

Syntax:
STP Msti Priority [<msti>] [<priority>]

Parameters:
<msti> : STP bridge instance no (0-7, CIST=0, MSTI1=1, ...)
<priority> : STP bridge priority (0/16/32/48/.../224/240)

Default:
128

Example:
Set MST1 priority value in 48.

```
NS3550-8T-2S:/>stp msti priority 1 48
```

STP MSTI Map

Description:
Show or clear MSTP MSTI VLAN mapping configuration.

Syntax:
STP Msti Map [<msti>] [clear]

Parameters:
<msti>: STP bridge instance no (0-7, CIST=0, MSTI1=1, ...)
Clear : Clear VID to MSTI mapping

Example:
Add MST1 priority value in 48.

```
NS3550-8T-2S:/>stp msti priority 1 48
```

STP MSTI Add

Description:
Add a VLAN to a MSTI.

Syntax:
STP Msti Add <msti> <vid>

Parameters:
<msti>: STP bridge instance no (0-7, CIST=0, MSTI1=1, ...)
<vid> : VLAN ID (1-4095)

Example:
Add MST1 in vlan1.

```
NS3550-8T-2S:/>stp msti add 1 1
```

STP Port Configuration

Description:
Show STP Port configuration.

Syntax:
STP Port Configuration [<port_list>]

Parameters:
<port_list>: Port list or 'all'. Port zero means aggregations.

Example:
Show STP status of Port1

```
NS3550-8T-2S:/>stp port configuration 1

Port   Mode         AdminEdge AutoEdge   restrRole restrTcn   Point2point
----   ---------    ----------------     ----------------     -----------
1      Disabled   Disabled   Enabled     Disabled   Disabled   Auto
```

STP Port Mode

Description:
Set or show the STP enabling for a port.

Syntax:
STP Port Mode [<port_list>] [enable|disable]

Parameters:
<port_list>: Port list or 'all'. Port zero means aggregations.
Enable : Enable MSTP protocol
Disable : Disable MSTP protocol

Default:
disable

Example:

Enable STP function on port1

```
NS3550-8T-2S:/>stp port mode 1 enable
```

STP Port Edge

Description:

Set or show the STP adminEdge port parameter.

Syntax:

STP Port Edge [<port_list>] [enable|disable]

Parameters:

<port_list>: Port list or 'all', default: All ports
Enable : Configure MSTP adminEdge to Edge
Disable : Configure MSTP adminEdge to Non-edge

Default:

disable

Example:

Enable STP edge function on port1

```
NS3550-8T-2S:/>stp port edge 1 enable
```

STP Port AutoEdge

Description:

Set or show the STP autoEdge port parameter.

Syntax:

STP Port AutoEdge [<port_list>] [enable|disable]

Parameters:

<port_list>: Port list or 'all', default: All ports
Enable : Enable MSTP autoEdge
Disable : Disable MSTP autoEdge

Default:

enable

Example:

Disable STP edge function on port1

```
NS3550-8T-2S:/>stp port autoedge 1 disable
```

STP Port P2P

Description:

Set or show the STP point2point port parameter.

Syntax:

STP Port P2P [<port_list>] [enable|disable|auto]

Parameters:

<port_list>: Port list or 'all', default: All ports
enable : Enable MSTP point2point
disable : Disable MSTP point2point
auto : Automatic MSTP point2point detection

Default:
auto

Example:
Disable STP P2P function on port1

```
NS3550-8T-2S:/>stp port p2p 1 disable
```

STP Port RestrictedRole

Description:
Set or show the MSTP restrictedRole port parameter.

Syntax:
STP Port RestrictedRole [<port_list>] [enable|disable]

Parameters:
<port_list>: Port list or 'all', default: All ports
enable : Enable MSTP restricted role
disable : Disable MSTP restricted role

Default:
disable

Example:
Eisable STP restricted role on port1

```
NS3550-8T-2S:/>stp port restrictedrole 1 enable
```

STP Port RestrictedTcn

Description:
Set or show the MSTP restrictedTcn port parameter.

Syntax:
STP Port RestrictedTcn [<port_list>] [enable|disable]

Parameters:

<port_list>: Port list or 'all', default: All ports
enable : Enable MSTP restricted TCN
disable : Disable MSTP restricted TCN

Default:

disable

Example:

Eisable STP restricted TCN on port1

```
NS3550-8T-2S:/>stp port restrictedtcn 1 enable
```

STP Port bpduGuard

Description:

Set or show the bpduGuard port parameter.

Syntax:

STP Port bpduGuard [<port_list>] [enable|disable]

Parameters:

<port_list>: Port list or 'all', default: All ports
enable : Enable port BPDU Guard
disable : Disable port BPDU Guard

Default:

disable

Example:

Eisable BPDU guard on port1

```
NS3550-8T-2S:/>stp port bpduguard 1 enable
```

STP Port Statistic

Description:

Show STP port statistics.

Syntax:

STP Port Statistics [<port_list>] [clear]

Parameters:

<port_list>: Port list or 'all', default: All ports
clear : Clear the selected port statistics

Example:

Show STP port statistics.

```
NS3550-8T-2S:/>stp port statistics
Port          Rx MSTP    Tx MSTP    Rx RSTP    Tx RSTP    Rx STP     Tx STP     Rx TCN
Tx TCN    Rx III.   Rx Unk.
----------  --------  --------  --------  --------  -------  -------  -------  -------  -------  -------
```

STP Port Mcheck

Description:

Set the STP mCheck (Migration Check) variable for ports.

Syntax:

STP Port Mcheck [<port_list>]

Parameters:

<port_list>: Port list or 'all', default: All ports

Example:

Set the STP mCheck (Migration Check) variable for port 1.

```
NS3550-8T-2S:/>stp port mcheck 1
```

STP MSTI Port Configuration

Description:

Show the STP port instance configuration.

Syntax:

STP Msti Port Configuration [<msti>] [<port_list>]

Parameters:
<msti> : STP bridge instance no (0-7, CIST=0, MSTI1=1, ...)
<port_list>: Port list or 'all', default: All ports
Default:
auto

STP MSTI Port Cost

Description:
Set or show the STP port instance path cost.

Syntax:
STP Msti Port Cost [<msti>] [<port_list>] [<path_cost>]

Parameters:
<msti> : STP bridge instance no (0-7, CIST=0, MSTI1=1, ...)
<port_list>: Port list or 'all'. Port zero means aggregations.
<path_cost>: STP port path cost (1-200000000) or 'auto'

Default:
auto

Example:
Set MSTI7 in port1

```
NS3550-8T-2S:/>stp msti port cost 7 1

MSTI   Port   Path Cost
----   ----   ----------
MST7   1      Auto
```

STP MSTI Port Priority

Description:
Set or show the STP port instance priority.

Syntax:
STP Msti Port Priority [<msti>] [<port_list>] [<priority>]

Parameters:
<msti> : STP bridge instance no (0-7, CIST=0, MSTI1=1, ...)
<port_list>: Port list or 'all'. Port zero means aggregations.
<priority> : STP port priority (0/16/32/48/.../224/240)

Default:
128

6.9 Link Aggregation Command

Aggregation Configuration

Description:
Show link aggregation configuration.

Syntax:
Aggr Configuration

Aggregation Add

Description:
Add or modify link aggregation.

Syntax:
Aggr Add <port_list> [<aggr_id>]

Parameters:

<port_list>: Port list or 'all', default: All ports
<aggr_id> : Aggregation ID

Example:

Add port 1~4 in Group1

```
NS3550-8T-2S:/>aggr add 1-4 1
```

Aggregation Delete

Description:

Delete link aggregation.

Syntax:
Aggr Delete <aggr_id>

Parameters:
<aggr_id>: Aggregation ID

Example:
Delete Group2

```
NS3550-8T-2S:/>aggr delete 2
```

Aggregation Lookup

Description:
Lookup link aggregation.

Syntax:
Aggr Lookup [<aggr_id>]

Parameters:
<aggr_id>: Aggregation ID

Aggregation Mode

Description:
Set or show the link aggregation traffic distribution mode.

Syntax:
Aggr Mode [smac|dmac|ip|port] [enable|disable]

Parameters:
smac : Source MAC address
dmac : Destination MAC address
ip : Source and destination IP address
port : Source and destination UDP/TCP port
enable : Enable field in traffic distribution
disable: Disable field in traffic distribution

Default Setting:

SMAC : Enabled
DMAC : Disabled
IP : Enabled
Port : Enabled

Example:

Disable SMAC mode

```
NS3550-8T-2S:/>Aggr mode smac disable
```

6.10 Link Aggregation Control Protocol Command

LACP Configuration

Description:

Show LACP configuration.

Syntax:

LACP Configuration [<port_list>]

Parameters:

<port_list>: Port list or 'all', default: All ports

Example:

Show LACP configuration

```
NS3550-8T-2S:/>lacp configuration

Port   Mode       Key    Role
----   --------   ----   ------
1      Disabled   Auto   Active
2      Disabled   Auto   Active
3      Disabled   Auto   Active
4      Disabled   Auto   Active
5      Disabled   Auto   Active
6      Disabled   Auto   Active
7      Disabled   Auto   Active
8      Disabled   Auto   Active
9      Disabled   Auto   Active
10     Disabled   Auto   Active
```

LACP Mode

Description:

Set or show LACP mode.

Syntax:

LACP Mode [<port_list>] [enable|disable]

Parameters:

<port_list>: Port list or 'all', default: All ports
enable : Enable LACP protocol
disable: Disable LACP protocol
(default: Show LACP mode)

Default Setting:

disable

Example:

Enable LACP for port1~4

```
NS3550-8T-2S:/>lacp mode 1-4 enable
```

LACP Key

Description:

Set or show the LACP key.

Syntax:
LACP Key [<port_list>] [<key>]

Parameters:
<port_list>: Port list or 'all', default: All ports
<key> : LACP key (1-65535) or 'auto'

Default Setting:
auto

Example:
Set key1 for port1~4

```
NS3550-8T-2S:/>lacp key 1-4 1
```

LACP Role

Description:
Set or show the LACP role.

Syntax:
LACP Role [<port_list>] [active|passive]

Parameters:
<port_list>: Port list or 'all', default: All ports
active : Initiate LACP negotiation
passive: Listen for LACP packets
(default: Show LACP role)

Default Setting:
active

Example:
Set passive for port1~4

```
NS3550-8T-2S:/>lacp role 1-4 passive
```

LACP Status

Description:
Show LACP Status.

Syntax:
LACP Status [<port_list>]

Parameters:
<port_list>: Port list or 'all', default: All ports

Example:
Show LACP status of port1~4

```
NS3550-8T-2S:/>lacp status 1-4

Port   Mode         Key      Aggr ID   Partner System ID   Partner Port
----   --------     -----    -------   -----------------   ------------
1      Disabled     1        -         -                   -
2      Disabled     1        -         -                   -
3      Disabled     1        -         -                   -
4      Disabled     1        -         -                   -
```

LACP Statistics

Description:
Show LACP Statistics.

Syntax:

LACP Statistics [<port_list>] [clear]

Parameters:

<port_list>: Port list or 'all', default: All ports
clear **:** Clear LACP statistics

Example:

Show LACP statistics of port1~4

```
NS3550-8T-2S:/>lacp statistics 1-4

Port   Rx Frames     Tx Frames     Rx Unknown    Rx Illegal
------ ----------    ----------    ----------    ----------
1      0             0             0             0
2      0             0             0             0
3      0             0             0             0
4      0             0             0             0
```

6.11 LLDP Command

LLDP Configuration

Description:
Show LLDP configuration.

Syntax:
LLDP Configuration [<port_list>]

Parameters:
<port_list>: Port list or 'all', default: All ports

Example:
Show LLDP configuration of port1~4

```
NS3550-8T-2S:/>lldp configuration 1-4

LLDP Configuration:
===================

Interval      : 30
Hold          : 3
Tx Delay      : 2
Reinit Delay: 2

Port Mode       Port Descr System Name System Descr System Capa Mgmt Addr CDP awareness
---- --------   ---------- ----------- ------------ ----------- --------- -------------
1    Enabled    Enabled    Enabled     Enabled      Enabled     Enabled   Disabled
2    Enabled    Enabled    Enabled     Enabled      Enabled     Enabled   Disabled
3    Enabled    Enabled    Enabled     Enabled      Enabled     Enabled   Disabled
4    Enabled    Enabled    Enabled     Enabled      Enabled     Enabled   Disabled
```

LLDP Mode

Description:
Set or show LLDP mode.

Syntax:
LLDP Mode [<port_list>] [enable|disable|rx|tx]

Parameters:
<port_list>: Port list or 'all', default: All ports
enable : Enable LLDP reception and transmission
disable: Disable LLDP
rx : Enable LLDP reception only
tx : Enable LLDP transmission only
(default: Show LLDP mode)

Default Setting:
disable

Example:
Enable port1 LLDP function.

```
NS3550-8T-2S:/>lldp mode 1 enable
```

LLDP Optional TLV

Description:
Show or Set LLDP Optional TLVs.

Syntax:
LLDP Optional_TLV [<port_list>] [port_descr|sys_name|sys_descr|sys_capa|mgmt_addr] [enable|disable]

Parameters:
<port_list>: Port list or 'all', default: All ports

port_descr : Description of the port
sysm_name : System name
sys_descr : Description of the system
sys_capa : System capabilities
mgmt_addr : Master's IP address
(default: Show optional TLV's configuration)
enable : Enables TLV
disable : Disable TLV
(default: Show optional TLV's configuration)

Default Setting:
Description of the port: Enable
System name: Enable
Description of the system: Enable
System capabilities: Enable
Master's IP address: Enable

Example:
Disable description of the port for port1

```
NS3550-8T-2S:/>lldp optional_tlv 1 port_descr disable
```

LLDP Interval

Description:
Set or show LLDP Tx interval.

Syntax:
LLDP Interval [<interval>]

Parameters:
<interval>: LLDP transmission interval (5-32768)

Default Setting:
30

Example:
Set transmission interval in 10

```
NS3550-8T-2S:/>lldp interval 10
```

LLDP Hold

Description:
Set or show LLDP Tx hold value.

Syntax:
LLDP Hold [<hold>]

Parameters:
<hold>: LLDP hold value (2-10)

Default Setting:
3

Example:
Set LLDP hold value in 10

```
NS3550-8T-2S:/>lldp hold 10
```

LLDP Delay

Description:
Set or show LLDP Tx delay.

Syntax:
LLDP Delay [<delay>]

Parameters:
<delay>: LLDP transmission delay (1-8192)

Default Setting:
2

Example:
Set LLDP delay value in 1

```
NS3550-8T-2S:/>lldp delay 1
```

LLDP Reinit

Description:
Set or show LLDP reinit delay.

Syntax:
LLDP Reinit [<reinit>]

Parameters:
<reinit>: LLDP reinit delay (1-10)

Default Setting:
2

Example:

Set LLDP reinit delay value in 3

```
NS3550-8T-2S:/>lldp reinit 3
```

LLDP Statistics

Description:

Show LLDP Statistics.

Syntax:

LLDP Statistics [<port_list>] [clear]

Parameters:

<port_list>: Port list or 'all', default: All ports
clear : Clear LLDP statistics

Example:

Show LLDP Statistics of port 1

```
NS3550-8T-2S:/>lldp statistics 1

LLDP global counters
Neighbor entries was last changed at - (18819 sec. ago).
Total Neighbors Entries Added      0.
Total Neighbors Entries Deleted    0.
Total Neighbors Entries Dropped    0.
Total Neighbors Entries Aged Out 0.

LLDP local counters
         Rx          Tx          Rx          Rx          Rx TLV     Rx TLV     Rx TLV
Port     Frames      Frames      Errors      Discards Errors     Unknown    Organz.    Aged
----     ------      ------      ------      --------    ------     -------    -------    -----
1        0           0           0           0           0          0          0          0
```

LLDP Info

Description:

Show LLDP neighbor device information.

Syntax:

LLDP Info [<port_list>]

Parameters:

<port_list>: Port list or 'all', default: All ports

6.12 LLDPMED Command

LLDPMED Configuration

Description:

Show LLDP-MED configuration.

Syntax:

LLDPMED Configuration [<port_list>]

Parameters:

<port_list>: Port list or 'all', default: All ports

Example:

Show LLDP-MED configuration of port1~4

```
NS3550-8T-2S:/>lldpmed configuration 1-4

LLDP-MED Configuration:
=======================

Fast Start Repeast Count : 4
```

```
Location Coordinates      : Latitude                - 0.0000 North
                            Longitude               - 0.0000 East
                            Altitude                - 0.0000 meter(s)
                            Map datum                 - WGS84
Civic Address Location    :


Port        Policies
1           none
2           none
3           none
4           none
```

LLDPMED Civic

Description:
Set or show LLDP-MED Civic Address Location.

Syntax:
LLDPMED Civic
[country|state|county|city|district|block|street|leading_street_direction|trailing_street_suffix|str_suf|house_no|house_no_suffix|landmark|additional_info|name|zip_code|building|apartment|floor|room_number|place_type|postal_com_name|p_o_box|additional_code] [<civic_value>]

Parameters:
country : Country
state : National subdivisions (state, caton, region, province, prefecture)
county : County, parish,gun (JP), district(IN)
city : City, townchip, shi (JP)
district : City division,borough, city, district, ward,chou (JP)
block : Neighborhood, block
street : Street
leading_street_direction : Leading street direction
trailing_street_suffix : Trailing street suffix
str_suf : Street Suffix
house_no : House Number
house_no_suffix : House number suffix
landmark : Landmark or vanity address
additional_info : Additional location information
name : Bame(residence and office occupant)
zip_code : Postal/zip code
building : Building (structure)
apartment : Unit (apartment, suite)
floor : Floor
room_number : Room number
place_type : Placetype
postal_com_name : Postal community name
p_o_box : Post office box (P.O. Box)
additional_code : Addtional code
(default: Show Civic Address Location configuration)
<civic_value>: lldpmed The value for the Civic Address Location entry.

LLDPMED ECS

Description:
Set or show LLDP-MED Emergency Call Service.

Syntax:
LLDPMED ecs [<ecs_value>]

Parameters:
<ecs_value>: lldpmed The value for the Emergency Call Service

LLDPMED Policy Delete

Description:

Delete the selected policy.

Syntax:

LLDPMED policy delete [<policy_list>]

Parameters:

<policy_list>: List of policies to delete

Example:

Delete the policy 1

```
NS3550-8T-2S:/>lldpmed policy delete 1
```

LLDPMED Policy Add

Description:

Adds a policy to the list of polices.

Syntax:

LLDPMED policy add [voice|voice_signaling|guest_voice|guest_voice_signaling|softphone_voice|video_conferencing|streaming_video|video_signaling] [tagged|untagged] [<vlan_id>] [<l2_priority>] [<dscp>]

Parameters:

voice : Voice for use by dedicated IP Telephony handsets and other similar appliances supporting interactive voice services. These devices are typically deployed on a separate VLAN for ease of deployment and enhanced security by isolation from data applications

voice_signaling : Voice Signaling (conditional) for use in network topologies that require a different policy for the voice signaling than for the voice media.

guest_voice : Guest Voice to support a separate limited feature-set voice service for guest users and visitors with their own IP Telephony handsets and other similar appliances supporting interactive voice services.

guest_voice_signaling : Guest Voice Signaling (conditional) for use in network topologies that require a different policy for the guest voice signaling than for the guest voice media.

softphone_voice : Softphone Voice for use by softphone applications on typical data centric devices, such as PCs or laptops. This class of endpoints frequently does not support multiple VLANs, if at all,and are typically configured to use an untagged VLAN or a single tagged data specific VLAN.

video_conferencing : Video Conferencing for use by dedicated Video Conferencing equipment and other similar appliances supporting real-time interactive video/audio services.

streaming_video : Streaming Video for use by broadcast or multicast based video content distribution and other similar applications supporting streaming video services that require specific network policy treatment. Video applications relying on TCP with buffering would not be an intended use of this application type.

video_signaling : Video Signaling (conditional) for use in network topologies that require a separate policy for the video signaling than for the video media.

tagged : The device is using tagged frames

unragged : The device is using untagged frames

<vlan_id> : VLAN id

<l2_priority>: This field may specify one of eight priority levels (0 through 7), as defined by IEEE 802.1D-2004 [3].

<dscp> : This field shall contain the DSCP value to be used to provide Diffserv node behavior for the specified application type as defined in IETF RFC 2474 [5]. This 6 bit field may contain one of 64 code point values (0 through 63). A value of 0 represents use of the default DSCP value as defined in RFC 2475.

LLDPMED Port Policy

Description:

Set or show LLDP-MED port polcies.

Syntax:

LLDPMED port policies [<port_list>] [<policy_list>]

Parameters:

<port_list> : Port list or 'all', default: All ports

<policy_list>: List of policies to delete

LLDPMED Coordinates

Description:
Set or show LLDP-MED Location.

Syntax:
LLDPMED Coordinates [latitude|longitude|altitude] [north|south|west|east|meters|floor] [coordinate_value]

Parameters:
latitude : Latitude, 0 to 90 degress with max. 4 digits (Positive numbers are north of the equator and negative numbers are south of the equator).
longitude : Longitude,0 to 180 degress with max. 4 digits (Positive values are East of the prime meridian and negative numbers are West of the prime meridian.
altitude : Altitude, Meters or floors with max. 4 digits.
(default: Show coordinate location configuration)
north|south|west|east|meters|floor:
North : North (Valid for latitude)
South : South (Valid for latitude)
West : West (Valid for longitude)
East : East (Valid for longitude)
Meters : Meters (Valid for altitude)
Floor : Floor (Valid for altitude)
lldpmed Coordinate value
coordinate_value : lldpmed Coordinate value

LLDPMED Datum

Description:
Set or show LLDP-MED Coordinates map datum.

Syntax:
LLDPMED Datum [wgs84|nad83_navd88|nad83_mllw]

Parameters:

wgs84|nad83_navd88|nad83_mllw:
wgs84 : WGS84
nad83_navd88 : NAD83_NAVD88
nad83_mllw : NAD83_MLLW
lldpmed Coordinate datum

LLDPMED Fast

Description:

Set or show LLDP-MED Fast Start Repeat Count.

Syntax:

LLDPMED Fast [<count>]

Parameters:

<count>: The number of times the fast start LLDPDU are being sent during the activation of the fast start mechanism defined by LLDP-MED (1-10).

LLDPMED Info

Description:

Show LLDP-MED neighbor device information.

Syntax:

LLDPMED Info [<port_list>]

Parameters:

<port_list>: Port list or 'all', default: All ports

6.13 EEE Command

EEE Configuration

Description:
Show eee configuration.

Syntax:
EEE Configuration [<port_list>]

Parameters:
<port_list>: Port list or 'all', default: All ports

Example:
Show EEE configuration of port1~4

```
NS3550-8T-2S:/>eee configuration 1-4

EEE Configuration:
==================


Port   Mode       Urgent queues
----   -------    -------------
1      Disabled none
2      Disabled none
3      Disabled none
4      Disabled none
```

EEE Mode

Description:
Set or show the eee mode.

Syntax:
EEE Mode [<port_list>] [enable|disable]

Parameters:
<port_list>: Port list or 'all', default: All ports
enable : Enable EEE
disable: Disable EEE
(default: Show eee mode)

Default Setting:
Disabled

Example:
Enable EEE mode for port1~4

```
NS3550-8T-2S:/>eee mode enable 1-4
```

EEE Urgent Queues

Description:
Set or show EEE Urgent queues.

Syntax:
EEE Urgent_queues [<port_list>] [<queue_list>]

Parameters:
<port_list> : Port list or 'all', default: All ports
<queue_list>: List of queues to configure as urgent queues (1-8 or none)

Default Setting:
none

6.14 Thermal Command

Thermal Priority Temperature

Description:
Set or show the temperature at which the ports shall be shut down.

Syntax:
Thermal prio_temp [<prio_list>] [<shut_down_temp>]

Parameters:
<prio_list> : List of priorities (0-3)
<shut_down_temp>: Temperature at which ports shall be shut down (0-255 degree C)

Example:
Show thermal priority temperature.

```
NS3550-8T-2S:/> Thermal prio_temp

Priority   Temp.
---------  -----
0            255 C
1            255 C
2            255 C
3            255 C
```

Thermal Port Priority

Description:
Set or show the ports priority.

Syntax:
Thermal port_prio [<port_list>] [<prio>]

Parameters:
<port_list>: Port list or 'all', default: All ports
<prio> : Priority (0-3)

Default Setting:
0

Example:
Set thermal port priority in 2

```
NS3550-8T-2S:/> Thermal port_prio 2
```

Thermal Status

Description:
Shows the chip temperature.

Syntax:
Thermal status

Example:
Shows the chip temperature.

```
NS3550-8T-2S:/> Thermal status
Port   Chip Temp.
----   ----------
1        47 C
2        47 C
3        47 C
4        47 C
5        47 C
6        47 C
7        47 C
```

```
8       47 C
9       47 C
10      47 C
```

Thermal Configuration

Description:
Show thermal_protect configuration.

Syntax:
Thermal configuration

6.15 Quality of Service Command

QoS Configuration

Description:
Show QoS Configuration.

Syntax:
QoS Configuration [<port_list>]

Parameters:
<port_list>: Port list or 'all', default: All ports

QoS Port Classification Class

Description:
Set or show the default QoS class.

Syntax:
QoS Port Classification Class [<port_list>] [<class>]

Parameters:
<port_list>: Port list or 'all', default: All ports
<class> : QoS class (0-7)

Default Setting:
0

Example:
Set default QoS class in 1 for port 1

```
NS3550-8T-2S:/>qos Port Classification Class 1 1
```

QoS Port Classification DPL

Description:
Set or show the default Drop Precedence Level.

Syntax:
QoS Port Classification DPL [<port_list>] [<dpl>]

Parameters:
<port_list>: Port list or 'all', default: All ports
<dpl> : Drop Precedence Level (0-1)

Default Setting:
0

Example:
Set the default Drop Precedence Level in 1 for port1

```
NS3550-8T-2S:/>qos Port Classification dpl 1 1
```

QoS Port Classification PCP

Description:
Set or show the default PCP for an untagged frame.

Syntax:
QoS Port Classification PCP [<port_list>] [<pcp>]

Parameters:
<port_list>: Port list or 'all', default: All ports
<pcp> : Priority Code Point (0-7)

Default Setting:
0

Example:
Set the default PCP for an untagged frame in 1 for port1

```
NS3550-8T-2S:/>qos Port Classification pcp 1 1
```

QoS Port Classification DEI

Description:
Set or show the default DEI for an untagged frame.

Syntax:
QoS Port Classification DEI [<port_list>] [<dei>]

Parameters:
<port_list>: Port list or 'all', default: All ports
<dei> : Drop Eligible Indicator (0-1)

Default Setting:
0

Example:
Set the default DEI for an untagged frame in 1 for port1.

```
NS3550-8T-2S:/>qos Port Classification dei 1 1
```

QoS Port Classification Tag

Description:
Set or show if the classification is based on the PCP and DEI values in tagged frames.

Syntax:

QoS Port Classification Tag [<port_list>] [enable|disable]

Parameters:
<port_list>: Port list or 'all', default: All ports
enable : Enable tag classification
disable : Disable tag classification
(default: Show tag classification mode)

Default Setting:
disable

Example:
Enable QoS port classification Tag.

```
NS3550-8T-2S:/>qos Port Classification tag 1-10 enable
```

QoS Port Classification Map

Description:
Set or show the port classification map.
This map is used when port classification tag is enabled,and the purpose is to translate the Priority Code Point (PCP) and Drop Eligible Indicator (DEI) from a tagged frame to QoS class and DP level.

Syntax:
QoS Port Classification Map [<port_list>] [<pcp_list>] [<dei_list>] [<class>] [<dpl>]

Parameters:
<port_list>: Port list or 'all', default: All ports
<pcp_list> : PCP list or 'all', default: All PCPs (0-7)
<dei_list> : DEI list or 'all', default: All DEIs (0-1)
<class> : QoS class (0-7)
<dpl> : Drop Precedence Level (0-1)

QoS Port Classification DSCP

Description:
Set or show if the classification is based on DSCP value in IP frames.

Syntax:
QoS Port Classification DSCP [<port_list>] [enable|disable]

Parameters:
<port_list>: Port list or 'all', default: All ports
enable : Enable DSCP based classification
disable : Disable DSCP based classification
(default: Show DSCP based classification mode)

Default Setting:
disable

Example:
Enable QoS port classification DSCP.

```
NS3550-8T-2S:/>qos Port Classification dscp 1-10 enable
```

QoS Port Policer Mode

Description:
Set or show the port policer mode

Syntax:
QoS Port Policer Mode [<port_list>] [enable|disable]

Parameters:
<port_list>: Port list or 'all', default: All ports
enable : Enable port policer
disable : Disable port policer

(default: Show port policer mode)

Default Setting:
disable

Example:
Enable QoS port policer

```
NS3550-8T-2S:/>qos Port Policer Mode 1-10 enable
```

QoS Port Policer Rate

Description:
Set or show the port policer rate.

Syntax:
QoS Port Policer Rate [<port_list>] [<rate>]

Parameters:
<port_list>: Port list or 'all', default: All ports
<rate> : Rate in kbps or fps (100-15000000)

Default Setting:
500

Example:
Set the port policer rate in 1000

```
NS3550-8T-2S:/>qos Port Policer Rate 1-10 1000
```

QoS Port Policer Unit

Description:
Set or show the port policer unit.

Syntax:
QoS Port Policer Unit [<port_list>] [kbps|fps]

Parameters:
<port_list>: Port list or 'all', default: All ports
kbps : Unit is kilo bits per second
fps : Unit is frames per second
(default: Show port policer unit)

Default Setting:
kbps

Example:
Set the port policer unit in fps

```
NS3550-8T-2S:/>qos Port Policer unit 1-10 fps
```

QoS Port Scheduler Mode

Description:
Set or show the port scheduler mode.

Syntax:
QoS Port Scheduler Mode [<port_list>] [strict|weighted]

Parameters:
<port_list>: Port list or 'all', default: All ports
strict : Strict mode
weighted: Weighted mode
(default: Show port scheduler mode)

Default Setting:

strict

Example:

Set the port schedule mode in weighted mode

```
NS3550-8T-2S:/>qos Port Scheduler Mode 1-10 weighted
```

QoS Port Scheduler Weight

Description:

Set or show the port scheduler weight.

Syntax:

QoS Port Scheduler Weight [<port_list>] [<queue_list>] [<weight>]

Parameters:

<port_list> : Port list or 'all', default: All ports
<queue_list>: Weighted queue list or 'all', default: All weighted queues (0-5)
<weight> : Scheduler weight (1-100)

QoS Port QueueShaper Mode

Description:

Set or show the port queue shaper mode.

Syntax:

QoS Port QueueShaper Mode [<port_list>] [<queue_list>] [enable|disable]

Parameters:

<port_list> : Port list or 'all', default: All ports
<queue_list>: Queue list or 'all', default: All queues (0-7)
enable : Enable port queue shaper
disable : Disable port queue shaper
(default: Show port queue shaper mode)

Default Setting:

disable

Example:

Enable port queue shaper for all port & queue

```
NS3550-8T-2S:/>qos Port QueueShaper Mode 1-10 0-7 enable
```

QoS Port QueueShaper Rate

Description:

Set or show the port queue shaper rate.

Syntax:

QoS Port QueueShaper Rate [<port_list>] [<queue_list>] [<bit_rate>]

Parameters:

<port_list> : Port list or 'all', default: All ports
<queue_list>: Queue list or 'all', default: All queues (0-7)
<bit_rate> : Rate in kilo bits per second (100-3300000)

Default Setting:

500kbps

Example:

Set the port queue shaper rate in 1000

```
NS3550-8T-2S:/>qos Port QueueShaper rate 1-10 0-7 1000
```

QoS Port QueueShaper Excess

Description:

Set or show the port queue excess bandwidth mode.

Syntax:

QoS Port QueueShaper Excess [<port_list>] [<queue_list>] [enable|disable]

Parameters:

<port_list> : Port list or 'all', default: All ports
<queue_list>: Queue list or 'all', default: All queues (0-7)
enable : Enable use of excess bandwidth
disable : Disable use of excess bandwidth
(default: Show port queue excess bandwidth mode)

Default Setting:

disable

Example:

Enable the port queue excess bandwidth mode.

```
NS3550-8T-2S:/>qos Port QueueShaper Excess 1-10 0-7 enable
```

QoS Port Shaper Mode

Description:

Set or show the port shaper mode.

Syntax:

QoS Port Shaper Mode [<port_list>] [enable|disable]

Parameters:

<port_list>: Port list or 'all', default: All ports
enable : Enable port shaper
disable : Disable port shaper
(default: Show port shaper mode)

Default Setting:

Enable

Example:

Enable port shaper mode.

```
NS3550-8T-2S:/>qos Port Shaper Mode 1-10 enable
```

QoS Port Shaper Rate

Description:

Set or show the port shaper rate.

Syntax:

QoS Port Shaper Rate [<port_list>] [<bit_rate>]

Parameters:

<port_list>: Port list or 'all', default: All ports
<bit_rate> : Rate in kilo bits per second (100-3300000)

Default Setting:

500kbps

Example:

Set the port shaper rate in 1000.

```
NS3550-8T-2S:/>qos Port Shaper Rate 1-10 1000
```

QoS Port TagRemarking Mode

Description:

Set or show the port tag remarking mode.

Syntax:

QoS Port TagRemarking Mode [<port_list>] [classified|default|mapped]

Parameters:

<port_list>: Port list or 'all', default: All ports
classified: Use classified PCP/DEI values
default : Use default PCP/DEI values
mapped : Use mapped versions of QoS class and DP level
(default: Show port tag remarking mode)

Default Setting:

classified

Example:

Set the port tag remarking mode in mapped.

```
NS3550-8T-2S:/>qos Port TagRemarking Mode 1-10 mapped
```

QoS Port TagRemarking PCP

Description:

Set or show the default PCP. This value is used when port tag remarking mode is set to 'default'.

Syntax:

QoS Port TagRemarking PCP [<port_list>] [<pcp>]

Parameters:

<port_list>: Port list or 'all', default: All ports
<pcp> : Priority Code Point (0-7)

Default Setting:

0

Example:

Set the default PCP in 1.

```
NS3550-8T-2S:/>qos Port TagRemarking PCP 1-10 1
```

QoS Port TagRemarking DEI

Description:

Set or show the default DEI. This value is used when port tag remarking mode is set to 'default'.

Syntax:

QoS Port TagRemarking DEI [<port_list>] [<dei>]

Parameters:

<port_list>: Port list or 'all', default: All ports
<dei> : Drop Eligible Indicator (0-1)

Default Setting:

0

Example:

Set the default EDI in 1.

```
NS3550-8T-2S:/>qos Port TagRemarking EDI 1-10 1
```

QoS Port TagRemarking Map

Description:

Set or show the port tag remarking map. This map is used when port tag remarking mode is set to 'mapped', and the purpose is to translate the classified QoS class (0-7) and DP level (0-1) to PCP and DEI.

Syntax:

QoS Port TagRemarking Map [<port_list>] [<class_list>] [<dpl_list>] [<pcp>] [<dei>]

Parameters:

<port_list> : Port list or 'all', default: All ports
<class_list>: QoS class list or 'all', default: All QoS classes (0-7)
<dpl_list> : DP level list or 'all', default: All DP levels (0-1)
<pcp> : Priority Code Point (0-7)
<dei> : Drop Eligible Indicator (0-1)

QoS Port DSCP Translation

Description:

Set or show DSCP ingress translation mode.
If translation is enabled for a port, incoming frame DSCP value is translated and translated value is used for QoS classification.

Syntax:

QoS Port DSCP Translation [<port_list>] [enable|disable]

Parameters:

<port_list>: Port list or 'all', default: All ports
enable : Enable DSCP ingress translation
disable : Disable DSCP ingress translation
(default: Show DSCP ingress translation mode)

Default Setting:

disable

Example:

Enable DSCP ingress translation on all port.

```
NS3550-8T-2S:/>qos Port DSCP Translation 1-10 enable
```

QoS Port DSCP Classification

Description:
Set or show DSCP classification based on QoS class and DP level.
This enables per port to map new DSCP value based on QoS class and DP level.

Syntax:
QoS Port DSCP Classification [<port_list>] [none|zero|selected|all]

Parameters:
<port_list>: Port list or 'all', default: All ports
none : No DSCP ingress classification
zero : Classify DSCP if DSCP = 0
selected : Classify DSCP for which class. mode is 'enable'
all : Classify all DSCP
(default: Show port DSCP ingress classification mode)

Default Setting:
none

Example:
Set DSCP classification based on QoS class and DP level in zero

```
NS3550-8T-2S:/> QoS Port DSCP Classification 1-10 zero
```

QoS Port DSCP EgressRemark

Description:
Set or show the port DSCP remarking mode.

Syntax:
QoS Port DSCP EgressRemark [<port_list>] [disable|enable|remap_dp_unaware|remap_dp_aware]

Parameters:
<port_list>: Port list or 'all', default: All ports
disable : Disable DSCP egress rewrite
enable : Enable DSCP egress rewrite with the value received from analyzer
remap_dp_unaware : Rewrite DSCP in egress frame with remapped DSCP where remap is DP unaware or DP = 0
remap_dp_aware : Rewrite DSCP in egress frame with remapped DSCP where remap is DP aware and DP = 1
(default: Show port DSCP egress remarking mode)

Default Setting:
disable

Example:
Enable DSCP egress rewrite

```
NS3550-8T-2S:/> QoS Port DSCP EgressRemark 1-10 enable
```

QoS DSCP Map

Description:
Set or show DSCP mapping table.
This table is used to map QoS class and DP level based on DSCP value.
DSCP value used to map QoS class and DPL is either translated DSCP value or incoming frame DSCP value.

Syntax:
QoS DSCP Map [<dscp_list>] [<class>] [<dpl>]

Parameters:
<dscp_list>: DSCP (0-63, BE, CS1-CS7, EF or AF11-AF43) list or 'all'
(default: Show DSCP ingress map table i.e. DSCP->(class, DPL))
<class> : QoS class (0-7)
<dpl> : Drop Precedence Level (0-1)

QoS DSCP Translation

Description:
Set or show global ingress DSCP translation table.
If port DSCP translation is enabled, translation table is used to translate incoming frames DSCP value and translated value is used to map QoS class and DP level.

Syntax:
QoS DSCP Translation [<dscp_list>] [<trans_dscp>]

Parameters:
<dscp_list> : DSCP (0-63, BE, CS1-CS7, EF or AF11-AF43) list or 'all'
(default: Show DSCP translation table)
<trans_dscp>: Translated DSCP: 0-63, BE, CS1-CS7, EF or AF11-AF43

QoS DSCP Trust

Description:
Set or show trusted DSCP value which is used for QoS classification.
The DSCP value to be checked for trust is either translated value ifDSCP translation is enabled for the ingress port or incoming frame DSCPvalue if translation is disabled for the port. Trusted DSCP value is onlyused for QoS classification.

Syntax:
QoS DSCP Trust [<dscp_list>] [enable|disable]

Parameters:
<dscp_list>: DSCP (0-63, BE, CS1-CS7, EF or AF11-AF43) list or 'all'
enable : Set DSCP as trusted DSCP
disable : Set DSCP as un-trusted DSCP
(default: Show DSCP Trust status)

Default Setting:
disable

QoS DSCP Classification Mode

Description:
Set or show DSCP ingress classification mode.
If port DSCP classification is 'selected', DSCP will be classified based on QoS class and DP level only for DSCP value with classification mode 'enabled'. DSCP may be translated DSCP if translation is enabled for the port.

Syntax:
QoS DSCP Classification Mode [<dscp_list>] [enable|disable]

Parameters:
<dscp_list>: DSCP (0-63, BE, CS1-CS7, EF or AF11-AF43) list or 'all'
enable : Enable DSCP ingress classification
disable : Disable DSCP ingress classification
(default: Show DSCP classification mode)

Default Setting:
disable

QoS DSCP EgressRemap

Description:
Set or show DSCP egress remap table. This table is used if the port egress remarking mode is 'remap' and the purpose is to map the DSCP and DP level to a new DSCP value.

Syntax:
QoS DSCP EgressRemap [<dscp_list>] [<dpl_list>] [<dscp>]

Parameters:
<dscp_list>: DSCP (0-63, BE, CS1-CS7, EF or AF11-AF43) list or 'all'
<dpl_list> : DP level list or 'all', default: All DP levels (0-1)
<dscp> : Egress remapped DSCP: 0-63, BE, CS1-CS7, EF or AF11-AF43

QoS Storm Unicast

Description:
Set or show the unicast storm rate limiter.

Syntax:
QoS Storm Unicast [enable|disable] [<packet_rate>]

Parameters:
enable : Enable unicast storm control
disable : Disable unicast storm control
<packet_rate>: Rate in fps (1, 2, 4, ..., 512, 1k, 2k, 4k, ..., 32768k)

Default Setting:
disable

Example:
Enable unicast storm control in 2fps

```
NS3550-8T-2S:/> QoS Storm Unicast enable 2
```

QoS Storm Multicast

Description:

Set or show the multicast storm rate limiter.

Syntax:

QoS Storm Multicast [enable|disable] [<packet_rate>]

Parameters:

enable : Enable multicast storm control
disable : Disable multicast storm control
<packet_rate>: Rate in fps (1, 2, 4, ..., 512, 1k, 2k, 4k, ..., 32768k)

Default Setting:

disable

Example:

Enable multicast storm control in 2fps

```
NS3550-8T-2S:/> QoS Storm multicast enable 2
```

QoS QCL Add

Description:

Add or modify QoS Control Entry (QCE).
If the QCE ID parameter <qce_id> is specified and an entry with this QCE ID already exists, the QCE will be modified. Otherwise, a new QCE will be added. If the QCE ID is not specified, the next available QCE ID will be used. If the next QCE ID parameter <qce_id_next> is specified, the QCE will be placed before this QCE in the list. If the next QCE ID is not specified and if it is a new entry added, the QCE will be placed last in the list. Otherwise if the next QCE ID is not specified and if existing QCE is modified, QCE will be in the same location in the list. To modify and move the entry to last in the list, use the word 'last' for <qce_id_next>.

Syntax:

QoS QCL Add [<qce_id>] [<qce_id_next>] [<port_list>] [<tag>] [<vid>] [<pcp>] [<dei>] [<smac>] [<dmac_type>] [(etype [<etype>]) | (LLC [<DSAP>] [<SSAP>] [<control>]) | (SNAP [<PID>]) | (ipv4 [<protocol>] [<sip>] [<dscp>] [<fragment>] [<sport>] [<dport>]) | (ipv6 [<protocol>] [<sip_v6>] [<dscp>] [<sport>] [<dport>])] [<class>] [<dp>] [<classified_dscp>]

Parameters:

<qce_id> : QCE ID (1-256), default: Next available ID
<qce_id_next> : Next QCE ID: "next_id (1-256) or 'last'"
<port_list> : Port List: "port <port_list> or 'all'", default: All ports
<tag> : Frame tag: untag|tag|any
<vid> : VID: 1-4095 or 'any', either a specific VID or range of VIDs
<pcp> : Priority Code Point: specific(0, 1, 2, 3, 4, 5, 6, 7) or range(0-1, 2-3, 4-5, 6-7, 0-3, 4-7) or 'any'
<dei> : Drop Eligible Indicator: 0-1 or 'any'
<smac> : Source MAC address: (xx-xx-xx) or 'any', 24 MS bits (OUI)
<dmac_type> : Destination MAC type: unicast|multicast|broadcast|any
etype : Ethernet Type keyword
<etype> : Ethernet Type: 0x600-0xFFFF or 'any' but excluding 0x800(IPv4) and 0x86DD(IPv6)
llc : LLC keyword
<dsap> : Destination Service Access Point: 0x00-0xFF or 'any'
<ssap> : Source Service Access Point: 0x00-0xFF or 'any'
<control> : LLC control: 0x00-0xFF or 'any'
snap : SNAP keyword
<pid> : Protocol ID (EtherType) or 'any'
ipv4 : IPv4 keyowrd
<protocol> : IP protocol number: (0-255, TCP or UDP) or 'any'
<sip> : Source IP address: (a.b.c.d/n) or 'any'
<dscp> : DSCP:(0-63,BE,CS1-CS7,EF or AF11-AF43)or'any',specific/range
<fragment> : IPv4 frame fragmented: yes|no|any
<sport> : Source TCP/UDP port:(0-65535) or 'any',specific or port range
<dport> : Dest. TCP/UDP port:(0-65535) or 'any', specific or port range
ipv6 : IPv6 keyowrd
<sip_v6> : IPv6 source address: (a.b.c.d/n) or 'any', 32 LS bits
<class> : QoS Class: "class (0-7)", default: basic classification
<dp> : DP Level: "dp (0-1)", default: basic classification
<classified_dscp>: DSCP: "dscp (0-63, BE, CS1-CS7, EF or AF11-AF43)"

QoS QCL Delete

Description:

Delete QCE entry from QoS Control list.

Syntax:

QoS QCL Delete <qce_id>

Parameters:

<qce_id>: QCE ID (1-256), default: Next available ID

Default Setting:

disable

Example:

Enable multicast storm control in 2fps

```
NS3550-8T-2S:/> QoS Storm multicast enable 2
```

QoS QCL Lookup

Description:

Lookup QoS Control List.

Syntax:

QoS QCL Lookup [<qce_id>]

Parameters:

<qce_id>: QCE ID (1-256), default: Next available ID

Default Setting:

disable

Example:

Enable multicast storm control in 2fps

```
NS3550-8T-2S:/> QoS Storm multicast enable 2
```

QoS QCL Status

Description:

Show QCL status. This can be used to display if there is any conflict in QCE for differnet user types.

Syntax:

QoS QCL status [combined|static|voice_vlan|conflicts]

Parameters:

combined|static|voice_vlan|conflicts: combined **:** Shows the combined status
static : Shows the static user configured status
voice_vlan : Shows the status by Voice VLAN
conflicts : Shows all conflict status
(default : Shows the combined status)

QoS QCL Refresh

Description:

Resolve QCE conflict status. Same H/W resource is shared by multiple applications and it may not be available even before MAX QCE entry. So user can release the resource in use by other applications and use this command to acquire the resource.

Syntax:

QoS QCL refresh

Parameters:

combined|static|voice_vlan|conflicts: combined **:** Shows the combined status
static : Shows the static user configured status
voice_vlan : Shows the status by Voice VLAN
conflicts : Shows all conflict status
(default : Shows the combined status)

Default Setting:

disable

Example:

Enable multicast storm control in 2fps

```
NS3550-8T-2S:/> QoS Storm multicast enable 2
```

6.16 Mirror Command

Mirror Configuration

Description:
Show mirror configuration.

Syntax:
Mirror Configuration [<port_list>]

Parameters:
<port_list>: Port list or 'all', default: All ports

Example:
Show mirror configuration.

```
NS3550-8T-2S:/>mirror configuration
```

Mirror Port

Description:
Set or show the mirror port.

Syntax:
Mirror Port [<port>|disable]

Parameters:
<port>|disable: Mirror port or 'disable', default: Show port

Default Setting:
disable

Example:
Set port 2 for the mirror port.

```
NS3550-8T-2S:/>mirror port 2
```

Mirror Mode

Description:
Set or show the mirror mode.

Syntax:
Mirror Mode [<port_list>] [enable|disable|rx|tx]

Parameters:
<port_list>: Port list or 'all', default: All ports
enable : Enable Rx and Tx mirroring
disable: Disable Mirroring
rx : Enable Rx mirroring
tx : Enable Tx mirroring
(default: Show mirror mode)

Default Setting:
disable

Example:
Enable the mirror mode for port 1-4.

```
NS3550-8T-2S:/>mirror mode 1-4 enable
```

6.17 Configuration Command

Configuration Save

Description:
Save configuration to TFTP server.

Syntax:
Config Save <ip_server> <file_name>

Parameters:
<ip_server>: TFTP server IP address (a.b.c.d)
<file_name>: Configuration file name

Configuration Load

Description:
Load configuration from TFTP server.

Syntax:
Config Load <ip_server> <file_name> [check]

Parameters:
<ip_server>: TFTP server IP address (a.b.c.d)
<file_name>: Configuration file name
check : Check configuration file only, default: Check and apply file

6.18 Firmware Command

Firmware Load

Description:
Load new firmware from TFTP server.

Syntax:
Firmware Load <ip_addr_string> <file_name>

Parameters:
<ip_addr_string>: IP host address (a.b.c.d) or a host name string
<file_name> : Firmware file name

Firmware IPv6 Load

Description:
Load new firmware from IPv6 TFTP server.

Syntax:
Firmware IPv6 Load <ipv6_server> <file_name>

Parameters:
<ipv6_server>: TFTP server IPv6 address
<file_name> : Firmware file name

Firmware Information

Description:
Display information about active and alternate firmware images.

Syntax:
Firmware Information

Firmware Swap

Description:
Activate the alternate firmware image..
Syntax:
Firmware Swap

6.19 UPnP Command

UPnP Configuration

Description:
Show UPnP configuration.

Syntax:
UPnP Configuration

Example:
Show UPnP configuration.

```
NS3550-8T-2S:/>upnp configuration

UPnP Configuration:
====================

UPnP Mode                    : Disabled
UPnP TTL                     : 4
UPnP Advertising Duration : 100
```

UPnP Mode

Description:
Set or show the UPnP mode.

Syntax:
UPnP Mode [enable|disable]

Parameters:
enable : Enable UPnP
disable: Disable UPnP
(default: Show UPnP mode)

Default Setting:
disable

Example:
Enable the UPnP mode.

```
NS3550-8T-2S:/>upnp mode enable
```

UPnP TTL

Description:
Set or show the TTL value of the IP header in SSDP messages.

Syntax:
UPnP TTL [<ttl>]

Parameters:
<ttl>: ttl range (1..255), default: Show UPnP TTL

Default Setting:
4

Example:
Set the value 10 for TTL value of the IP header in SSDP messages.

```
NS3550-8T-2S:/>upnp ttl 10
```

UPnP Advertising Duration

Description:
Set or show UPnP Advertising Duration.

Syntax:
UPnP Advertising Duration [<duration>]

Parameters:
<duration>: duration range (100..86400), default: Show UPnP duration range

Default Setting:
100

Example:

Set value 1000 for UPnP Advertising Duration.

```
NS3550-8T-2S:/>upnp advertising duration 1000
```

6.20 MVR Command

MVR Configuration

Description:

Show the MVR configuration.

Syntax:

MVR Configuration

Example:

Show the MVR configuration.

```
NS3550-8T-2S:/>mvr configuration

MVR Configuration:
==================

MVR Mode: Disabled
Muticast VLAN ID: 100

Port   Port Mode      Port Type      Immediate Leave
----   -----------   -----------   ---------------
1      Disabled       Receive        Disabled
2      Disabled       Receive        Disabled
3      Disabled       Receive        Disabled
4      Disabled       Receive        Disabled
5      Disabled       Receive        Disabled
6      Disabled       Receive        Disabled
7      Disabled       Receive        Disabled
8      Disabled       Receive        Disabled
9      Disabled       Receive        Disabled
10     Disabled       Receive        Disabled
```

MVR Group

Description:

Show the MVR group.

Syntax:

MVR Group

MVR Status

Description:

Show the MVR status.

Syntax:

MVR Status

MVR Mode

Description:

Set or show the MVR mode.

Syntax:

MVR Mode [enable|disable]

Parameters:

enable : Enable MVR mode

disable : Disable MVR mode
(default: Show MVR mode)

Default Setting:
disable

Example:
Enable MVR mode.

```
NS3550-8T-2S:/>mvr mode enable
```

MVR Port Mode

Description:
Set or show the MVR port mode.

Syntax:
MVR Port Mode [<port_list>] [enable|disable]

Parameters:
<port_list>: Port list or 'all', default: All ports
enable : Enable MVR mode
disable : Disable MVR mode
(default: Show MVR mode)

Default Setting:
disable

Example:
Enable the MVR port mode for port 1-4.

```
NS3550-8T-2S:/>mvr port mode 1-4 enable
```

MVR Multicast VLAN

Description:
Set or show MVR multicast VLAN ID.

Syntax:
MVR Multicast VLAN [<vid>]

Parameters:
<vid>: VLAN ID (1-4095), default: Show current MVR multicast VLAN ID

Default Setting:
100

Example:
Set VLAN 1000 for MVR multicast VLAN ID.

```
NS3550-8T-2S:/>mvr multicast vlan 1000
```

MVR Port Type

Description:
Set or show MVR port type.

Syntax:
MVR Port Type [<port_list>] [source|receiver]

Parameters:
<port_list>: Port list or 'all', default: All ports
source : Enable source mode
receiver : Disable receiver mode
(default: Show MVR port type)

Default Setting:
receive

Example:
Set source type for MVR port type of port 1.

```
NS3550-8T-2S:/>mvr port type 1 source
```

MVR Immediate Leave

Description:
Set or show MVR port state about immediate leave.

Syntax:
MVR Immediate Leave [<port_list>] [enable|disable]

Parameters:
<port_list>: Port list or 'all', default: All ports
enable : Enable Immediate-leave mode
disable : Disable Immediate-leave mode
(default: Show MVR Immediate-leave mode)

Default Setting:
disable

Example:

Enable MVR port state about immediate leave for port 1.

```
NS3550-8T-2S:/>mvr immediate leave 1 enable
```

6.21 Voice VLAN Command

Voice VLAN Configuration

Description:

Show Voice VLAN configuration.

Syntax:

Voice VLAN Configuration

Example:

Show Voice VLAN configuration.

```
NS3550-8T-2S:/>voice vlan configuration

V oice VLAN Configuration:
==========================

Voice VLAN Mode                    : Disabled
Voice VLAN VLAN ID                 : 1000
Voice VLAN Age Time(seconds)   : 86400
Voice VLAN Traffic Class         : 7

Voice VLAN OUI Table:
=====================

Telephony OUI Description
------------- -----------
00-03-6B         Cisco phones
00-0F-E2         H3C phones
00-60-B9         Philips and NEC AG phones
00-D0-1E         Pingtel phones
00-E0-75         Polycom phones
00-E0-BB         3Com phones
00-01-E3         Siemens AG phones

Voice VLAN Port Configuration:
==============================


Port   Mode         Security   Discovery Protocol
----   --------   --------   ------------------
1       Disabled   Disabled      OUI
2       Disabled   Disabled      OUI
3       Disabled   Disabled      OUI
4       Disabled   Disabled      OUI
5       Disabled   Disabled      OUI
6       Disabled   Disabled      OUI
7       Disabled   Disabled      OUI
8       Disabled   Disabled      OUI
9       Disabled   Disabled      OUI
10      Disabled   Disabled      OUI
```

Voice VLAN Mode

Description:

Set or show the Voice VLAN mode.
We must disable MSTP feature before we enable Voice VLAN.
It can avoid the conflict of ingress filter.

Syntax:

Voice VLAN Mode [enable|disable]

Parameters:

enable : Enable Voice VLAN mode.
disable: Disable Voice VLAN mode
(default: Show flow Voice VLAN mode)

Default Setting:

disable

Example:

Enable the Voice VLAN mode.

```
NS3550-8T-2S:/>voice vlan mode enable
```

Voice VLAN ID

Description:

Set or show Voice VLAN ID.

Syntax:

Voice VLAN ID [<vid>]

Parameters:

<vid>: VLAN ID (1-4095)

Default Setting:

1000

Example:

Set ID 2 for Voice VLAN ID.

```
NS3550-8T-2S:/>voice vlan id 2
```

Voice VLAN Agetime

Description:

Set or show Voice VLAN age time.

Syntax:

Voice VLAN Agetime [<age_time>]

Parameters:

<age_time>: MAC address age time (10-10000000) default: Show age time

Default Setting:

86400sec

Example:

Set Voice VLAN age time in 100sec.

```
NS3550-8T-2S:/>voice valn agetime 100
```

Voice VLAN Traffic Class

Description:

Set or show Voice VLAN ID.

Syntax:

Voice VLAN Traffic Class [<class>]

Parameters:

<class>: Traffic class (0-7)

Default Setting:

7

Example:

Set 4 traffic class for voice VLAN

```
NS3550-8T-2S:/>voice vlan traffic class4
```

Voice VLAN OUI Add

Description:

Add Voice VLAN OUI entry.
Modify OUI table will restart auto detect OUI process. The maximum entry number is (16).

Syntax:

Voice VLAN OUI Add <oui_addr> [<description>]

Parameters:

<oui_addr> : OUI address (xx-xx-xx). The null OUI address isn't allowed
<description>: Entry description. Use 'clear' or "" to clear the string
No blank or space characters are permitted as part of a contact. (only in CLI)

Example:

Add Voice VLAN OUI entry.

```
NS3550-8T-2S:/>voice vlan oui add 00-11-22 test
```

Voice VLAN OUI Delete

Description:

Delete Voice VLAN OUI entry.
Modify OUI table will restart auto detect OUI process.

Syntax:

Voice VLAN OUI Delete <oui_addr>

Parameters:

<oui_addr>: OUI address (xx-xx-xx). The null OUI address isn't allowed

Example:

Delete Voice VLAN OUI entry.

```
NS3550-8T-2S:/>voice vlan oui delete 00-11-22
```

Voice VLAN OUI Clear

Description:

Clear Voice VLAN OUI entry.
Modify OUI table will restart auto detect OUI process.

Syntax:

Voice VLAN OUI Clear

Example:

Clear Voice VLAN OUI entry.

```
NS3550-8T-2S:/>voice vlan oui clear
```

Voice VLAN OUI Lookup

Description:
Clear Voice VLAN OUI entry. Modify OUI table will restart auto detect OUI process.

Syntax:
Voice VLAN OUI Clear

Example:
Lookup Voice VLAN OUI entry.

```
NS3550-8T-2S:/>voice vlan oui lookup
```

Voice VLAN Port Mode

Description:
Set or show the Voice VLAN port mode.
When the port mode isn't disabled, we must disable MSTP feature before we enable Voice VLAN. It can avoid the conflict of ingress filter.

Syntax:
Voice VLAN Port Mode [<port_list>] [disable|auto|force]

Parameters:
<port_list>: Port list or 'all', default: All ports
disable : Disjoin from Voice VLAN.
auto : Enable auto detect mode. It detects whether there is VoIP phone attached on the specific port and configure the Voice VLAN members automatically.
force : Forced join to Voice VLAN.
(default: Show Voice VLAN port mode)

Default Setting:
disable

Example:
Set auto mode for port 1-4 of Voice VLAN port mode.

```
NS3550-8T-2S:/>voice vlan port mode 1-4 auto
```

Voice VLAN Security

Description:
Set or show the Voice VLAN port security mode. When the function is enabled, all non-telephone MAC address in Voice VLAN will be blocked 10 seconds.

Syntax:
Voice VLAN Security [<port_list>] [enable|disable]
Parameters:
<port_list>: Port list or 'all', default: All ports
enable : Enable Voice VLAN security mode.
disable: Disable Voice VLAN security mode
(default: Show flow Voice VLAN security mode)

Default Setting:
disable

Example:
Enable the Voice VLAN port security mode for port 1-4.

```
NS3550-8T-2S:/>voice vlan security 1-4 enable
```

6.22 Loop Protect Command

Loop Protect Configuration

Description:
Show Loop Protection configuration.

Syntax:
Loop Protect Configuration

Loop Protect Mode

Description:
Set or show the Loop Protection mode.

Syntax:
Loop Protect Mode [enable|disable]

Parameters:
enable : Enable Loop Protection
disable: Disable Loop Protection

Default Setting:
enable

Loop Protect Transmit

Description:
Set or show the Loop Protection transmit interval.

Syntax:
Loop Protect Transmit [<transmit-time>]

Parameters:
Transmit time interval (1-10 seconds)

Default Setting:
5

Loop Protect Shutdown

Description:
Set or show the Loop Protection shutdown time.

Syntax:
Loop Protect Shutdown [<shutdown-time>]

Parameters:
Shutdown time interval (0-604800 seconds)
A value of zero disables re-enabling the port

Default Setting:
10

Loop Protect Port Configuration

Description:
Show Loop Protection port configuration.

Syntax:
Loop Protect Port Configuration [<port_list>]

Parameters:
<port_list>: Port list or 'all', default: All ports

Loop Protect Port Mode

Description:
Set or show the Loop Protection port mode.

Syntax:
Loop Protect Port Mode [<port_list>] [enable|disable]

Parameters:
<port_list>: Port list or 'all', default: All ports
enable : Enable Loop Protection
disable: Disable Loop Protection

Loop Protect Port Action

Description:
Set or show the Loop Protection port action.

Syntax:
Loop Protect Port Action [<port_list>] [shutdown|shut_log|log]

Parameters:
<port_list>: Port list or 'all', default: All ports
shutdown : Shutdown the port
shut_log : Shutdown the port and Log event
log : (Only) Log the event

6.23 IPMC Command

IPMC Configuration

Description:
Show IPMC snooping configuration.

Syntax:
IPMC Configuration [mld|igmp]

Parameters:
mld|igmp:
mld : IPMC for IPv6 MLD
igmp: IPMC for IPv4 IGMP

IPMC Mode

Description:
Set or show the IPMC snooping mode.
Syntax:
IPMC Mode [mld|igmp] [enable|disable]

Parameters:
mld|igmp:
mld : IPMC for IPv6 MLD
igmp: IPMC for IPv4 IGMP
enable : Enable IPMC snooping
disable: Disable IPMC snooping
(default: Show global IPMC snooping mode)

Default Setting:
disable

Example:
Enable IGMP snooping

```
NS3550-8T-2S:/>ipmc mode igmp enable
```

IPMC Flooding

Description:
Set or show the IPMC unregistered addresses flooding operation.
Syntax:
IPMC Flooding [mld|igmp] [enable|disable]

Parameters:
mld|igmp:
mld : IPMC for IPv6 MLD
igmp: IPMC for IPv4 IGMP
enable : Enable IPMC flooding
disable: Disable IPMC flooding
(default: Show global IPMC flooding mode)

Default Setting:
enable

Example:
Enable IGMP flooding

```
NS3550-8T-2S:/>ipmc flooding igmp enable
```

IPMC Leave Proxy

Description:
Set or show the mode of IPMC Leave Proxy.

Syntax:
IPMC Leave Proxy [mld|igmp] [enable|disable]

Parameters:
mld|igmp:
mld : IPMC for IPv6 MLD
igmp: IPMC for IPv4 IGMP
enable : Enable IPMC Leave Proxy
disable: Disable IPMC Leave Proxy
(default: Show global IPMC Leave Proxy mode)

Default Setting:
disable

Example:
Enable IGMP Leave Proxy

```
NS3550-8T-2S:/>ipmc leave proxy igmp enable
```

IPMC Proxy

Description:
Set or show the mode of IPMC Proxy.

Syntax:
IPMC Proxy [mld|igmp] [enable|disable]

Parameters:
mld|igmp:
mld : IPMC for IPv6 MLD
igmp: IPMC for IPv4 IGMP
enable : Enable IPMC Proxy
disable: Disable IPMC Proxy
(default: Show global IPMC Proxy mode)

Default Setting:
disable

Example:
Enable IGMP Proxy

```
NS3550-8T-2S:/>ipmc proxy igmp enable
```

IPMC State

Description:
Set or show the IPMC snooping state for VLAN.

Syntax:
IPMC State [mld|igmp] [<vid>] [enable|disable]

Parameters:
mld|igmp:
mld : IPMC for IPv6 MLD
igmp: IPMC for IPv4 IGMP
<vid> : VLAN ID (1-4095) or 'any', default: Show all VLANs
enable : Enable MLD snooping
disable: Disable MLD snooping

Default Setting:
disable

Example:
Enable IGMP snooping state for VLAN 1

```
NS3550-8T-2S:/>ipmc state igmp 1 enable
```

IPMC Querier

Description:
Set or show the IPMC snooping querier mode for VLAN.

Syntax:
IPMC Querier [mld|igmp] [<vid>] [enable|disable]

Parameters:
mld|igmp:
mld : IPMC for IPv6 MLD
igmp: IPMC for IPv4 IGMP
<vid> : VLAN ID (1-4095) or 'any', default: Show all VLANs
enable : Enable MLD querier
disable: Disable MLD querier

Default Setting:
disable

Example:
Enable IGMP querier for VLAN 1

```
NS3550-8T-2S:/>ipmc querier igmp 1 enable
```

IPMC Fastleave

Description:
Set or show the IPMC snooping fast leave port mode.

Syntax:
IPMC Fastleave [mld|igmp] [<port_list>] [enable|disable]

Parameters:
mld|igmp:
mld : IPMC for IPv6 MLD

igmp: IPMC for IPv4 IGMP
<port_list>: Port list or 'all', default: All ports
enable : Enable MLD fast leave
disable: Disable MLD fast leave
(default: Show IPMC fast leave mode)

Default Setting:
disable

Example:
Enable IGMP fast leave for all port

```
NS3550-8T-2S:/>ipmc fastleave igmp 1-10 enable
```

IPMC Throttling

Description:
Set or show the IPMC port throttling status.

Syntax:
IPMC Throttling [mld|igmp] [<port_list>] [limit_group_number]

Parameters:
mld|igmp :
mld : IPMC for IPv6 MLD
igmp: IPMC for IPv4 IGMP
<port_list>: Port list or 'all', default: All ports
0 : No limit
1~10 : Group learn limit
(default: Show IPMC Port Throttling)

Default Setting:
Unlimited

Example:
Set the max. learn 10 groups for ICMP port throttling

```
NS3550-8T-2S:/>ipmc throttling igmp 1-10 10
```

IPMC Filtering

Description:
Set or show the IPMC port group filtering list.

Syntax:
IPMC Filtering [mld|igmp] [<port_list>] [add|del] [group_addr]

Parameters:
mld|igmp :
mld : IPMC for IPv6 MLD
igmp: IPMC for IPv4 IGMP
<port_list>: Port list or 'all', default: All ports
add : Add new port group filtering entry
del : Del existing port group filtering entry
(default: Show IPMC port group filtering list)
group_addr : IPv4/IPv6 multicast group address, accordingly

IPMC Router

Description:
Set or show the IPMC snooping router port mode.

Syntax:
IPMC Router [mld|igmp] [<port_list>] [enable|disable]

Parameters:
mld|igmp :

mld : IPMC for IPv6 MLD
igmp: IPMC for IPv4 IGMP
<port_list>: Port list or 'all', default: All ports
enable : Enable IPMC router port
disable : Disable IPMC router port
(default: Show IPMC router port mode)

Example:
Enable port 1 in IPMC router port

```
NS3550-8T-2S:/>ipmc riuter igmp 1 enable
```

IPMC Status

Description:
Show IPMC operational status, accordingly.

Syntax:
IPMC Status [mld|igmp] [<vid>]
Parameters:
mld|igmp:
mld : IPMC for IPv6 MLD
igmp: IPMC for IPv4 IGMP
<vid> : VLAN ID (1-4095) or 'any', default: Show all VLANs

Example:
Show VLAN 1 IPMC operational status

```
NS3550-8T-2S:/>ipmc status igmp 1
```

IPMC Group

Description:
Show IPMC group addresses, accordingly.

Syntax:
IPMC Groups [mld|igmp] [<vid>]

Parameters:
mld|igmp:
mld : IPMC for IPv6 MLD
igmp: IPMC for IPv4 IGMP
<vid> : VLAN ID (1-4095) or 'any', default: Show all VLANs

Example:
Show VLAN 1 IPMC group addresses, accordingly.

```
NS3550-8T-2S:/>ipmc groups igmp 1
```

IPMC Version

Description:
Show IPMC Versions.

Syntax:
IPMC Version [mld|igmp] [<vid>]

Parameters:
mld|igmp:
mld : IPMC for IPv6 MLD
igmp: IPMC for IPv4 IGMP
<vid> : VLAN ID (1-4095) or 'any', default: Show all VLANs

Example:
Show VLAN 1 IPMC Versions.

```
NS3550-8T-2S:/>ipmc version igmp 1
```

IPMC SSM

Description:
Show SSM related information for IPMC.

Syntax:
IPMC SSM [mld|igmp] [<vid>] [<port_list>]

Parameters:
mld|igmp :
mld : IPMC for IPv6 MLD
igmp: IPMC for IPv4 IGMP
<vid> : VLAN ID (1-4095) or 'any', default: Show all VLANs
<port_list>: Port list or 'all', default: All ports

Example:
Show VLAN 1 & port 1-10 SSM related information for IPMC.

```
NS3550-8T-2S:/>ipmcssm igmp 1 1-10
```

IPMC Parameter RV

Description:
Set or show the IPMC Robustness Variable.

Syntax:
IPMC Parameter RV [mld|igmp] [<vid>] [ipmc_param_rv]

Parameters:
mld|igmp :
mld : IPMC for IPv6 MLD
igmp: IPMC for IPv4 IGMP
<vid> : VLAN ID (1-4095) or 'any', default: Show all VLANs
ipmc_param_rv:
-1 : Default Value (2)
1~255 : Robustness Variable
(default: Show IPMC Interface Robustness Variable

IPMC Parameter QI

Description:
Set or show the IPMC Query Interval.

Syntax:
IPMC Parameter QI [mld|igmp] [<vid>] [ipmc_param_qi]

Parameters:
mld|igmp :
mld : IPMC for IPv6 MLD
igmp: IPMC for IPv4 IGMP
<vid> : VLAN ID (1-4095) or 'any', default: Show all VLANs
ipmc_param_qi:
-1 : Default Value (125)
1~31744 : Query Interval in seconds
(default: Show IPMC Interface Query Interval

IPMC Parameter QRI

Description:
Set or show the IPMC Query Response Interval.

Syntax:
IPMC Parameter QRI [mld|igmp] [<vid>] [ipmc_param_qri]

Parameters:
mld|igmp :
mld : IPMC for IPv6 MLD
igmp: IPMC for IPv4 IGMP
<vid> : VLAN ID (1-4095) or 'any', default: Show all VLANs
ipmc_param_qri:
-1 : Default Value (100)
0~31744 : Query Response Interval in tenths of seconds
(default: Show IPMC Interface Query Response Interval

IPMC Parameter LLQI

Description:
Set or show the IPMC Last Listener Query Interval.

Syntax:
IPMC Parameter LLQI [mld|igmp] [<vid>] [ipmc_param_llqi]

Parameters:
mld|igmp :
mld : IPMC for IPv6 MLD
igmp: IPMC for IPv4 IGMP

<vid> : VLAN ID (1-4095) or 'any', default: Show all VLANs
ipmc_param_llqi:
-1 : Default Value (10)
0~31744 : Last Listener Query Interval in tenths of seconds
(default: Show IPMC Interface Last Listener Query Interval

IPMC Parameter URI

Description:
Set or show the IPMC Unsolicited Report Interval.

Syntax:
IPMC Parameter URI [mld|igmp] [<vid>] [ipmc_param_uri]

Parameters:
mld|igmp :
mld : IPMC for IPv6 MLD
igmp: IPMC for IPv4 IGMP
<vid> : VLAN ID (1-4095) or 'any', default: Show all VLANs
ipmc_param_uri:
-1 : Default Value (1)
0~31744 : Unsolicited Report Interval in seconds
(default: Show IPMC Interface Unsolicited Report Interval

6.24 VLAN Control List Command

VCL MAC-based VLAN Configuration

Description:
Show VCL MAC-based VLAN configuration.

Syntax:
VCL Macvlan Configuration

VCL MAC-based VLAN Add

Description:
Add or modify VCL MAC-based VLAN entry.

Syntax:

VCL Macvlan Add <mac_addr> <vid> [<port_list>]

Parameters:
<mac_addr> : MAC address (xx-xx-xx-xx-xx-xx)
<vid> : VLAN ID (1-4095)
<port_list>: Port list or 'all', default: All ports

Example:
Add 00-11-22-33-44-55-66 in VLAN 20 for all port

```
NS3550-8T-2S:/>vcl macvlan add 00-11-22-33-44-55-66 20 1-10
```

VCL MAC-based VLAN Delete

Description:
Delete VCL MAC-based VLAN entry.

Syntax:
VCL Macvlan Del <mac_addr>

Parameters:
<mac_addr> : MAC address (xx-xx-xx-xx-xx-xx)

Example:
Delete 00-11-22-33-44-55-66 in MAC-based VLAN list

```
NS3550-8T-2S:/> vcl macvlan del 00-11-22-33-44-55-66
```

VCL Stasus

Description:
Show VCL MAC-based VLAN users configuration.

Syntax:
VCL Status [combined|static|nas|all]

Parameters:
combined|static|nas|all: VCL User

VCL Protocol-based VLAN Add Ethernet II

Description:
Add VCL protocol-based VLAN Ethernet-II protocol to group mapping.

Syntax:
VCL ProtoVlan Protocol Add Eth2 <ether_type>|arp|ip|ipx|at <group_id>
Parameters:
<ether_type>|arp|ip|ipx|at: Ether Type (0x0600 - 0xFFFF)
<group_id> : Protocol group ID

VCL Protocol-based VLAN Add SNAP

Description:
Add VCL protocol-based VLAN SNAP protocol to group mapping.

Syntax:
VCL ProtoVlan Protocol Add Snap <oui>|rfc_1042|snap_8021h <pid> <group_id>

Parameters:
<oui>|rfc_1042|snap_8021h: OUI value (Hexadecimal 00-00-00 to FF-FF-FF).
<pid> : PID value (0x0-0xFFFF). If OUI is 00-00-00, valid range of PID is from 0x0600-0xFFFF.
<group_id> : Protocol group ID

VCL Protocol-based VLAN Add LLC

Description:

Add VCL protocol-based VLAN LLC protocol to group mapping.

Syntax:
VCL ProtoVlan Protocol Add Llc <dsap> <ssap> <group_id>

Parameters:
<dsap> : DSAP value (0x00-0xFF)
<ssap> : SSAP value (0x00-0xFF)
<group_id>: Protocol group ID

VCL Protocol-based VLAN Delete Ethernet II

Description:
Delete VCL protocol-based VLAN Ethernet-II protocol to group mapping.

Syntax:
VCL ProtoVlan Protocol Delete Eth2 <ether_type>|arp|ip|ipx|at

Parameters:
<ether_type>|arp|ip|ipx|at: Ether Type (0x0600 - 0xFFFF)

VCL Protocol-based VLAN Delete SNAP

Description:
Delete VCL protocol-based VLAN SNAP protocol to group mapping.

Syntax:
VCL ProtoVlan Protocol Delete Snap <oui>|rfc_1042|snap_8021h <pid>

Parameters:
<oui>|rfc_1042|snap_8021h: OUI value (Hexadecimal 00-00-00 to FF-FF-FF).
<pid> : PID value (0x0-0xFFFF). If OUI is 00-00-00, valid range of PID is from 0x0600-0xFFFF.

VCL Protocol-based VLAN Delete LLC

Description:
Delete VCL protocol-based VLAN LLC protocol to group mapping.

Syntax:
VCL ProtoVlan Protocol Delete Llc <dsap> <ssap>

Parameters:
<dsap>: DSAP value (0x00-0xFF)
<ssap>: SSAP value (0x00-0xFF)

VCL Protocol-based VLAN Add

Description:
Add VCL protocol-based VLAN group to VLAN mapping.

Syntax:
VCL ProtoVlan Vlan Add [<port_list>] <group_id> <vid>

Parameters:
<port_list>: Port list or 'all', default: All ports
<group_id> : Protocol group ID
<vid> : VLAN ID (1-4095)

VCL Protocol-based VLAN Delete

Description:
Delete VCL protocol-based VLAN group to VLAN mapping.

Syntax:
VCL ProtoVlan Vlan Delete [<port_list>] <group_id>

Parameters:
<port_list>: Port list or 'all', default: All ports

<group_id> : Protocol group ID

VCL Protocol-based VLAN Configuration

Description:
Show VCL protocol-based VLAN entries.

Syntax:
VCL ProtoVlan Conf

6.25 SMTP Command

SMTP Configuration

Description:
Show SMTP configure.

Syntax:
SMTP Configuration

Default Setting:
disable

SMTP Mode

Description:
Enable or disable SMTP configure.

Syntax:
SMTP Mode [enable|disable]

Parameters:
enable : Enable SMTP mode
disable : Disable SMTP mode
(default: Show SMTP mode)

Default Setting:
disable

SMTP Server

Description:
Set or show SMTP server configure.

Syntax:
SMTP Server [<server>] [<port>]

Parameters:
<server>: SMTP server address
<port> : SMTP server port

Default Setting:
disable

SMTP Auth

Description:
Enable or disable SMTP authentication configure.

Syntax:
SMTP Auth [enable|disable]

Parameters:
enable : Enable SMTP Authentication
disable : Disable SMTP Authentication
(default: Show SMTP Authentication)

Default Setting:
disable

SMTP Auth_user

Description:
Set or show SMTP authentication user name configure.

Syntax:
SMTP Auth_user [<auth_user_text>]
Parameters:
<auth_user_text>: SMTP Authentication User Name

Default Setting:
disable

SMTP Auth_pass

Description:
Set or show SMTP authentication password configure.

Syntax:
SMTP Auth_pass [<auth_pass_text>]

Parameters:
<auth_pass_text>: SMTP Authentication Password

Default Setting:
disable

SMTP Mailfrom

Description:
Set or show SMTP e-mail from configure.

Syntax:
SMTP Mailfrom [<mailfrom_text>]

Parameters:
<mailfrom_text>: SMTP E-mail From address

Default Setting:
disable

SMTP Mailsubject

Description:
Set or show SMTP e-mail subject configure.

Syntax:
SMTP Mailsubject [<mailsubject_text>]

Parameters:
<mailsubject_text>: SMTP E-mail Subject

Default Setting:
disable

SMTP Mailto1

Description:
Set or show SMTP e-mail 1 to configure.

Syntax:
SMTP Mailto1 [<mailto1_text>]

Parameters:
<mailto1_text>: SMTP e-mail 1 to address

Default Setting:
disable

SMTP Mailto2

Description:
Set or show SMTP e-mail 2 to configure.

Syntax:
SMTP Mailto2 [<mailto2_text>]

Parameters:
<mailto1_text>: SMTP e-mail 2 to address

Default Setting:
disable

SMTP Test

Description:
Test the status for linking to SMTP server

Syntax:
SMTP Test

6.26 Ethernet Virtual Connections Command

EVC Configuration

Description:
Show EVC configuration.

Syntax:
EVC Configuration [<port_list>] [<policer_id>]

Parameters:
<port_list> : Port list or 'all', default: All ports
<policer_id>: Policer ID (1-128)

EVC Port DEI

Description:
Set or show port DEI mode.

Syntax:
EVC Port DEI [<port_list>] [<dei_mode>]

Parameters:
<port_list>: Port list or 'all', default: All ports
<dei_mode> : DEI mode: coloured|fixed

EVC Port Tag

Description:
Set or show port tag match mode.

Syntax:
EVC Port Tag [<port_list>] [<tag_mode>]

Parameters:
<port_list>: Port list or 'all', default: All ports
<tag_mode> : Tag mode: inner|outer

EVC Port Addr

Description:
Set or show port address match mode.

Syntax:
EVC Port Addr [<port_list>] [<addr_mode>]

Parameters:
<port_list>: Port list or 'all', default: All ports
<addr_mode>: IP/MAC address mode: source|destination

EVC Port L2CP

Description:
Set or show port L2CP mode

Syntax:
EVC Port L2CP [<port_list>] [<l2cp_list>] [<mode>]

Parameters:
<port_list>: Port list or 'all', default: All ports
<l2cp_list>: L2CP ID list (0-31). BPDU range: 0-15, GARP range: 16-31
<mode> : The mode takes the following values:
normal : Default forwarding
forward : Forward
redirect : Redirect to CPU

EVC Policer

Description:
Set or show EVC bandwidth profile.

Syntax:
EVC Policer [<policer_id>] [enable|disable] [<policer_mode>] [<cir>] [<cbs>] [<eir>] [<ebs>]

Parameters:
<policer_id> : Policer ID (1-128)
enable : Enable policer
disable : Disable policer
<policer_mode>: Policer_mode: coupled|aware
<cir> : Committed Information Rate [kbps]
<cbs> : Committed Burst Size [bytes]
<eir> : Excess Information Rate [kbps]
<ebs> : Excess Burst Size [bytes]

EVC Add

Description:
Add or modify EVC.

Syntax:
EVC Add <evc_id> [<vid>] [<ivid>] [<nni_list>] [<learning>] [inner] [<it_type>] [<it_vid_mode>] [<it_vid>] [<it_preserve>] [<it_pcp>] [<it_dei>] [outer] [<ot_vid>]

Parameters:
<evc_id> : EVC ID (1-128)
<vid> : EVC VLAN ID
<ivid> : Internal VLAN ID
<nni_list> : NNI port list (1-10) or 'none'
<learning> : Learning mode: enable|disable
inner : Inner tag action keyword
<it_type> : Inner tag type: none|c-tag|s-tag|s-custom-tag
<it_vid_mode>: Inner VID mode: normal|tunnel
<it_vid> : Inner tag VLAN ID (1-4095)
<it_preserve>: Inner tag preserved or fixed PCP/DEI: preserved|fixed
<it_pcp> : Inner tag PCP value (0-7)
<it_dei> : Inner tag DEI value (0-1)
outer : Outer tag action keyword
<ot_vid> : EVC outer tag VID for UNI ports

EVC Delete

Description:
Delete EVC.

Syntax:
EVC Delete <evc_id>

Parameters:
<evc_id>: EVC ID (1-128)

EVC Lookup

Description:
Lookup EVC.

Syntax:
EVC Lookup [<evc_id>]

Parameters:
<evc_id>: EVC ID (1-128)

EVC Status

Description:
Show EVC Status.

Syntax:
EVC Status [<evc_id>]

Parameters:
<evc_id>: EVC ID (1-128)

EVC Statistics

Description:
Show or clear EVC statistics.

Syntax:
EVC Statistics [<port_list>] [<class_list>] [<command>]

Parameters:
<port_list> : Port list or 'all', default: All ports
<class_list>: QoS class list, 0-7
<command> : Statistics command: clear|green|yellow|red|discard

EVC ECE Add

Description:
Add or modify EVC Control Entry (ECE):
- If <ece_id> is specified and the ECE exists, the ECE will be modified.
- If <ece_id> is omitted or the ECE does not exist, a new ECE will be added.
- If <ece_id_next> is specified, the ECE will be placed before this entry.
- If <ece_id_next> is 'last', the ECE will be placed at the end of the list.
- If <ece_id_next> is omitted and it is a new ECE, the ECE will be placed last.
- If <ece_id_next> is omitted and the ECE exists, the ECE will not be moved.

Syntax:
EVC ECE Add [<ece_id>] [<ece_id_next>] [uni] [<uni_list>] [<dmac_type>] [<smac>][tag] [<tag_type>] [<vid>] [<pcp>] [<dei>] [all | (ipv4 [<proto>] [<sip>] [<dscp>] [<fragment>] [<sport>] [<dport>]) | (ipv6 [<proto>] [<sip_v6>] [<dscp>] [<sport>] [<dport>])] [direction] [<direction>] [evc] [<evc_id>] [pop] [<pop>] [policy] [<policy>] [class] [<class>] [outer] [<ot_mode>] [<ot_preserve>] [<ot_pcp>] [<ot_dei>]

Parameters:
<ece_id> : ECE ID (1-128)
<ece_id_next>: Next ECE ID (1-128) or 'last'
uni : UNI keyword
<uni_list> : UNI port list (1-10)
<dmac_type> : DMAC type: any|unicast|multicast|broadcast
<smac> : SMAC or 'any'
tag : Tag matching keyword
<tag_type> : Tag type: tagged|untagged|any
<vid> : VLAN ID value/range (0-4095) or 'any'
<pcp> : PCP value/range (0-7) or 'any'
<dei> : DEI value, 0, 1 or 'any'
all : Keyword for matching any frame type
ipv4 : Keyword for matching IPv4 frames
<proto> : IP protocol value (0-255) or 'any'
<sip> : IPv4 source address (a.b.c.d/n) or 'any'
<dscp> : DSCP value/range (0-63) or 'any'
<fragment> : IPv4 fragment: any|fragment|non-fragment
<sport> : UDP/TCP source port value/range (0-65535) or 'any'
<dport> : UDP/TCP destination port value/range (0-65535) or 'any'
ipv6 : Keyword for matching IPv6 frames
<sip_v6> : IPv6 source address (a.b.c.d/n) or 'any'
direction : Direction keyword
<direction> : ECE direction: both|uni-to-nni|nni-to-uni

evc : EVC keyword
<evc_id> : EVC ID (1-128) or 'none'
pop : Pop keyword
<pop> : Tag pop count: 0|1|2
policy : Policy keyword
<policy> : ACL policy number (0-255)
class : Class keyword
<class> : QoS class, 'disable' or 0-7
outer : Outer tag action keyword
<ot_mode> : Outer tag for nni-to-uni direction: enable|disable
<ot_preserve>: Outer tag preserved or fixed PCP/DEI: preserved|fixed
<ot_pcp> : Outer tag PCP value (0-7)
<ot_dei> : Outer tag DEI value (0-1)

EVC ECE Delete

Description:
Delete ECE.

Syntax:
EVC ECE Delete <ece_id>

Parameters:
<ece_id>: ECE ID (1-128)

EVC ECE Lookup

Description:
Lookup ECE.

Syntax:
EVC ECE Lookup [<ece_id>]
Parameters:
<ece_id>: ECE ID (1-128)

EVC ECE Status

Description:
Show ECE Status.

Syntax:
EVC ECE Status [<ece_id>]

Parameters:
<ece_id>: ECE ID (1-128)

6.27 Ethernet Protection Switching Command

EPS Create

Description:
EPS create.

Syntax:
EPS create [<inst>] [domport|dompath|domservice|dommpls] [1p1|1f1] [<flow_w>] [<flow_p>] [<mep_w>] [<mep_p>][<mep_aps>] [enable|disable]

Parameters:
<inst> : Instance number
domport|dompath|domservice|dommpls: Flow domain

1p1|1f1 : EPS architecture

<flow_w> : Working flow instance number
<flow_p> : Protecting flow instance number
<mep_w> : Working MEP instance number
<mep_p> : Protecting MEP instance number
<mep_aps> : APS MEP instance number
enable|disable : enable/disable protection

EPS Config

Description:
EPS config operation.

Syntax:
EPS config [<inst>] [aps|noaps] [revert|norevert] [unidir|bidir] [w0s|w10s|w30s|w1m|w5m|w12m][h0s|h100ms|h500ms|h1s|h2s|h5s|h10s]

Parameters:
<inst> : Instance number
aps|noaps : APS enable/disable

revert|norevert : Revertive enable/disable

unidir|bidir : Unidirectional or bidirectional switching

w0s|w10s|w30s|w1m|w5m|w12m : Wait to restore timer value

h0s|h100ms|h500ms|h1s|h2s|h5s|h10s: Hold off timer value

EPS Command

Description:
EPS command set operation.

Syntax:
EPS command [<inst>] [clear|lockout|forced|manualp|manualw|exercise|freeze|lockoutlocal]

Parameters:
<inst> : Instance number
clear|lockout|forced|manualp|manualw|exercise|freeze|lockoutlocal: EPS protection command type - clear is 'no command active'

EPS State

Description:

Get protection state.

Syntax:
EPS state [<inst>]

Parameters:
<inst>: Instance number

6.28 Maintainence entity End Point Command

MEP Config

Description:
MEP instance configuration
'mep|mip' this entity is either a MEP or a MIP - end point or intermediate point
'ingress|egress' this entity is either a Ingress (down) or Egress (up) type of MEP/MIP
'domport|domevc' the domain is either Port or EVC
'level' is the MEG level
'port' is the residence port
'flow' is the related flow instance number - Port number in Port domain - EVC number in EVC domain
'vid' is used for TAGGED OAM in port domain
'itu|ieee' is the MEG ID format
'meg' is the MEG ID - max. 8 char in case of 'ieee' - 6 or 7 char in case of 'itu'
'mep' is the MEP ID.

Syntax:
MEP config [<inst>] [mep|mip] [ingress|egress] [<port>] [domport|domevc] [<level>] [itu|ieee] [<meg>] [<mep>] [<vid>] [<flow>] [enable|disable]

Parameters:
<inst> : Instance number
mep|mip : Mode of the MEP instance
ingress|egress: Direction of the MEP instance
<port> : Port number.
domport|domevc: Flow domain
<level> : MEP level (0-7)
itu|ieee : MEG format
ITU: ICC format as defined in Y.1731 ANNEX A
IEEE: String format Domain Name and Short Name as defined in 802.1ag
<meg> : MEG ID (max. 8 chars)
<mep> : This MEP id (0-0x1FFF)
<vid> : C-TAG only applicable for Port MEP
<flow> : Flow instance number (Port/EVC)
enable|disable: enable/disable

MEP Peer MEP

Description:
MEP Peer MEP id configuration.

Syntax:
MEP peer MEP [<inst>] [<mep>] [<mac_addr>] [enable|disable]

Parameters:
<inst> : Instance number
<mep> : This MEP id (0-0x1FFF)
<mac_addr> : MAC address ('xx-xx-xx-xx-xx-xx' or 'xx.xx.xx.xx.xx.xx' or 'xxxxxxxxxxxx', x is a hexadecimal digit)
enable|disable: enable/disable

MEP Continuity Check Configuration

Description:
MEP Continuity Check configuration
'prio' is the priority (PCP) of transmitted CCM frame
'300s|100s|10s|1s|6m|1m|6h' is the number of CCM frame pr. second.

Syntax:
MEP cc config [<inst>] [<prio>] [300s|100s|10s|1s|6m|1m|6h] [enable|disable]

Parameters:
<inst> : Instance number
<prio> : OAM PDU priority
300s|100s|10s|1s|6m|1m|6h: OAM period (100s -> 100 PDU pr. second)
enable|disable : enable/disable

MEP Loss Measurement Configuration

Description:
MEP Loss Measurement configuration
'prio' is the priority (PCP) of transmitted LM frame
'uni|multi' is selecting uni-cast or multi-cast transmission of LM frame
'single|dual' is selecting single-ended (LMM) or dual-ended (CCM) LM
'10s|1s|6m|1m|6h' is the number of LM frame pr. second
'flr' is the Frame Loss Ratio time interval.

Syntax:
MEP lm config [<inst>] [<prio>] [uni|multi] [single|dual] [10s|1s|6m|1m|6h] [<flr>] [enable|disable]

Parameters:
<inst> : Instance number
<prio> : OAM PDU priority
uni|multi : Destination address is unicast or multicast
single|dual : LM is single or dual ended
10s|1s|6m|1m|6h: LM period (10s -> 10 PDU pr. second)
<flr> : Frame loss ratio (in sec.)
enable|disable : enable/disable

MEP APS Configuration

Description:
MEP APS configuration
'prio' is the priority (PCP) of transmitted APS frame
'uni|multi' is selecting uni-cast or multi-cast transmission of APS frame
'laps|raps' is selecting ELPS or ERPS protocol
'octet' is the last octet in RAPS multicast MAC.

Syntax:
MEP aps config [<inst>] [<prio>] [uni|multi] [laps|raps] [<octet>] [enable|disable]

Parameters:
<inst> : Instance number
<prio> : OAM PDU priority
uni|multi : Destination address is unicast or multicast
laps|raps : Selection of Linear or Ring APS type
<octet> : The last octet in RAPS multicast MAC
enable|disable: enable/disable

MEP Client Configuration

Description:
MEP Client configuration
'domport|domevc' is the client domain - must be EVC
'level' is the client MEG level - the contained level in the AIS and LCK frames

'cflow' is the client flow instance - up to 10 possible client flows (EVC).

Syntax:

MEP client config [<inst>] [domport|domevc] [<level>] [<cflow>] [<cflow>] [<cflow>] [<cflow>] [<cflow>] [<cflow>] [<cflow>] [<cflow>] [<cflow>] [<cflow>]

Parameters:

<inst> : Instance number
domport|domevc: Flow domain
<level> : MEP level (0-7)
<cflow> : Client flow instance number (EVC)

MEP AIS Configuration

Description:

MEP AIS configuration
'prio' is the priority (PCP) of transmitted AIS frame
'1s|1m' is the number of AIS frame pr. second
'set|clear' is set or clear of protection usability. If set, the first 3 AIS frames are transmitted as fast as possible - this gives protection reliability in the path end-point.

Syntax:

MEP ais config [<inst>] [<prio>] [1s|1m] [set|clear] [enable|disable]

Parameters:

<inst> : Instance number
<prio> : OAM PDU priority
1s|1m : Transmit period for AIS
1s - to send OAM Frames in the rate of 1 per second
1m - to send OAM frames in the rate of 1 per minute
set|clear : Protection usability set/clear
enable|disable: enable/disable

MEP LCK Configuration

Description:

MEP LCK configuration
'prio' is the priority (PCP) of transmitted AIS frame
'1s|1m' is the number of AIS frame pr. second.

Syntax:

MEP lck config [<inst>] [<prio>] [1s|1m] [enable|disable]

Parameters:

<inst> : Instance number
<prio> : OAM PDU priority
1s|1m : Transmit period for LCK
1s - to send OAM Frames in the rate of 1 per second
1m - to send OAM frames in the rate of 1 per minute
enable|disable: enable/disable

MEP Link Trace Configuration

Description:

MEP Link Trace configuration
'prio' is the priority (PCP) of transmitted LTM frame
'mac_addr' is the unicast MAC of target MEP/MIP
'mep' is the peer MEP-ID of target MEP - only used if 'mac_addr is 'all zero'
'tll' is the TLL in the transmitted LTM.

Syntax:

MEP lt config [<inst>] [<prio>] [<mac_addr>] [<mep>] [<ttl>] [enable|disable]

Parameters:

<inst> : Instance number
<prio> : OAM PDU priority

<mac_addr> : MAC address ('xx-xx-xx-xx-xx-xx' or 'xx.xx.xx.xx.xx.xx' or 'xxxxxxxxxxxx', x is a hexadecimal digit)
<mep> : This MEP id (0-0x1FFF)
<ttl> : LT - Time To Live
enable|disable: enable/disable

MEP Loop Back Configuration

Description:

MEP Loop Back configuration
'set|clear' is set or clear of DEI of transmitted LBM frame
'prio' is the priority (PCP) of transmitted LBM frame
'uni|multi' is selecting uni-cast or multi-cast transmission of LBM frame
'mac_addr' is the unicast MAC of target MEP/MIP
'mep' is the peer MEP-ID of target MEP - only used if 'mac_addr is 'all zero'
'tosend' is the number of LBM to send
'size' is the size of the LBM data field
'gap' is the gap between LBM.

Syntax:

MEP lb config [<inst>] [set|clear] [<prio>] [uni|multi] [<mac_addr>] [<mep>] [<tosend>] [<size>] [<gap>] [enable|disable]

Parameters:

<inst> : Instance number
set|clear : OAM DEI set/clear
<prio> : OAM PDU priority
uni|multi : Destination address is unicast or multicast
<mac_addr> : MAC address ('xx-xx-xx-xx-xx-xx' or 'xx.xx.xx.xx.xx.xx' or 'xxxxxxxxxxxx', x is a hexadecimal digit)
<mep> : This MEP id (0-0x1FFF)
<tosend> : Number of LBM to send
<size> : Size of LBM data field in bytes (max 1400)
<gap> : Gap between LBM to send in 10ms. (max 100 - '0' is as fast as possible)
enable|disable: enable/disable

MEP Delay Measurement Configuration

Description:

MEP Delay Measurement configuration
'prio' is the priority (PCP) of transmitted DM frame
'uni|multi' is selecting uni-cast or multi-cast transmission of DM frame
'mep' is the peer MEP-ID of target MEP - only used if 'uni'
'oneway|twoway' is selecting one-way (1DM) or two-way (DMM) DM
'std|prop' is selecting standadized or proprietary DM. the latest is using off-standard follow-up message carrying the exact HW transmit timestamp
'rdtrp|flow' is selecting round-trip or flow delay calculation. Round-trip is not using the far-end timestamps to calculate the far-end residence time
'gap' Gap between transmitting 1DM/DMM PDU - in 10 ms.
'count' number of frames used for average calculation on the latest 'count' frames received
'us|ns' calculation results are shown in micro or nano seconds
'keep|reset' the action in case of total delay counter overflow - either 'keep' all results or 'reset' all results
'd2ford1' this is selecting to used two-way DMM for calculate one-way delay.

Syntax:

MEP dm config [<inst>] [<prio>] [uni|multi] [<mep>] [oneway|twoway] [std|prop] [rdtrp|flow] [<gap>] [<count>] [us|ns] [keep|reset] [d2ford1] [enable|disable]

Parameters:

<inst> : Instance number
<prio> : OAM PDU priority
uni|multi : Destination address is unicast or multicast
<mep> : This MEP id (0-0x1FFF)
oneway|twoway : DM is one-way or two-way
std|prop : Standard or Vitesse proprietary way(w/ follow-up packets) to send DM
rdtrp|flow : 2/4 timestamps selection
<gap> : Gap between 1DM/DMM to send in 10ms(10-65535).
<count> : The number of last records to calculate(10 - 2000)
us|ns : Time resolution
keep|reset : The action to counter when overflow happens
d2ford1 : Enable to use DMM/DMR packets to calculate one-way DM

enable|disable: enable/disable

MEP Test Signal Configuration

Description:
MEP Test Signal configuration
'set|clear' is set or clear of DEI of transmitted LBM frame
'prio' is the priority (PCP) of transmitted TST frame
'mep' is the peer MEP-ID of target MEP - only used if 'mac_addr is 'all zero'
'no_seq|seq' is without and with transmitted sequence numbers
'rate' is the TST frame transmission bit rate in Mbps'
'size' is the size of the un-tagged TST frame - four bytes will be added for each tag
'allzero|allone|onezero' is pattern contained in the TST frame data TLV.

Syntax:
MEP tst config [<inst>] [set|clear] [<prio>] [<mep>] [no_seq|seq] [<rate>] [<size>] [allzero|allone|onezero] [enable|disable]

Parameters:
<inst> : Instance number
set|clear : OAM DEI set/clear
<prio> : OAM PDU priority
<mep> : This MEP id (0-0x1FFF)
no_seq|seq : TST sequence number transmission
<rate> : Transmission bit rate of TST frames - in Mbps
<size> : Size of TST data field in bytes (max 1518)
allzero|allone|onezero: Data pattern to be filled in TST PDU
enable|disable : enable/disable

MEP State

Description:
MEP state get.

Syntax:
MEP state [<inst>]

Parameters:
<inst> : Instance number

MEP Loss Measurement State

Description:
MEP Loss Measurement state get.

Syntax:
MEP lm state [<inst>]

Parameters:
<inst> : Instance number

MEP Loss Measurement State Clear

Description:
MEP Loss Measurement state clear

Syntax:
MEP lm clear <inst>

Parameters:
<inst> : Instance number

MEP Link Trace State

Description:

MEP Link Trace state get.

Syntax:
MEP lt state [<inst>]

Parameters:
<inst> : Instance number

MEP Loop Back State

Description:
MEP Loop Back state get.

Syntax:
MEP lb state [<inst>]

Parameters:
<inst> : Instance number

MEP Delay Measurement State

Description:
MEP Delay Measurement state get.

Syntax:
MEP dm state [<inst>]

Parameters:
<inst> : Instance number

MEP Delay Measurement State Clear

Description:
MEP Delay Measurement state clear

Syntax:
MEP dm clear <inst>

Parameters:
<inst> : Instance number

MEP Test Signal State

Description:
MEP Test Signal state get
RX rate is shown in 100 Kbps.

Syntax:
MEP tst state [<inst>]

Parameters:
<inst> : Instance number

MEP Test Signal State Clear

Description:
MEP Test Signal state clear

Syntax:
MEP tst clear <inst>

Parameters:
<inst> : Instance number

6.29 Ethernet Ring Protection Switching Command

ERPS Command

Description:
Invoking an administrative command for a given protection group
[fs|ms|clear] : setting or clearing an administrative command for a given group
<port> : forced a block on the ring port where this command is issued
<group_id> : protection group id

Syntax:
Erps command [fs|ms|clear] <port> <group-id>

Parameters:
fs|ms|clear: administrative commands

<port> : Port number
<group-id> : protection group id 1 - 64

ERPS Version

Description:
Specifying protocol version for a given protection group
[v1|v2] : specifying protocol version for a given protection group
<group_id> : protection group id

Syntax:
Erps version [v1|v2] <group-id>

Parameters:
v1|v2 : ERPS protocol version to be supported
<group-id>: protection group id 1 - 64

ERPS Add

Description:
create a new ethernet ring protection group
<group-id> : protection group id
<east_port> : protection group Port 0
<west_port> : protection group Port 1, Port 1 can be 0 for sub-rings
[major|sub] : ring type i.e major-ring or sub-ring
[interconnected] : interconnection node or not
[[virtual_channel] : Virtual channel present or not
[<major-ring-id>] : major ring group Id for interconnected sub-ring

Syntax:
Erps add <group-id> <east_port> <west_port> [major|sub] [interconnected] [virtual_channel] [<major-ring-id>]

Parameters:
<group-id> : protection group id 1 - 64
<east_port> : Port 0 of a protection group
<west_port> : Port 1 of a protection group
major|sub : ring type
interconnected : Set for interconnected node
virtual_channel: Set for virtual channel
<major-ring-id>: major ring of a sub-ring, when configuring as an interconnected node

ERPS Reversion

Description:
Configuring reversion characteristics for a given node
[revertive|nonrevertive] : enabling or disabling reversion for a given group
<group_id> : protection group id

Syntax:
Erps reversion [revertive|nonrevertive] <group-id>

Parameters:
revertive|nonrevertive: specifying reversion parameters
<group-id> : protection group id 1 - 64

ERPS VLAN Add

Description:
Associating a given vlan to a protection group
<vid> : vlan to be protected
<group-id> : protection group-id for which vid belongs to.

Syntax:
Erps vlan add <vid> <group-id>

Parameters:
<vid> : VLAN ID (1-4095)
<group-id>: protection group id 1 - 64

ERPS VLAN Delete

Description:
Disassociating a given vlan to a protection group
<vid> : protected vlan to be deleted
<group-id> : protection group-id for which vid belongs to.

Syntax:
Erps vlan delete <vid> <group-id>

Parameters:
<vid> : VLAN ID (1-4095)
<group-id>: protection group id 1 - 64

ERPS MEP

Description:
Associating Port 0/1 MEP to a protection group
<east_sf_mep> : Mep_ID for finding out Continuity Check errors on Port 0
<west_sf_mep> : Mep_ID for finding out Continuity Check errors on Port 1
<east_raps_mep> : Mep_ID for transmitting R-APS frames on Port 0
<west_raps_mep> : Mep_ID for transmitting R-APS frames on Port 1
<group_id> : protection group id for which mep is associating.

Syntax:
Erps mep <east_sf_mep> <west_sf_mep> <east_raps_mep> <west_raps_mep> <group-id>

Parameters:
<east_sf_mep> : SF mep id for Port 0
<west_sf_mep> : SF mep id for Port 1
<east_raps_mep>: CC/RAPS mep id for Port 0
<west_raps_mep>: CC/RAPS mep id for Port 1
<group-id> : protection group id 1 - 64

ERPS RPL Neighbour

Description:
Selection of RPL neighbour for a protection group
(east|west) : selected east(Port 0) or west(Port 1) as RPL neighbour
<group-id> : protection group id for selecting RPL Block.

Syntax:
Erps rpl neighbour <rpl_port> <group-id>

Parameters:
<rpl_port>: RPL Block
<group-id>: protection group id 1 - 64

ERPS RPL Owner

Description:
Selection of RPL Block for a protection group
by default this node is considered as RPL Owner
(east|west) : select east(Port 0) or west(Port 1) as RPL Block
<group-id> : protection group id for selecting RPL Block.

Syntax:
Erps rpl owner <rpl_port> <group-id>

Parameters:
<rpl_port>: RPL Block
<group-id>: protection group id 1 - 64

ERPS RPL Neighbour Clear

Description:
make this node as non-neighbour for a protection group
<group-id> : protection group id for selecting RPL Block.

Syntax:
Erps rpl neighbour clear <group-id>

Parameters:
<group-id>: protection group id 1 - 64

ERPS RPL Owner Clear

Description:
making a node as Non-RPL Block for a protection group
After clear, this node is nore an rpl owner for the given group
(east|west) : selected east(Port 0) or west(Port 1) as RPL Block
<group-id> : protection group id for selecting RPL Block.

Syntax:
Erps rpl owner clear <group-id>

Parameters:
<group-id>: protection group id 1 - 64

ERPS Hold Off Timeout

Description:
configuring hold off timeout for a protection group
in milliseconds 0-10000 in the increments of 100ms
<hold_timeout> : hold-off timeout
<group-id> : protection group id for configuring hold-off time.

Syntax:
Erps hold off timeout <hold_timeout> <group-id>

Parameters:
<hold_timeout>: timer timeout values
<group-id> : protection group id 1 - 64

ERPS Guard-timeout

Description:
configuring guard timeout for a protection group
guard timeout should be configured in the increments of 10 milliseconds
minimum guard timeout 10ms and maximum 2 seconds
<guard_timeout> : guard timeout
<group-id> : protection group id for configuring guard time.

Syntax:
Erps guard-timeout <guard_timeout> <group-id>

Parameters:
<guard_timeout>: timer timeout values
<group-id> : protection group id 1 - 64

ERPS WRT-timeout

Description:
configuring wait to restore timeout for a protection group
in minutes in the range of 1 to 12 minutes
<wtr_timeout> : configuring wtr timeout
<group-id> : protection group id for configuring wtr time.

Syntax:
Erps wtr-timeout <wtr_timeout> <group-id>

Parameters:
<wtr_timeout>: timer timeout values
<group-id> : protection group id 1 - 64

ERPS Delete

Description:
deletion of a protection group
<group-id> : protection group id for deletion .

Syntax:
Erps delete <group-id>

Parameters:
<group-id>: protection group id 1 - 64

ERPS Topologychange

Description:
specifying topology change propagation parameters for a given protection group
[propagate|nopropagate] : enabling or disabling topology change propagation for a given group
<group_id> : protection group id
.

Syntax:
Erps topologychange [propagate|nopropagate] <group-id>

Parameters:
propagate|nopropagate: topology change propagation configuration
<group-id> : protection group id 1 - 64

ERPS Configurationt

Description:
deletion of a protection group
<group-id> : protection group id
[statistics] : for displaying R-APS statistics
[clear] : for clearing R-APS statistics.

Syntax:
Erps configuration [<group-id>] [statistics|clear]

Parameters:
<group-id> : protection group id 1 - 64
statistics|clear: ERPS statistics

6.30 PTP Command

PTP Configuration

Description:
Set or show PTP configuration.

Syntax:
PTP Configuration [<clock inst>]

Parameters:
<clock inst>: Clock instance number [0…3]

Default Setting:
disable

PTP PortState

Description:
Set or show PTP port state.

Syntax:
PTP PortState <clockinst> [<port_list>] [enable|disable|internal]

Parameters:
<clockinst>: Clock instance number [0…3]
<port_list>: Port list or "all", default: All ports
Enable: Enable PTP port.
Disable: Disable PTP port.
Internal: Enable PTP port as internal (in a distributed environment)

Default Setting:
Show actual port state

PTP ClockCreate

Description:
Create or show a PTP clock instance data..

Syntax:
PTP ClockCreate <clockinst> [<devtype>] [<twostep>] [<protocol>] [<oneway>] [<clockid>] [<tag_enable>] [<vid>] [<prio>]

Parameters:
<clockinst> : clock instance number [0..3]
<devtype> : The devtype parameter takes the following values:
ord : Ordinary/Boundary clock
p2p: Peer-to-peer transparent clock
e2e: End-to-end transparent clock
mst: Master only clock
slv: Slave only clock
(default: Show actual init parameters)
<twostep>: The twostep parameter takes the following values:
true: Follow-up messages are used
false: No follow-up messages are used
<protocol>: The protocol parameter takes the following values:
ethernet : The clock uses multicast Ethernet protocol
ip4multi : The clock uses IPv4 multicast protocol
ip4uni: The clock uses IPv4 unicast protocol
Note: IPv4 unicast protocol only works in Master only and Slave only clocks
See parameter <devtype>

In a unicast Slave only clock you also need configure which master clocks to request Announce and Sync messages from. See command UniConfig

<oneway>: The oneway parameter takes the following values:
true: The clock slave uses one-way measurements, i.e. no delay requests
false: The clock slave uses two-way measurements
<clockid>: 8 byte clock identity(xx:xx:xx:xx:xx:xx:xx:xx)
<tag_enable>: The tag_enable parameter takes the following values:
true: The ptp frames are tagged with the VLAN tag specified in the VID field.
Note : Packets are only tagged if the port is configured for vlan tagging. i.e: Port Type != Unaware and PortVLAN mode == None.
false: The ptp frames are sent untagged.
<vid>: The VID parameter takes the following values:
0 - 4095 : The range of VID's ptp can use to send tagged frames
<prio>: The Prio parameter takes the following values:
0 - 7: The range of Priorities ptp can use in the tagged frames

PTP ClockDelete

Description:
Delete a PTP clock instance.

Syntax:
PTP ClockDelete <clockinst> [<devtype>]

Parameters:
<clockinst>: clock instance number [0..3]
<devtype> : The devtype parameter takes the following values:
ord: Ordinary/Boundary clock
p2p: Peer-to-peer transparent clock
e2e: End-to-end transparent clock
mst: Master only clock
slv: Slave only clock
(default: Show actual init parameters**)**

PTP DefaultDS

Description:
Set or show PTP clock Default Data set priority1 and priority2 are used in the best master clock algorithm. Lower values take precedence.

Syntax:
PTP DefaultDS <clockinst> [<priority1>] [<priority2>] [<domain>]

Parameters:
<clockinst>: clock instance number [0..3]
<priority1>: [0..255] Clock priority 1 for PTP BMC algorithm
<priority2>: [0..255] Clock Priority 2 for PTP BMC algorithm
<domain>: [0..127] PTP clock domain id (0 = default) for PTP

PTP CurrentDS

Description:
Show PTP clock Current Data set.

Syntax:
PTP CurrentDS <clockinst>

Parameters:
<clockinst>: clock instance number [0..3]

PTP ParentDS

Description:
Show PTP clock Parent Data set.

Syntax:
PTP ParentDS <clockinst>

Parameters:
<clockinst>: clock instance number [0..3]

PTP Timingproperties

Description:
Set or show PTP clock Timing properties Data set.

Syntax:
PTP Timingproperties <clockinst> [<utcoffset>] [<valid>] [<leap59>] [<leap61>] [<timetrac>] [<freqtrac>] [<ptptimescale>] [<timesource>]

Parameters:
<clockinst>: clock instance number [0..3]
<utcoffset>: PTP clock offset between UTC and TAI in seconds
<valid>: The offsetvalid parameter takes the following values:
false: The UTC offset is not valid
true: The UTC offset is valid
<leap59>: The leap59 parameter takes the following values:
false: no leap59 in current day
true: last minute of current day contains 59 sec.
<leap61>: The leap61 parameter takes the following values:
false: no leap61 in current day
true: last minute of current day contains 61 sec.
<timetrac>: The timetraceable parameter takes the following values:
false: timing is not traceable
true: timing is traceable.
<freqtrac>: The freqtraceable parameter takes the following values:
False: frequency is not traceable
true: frequency is traceable.
<ptptimescale>: The timescale parameter takes the following values:
false: timing is not a PTP time scale
true: timing is a PTP time scale.
<timesource>: [0..255] Time source.
16 (0x10) ATOMIC_CLOCK
32 (0x20) GPS
48 (0x30) TERRESTRIAL_RADIO
64 (0x40) PTP
80 (0x50) NTP
96 (0x60) HAND_SET
144 (0x90) OTHER
160 (0xA0) INTERNAL_OSCILLATOR

PTP PortDataSet

Description:
Set or show PTP port data set.

Syntax:
PTP PortDataSet <clockinst> [<port_list>] [<announceintv>] [<announceto>] [<syncintv>] [<delaymech>] [<minpdelayreqintv>] [<delayasymmetry>] [<ingressLatency>] [<egressLatency>]

Parameters:
<clockinst>: clock instance number [0..3]
<port_list>: Port list or 'all', default: All ports
<announceintv>: [-3..4] Log2 of mean announce interval in sec.
<announceto>: [-1..10] Log2 of announce receipt timeout in sec.
<syncintv>: [-7..4] Log2 of sync interval in sec.
<delaymech>: The delaymech parameter takes the following values:
  e2e: The port is configured to use the delay request-response mechanism
  p2p: The port is configured to use the peer delay mechanism
<minpdelayreqintv>: [-7..5] Log2 of min delay req interval in sec.
<delayasymmetry>: path delay asymmetry measured in ns
<ingresslatency>: ingress latency measured in ns
<egresslatency>: egress latency measured in ns

PTP LocalClock

Description:
Update or show PTP current time, or set master clock ratio.

Syntax:
PTP LocalClock <clockinst> [update|show|ratio] [<clockratio>]

Parameters:
<clockinst>: clock instance number [0..3]
update|show|ratio: PTP local clock
  update: The local clock is synchronized to the eCos system clock
  show: The local clock current time is shown
  ratio: Set the local master clock frequency ratio in units of 0,1 PPB
    (ratio > 0 => faster clock, ratio < 0 => slower clock)
<clockratio>: [-10.000.000..+10.000.000] Clock frequency ratio in 0,1 PPB.

PTP Filter

Description:
Set or show PTP clock filter data.

Syntax:
PTP Filter <clockinst> [<def_delay_filt>] [<period>] [<dist>]

Parameters:
<clockinst>: clock instance number [0..3]
<def_delay_filt>: [1..6] Log2 of timeconstant in delay filter.
<period>: [1..1000] Measurement period in number of sync events.
  Note: In configurations with Timestamp enabled PHYs, the period is autom atically increased, if (period*dist < SyncPackets pr sec/4), i.e. max 4 adjustments are made pr sec.
<dist>: [1..10] Distance between servo update n number of measurement periods, if Distance is 1 the offset is averaged over the 'period', if Distance is >1 the offset is calculated using 'min' offset.

PTP Servo

Description:
Set or show PTP clock servo data.

Syntax:
PTP Servo <clockinst> [<displaystates>] [<ap_enable>] [<ai_enable>] [<ad_enable>] [<ap>] [<ai>] [<ad>]

Parameters:
<clockinst>: clock instance number [0..3]
<displaystates>: The displaystates parameter takes the following values:
  true: Display clock state and measurements
  false: don't display

<ap_enable>:
  true: Enable the 'P' component in regulator
  false: Disable the 'P' component in regulator
<ai_enable>:
  true: Enable the 'I' component in regulator
  false: Disable the 'I' component in regulator
<ad_enable>:
  true: Enable the 'D' component in regulator
  false: Disable the 'D' component in regulator
<ap>: [1..1000] 'P' component in regulator
<ai>: [1..10000] 'I' component in regulator.
<ad>: [1..10000] 'D' component in regulator.

PTP SlaveTableUnicast

Description:
Show the Unicast slave table of the requested unicast masters.

Syntax:
PTP SlaveTableUnicast <clockinst>

Parameters:
<clockinst>: clock instance number [0..3]

PTP SlaveTableUnicast

Description:
Set or show the Unicast Slave configuration.

Syntax:
PTP UniConfig <clockinst> [<index>] [<duration>] [<ip_addr>]

Parameters:
<clockinst>: clock instance number [0..3]
<index>: [0..4] Index in the slave table.
<duration>: [10..1000] Number of seconds for which the Announce/Sync messages are requested.
<ip_addr>: IPv4 address of requested master clock.

PTP ForeignMasters

Description:
Show PTP port foreign masters data set.

Syntax:
PTP ForeignMasters <clockinst> [<port_list>]

Parameters:
<clockinst>: clock instance number [0..3]
<port_list>: Port list or 'all', default: All ports

PTP EgressLatency

Description:
Show or clear the One-step egress latency observed in systems where the timestam ping is done in SW.

Syntax:
PTP EgressLatency [show|clear]

Parameters:
  show: Show the observed Egress latency
  clear: Clear the observed Egress latency

PTP MasterTableUnicast

Description:
Show the Unicast master table of the slaves that have requested unicast communication.

Syntax:
PTP MasterTableUnicast <clockinst>

Parameters:
<clockinst>: clock instance number [0..3]

PTP ExtClockMode

Description:
Update or show the 1PPS and External clock output configuration and vcxo frequency rate adjustment option.
Luton26 has only one physical port, i.e. the one pps mode overrules the external clock outout, therefore if one_pps_mode != disable, the ext_enable is ignored. (If vcxo mode is changed, the node must be restarted).

Syntax:
PTP ExtClockMode [<one_pps_mode>] [<ext_enable>] [<clockfreq>] [<vcxo_enable>]

Parameters:
<one_pps_mode>:
output: Enable the 1 pps clock output
input: Enable the 1 pps clock input
disable: Disable the 1 pps clock in/out-put
<ext_enable>:
true: Enable the external clock output
false: Disable the external clock output
<clockfreq>: [1..25.000.000] External Clock output frequency in Hz.
<vcxo_enable> :
true: Enable the external VCXO rate adjustment
false: Disable the external VCXO rate adjustment

PTP OnePpsAction

Description:
Show [and clear] One PPS statistics.

Syntax:
PTP OnePpsAction [<one_pps_clear>]

Parameters:
<one_pps_clear>: default Dump statistics [1] Clear statistics.

7. SWITCH OPERATION

7.1 Address Table

The **Industrial Managed Switch** is implemented with an address table. This address table composed of many entries. Each entry is used to store the address information of some node in network, including MAC address, port no, etc. This in-formation comes from the learning process of **Industrial Managed Switch**.

7.2 Learning

When one packet comes in from any port, the **Industrial Managed Switch** will record the source address, port no. And the other related information in address table. This information will be used to decide either forwarding or filtering for future packets.

7.3 Forwarding & Filtering

When one packet comes from some port of the **Industrial Managed Switch**, it will also check the destination address besides the source address learning. The **Industrial Managed Switch** will lookup the address-table for the destination address. If not found, this packet will be forwarded to all the other ports except the port, which this packet comes in. And these ports will transmit this packet to the network it connected. If found, and the destination address is located at different port from this packet comes in, the **Industrial Managed Switch** will forward this packet to the port where this destination address is located according to the information from address table. But, if the destination address is located at the same port with this packet comes in, then this packet will be filtered. Thereby increasing the network throughput and availability

7.4 Store-and-Forward

Store-and-Forward is one type of packet-forwarding techniques. A Store-and-Forward **Industrial Managed Switch** stores the incoming frame in an internal buffer, do the complete error checking before transmission. Therefore, no error packets occurrence, it is the best choice when a network needs efficiency and stability.

The **Industrial Managed Switch** scans the destination address from the packet-header, searches the routing table pro-vided for the incoming port and forwards the packet, only if required. The fast forwarding makes the switch attractive for connecting servers directly to the network, thereby increasing throughput and availability. How-ever, the switch is most commonly used to segment existence hubs, which nearly always improves overall performance. An Ethernet Switching can be easily configured in any Ethernet network environment to signifi-cantly boost bandwidth using conventional cabling and adapters.

Due to the learning function of the **Industrial Managed Switch**, the source address and corresponding port number of each incoming and outgoing packet are stored in a routing table. This information is subsequently used to filter packets whose destination address is on the same segment as the source address. This confines network traffic to its respective domain and reduce the overall load on the network.

The **Industrial Managed Switch** performs **"Store and Fforward"** therefore, no error packets occur. More reliably, it reduces the re-transmission rate. No packet loss will occur.

7.5 Auto-Negotiation

The STP ports on the **Industrial Managed Switch** have built-in **"Auto-negotiation"**. This technology automatically sets the best possible bandwidth when a connection is established with another network device (usually at Power On or Reset). This is done by detect the modes and speeds at the second of both device is connected and capable of, both 10Base-T and 100Base-TX devices can connect with the port in either Half- or Full-Duplex mode. 1000Base-T can be only connected in Full-duplex mode.

8. TROUBLE SHOOTING

This chapter contains information to help you solve problems. If the **Industrial Managed Switch** is not functioning properly, make sure the Ethernet Switch was set up according to instructions in this manual.

The per port LED is not lit

Solution:

Check the cable connection of the **Industrial Managed Switch**.

Performance is bad

Solution:

Check the speed duplex mode of the partner device. The **Industrial Managed Switch** is run at Auto-negotiation mode and if the partner is set to half duplex, then the performance will be poor.

Per port LED is lit, but the traffic is irregular

Solution:

Check that the attached device is not set to dedicate full duplex. Some devices use a physical or software switch to change duplex modes. Auto-negotiation may not recognize this type of full-duplex setting.

Why the Industrial Managed Switch doesn't connect to the network

Solution:

Check per port LED on the **Industrial Managed Switch**. Try another port on the **Industrial Managed Switch** Make sure the cable is installed properly Make sure the cable is the right type Turn off the power. After a while, turn on power again.

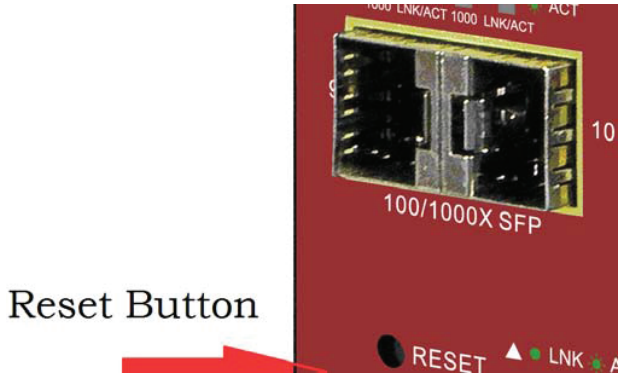
Can I install MGB-SX or other non wide temperature SFP module into SFP slot of Industrial Managed Switch?

Solution:

Yes, it does. However, since the MGB-SX and other non wide temperature SFP module cannot operate under -40 to 75 Degree C. Please pay attention to this point and consider use IFS wide temperature SFP module for **Industrial Managed Switch**.

■ **While IP Address be changed or forgotten admin password** –

To reset the IP address to the default IP Address **"192.168.0.100"** or reset the password to default value. Press the hardware **reset button** at the front panel about **5 seconds.** After the device is rebooted, you can login the management WEB interface within the same subnet of 192.168.0.xx.



APPENDEX A

A.1 Switch's Data RJ-45 Pin Assignments - 1000Mbps, 1000Base-T

PIN NO	MDI	MDI-X
1	BI_DA+	BI_DB+
2	BI_DA-	BI_DB-
3	BI_DB+	BI_DA+
4	BI_DC+	BI_DD+
5	BI_DC-	BI_DD-
6	BI_DB-	BI_DA-
7	BI_DD+	BI_DC+
8	BI_DD-	BI_DC-

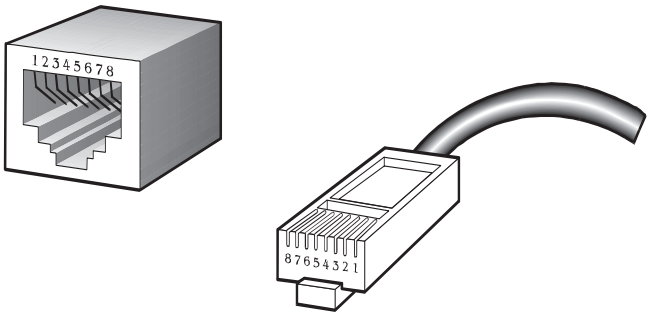
Implicit implementation of the crossover function within a twisted-pair cable, or at a wiring panel, while not expressly forbidden, is beyond the scope of this standard.

A.2 10/100Mbps, 10/100Base-TX

When connecting your 10/100Mbps Ethernet Switch to another switch, a bridge or a hub, a straight or crossover cable is necessary. Each port of the Switch supports auto-MDI/MDI-X detection. That means you can directly connect the Switch to any Ethernet devices without making a crossover cable. The following table and diagram show the standard RJ-45 receptacle/ connector and their pin assignments:

RJ-45 Connector pin assignment		
Contact	MDI Media Dependant Interface	MDI-X Media Dependant Interface-Cross
1	Tx + (transmit)	Rx + (receive)
2	Tx - (transmit)	Rx - (receive)
3	Rx + (receive)	Tx + (transmit)
4, 5	Not used	
6	Rx - (receive)	Tx - (transmit)
7, 8	Not used	

The standard cable, RJ-45 pin assignment



The standard RJ-45 receptacle/connector

There are 8 wires on a standard UTP/STP cable and each wire is color-coded. The following shows the pin allocation and color of straight cable and crossover cable connection:

Straight Cable		**SIDE 1**	**SIDE2**
1 2 3 4 5 6 7 8	SIDE 1	1 = White / Orange	1 = White / Orange
		2 = Orange	2 = Orange
		3 = White / Green	3 = White / Green
		4 = Blue	4 = Blue
		5 = White / Blue	5 = White / Blue
		6 = Green	6 = Green
		7 = White / Brown	7 = White / Brown
		8 = Brown	8 = Brown
1 2 3 4 5 6 7 8	SIDE 2		
Crossover Cable		**SIDE 1**	**SIDE2**
1 2 3 4 5 6 7 8	SIDE 1	1 = White / Orange	1 = White / Green
		2 = Orange	2 = Green
		3 = White / Green	3 = White / Orange
		4 = Blue	4 = Blue
		5 = White / Blue	5 = White / Blue
		6 = Green	6 = Orange
		7 = White / Brown	7 = White / Brown
		8 = Brown	8 = Brown
1 2 3 4 5 6 7 8	SIDE 2		

Figure A-1: Straight-Through and Crossover Cable

Please make sure your connected cables are with same pin assignment and color as above picture before deploying the cables into your network.

APPENDEX B : GLOSSARY

A

ACE

ACE is an acronym for **A**ccess **C**ontrol **E**ntry. It describes access permission associated with a particular ACE ID.

There are three ACE frame types (Ethernet Type, ARP, and IPv4) and two ACE actions (permit and deny). The ACE also contains many detailed, different parameter options that are available for individual application.

ACL

ACL is an acronym for **A**ccess **C**ontrol **L**ist. It is the list table of ACEs, containing access control entries that specify individual users or groups permitted or denied to specific traffic objects, such as a process or a program.

Each accessible traffic object contains an identifier to its ACL. The privileges determine whether there are specific traffic object access rights.

ACL implementations can be quite complex, for example, when the ACEs are prioritized for the various situation. In networking, the ACL refers to a list of service ports or network services that are available on a host or server, each with a list of hosts or servers permitted or denied to use the service. ACL can generally be configured to control inbound traffic, and in this context, they are similar to firewalls.

There are 3 web-pages associated with the manual ACL configuration:

ACL|Access Control List: The web page shows the ACEs in a prioritized way, highest (top) to lowest (bottom). Default the table is empty. An ingress frame will only get a hit on one ACE even though there are more matching ACEs. The first matching ACE will take action (permit/deny) on that frame and a counter associated with that ACE is incremented. An ACE can be associated with a Policy, 1 ingress port, or any ingress port (the whole switch). If an ACE Policy is created then that Policy can be associated with a group of ports under the "Ports" web-page. There are number of parameters that can be configured with an ACE. Read the Web page help text to get further information for each of them. The maximum number of ACEs is 64.
ACL|Ports: The ACL Ports configuration is used to assign a Policy ID to an ingress port. This is useful to group ports to obey the same traffic rules. Traffic Policy is created under the "Access Control List" - page. You can you also set up specific traffic properties (Action / Rate Limiter / Port copy, etc) for each ingress port. They will though only apply if the frame gets past the ACE matching without getting matched. In that case a counter associated with that port is incremented. See the Web page help text for each specific port property.
ACL|Rate Limiters: Under this page you can configure the rate limiters. There can be 15 different rate limiters, each ranging from 1-1024K packets per seconds. Under "Ports" and "Access Control List" web-pages you can assign a Rate Limiter ID to the ACE(s) or ingress port(s).

AES

AES is an acronym for **A**dvanced **E**ncryption **S**tandard. The encryption key protocol is applied in 802.1i standard to improve WLAN security. It is an encryption standard by the U.S. government, which will replace DES and 3DES. AES has a fixed block size of 128 bits and a key size of 128, 192, or 256 bits.

APS

APS is an acronym for **A**utomatic **P**rotection **S**witching. This protocol is used to secure that switching is done bidirectional in the two ends of a protection group, as defined in G.8031.

Aggregation

Using multiple ports in parallel to increase the link speed beyond the limits of a port and to increase the redundancy for higher availability.

(Also *Port Aggregation, Link Aggregation*).

ARP

ARP is an acronym for **A**ddress **R**esolution **P**rotocol. It is a protocol that used to convert an IP address into a physical address, such as an Ethernet address. ARP allows a host to communicate with other hosts when only the Internet address of its neighbors is known. Before using IP, the host sends a broadcast ARP request containing the Internet address of the desired destination system.

ARP Inspection

ARP Inspection is a secure feature. Several types of attacks can be launched against a host or devices connected to Layer 2 networks by "poisoning" the ARP caches. This feature is used to block such attacks. Only valid ARP requests and responses can go through the switch device.

Auto-Negotiation

Auto-negotiation is the process where two different devices establish the mode of operation and the speed settings that can be shared by those devices for a link.

C

CC

CC is an acronym for **C**ontinuity **C**heck. It is a MEP functionality that is able to detect loss of continuity in a network by transmitting CCM frames to a peer MEP.

CCM

CCM is an acronym for **C**ontinuity **C**heck **M**essage. It is a OAM frame transmitted from a MEP to it's peer MEP and used to implement CC functionality.

CDP

CDP is an acronym for **C**isco **D**iscovery **P**rotocol.

D

DEI

DEI is an acronym for **D**rop **E**ligible **I**ndicator. It is a 1-bit field in the VLAN tag.

DES

DES is an acronym for **D**ata **E**ncryption **S**tandard. It provides a complete description of a mathematical algorithm for encrypting (enciphering) and decrypting (deciphering) binary coded information.

Encrypting data converts it to an unintelligible form called cipher. Decrypting cipher converts the data back to its original form called plaintext. The algorithm described in this standard specifies both enciphering and deciphering operations which are based on a binary number called a key.

DHCP

DHCP is an acronym for **D**ynamic **H**ost **C**onfiguration **P**rotocol. It is a protocol used for assigning dynamic IP addresses to devices on a network.

DHCP used by networked computers (clients) to obtain IP addresses and other parameters such as the default gateway, subnet mask, and IP addresses of DNS servers from a DHCP server.

The DHCP server ensures that all IP addresses are unique, for example, no IP address is assigned to a second client while the first client's assignment is valid (its lease has not expired). Therefore, IP address pool management is done by the server and not by a human network administrator.

Dynamic addressing simplifies network administration because the software keeps track of IP addresses rather than requiring an administrator to manage the task. This means that a new computer can be added to a network without the hassle of manually assigning it a unique IP address.

DHCP Relay

DHCP Relay is used to forward and to transfer DHCP messages between the clients and the server when they are not on the same subnet domain.

The DHCP option 82 enables a DHCP relay agent to insert specific information into a DHCP request packets when forwarding client DHCP packets to a DHCP server and remove the specific information from a DHCP reply packets when forwarding server DHCP packets to a DHCP client. The DHCP server can use this information to implement IP address or other assignment policies. Specifically the option works by setting two sub-options: Circuit ID (option 1) and Remote ID (option2). The Circuit ID sub-option is supposed to include information specific to which circuit the request came in on. The Remote ID sub-option was designed to carry information relating to the remote host end of the circuit.

The definition of Circuit ID in the switch is 4 bytes in length and the format is "vlan_id" "module_id" "port_no". The parameter of "vlan_id" is the first two bytes represent the VLAN ID. The parameter of "module_id" is the third byte for the module ID (in standalone switch it always equal 0, in stackable switch it means switch ID). The parameter of "port_no" is the fourth byte and it means the port number.
The Remote ID is 6 bytes in length, and the value is equal the DHCP relay agents MAC address.

DHCP Snooping

DHCP Snooping is used to block intruder on the untrusted ports of the switch device when it tries to intervene by injecting a bogus DHCP reply packet to a legitimate conversation between the DHCP client and server.

DNS

DNS is an acronym for **D**omain **N**ame **S**ystem. It stores and associates many types of information with domain names. Most importantly, DNS translates human-friendly domain names and computer hostnames into computer-friendly IP addresses. For example, the domain name www.example.com might translate to 192.168.0.1.

DoS

DoS is an acronym for **D**enial of **S**ervice. In a denial-of-service (DoS) attack, an attacker attempts to prevent legitimate users from accessing information or services. By targeting at network sites or network connection, an attacker may be able to prevent network users from accessing email, web sites, online accounts (banking, etc.), or other services that rely on the affected computer.

Dotted Decimal Notation

Dotted Decimal Notation refers to a method of writing IP addresses using decimal numbers and dots as separators between octets.
An IPv4 dotted decimal address has the form x.y.z.w, where x, y, z, and w are decimal numbers between 0 and 255.

DSCP

DSCP is an acronym for **D**ifferentiated **S**ervices **C**ode **P**oint. It is a field in the header of IP packets for packet classification purposes.

E

EEE

EEE is an abbreviation for Energy Efficient Ethernet defined in IEEE 802.3az.

EPS

EPS is an abbreviation for Ethernet Protection Switching defined in ITU/T G.8031.

Ethernet Type

Ethernet Type, or EtherType, is a field in the Ethernet MAC header, defined by the Ethernet networking standard. It is used to indicate which protocol is being transported in an Ethernet frame.

F

FTP

FTP is an acronym for **F**ile **T**ransfer **P**rotocol. It is a transfer protocol that uses the Transmission Control Protocol (TCP) and provides file writing and reading. It also provides directory service and security features.

Fast Leave

IGMP snooping Fast Leave processing allows the switch to remove an interface from the forwarding-table entry without first sending out group specific queries to the interface. The VLAN interface is pruned from the multicast tree for the multicast group specified in the original leave message. Fast-leave processing ensures optimal bandwidth management for all hosts on a switched network, even when multiple multicast groups are in use simultaneously.

H

HTTP

HTTP is an acronym for **H**ypertext **T**ransfer **P**rotocol. It is a protocol that used to transfer or convey information on the World Wide Web (WWW).

HTTP defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands. For example, when you enter a URL in your browser, this actually sends an HTTP command to the Web server directing it to fetch and transmit the requested Web page. The other main standard that controls how the World Wide Web works is HTML, which covers how Web pages are formatted and displayed.

Any Web server machine contains, in addition to the Web page files it can serve, an HTTP daemon, a program that is designed to wait for HTTP requests and handle them when they arrive. The Web browser is an HTTP client, sending requests to server machines. An HTTP client initiates a request by establishing a Transmission Control Protocol (TCP) connection to a particular port on a remote host (port 80 by default). An HTTP server listening on that port waits for the client to send a request message.

HTTPS

HTTPS is an acronym for **H**ypertext **T**ransfer **P**rotocol over **S**ecure Socket Layer. It is used to indicate a secure HTTP connection.

HTTPS provide authentication and encrypted communication and is widely used on the World Wide Web for security-sensitive communication such as payment transactions and corporate logons.

HTTPS is really just the use of Netscape's Secure Socket Layer (SSL) as a sublayer under its regular HTTP application layering. (HTTPS uses port 443 instead of HTTP port 80 in its interactions with the lower layer, TCP/IP.) SSL uses a 40-bit key size for the RC4 stream encryption algorithm, which is considered an adequate degree of encryption for commercial exchange.

I

ICMP

ICMP is an acronym for **I**nternet **C**ontrol **M**essage **P**rotocol. It is a protocol that generated the error response, diagnostic or routing purposes. ICMP messages generally contain information about routing difficulties or simple exchanges such as time-stamp or echo transactions. For example, the PING command uses ICMP to test an Internet connection.

IEEE 802.1X

IEEE 802.1X is an IEEE standard for port-based Network Access Control. It provides authentication to devices attached to a LAN port, establishing a point-to-point connection or preventing access from that port if authentication fails. With 802.1X, access to all switch ports can be centrally controlled from a server, which means that authorized users can use the same credentials for authentication from any point within the network.

IGMP

IGMP is an acronym for **I**nternet **G**roup **M**anagement **P**rotocol. It is a communications protocol used to manage the membership of Internet Protocol multicast groups. IGMP is used by IP hosts and adjacent multicast routers to establish multicast group memberships. It is an integral part of the IP multicast specification, like ICMP for unicast connections. IGMP can be used for online video and gaming, and allows more efficient use of resources when supporting these uses.

IGMP Querier

A router sends IGMP Query messages onto a particular link. This router is called the Querier.

IMAP

IMAP is an acronym for **I**nternet **M**essage **A**ccess **P**rotocol. It is a protocol for email clients to retrieve email messages from a mail server.

IMAP is the protocol that IMAP clients use to communicate with the servers, and SMTP is the protocol used to transport mail to an IMAP server.

The current version of the Internet Message Access Protocol is IMAP4. It is similar to Post Office Protocol version 3 (POP3), but offers additional and more complex features. For example, the IMAP4 protocol leaves your email messages on the server rather than downloading them to your computer. If you wish to remove your messages from the server, you must use your mail client to generate local folders, copy messages to your local hard drive, and then delete and expunge the messages from the server.

IP

IP is an acronym for **I**nternet **P**rotocol. It is a protocol used for communicating data across a internet network.

IP is a "best effort" system, which means that no packet of information sent over it is assured to reach its destination in the same condition it was sent. Each device connected to a Local Area Network (LAN) or Wide Area Network (WAN) is given an Internet Protocol address, and this IP address is used to identify the device uniquely among all other devices connected to the extended network.

The current version of the Internet protocol is IPv4, which has 32-bits Internet Protocol addresses allowing for in excess of four billion unique addresses. This number is reduced drastically by the practice of webmasters taking addresses in large blocks, the bulk of which remain unused. There is a rather substantial movement to adopt a new version of the Internet Protocol, IPv6, which would have 128-bits Internet Protocol addresses. This number can be represented roughly by a three with thirty-nine zeroes after it. However, IPv4 is still the protocol of choice for most of the Internet.

IPMC

IPMC is an acronym for **IP** **M**ulti**C**ast.

IP Source Guard

IP Source Guard is a secure feature used to restrict IP traffic on DHCP snooping untrusted ports by filtering traffic based on the DHCP Snooping Table or manually configured IP Source Bindings. It helps prevent IP spoofing attacks when a host tries to spoof and use the IP address of another host.

L

LACP

LACP is an IEEE 802.3ad standard protocol. The **L**ink **A**ggregation **C**ontrol **P**rotocol, allows bundling several physical ports together to form a single logical port.

LLDP

LLDP is an IEEE 802.1ab standard protocol.
The **L**ink **L**ayer **D**iscovery **P**rotocol(LLDP) specified in this standard allows stations attached to an IEEE 802 LAN to advertise, to other stations attached to the same IEEE 802 LAN, the major capabilities provided by the system incorporating that station, the management address or addresses of the entity or entities that provide management of those capabilities, and the identification of the stations point of attachment to the IEEE 802 LAN required by those management entity or entities. The information distributed via this protocol is stored by its recipients in a standard Management Information Base (MIB), making it possible for the information to be accessed by a Network Management System (NMS) using a management protocol such as the Simple Network Management Protocol (SNMP).

LLDP-MED

LLDP-MED is an extendsion of IEEE 802.1ab and is defined by the telecommunication industry association (TIA-1057).

LOC

LOC is an acronym for **L**oss **O**f **C**onnectivity and is detected by a MEP and is indicating lost connectivity in the network. Can be used as a switch criteria by EPS

M

MAC Table

Switching of frames is based upon the DMAC address contained in the frame. The switch builds up a table that maps MAC addresses to switch ports for knowing which ports the frames should go to (based upon the DMAC address in the frame). This table contains both static and dynamic entries. The static entries are configured by the network administrator if the administrator wants to do a fixed mapping between the DMAC address and switch ports.

The frames also contain a MAC address (SMAC address), which shows the MAC address of the equipment sending the frame. The SMAC address is used by the switch to automatically update the MAC table with these dynamic MAC addresses. Dynamic entries are removed from the MAC table if no frame with the corresponding SMAC address have been seen after a configurable age time.

MEP

MEP is an acronym for **M**aintenance **E**ntity **E**ndpoint and is an endpoint in a Maintenance Entity Group (ITU-T Y.1731).

MD5

MD5 is an acronym for **M**essage-**D**igest algorithm **5**. MD5 is a message digest algorithm, used cryptographic hash function with a 128-bit hash value. It was designed by Ron Rivest in 1991. MD5 is officially defined in RFC 1321 - The MD5 Message-Digest Algorithm.

Mirroring

For debugging network problems or monitoring network traffic, the switch system can be configured to mirror frames from multiple ports to a mirror port. (In this context, mirroring a frame is the same as copying the frame.)

Both incoming (source) and outgoing (destination) frames can be mirrored to the mirror port.

MLD

MLD is an acronym for **M**ulticast **L**istener **D**iscovery for IPv6. MLD is used by IPv6 routers to discover multicast listeners on a directly attached link, much as IGMP is used in IPv4. The protocol is embedded in ICMPv6 instead of using a separate protocol.

MVR

Multicast VLAN Registration (MVR) is a protocol for Layer 2 (IP)-networks that enables multicast-traffic from a source VLAN to be shared with subscriber-VLANs.
The main reason for using MVR is to save bandwidth by preventing duplicate multicast streams being sent in the core network, instead the stream(s) are received on the MVR-VLAN and forwarded to the VLANs where hosts have requested it/them(Wikipedia).

N

NAS

NAS is an acronym for Network Access Server. The NAS is meant to act as a gateway to guard access to a protected source. A client connects to the NAS, and the NAS connects to another resource asking whether the client's supplied credentials are valid. Based on the answer, the NAS then allows or disallows access to the protected resource. An example of a NAS implementation is IEEE 802.1X.

NetBIOS

NetBIOS is an acronym for **Net**work **B**asic **I**nput/**O**utput **S**ystem. It is a program that allows applications on separate computers to communicate within a Local Area Network (LAN), and it is not supported on a Wide Area Network (WAN).

The NetBIOS giving each computer in the network both a NetBIOS name and an IP address corresponding to a different host name, provides the session and transport services described in the Open Systems Interconnection (OSI) model.

NFS

NFS is an acronym for **N**etwork **F**ile **S**ystem. It allows hosts to mount partitions on a remote system and use them as though they are local file systems.

NFS allows the system administrator to store resources in a central location on the network, providing authorized users continuous access to them, which means NFS supports sharing of files, printers, and other resources as persistent storage over a computer network.

NTP

NTP is an acronym for **N**etwork **T**ime **P**rotocol, a network protocol for synchronizing the clocks of computer systems. NTP uses UDP (datagrams) as transport layer.

O

OAM

OAM is an acronym for **O**peration **A**dministration and **M**aintenance.

It is a protocol described in ITU-T Y.1731 used to implement carrier ethernet functionality. MEP functionality like CC and RDI is based on this.

Optional TLVs.

A LLDP frame contains multiple TLVs

For some TLVs it is configurable if the switch shall include the TLV in the LLDP frame. These TLVs are known as optional TLVs. If an optional TLVs is disabled the corresponding information is not included in the LLDP frame.

OUI

OUI is the organizationally unique identifier. An OUI address is a globally unique identifier assigned to a vendor by IEEE. You can determine which vendor a device belongs to according to the OUI address which forms the first 24 bits of a MAC address.

P

PCP

PCP is an acronym for Priority Code Point. It is a 3-bit field storing the priority level for the 802.1Q frame. It is also known as User Priority.

PD

PD is an acronym for **P**owered **D**evice. In a PoE> system the power is delivered from a PSE (power sourcing equipment) to a remote device. The remote device is called a PD.

PHY

PHY is an abbreviation for Physical Interface Transceiver and is the device that implement the Ethernet physical layer (IEEE-802.3).

PING

ping is a program that sends a series of packets over a network or the Internet to a specific computer in order to generate a response from that computer. The other computer responds with an acknowledgment that it received the packets. Ping was created to verify whether a specific computer on a network or the Internet exists and is connected.

ping uses Internet Control Message Protocol (ICMP) packets. The PING Request is the packet from the origin computer, and the PING Reply is the packet response from the target.

PoE

PoE is an acronym for **P**ower **O**ver **E**thernet.
Power Over Ethernet is used to transmit electrical power, to remote devices over standard Ethernet cable. It could for example be used for powering IP telephones, wireless LAN access points and other equipment, where it would be difficult or expensive to connect the equipment to main power supply.

Policer

A policer can limit the bandwidth of received frames. It is located in front of the ingress queue.

POP3

POP3 is an acronym for **P**ost **O**ffice **P**rotocol version 3. It is a protocol for email clients to retrieve email messages from a mail server.

POP3 is designed to delete mail on the server as soon as the user has downloaded it. However, some implementations allow users or an administrator to specify that mail be saved for some period of time. POP can be thought of as a "store-and-forward" service.

An alternative protocol is Internet Message Access Protocol (IMAP). IMAP provides the user with more capabilities for retaining e-mail on the server and for organizing it in folders on the server. IMAP can be thought of as a remote file server.

POP and IMAP deal with the receiving of e-mail and are not to be confused with the Simple Mail Transfer Protocol (SMTP). You send e-mail with SMTP, and a mail handler receives it on your recipient's behalf. Then the mail is read using POP or IMAP. IMAP4 and POP3 are the two most prevalent Internet standard protocols for e-mail retrieval. Virtually all modern e-mail clients and servers support both.

PPPoE

PPPoE is an acronym for Point-to-Point Protocol over Ethernet.
It is a network protocol for encapsulating Point-to-Point Protocol (PPP) frames inside Ethernet frames. It is used mainly with ADSL services where individual users connect to the ADSL transceiver (modem) over Ethernet and in plain Metro Ethernet networks (Wikipedia).

Private VLAN

In a private VLAN, communication between ports in that private VLAN is not permitted. A VLAN can be configured as a private VLAN.

PTP

PTP is an acronym for Precision Time Protocol, a network protocol for synchronizing the clocks of computer systems.

Q

QCE

QCE is an acronym for **Q**oS **C**ontrol **E**ntry. It describes QoS class associated with a particular QCE ID.

There are six QCE frame types: Ethernet Type, VLAN, UDP/TCP Port, DSCP, TOS, and Tag Priority. Frames can be classified by one of 4 different QoS classes: "Low", "Normal", "Medium", and "High" for individual application.

QCL

QCL is an acronym for **Q**oS **C**ontrol **L**ist. It is the list table of QCEs, containing QoS control entries that classify to a specific QoS class on specific traffic objects.

Each accessible traffic object contains an identifier to its QCL. The privileges determine specific traffic object to specific QoS class.

QL

QL In SyncE this is the Quality Level of a given clock source. This is received on a port in a SSM indicating the quality of the clock received in the port.

QoS

QoS is an acronym for **Q**uality **o**f **S**ervice. It is a method to guarantee a bandwidth relationship between individual applications or protocols.

A communications network transports a multitude of applications and data, including high-quality video and delay-sensitive data such as real-time voice. Networks must provide secure, predictable, measurable, and sometimes guaranteed services.

Achieving the required QoS becomes the secret to a successful end-to-end business solution. Therefore, QoS is the set of techniques to manage network resources.

R

RARP

RARP is an acronym for **R**everse **A**ddress **R**esolution **P**rotocol. It is a protocol that is used to obtain an IP address for a given hardware address, such as an Ethernet address. RARP is the complement of ARP.

RADIUS

RADIUS is an acronym for **Re**mote **A**uthentication **D**ial In **U**ser **S**ervice. It is a networking protocol that provides centralized access, authorization and accounting management for people or computers to connect and use a network service.

RDI

RDI is an acronym for **R**emote **D**efect **I**ndication. It is a OAM functionallity that is used by a MEP to indicate defect detected to the remote peer MEP

Router Port

A router port is a port on the Ethernet switch that leads switch towards the Layer 3 multicast device.

RSTP

In 1998, the IEEE with document 802.1w introduced an evolution of STP: the **R**apid **S**panning **T**ree **P**rotocol, which provides for faster spanning tree convergence after a topology change. Standard IEEE 802.1D-2004 now incorporates

RSTP and obsoletes STP, while at the same time being backwards-compatible with STP.

S

SAMBA

Samba is a program running under UNIX-like operating systems that provides seamless integration between UNIX and Microsoft Windows machines. Samba acts as file and print servers for Microsoft Windows, IBM OS/2, and other SMB client machines. Samba uses the Server Message Block (SMB) protocol and Common Internet File System (CIFS), which is the underlying protocol used in Microsoft Windows networking.

Samba can be installed on a variety of operating system platforms, including Linux, most common Unix platforms, OpenVMS, and IBM OS/2.

Samba can also register itself with the master browser on the network so that it would appear in the listing of hosts in Microsoft Windows "Neighborhood Network".

SHA

SHA is an acronym for **S**ecure **H**ash **A**lgorithm. It designed by the National Security Agency (NSA) and published by the NIST as a U.S. Federal Information Processing Standard. Hash algorithms compute a fixed-length digital representation (known as a message digest) of an input data sequence (the message) of any length.

Shaper

A shaper can limit the bandwidth of transmitted frames. It is located after the ingress queues.

SMTP

SMTP is an acronym for **S**imple **M**ail **T**ransfer **P**rotocol. It is a text-based protocol that uses the Transmission Control Protocol (TCP) and provides a mail service modeled on the FTP file transfer service. SMTP transfers mail messages between systems and notifications regarding incoming mail.

SNAP

The SubNetwork Access Protocol (SNAP) is a mechanism for multiplexing, on networks using IEEE 802.2 LLC, more protocols than can be distinguished by the 8-bit 802.2 Service Access Point (SAP) fields. SNAP supports identifying protocols by Ethernet type field values; it also supports vendor-private protocol identifier.

SNMP

SNMP is an acronym for **S**imple **N**etwork **M**anagement **P**rotocol. It is part of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol for network management. SNMP allow diverse network objects to participate in a network management architecture. It enables network management systems to learn network problems by receiving traps or change notices from network devices implementing SNMP.

SNTP

SNTP is an acronym for **S**imple **N**etwork **T**ime **P**rotocol, a network protocol for synchronizing the clocks of computer systems. SNTP uses UDP (datagrams) as transport layer.

SPROUT

Stack **P**rotocol using **ROU**ting **T**echnology. An advanced protocol for almost instantaneous discovery of topology changes within a stack as well as election of a master switch. SPROUT also calculates parameters for setting up each switch to perform shortest path forwarding within the stack.

SSID

Service **S**et **Id**entifier is a name used to identify the particular 802.11 wireless LANs to which a user wants to attach. A client device will receive broadcast messages from all access points within range advertising their SSIDs, and can choose one to connect to based on pre-configuration, or by displaying a list of SSIDs in range and asking the user to select one (wikipedia).

SSH

SSH is an acronym for **S**ecure **SH**ell. It is a network protocol that allows data to be exchanged using a secure channel between two networked devices. The encryption used by SSH provides confidentiality and integrity of data over an insecure network. The goal of SSH was to replace the earlier rlogin, TELNET and rsh protocols, which did not provide strong authentication or guarantee confidentiality (Wikipedia).

SSM

SSM In SyncE this is an abbreviation for Synchronization Status Message and is containing a QL indication.

STP

Spanning **T**ree **P**rotocol is an OSI layer-2 protocol which ensures a loop free topology for any bridged LAN. The original STP protocol is now obsoleted by RSTP.

Switch ID

Switch IDs (1-16) are used to uniquely identify the switches within a stack. The Switch ID of each switch is shown on the display on the front of the switch and is used widely in the web pages as well as in the CLI commands.

SyncE

SyncE Is an abbreviation for Synchronous Ethernet. This functionality is used to make a network 'clock frequency' synchronized. Not to be confused with real time clock synchronized (IEEE 1588).

T

TACACS+

TACACS+ is an acronym for **T**erminal **A**cess **C**ontroller **A**ccess **C**ontrol **S**ystem **P**lus. It is a networking protocol which provides access control for routers, network access servers and other networked computing devices via one or more centralized servers. TACACS+ provides separate authentication, authorization and accounting services.

Tag Priority

Tag Priority is a 3-bit field storing the priority level for the 802.1Q frame.

TCP

TCP is an acronym for **T**ransmission **C**ontrol **P**rotocol. It is a communications protocol that uses the Internet Protocol (IP) to exchange the messages between computers.

The TCP protocol guarantees reliable and in-order delivery of data from sender to receiver and distinguishes data for multiple connections by concurrent applications (for example, Web server and e-mail server) running on the same host.

The applications on networked hosts can use TCP to create connections to one another. It is known as a connection-oriented protocol, which means that a connection is established and maintained until such time as the message or messages to be exchanged by the application programs at each end have been exchanged. TCP is responsible for ensuring that a message is divided into the packets that IP manages and for reassembling the packets back into the complete message at the other end.

Common network applications that use TCP include the World Wide Web (WWW), e-mail, and File Transfer Protocol (FTP).

TELNET

TELNET is an acronym for **TEL**etype **NET**work. It is a terminal emulation protocol that uses the Transmission Control Protocol (TCP) and provides a virtual connection between TELNET server and TELNET client.

TELNET enables the client to control the server and communicate with other servers on the network. To start a Telnet session, the client user must log in to a server by entering a valid username and password. Then, the client user can enter commands through the Telnet program just as if they were entering commands directly on the server console.

TFTP

TFTP is an acronym for **T**rivial **F**ile **T**ransfer **P**rotocol. It is transfer protocol that uses the User Datagram Protocol (UDP) and provides file writing and reading, but it does not provides directory service and security features.

ToS

ToS is an acronym for **T**ype **o**f **S**ervice. It is implemented as the IPv4 ToS priority control. It is fully decoded to determine the priority from the 6-bit ToS field in the IP header. The most significant 6 bits of the ToS field are fully decoded into 64 possibilities, and the singular code that results is compared against the corresponding bit in the IPv4 ToS priority control bit (0~63).

TLV

TLV is an acronym for **T**ype **L**ength **V**alue. A LLDP frame can contain multiple pieces of information. Each of these pieces of information is known as TLV.

TKIP

TKIP is an acronym for **T**emporal **K**ey **I**ntegrity **P**rotocol. It used in WPA to replace WEP with a new encryption algorithm. TKIP comprises the same encryption engine and RC4 algorithm defined for WEP. The key used for encryption in TKIP is 128 bits and changes the key used for each packet.

U

UDP

UDP is an acronym for **U**ser **D**atagram **P**rotocol. It is a communications protocol that uses the Internet Protocol (IP) to exchange the messages between computers.

UDP is an alternative to the Transmission Control Protocol (TCP) that uses the Internet Protocol (IP). Unlike TCP, UDP does not provide the service of dividing a message into packet datagrams, and UDP doesn't provide reassembling and sequencing of the packets. This means that the application program that uses UDP must be able to make sure that the entire message has arrived and is in the right order. Network applications that want to save processing time because they have very small data units to exchange may prefer UDP to TCP.

UDP provides two services not provided by the IP layer. It provides port numbers to help distinguish different user requests and, optionally, a checksum capability to verify that the data arrived intact.

Common network applications that use UDP include the Domain Name System (DNS), streaming media applications such as IPTV, Voice over IP (VoIP), and Trivial File Transfer Protocol (TFTP).

UPnP

UPnP is an acronym for **U**niversal **P**lug and **P**lay. The goals of UPnP are to allow devices to connect seamlessly and to simplify the implementation of networks in the home (data sharing, communications, and entertainment) and in corporate environments for simplified installation of computer components

User Priority

User Priority is a 3-bit field storing the priority level for the 802.1Q frame.

V

VLAN

Virtual LAN. A method to restrict communication between switch ports. VLANs can be used for the following applications:

VLAN unaware switching: This is the default configuration. All ports are VLAN unaware with Port VLAN ID 1 and members of VLAN 1. This means that MAC addresses are learned in VLAN 1, and the switch does not remove or insert VLAN tags.

VLAN aware switching: This is based on the IEEE 802.1Q standard. All ports are VLAN aware. Ports connected to VLAN aware switches are members of multiple VLANs and transmit tagged frames. Other ports are members of one VLAN, set up with this Port VLAN ID, and transmit untagged frames.

Provider switching: This is also known as Q-in-Q switching. Ports connected to subscribers are VLAN unaware, members of one VLAN, and set up with this unique Port VLAN ID. Ports connected to the service provider are VLAN aware, members of multiple VLANs, and set up to tag all frames. Untagged frames received on a subscriber port are forwarded to the provider port with a single VLAN tag. Tagged frames received on a subscriber port are forwarded to the provider port with a double VLAN tag.

VLAN ID

VLAN ID is a 12-bit field specifying the VLAN to which the frame belongs.

Voice VLAN

Voice VLAN is VLAN configured specially for voice traffic. By adding the ports with voice devices attached to voice VLAN, we can perform QoS-related configuration for voice data, ensuring the transmission priority of voice traffic and voice quality.

W

WEP

WEP is an acronym for **W**ired **E**quivalent **P**rivacy. WEP is a deprecated algorithm to secure IEEE 802.11 wireless networks. Wireless networks broadcast messages using radio, so are more susceptible to eavesdropping than wired networks. When introduced in 1999, WEP was intended to provide confidentiality comparable to that of a traditional wired network (Wikipedia).

WiFi

WiFi is an acronym for **Wi**reless **Fi**delity. It is meant to be used generically when referring of any type of 802.11 network, whether 802.11b, 802.11a, dual-band, etc. The term is promulgated by the Wi-Fi Alliance.

WPA

WPA is an acronym for **W**i-Fi **P**rotected **A**ccess. It was created in response to several serious weaknesses researchers had found in the previous system , Wired Equivalent Privacy (WEP). WPA implements the majority of the IEEE 802.11i

standard, and was intended as an intermediate measure to take the place of WEP while 802.11i was prepared. WPA is specifically designed to also work with pre-WPA wireless network interface cards (through firmware upgrades), but not necessarily with first generation wireless access points. WPA2 implements the full standard, but will not work with some older network cards (Wikipedia).

WPA-PSK

WPA-PSK is an acronym for **W**i-Fi **P**rotected **A**ccess - **P**re **S**hared **K**ey. WPA was designed to enhance the security of wireless networks. There are two flavors of WPA: enterprise and personal. Enterprise is meant for use with an IEEE 802.1X authentication server, which distributes different keys to each user. Personal WPA utilizes less scalable 'pre-shared key' (PSK) mode, where every allowed computer is given the same passphrase. In PSK mode, security depends on the strength and secrecy of the passphrase. The design of WPA is based on a Draft 3 of the IEEE 802.11i standard (Wikipedia)

WPA-Radius

WPA-Radius is an acronym for **W**i-Fi **P**rotected **A**ccess - Radius (802.1X authentication server). WPA was designed to enhance the security of wireless networks. There are two flavors of WPA: enterprise and personal. Enterprise is meant for use with an IEEE 802.1X authentication server, which distributes different keys to each user. Personal WPA utilizes less scalable 'pre-shared key' (PSK) mode, where every allowed computer is given the same passphrase. In PSK mode, security depends on the strength and secrecy of the passphrase. The design of WPA is based on a Draft 3 of the IEEE 802.11i standard (Wikipedia)

WPS

WPS is an acronym for **W**i-Fi **P**rotected **S**etup. It is a standard for easy and secure establishment of a wireless home network. The goal of the WPS protocol is to simplify the process of connecting any home device to the wireless network (Wikipedia).

WTR

WTR is an acronym for **W**ait **T**o **R**estore. This is the time a fail on a resource has to be 'not active' before restoration back to this (previously failing) resource is done.

This Page Left Intentionally Blank

IFS NS3550-8T-2S Quick Installation Guide

P/N 1072772 • REV A • ISS 24JUN14

Intended use

Use this product only for the purpose it was designed for; refer to the data sheet and user documentation for details. For the latest product information, contact your local supplier or visit us online at www.interlogix.com.

Manufacturer

UTC Building & Industrial Systems, Inc.
2955 Red Hill Avenue
Costa Mesa, CA 92626-5923, USA

EU authorized manufacturing representative:
UTC Fire & Security B.V., Kelvinstraat 7,
6003 DH Weert, The Netherlands

Certification

CE

TABLE OF CONTENTS

INTRODUCTION

The IFS NS3550-8T-2S is an 8 port Gigabit Industrial Switch with 2 SFP fiber ports and robust layer 2 features.

Package Contents

Open the box of the Industrial Managed Switch and carefully unpack it. The box should contain the following items:

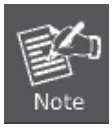
Check the contents of your package for following parts:

☑ **The Industrial Managed Switch**	x1
☑ **User's Manual CD**	x1
☑ **Quick Installation Guide**	x1
☑ **DIN Rail Kit**	x1
☑ **Wall Mounting Kit**	x1
☑ **Dust Cap**	X10

If any of these are missing or damaged, please contact your dealer immediately, if possible, retain the original carton and packaging material in case of a need to return the product for repair/replacement.

Requirements

- **Workstations** of subscribers running Windows 98/ME, NT4.0, 2000/XP, 2003, Vista 7, MAC OS9 or later, Linux, UNIX or other platform compatible with **TCP/IP** protocols.
- **Workstation** installed with **Ethernet NIC** (Network Interface Card)
- **Serial Port** connection (Terminal)
  - Above PC with COM Port (DB9 / RS-232) or USB-to-RS-232 converter
- Ethernet Port connection
  - Network cables - Use standard network (UTP) cables with RJ45 connectors.
- Above Workstation installed with **WEB Browser** and **JAVA runtime environment** Plug-in

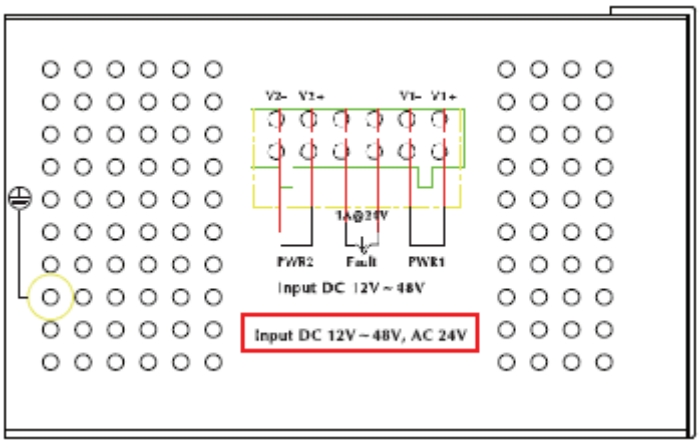


It is recommended to use Internet Explore 7.0 or above to access the Industrial Managed Switch.

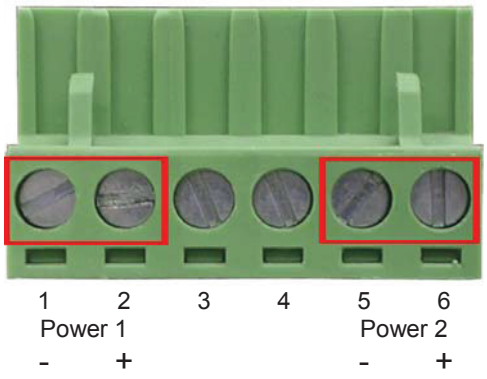
Wiring the Power Input

The 6-contact terminal block connector on the rear panel of NS3550-8T-2S is used for two DC redundant powers inputs. Please follow the steps below to insert the power wire.

1. Insert positive / negative DC power wires into contacts 1 and 2 for DC POWER 1, or 5 and 6 for DC POWER 2.



2. Tighten the wire-clamp screws to prevent the wires from loosening.



Note

The wire gauge for the terminal block should be in the range of between 12 ~ 24 AWG.

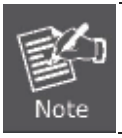
Starting Web Management

This section introduces the configuration and functions of the Web-Based management.

About Web-based Management

The Industrial Managed Switch offers management features that allow users to manage the Industrial Managed Switch from anywhere on the network through a standard browser such as Microsoft Internet Explorer.

The Web-Based Management supports Internet Explorer 7.0 or higher. It is based on Java Applets to reduce network bandwidth consumption, enhance access speed and present an easy viewing screen.



By default, IE 7.0 or higher does not allow Java Applets to open sockets. The user has to explicitly modify the browser setting to enable Java Applets to use network ports.

To configure the Industrial Managed Switch through an Ethernet connection, make sure the workstation is be set on same the IP subnet address with the Industrial Managed Switch.

For example, the default IP address of the Industrial Managed Switch is ***192.168.0.100***, then the management PC should be set as **192.168.0.x** (where x is a number between 1 and 254, except 100), and the default subnet mask is 255.255.255.0.

If you have changed the default IP address of the Industrial Managed Switch to 192.168.1.1 with subnet mask 255.255.255.0 via console, then the workstation should be set at 192.168.1.x (where x is a number between 2 and 254) to do the relative configuration on the workstation.

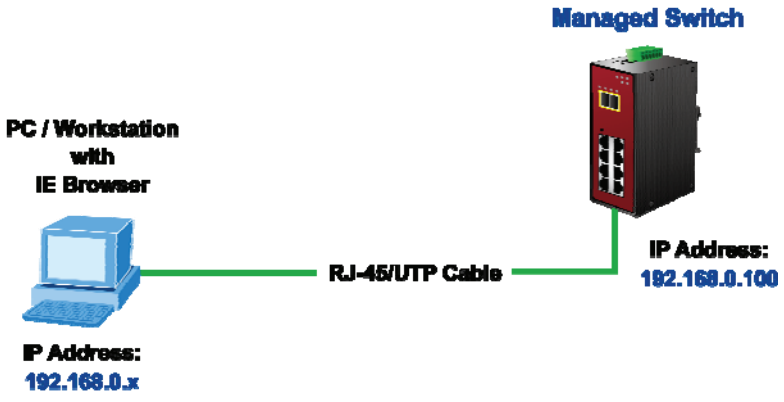


Figure 1: Web Management Diagram

- **Logging into the switch**

1. Use Internet Explorer 7.0 or above Web browser. Enter the factory-default IP address to access the Web interface. The factory-default IP Address is as follows:

http://192.168.0.100

2. When the following login screen appears, please enter the default username **"admin"** with password "**admin**" (or the username/password you have changed via console) to login to the main screen of Industrial Managed Switch. The login screen is shown in Figure 2.

Figure 2: Login Screen

Default User name: **admin**

Default Password: **admin**

After entering the username and password, the main screen appears as shown in Figure 3.

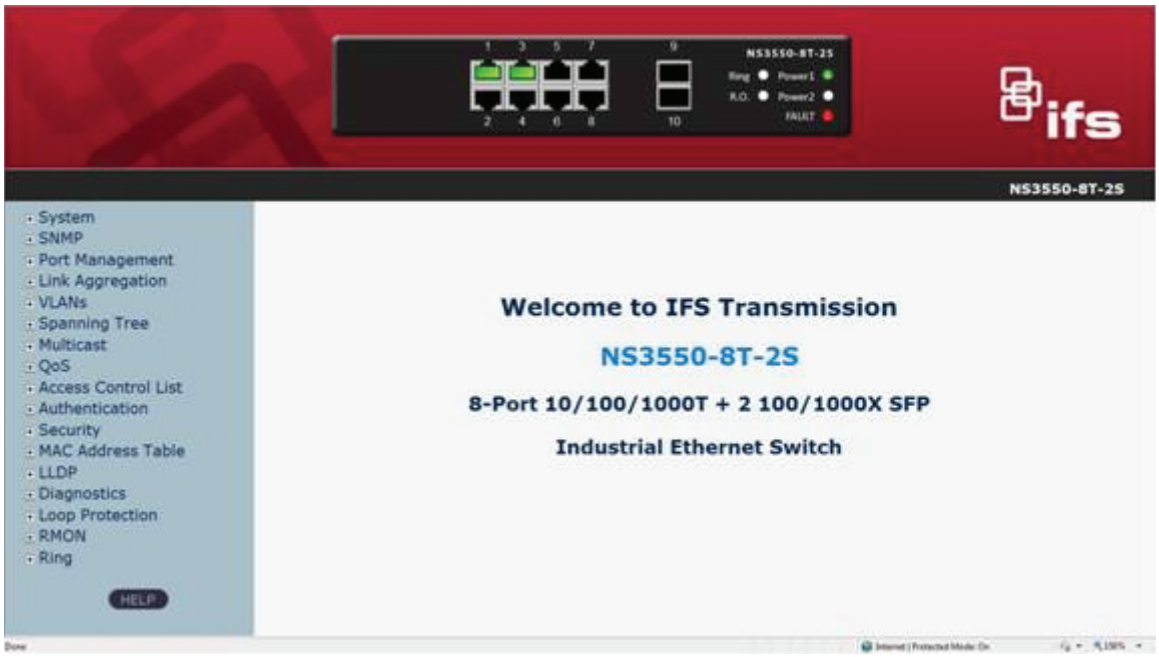


Figure 3: Default Main Page

Note

1. It is recommended to use Internet Explore 7.0 or above to access Industrial Managed Switch.
2. If the IP address of the switch is changed, the change will take effect immediately after you click on the **Save** button, Therefore, you need to use the new IP address to access the Web interface.
3. For security reasons, please change and memorize the new password after the first setup.
4. The Switch only accepts command in lowercase letters in the web interface.

Main Menu

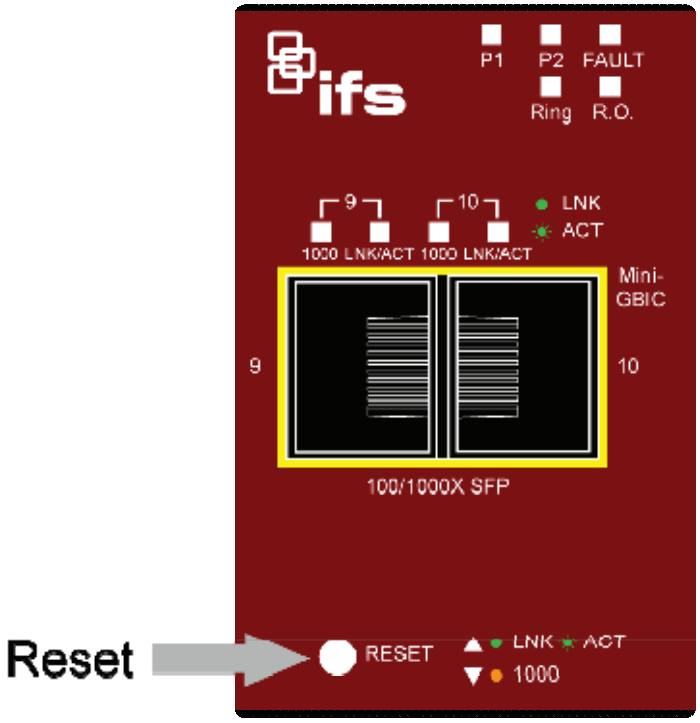
Using the onboard web agent, you can define system parameters, manage and control the Industrial Managed Switch, and all its ports, or monitor network conditions. Via the Web-Management, the administrator can setup the Industrial Managed Switch by select the functions those listed in the Main Function. The screen is shown in Figure 4.

Figure 4: NS3550-8T-2S Industrial Managed Switch Main Functions Menu

TROUBLESHOOTING

Resetting the IP address and Admin Password

To reset the IP address to the default IP Address “192.168.0.100” or reset the password to default value, press the hardware **reset button** at the front panel about **10 seconds.** After the device is rebooted, you can login the management WEB interface within the same subnet of 192.168.0.xx.



Contacting Technical Support

Contact technical support if you encounter any difficulties during this installation. Please make sure you have the requested diagnostic or log files ready before you contact us by phone or go to www.interlogix.com/customer-support.

IFS / Interlogix online FAQ :

http://www.interlogix.com/transmission

US Support

By Phone

1-855-286-8889
Option 1 - Order Services
Option 2 - Technical Support

1-855-662-8439 (MobileView)
Option 1 - Order Services
Option 2 - Technical Support

By Mail

UTC Building & Industrial Systems
3211 Progress Drive
Lincolnton, NC 28092

By Email

Orders	orders@interlogix.com
Expedited Orders	orders.expedited@interlogix.com
Technical Support	techsupport@interlogix.com
Returns & Warranty	rma@interlogix.com
General Questions	questions@interlogix.com
Pre-Sales	presales@interlogix.com
Licensing	licenses@interlogix.com
Training Inquiries	traininginquiries@lenel.com

MobileView Support MobileViewCS@fs.utc.com

MobileView Tech Support MobileViewTS@fs.utc.com

EMEA Support

By Phone +32 (0)2 725 1120

By Mail

EMEA Headquarters
UTC Fire & Security EMEA BVBA
(Europe, Middle East & Africa)
Kouterveldstraat 2
1831 Diegem-Brussels, Belgium

By Email Email emea@fs.com

This Page Left Intentionally Blank

GIGABIT 1000BASE-SX FIBER SFP TRANSCEIVER, SM

Operations & Maintenance Manual
December 2015

Mini-GBIC SFP & SFP+ Transceivers

Small Form-factor Pluggable Transceiver Modules

OVERVIEW

The IFS family of Small Form-factor Pluggable (SFP) Transceiver Modules are designed for high performance integrated duplex data transmission over optical fiber. These SFP transceiver modules are compliant with the industry's SFP Multi-source Agreement (MSA) standard.

The IFS SFP Transceiver Modules offer the ability to enable the SFP ports on any Ethernet equipment that have a built-in SFP Mini-GBIC interface. These modules are hot-swappable without any interruption of the host equipment operation.

These SFP modules are available in 100Base-FX/BX or 1000Base-TP/FX/BX configurations allowing for use of either one fiber or two fiber transmission over single mode or multi-mode optical fiber. The 10 Gigabit SFP+ modules are available for single mode and multi-mode fiber for use in IFS switches that support 10G SFP+ slots for high-bandwidth switch trunking and communication links.

Additionally, certain SFPs are available as wide-temperature versions for use in industrial equipment deployed in harsh environments.

STANDARD FEATURES

Design

- Plug-and-play capability for easy installation
- Hot-swappable
- Low power dissipation

Optical Performance

- Available in wide-temperature versions for harsh industrial applications
- Data rates of 100Mbps, 1.25Gbps or 10Gbps
- Single mode or multi-mode fiber
- 1 or 2 fiber configurations
- RJ-45 1.25Gbps SFP available

Standards Compliance

- Mini-GBIC Interface compliant
- Multi-source Agreement (MSA) compliant
- Class 1 laser safety standard IEC 60825 compliant

Warranty

- 3-year warranty

Specifications

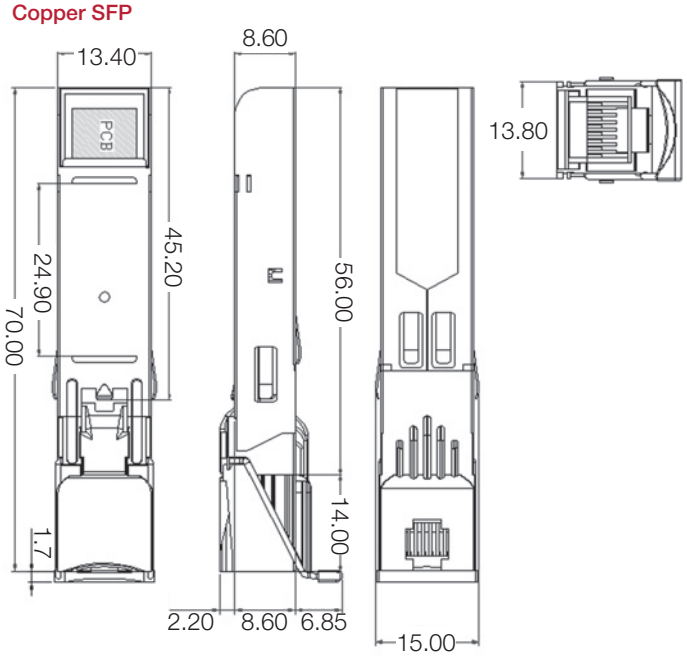
Pin	Signal Name	Description
1	VeeT	Transmitter Ground
2	TX_FAULT	Transmitter Fault Indication
3	TX_DISABLE	Transmitter Disable
4	MOD_DEF (2)	SDA Serial Data Signal
5	MOD_DEF (1)	SCL Serial Clock Signal
6	MOD_DEF (0)	TTL Low to indicate the SFP is present
7	RATE SELECT	Not Connected (Open Circuit)
8	LOS	Receiver Loss of Signal
9	VeeR	Receiver Ground
10	VeeR	Receiver Ground
11	VeeR	Receiver Ground
12	RD-	Inv. Received Data Out (Differential PECL, AC coupled)
13	RD+	Received Data Out (Differential PECL, AC coupled)
14	VeeR	Receiver Ground
15	VccR	Receiver Power Supply
16	VccT	Transmitter Power Supply
17	VeeT	Transmitter Ground
18	TD+	Transmit Data In (Differential PECL, AC coupled)
19	TD-	Inv. Transmit Data In (Differential PECL, AC coupled)
20	VeeT	Transmitter Ground

Electrical and Mechanical	
Input Voltage	3.3V DC
Dimensions (W x D x H)	2.20 x 0.59 x 0.49 in. (59 x 15 x 12.4 mm)
Weight (ounces, grams)	0.6 oz, 18g
Storage Temperature	-40ºC~85°C
Relative Humidity	5%~95% (non-condensing)
Reliability	>50,000 hrs @ 25°C

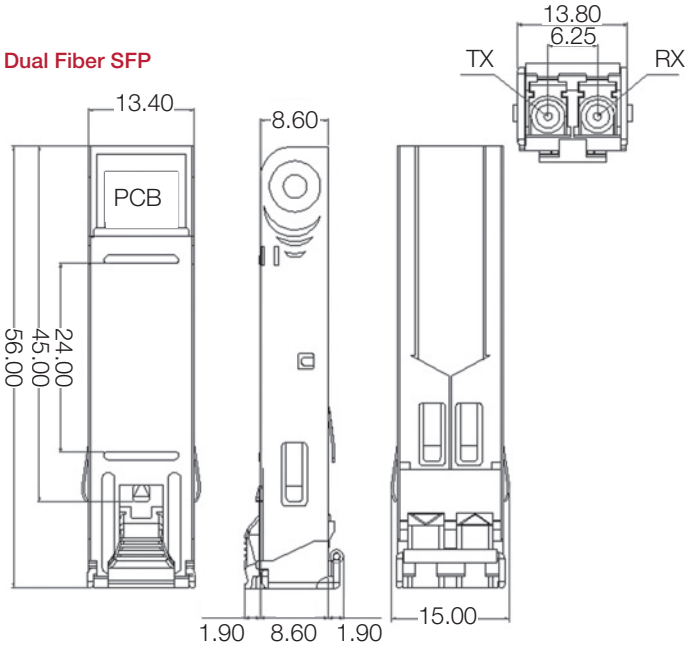
Standards Compliance	
EMI	EN55022:2010, Class A EN61000-3-2: A1+A2:2009 EN61000-3-2: 2008
EMS	EN55024: 2010 IEC 61000-4-2:2008 IEC 61000-4-3:A1+A2:2010 IEC 61000-4-4:2012 IEC 61000-4-5:2005 IEC 61000-4-6:2008 IEC 61000-4-8:2009 IEC 61000-4-11:2004 AS/NZS Cispr22: 2010
Regulatory Standards	FCC CFR 47, Part 15B, FDA 21 CFR 1040, CE Directive 2004/108/EC, EN60825-1 Laser Safety

Dimensional Diagrams

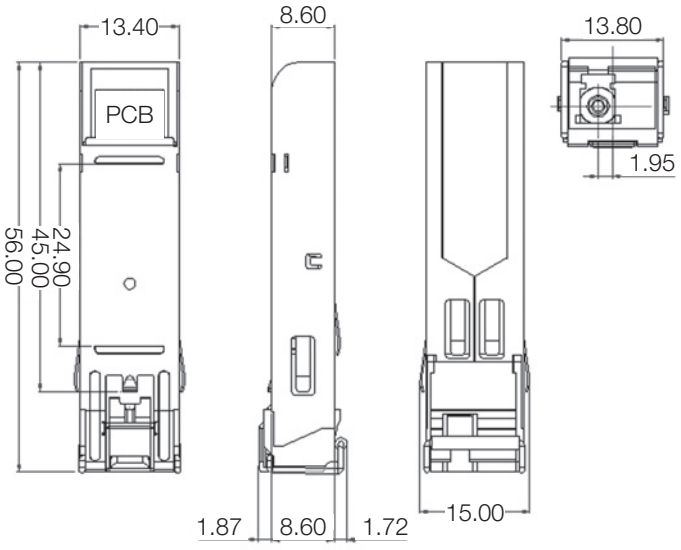
Copper SFP



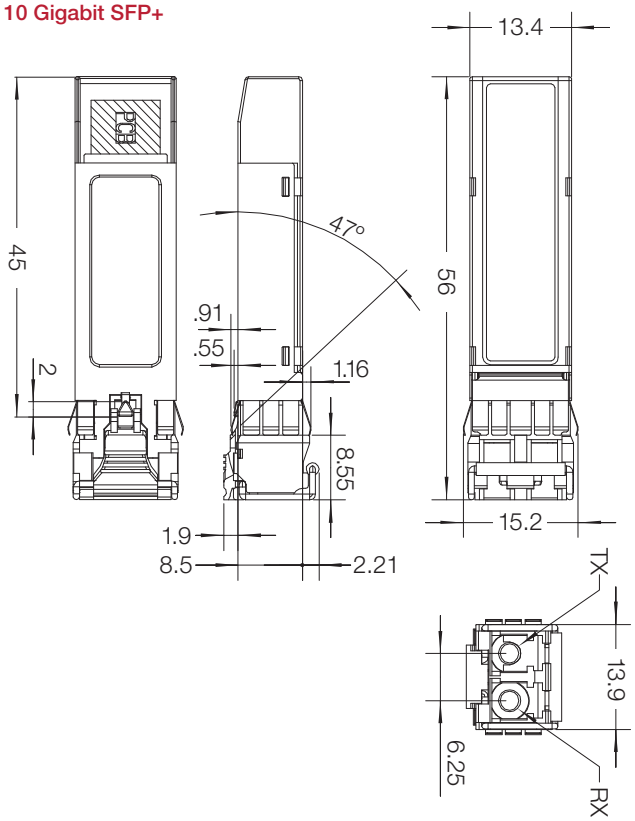
Dual Fiber SFP



Single Fiber SFP



10 Gigabit SFP+



Dimensions are in millimeters.
All dimensions are ±0.20mm unless otherwise specified.

This Page Left Intentionally Blank

IFS SFP Transceiver User Manual

P/N 1069181 • REV 1.0 • ISS 6-AUG-2014

Manufacturer

Interlogix

3211 Progress Drive, Lincolnton, NC 28092 USA

Authorized EU manufacturing representative:

UTC Climate Controls & Security B.V.,

Kelvinstraat 7, 6003 DH Weert, Netherlands

Version This document applies to IFS SFP Transceiver version 02.02

Certification N4131

FCC compliance **Class B:** This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications.

There is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

European Union directives **2004/108/EC (EMC directive)**: Hereby, UTC Building & Industrail Systems, Inc. declares that this device is in compliance with the essential requirements and other relevant provisions of Directive 2004/108/EC

2002/96/EC (WEEE directive): Products marked with this symbol cannot be disposed of as unsorted municipal waste in the European Union. For proper recycling, return this product to your local supplier upon the purchase of equivalent new equipment, or dispose of it at designated collection points. For more information see: www.recyclethis.info.

Contact information For contact information, see www.interlogix.com or www.utcfssecurityproducts.eu

Safety Notices

The fiber optic SFP transceiver modules are equipped with a Class 1 laser, which emits invisible radiation. Read the following safety warnings carefully.

Class 1 Laser Product
Complies with FDA Regulation 21 CFR 1040.10 and 1040.11

Class 1 radiation is present when the device or system is powered up. Do not look directly into a laser aperture, as prolonged exposure may cause eye damage.

Only trained and qualified personnel should be allowed to install or replace these SFP modules

Content

Overview

Thank you for purchasing an IFS SFP transceiver. The IFS SFP transceiver can be installed into any IFS network equipment with a 100Base-FX or 1000Base-SX/LX mini-GBIC interface. This user guide provides an overview of the various IFS SFPs (also known as mini-GBIC) transceiver modules available from Interlogix. This user guide also provides instructions for installing, connecting and removing these transceivers. These SFP transceiver modules are hot-pluggable, which means you can insert and remove these modules into any IFS network equipment with a mini-GBIC port without interrupting the host system. The IFS SFP line also features a selection of environmentally hardened SFPs designed for operating in environments from -40~75 degrees Celsius.

Checklist

The SFP package should contain the following items:

- The SFP Transceiver Module x1
- This User Manual x1

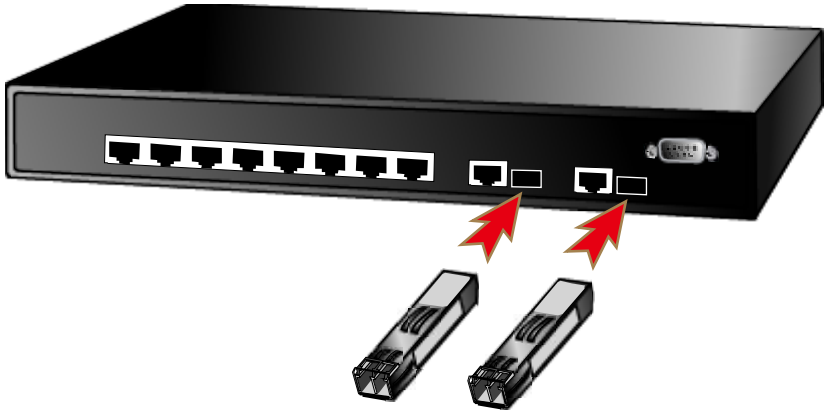
If any items are missing or damaged, please consult Interlogix or the dealer/distributor from whom you purchased your SFP transceiver module.

Installing an IFS SFP Module

This section describes how to insert an IFS SFP transceiver into a mini-GBIC slot.

The IFS SFP transceivers are hot-pluggable and hot-swappable. You can insert and remove an IFS SFP transceiver in any IFS network equipment with a mini-GBIC port without having to power down the switch or media converter. As shown in Figure 1.

Figure 1: Inserting an IFS SFP tranceiver



Install the IFS SFP into an IFS network switch or media converter before connecting a cable coming from another switch, workstation or media converter.

1. Make sure both pieces of network equipment that you are connecting together are using the same media type SFP. For example: 100Base-FX to 100Base-FX or 1000Base-SX to 1000Base-SX.
2. Check to make sure that the fiber-optic cable type matches the SFP transceiver model.
    - S20 Series and S25 Series optics operate with multimode OM1, OM2 or OM3 fiber. LC type fiber connectors are required.
    - S30 Series and S35 Series optics operate with single mode fiber. LC type fiber connectors are required.

Connecting the fiber cable

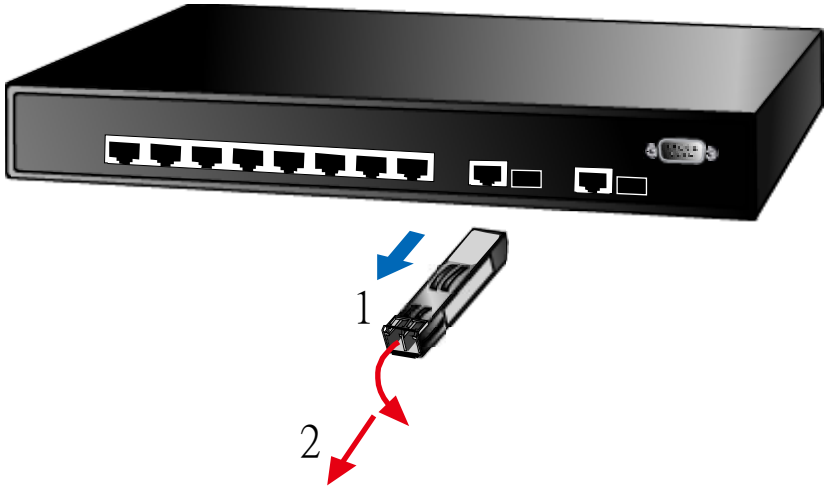
1. Insert the duplex LC connector from the network fiber cable into the SFP transceiver.

2. Connect the other end of the cable to a device – i.e. switches with an SFP installed, fiber NIC on a workstation or a Media Converter.
3. Check the LNK/ACT LED of the SFP slot of the switch / converter. Ensure that the SFP transceiver is operating correctly.
4. Check the link mode of the SFP port to see if there is any link failure. With some fiber-NICs or Media Converters, setting the link mode to **"1000 Force"** or **"100 Force"** may be needed for proper operation.

Removing the SFP transceiver

1. Make sure there is no network activity by consulting with a network administrator before removing the SFP or use the switch or media converters management interface (if available) to disable the port in advance.
2. Gently remove the fiber optic cable connector.
3. Flip the wire handle of the SFP module out to a horizontal position.
4. Pull out the SFP module gently out of the mini-GIBIC slot with the wire handle.

Figure 2: Pull out the SFP transceiver



Caution: Never pull out the SFP transceiver module without using the pull handle or the push bolts on the module. Directly pulling out the SFP module with force could damage the SFP module and mini-GIBIC slot of the network device.

SFP Specifications

The IFS SFP transceivers are available in the following models.

Twisted Pair SFP	**1000 Base TX**	**GigE**	
Part #	Connector	Wire Type	Max Distance
S30-RJ	RJ 45	Cat 5e	100M (328 ft)

Fast Ethernet **100 Base FX**

Part #	Fiber Connector	# of Fibers	Fiber Type	Max Distance	Wave Length	Optical Budget (dBm)	Optical Power (dBm)	Receiver Sensitivitiy (dBm)	Operating Temperature
S20-2MLC2	LC	2	Multimode	2km (1.2mi)	1310nm	12	-20 ~ -14	-32	0 to + 50C (32 to 122F)
S25-2MLC2	LC	2	Multimode	2km (1.2mi)	1310nm	12	-20 ~ -14	-32	-40 to +75C (-40 to 167F)

Fast Ethernet **100 Base LX**

Part #	Fiber Connector	# of Fibers	Fiber Type	Max Distance	Wave Length	Optical Budget (dBm)	Optical Power (dBm)	Receiver Sensitivitiy (dBm)	Operating Temperature
S20-2SLC20	LC	2	Single Mode	20km (12mi)	1310nm	19	-15 ~ -8	-34	0 to + 50C (32 to 122F)
S25-2SLC20	LC	2	Single Mode	20km (12mi)	1310nm	19	-15 ~ -8	-34	-40 to +75C (-40 to 167F)

Fast Ethernet **100 Base BX**

Part #	Fiber Connector	# of Fibers	Fiber Type	Max Distance	Wave Length TX RX	Optical Budget (dBm)	Optical Power (dBm)	Receiver Sensitivitiy (dBm)	Operating Temperature
S20-1SLC/A-20	LC	1	Single Mode	20km (12mi)	1310/1550nm	18	-14 ~ -8	-32	0 to + 50C (32 to 122F)
S25-1SLC/B-20	LC	1	Single Mode	20km (12mi)	1550/1310nm	18	-14 ~ -8	-32	-40 to +75C (-40 to 167F)

Gigabit Ethernet 1000 Base SX

Part #	Fiber Connector	# of Fibers	Fiber Type OM1 & OM2	Max Distance OM1/OM2	Wave Length	Optical Budget (dBm)	Optical Power (dBm)	Receiver Sensitivitiy (dBm)	Operating Temperature
S30-2MLC	LC	2	Multimode	220/550m (720/1800ft)	850nm	7.5	-9.5 ~ -1	-17	0 to + 50C (32 to 122F)
S35-2MLC	LC	2	Multimode	220/550m (720/1800ft)	850nm	7.5	-14 ~ -8	-17	-40 to +75C (-40 to 167F)

OM1 Multimode fiber @ 200/500MHz-km

OM2 Multimode fiber @ 500.500MHZ-km Laser Rated for GbE LANs

Gigabit Ethernet 1000 Base SX

Part #	Fiber Connector	# of Fibers	Fiber Type OM3	Max Distance OM3	Wave Length	Optical Budget (dBm)	Optical Power (dBm)	Receiver Sensitivitiy (dBm)	Operating Temperature
S30-2MLC-2	LC	2	Multimode	2km (1.2mi)	1310nm	10	-9 ~ -1	-19	0 to + 50C (32 to 122F)

OM3 Multimode fiber @ 2000/500MHz-km Optimized got 850nm VCSELs

Gigabit Ethernet 1000 Base LX

Part #	Fiber Connector	# of Fibers	Fiber Type	Max Distance	Wave Length	Optical Budget (dBm)	Optical Power (dBm)	Receiver Sensitivitiy (dBm)	Operating Temperature
S30-2SLC-10	LC	2	Single Mode	10km (6.2mi)	1310nm	18	-9.5 ~ -3	-20	0 to + 50C (32 to 122F)
S35-2SLC-10	LC	2	Single Mode	10km (6.2mi)	1310nm	18	-9.5 ~ -3	-20	-40 to +75C (-40 to 167F)
S30-2SLC-30	LC	2	Single Mode	30km (18.6mi)	1310nm	18	-2 ~ +3	-23	0 to + 50C (32 to 122F)
S35-2SLC-30	LC	2	Single Mode	30km (18.6mi)	1310nm	18	-2 ~ +3	-23	-40 to +75C (-40 to 167F)

Gigabit Ethernet 1000 Base ZX

Part #	Fiber Connector	# of Fibers	Fiber Type	Max Distance	Wave Length	Optical Budget (dBm)	Optical Power (dBm)	Receiver Sensitivitiy (dBm)	Operating Temperature
S30-2SLC-70	LC	2	Single Mode	70km (43mi)	1550nm	19*	-15 ~ -8	-34	0 to + 50C (32 to 122F)
S35-2SLC-70	LC	2	Single Mode	70km (43mi)	1550nm	19*	-15 ~ -8	-34	-40 to +75C (-40 to 167F)

* Note: High Power Optic. There must be a minimum of 5dB of optical loss to the fiber for proper operation.

Gigabit Ethernet 1000 Base BX

Part #	Fiber Connector	# of Fibers	Fiber Type	Max Distance	Wave Length TX RX	Optical Budget (dBm)	Optical Power (dBm)	Receiver Sensitivitiy (dBm)	Operating Temperature
S30-1SLC/A-10	LC	1	Single Mode	10km (6.2mi)	1310/1490nm	11	-9 ~ -3	-20	0 to + 50C (32 to 122F)
S30-1SLC/B-10	LC	1	Single Mode	10km (6.2mi)	1490/1310nm	11	-9 ~ -3	-20	0 to + 50C (32 to 122F)
S30-1SLC/A-20	LC	1	Single Mode	20km (12mi)	1310/1490nm	15	-8 ~ -2	-23	0 to + 50C (32 to 122F)
S30-1SLC/B-20	LC	1	Single Mode	20km (12mi)	1490/1310nm	15	-8 ~ -2	-23	0 to + 50C (32 to 122F)

Gigabit Ethernet 1000 Base BX

Part #	Fiber Connector	# of Fibers	Fiber Type	Max Distance	Wave Length TX RX	Optical Budget (dBm)	Optical Power (dBm)	Receiver Sensitivitiy (dBm)	Operating Temperature
S30-1SLC/A-60	LC	1	Single Mode	60km (37mi)	1310/1490nm	24	0 ~ +5	-24	0 to + 50C (32 to 122F)
S30-1SLC/B-60	LC	1	Single Mode	60km (37mi)	1490/1310nm	24	0 ~ +5	-24	0 to + 50C (32 to 122F)

* Note: High Power Optic. There must be a minimum of 5dB of optical loss to the fiber for proper operation.

10GBase-SR SFP+

Part #	Fiber Connector	# of Fibers	Fiber Type OM3	Max Distance OM3	Wave Length	Optical Budget (dBm)	Optical Power (dBm)	Receiver Sensitivitiy (dBm)	Operating Temperature
S40-2MLC	LC	2	Multimode	300m*	850nm	10	-7.3 ~ -1	-11	0 to + 50C (32 to 122F)

*OM3 Multimode fiber @ 2000/500MHz-km Optimized got 850nm VCSELs maximum distance of 300m.

10GBase-LR SFP+

Part #	Fiber Connector	# of Fibers	Fiber Type	Max Distance	Wave Length	Optical Budget (dBm)	Optical Power (dBm)	Receiver Sensitivitiy (dBm)	Operating Temperature
S40-2SLC-10	LC	2	Single Mode	10km (6.2mi)	1310nm	15	-8.0 ~ -1	-12	0 to + 50C (32 to 122F)

* Note: High Power Optic. There must be a minimum of 5dB of optical loss to the fiber for proper operation.

Appendix A

Fiber Optical Cable Connection Parameters

The wiring details are as below:

- Fiber Optical patch Cables:

Standard	Fiber Type	Cable Specification
1000Base-SX (850nm)	Multi-mode	50/125μm or 62.5/125μm
1000Base-LX (1310nm)	Single mode	9/125μm
1000Base-LX (1550nm)	Single mode	9/125μm
100Base-FX (1310nm)	Multi-mode	50/125μm or 62.5/125μm
	Single mode	9/125μm
10 Gig Base SR (850nm)	Multi-mode	50/125um (OM3)
10 Gig Base LR (1310nm)	Single-mode	9/125um

This Page Left Intentionally Blank

GIGABIT RJ-45 TRANSCEIVER, CAT5E

Operations & Maintenance Manual
December 2015

North America
T 855-286-8889

Latin America
T 561-998-6114

Mini-GBIC SFP & SFP+ Transceivers

Small Form-factor Pluggable Transceiver Modules

Ordering Information

Fast (100Mbps)

Part No.	PHY Type	# of Fibers	Fiber Type	Connector	TX Wavelength	RX Wavelength	Max. Distance	Power (dBm)	RX Sen. (dBm)	Power Budget	Operating Temperature
100Base-FX											
S20-2MLC-2	100Base-FX	2	Multi-mode	LC	1310nm	1310nm	2km	-20 ~ -14	-32	12	0 ~ 50°C
S25-2MLC-2	100Base-FX	2	Multi-mode	LC	1310nm	1310nm	2km	-20 ~ -14	-32	12	-40 ~ 75°C
100Base-LX											
S20-2SLC-20	100Base-LX	2	Single mode	LC	1310nm	1310nm	20km	-15 ~ -8	-34	19	0 ~ 50°C
S25-2SLC-20	100Base-LX	2	Single mode	LC	1310nm	1310nm	20km	-15 ~ -8	-34	19	-40 ~ 75°C
100Base-BX											
S20-1SLC/A-20	100Base-BX20-U	1	Single mode	LC	1310nm	1550nm	20km	-14 ~ -8	-32	18	0 ~ 50°C
S20-1SLC/B-20	100Base-BX20-D	1	Single mode	LC	1550nm	1310nm	20km	-14 ~ -8	-32	18	0 ~ 50°C

Gigabit (1000Mbps)

Part No.	PHY Type	# of Fibers	Fiber Type	Connector	TX Wavelength	RX Wavelength	Max. Distance	Power (dBm)	RX Sen. (dBm)	Power Budget	Operating Temperature
Copper-RJ45											
S30-RJ	SFP-1000T	-	Copper	RJ-45	-	-	100m	-	-	-	0 ~ 50°C
1000Base-SX											
S30-2MLC	1000Base-SX	2	Multi-mode	LC	850nm	850nm	220m/550m*	-9.5 ~ -4	-17	7.5	0 ~ 50°C
S35-2MLC	1000Base-SX	2	Multi-mode	LC	850nm	850nm	220m/550m*	-9.5 ~ -4	-17	7.5	-40 ~ 75°C
S30-2MLC-2	1000Base-SX2	2	Multi-mode	LC	1310nm	1310nm	2km**	-9 ~ -1	-19	10	0 ~ 50°C
1000Base-LX/LHX/ZX											
S30-2SLC-10	1000Base-LX	2	Single mode	LC	1310nm	1310nm	10km	-9.5 ~ -3	-20	10.5	0 ~ 50°C
S35-2SLC-10	1000Base-LX	2	Single mode	LC	1310nm	1310nm	10km	-9.5 ~ -3	-20	10.5	-40 ~ 75°C
S30-2SLC-30	1000Base-LHX	2	Single mode	LC	1310nm	1310nm	30km	-2 ~ +3	-23	21	0 ~ 50°C
S35-2SLC-30	1000Base-LHX	2	Single mode	LC	1310nm	1310nm	30km	-2 ~ +3	-23	21	-40 ~ 75°C
S30-2SLC-70	1000Base-ZX	2	Single mode	LC	1550nm	1550nm	70km	0 ~ +5	-24	24	0 ~ 50°C
S35-2SLC-70	1000Base-ZX	2	Single mode	LC	1550nm	1550nm	70km	0 ~ +5	-24	24	-40 ~ 75°C
1000Base-BX											
S30-1SLC/A-10	1000Base-BX10-U	1	Single mode	LC	1310nm	1490nm	10km	-9 ~ -3	-20	11	0 ~ 50°C
S30-1SLC/B-10	1000Base-BX10-D	1	Single mode	LC	1490nm	1310nm	10km	-9 ~ -3	-20	11	0 ~ 50°C
S30-1SLC/A-20	1000Base-BX20-U	1	Single mode	LC	1310nm	1490nm	20km	-8 ~ -2	-23	15	0 ~ 50°C
S30-1SLC/B-20	1000Base-BX20-D	1	Single mode	LC	1490nm	1310nm	20km	-8 ~ -2	-23	15	0 ~ 50°C
S30-1SLC/A-60	1000Base-BX60-U	1	Single mode	LC	1310nm	1490nm	60km	0 ~ +5	-24	24	0 ~ 50°C
S30-1SLC/B-60	1000Base-BX60-D	1	Single mode	LC	1490nm	1310nm	60km	0 ~ +5	-24	24	0 ~ 50°C

10 Gigabit (10,000Mbps)

Part No.	PHY Type	# of Fibers	Fiber Type	Connector	TX Wavelength	RX Wavelength	Max. Distance	Power (dBm)	RX Sen. (dBm)	Power Budget	Operating Temperature
10 Gigabit (SFP+)											
S40-2MLC	10GBase-SR	2	Multi-mode	LC	850nm	850nm	300m***	-7.0 avg	-11	7	0 ~ 70°C
S40-2SLC-10	10GBase-LR	2	Single mode	LC	1310nm	1310nm	10km	-8.0 avg	-12	10	0 ~ 70°C

* 220m distance is based on 62.5/125 (OM1) fiber. 550m distance is based on 50/125 (OM2) fiber.
** Requires laser optimized 50/125 (OM3) fiber to achieve 2km distance. Fiber should be tested and verified to OM3 standard.
*** 300m distance with 10G is based on 50/125 (OM3) fiber.

Legend

SFP Type Heading
Standard SFP
Hardened SFP (wide-temp)

interlogix
United Technologies

interlogix.com

Specifications subject to change without notice.

408-3849 2014/08 (79013)

This Page Left Intentionally Blank

DELL 22-INCH VIDEO DISPLAY MONITOR

Operations & Maintenance Manual
December 2015

Dell Professional Series P2213 22" (56 cm) and P1913 & P1913S 19" (48 cm) Monitors with LED backlights

Dell Professional P1913S 19" Monitor

Dell Professional P1913 19" Monitor

Dell Professional P2213 22" Monitor

For the comfort, convenience and performance you need to be productive, choose Dell Professional Series P2213, P1913 or P1913S monitors

Designed to bring you the comfort, convenience and performance you need, the Dell Professional Series P2213, P1913, and P1913S monitors help you to be productive. They come with full adjustability features such as an optimal[1] 130 mm height adjustment range, tilt, swivel and pivot capabilities, and a range of connectivity options including DisplayPort, all in an eco-conscious design.

Perfect for:

- Large companies that want to reduce their carbon footprint and overall energy consumption, and that value their employees' viewing comfort
- Small and medium businesses looking for affordable monitors with good viewing comfort and screen performance
- Educational institutions for computer labs or classrooms
- Government offices

Dell Professional Series P2213 22", P1913 19" and P1913S 19" Monitors with LED backlights

Designed for optimal comfort and convenience

- **Improved height adjustability** (130 mm) Maximize your viewing comfort by easily adjusting the monitor to an optimal height[1]
- **Additional comfort-enabling features such as tilt, swivel and pivot (with enhanced menu rotation)** With the Enhanced Menu Rotation software[2] you can easily rotate the monitor from landscape to portrait viewing and vice versa. Other comfort-enabling features include tilt and swivel and allow you to adjust the screen to your preferred angle.
- **Dell Display Manager software (Auto mode, PowerNap)** Enjoy great ease of use with Dell Display Manager — your one-stop software application that allows manual adjustment or auto assignment of optimum preset modes to specific software applications. It also lets you manage your monitor's power consumption via PowerNap.
- **Connectivity options**
  - DisplayPort 1.2[3], VGA, DVI (HDCP), 2 x USB ports — Seamlessly connect your monitor with your desktop, laptop and other peripherals with the wide array of connectivity ports.

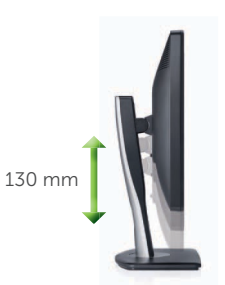
Excellent screen performance

- **Screen clarity**
  - Experience great work productivity with crystal clear resolution of 1650 x 1050 for P2213, 1440 x 900 for P1913 and 1280 x 1024 for P1913S (max)
  - High dynamic contrast ratio of 2 million:1 so you can see your work in razor-sharp clarity, and experience smooth, jitter-free moving images
  - High color gamut[4] of 83%, and 16.7 million colors — Get a wide range of true-to-life colors
- **Premium Panel Guarantee** — A free panel exchange is guaranteed in the event that you discover even one bright pixel in the Professional Series monitors during the Limited Hardware Warranty[5] period, thus ensuring the quality of the monitor

Eco-design

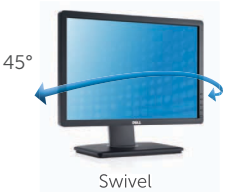
- **Made of environmentally-responsible materials**
  - BFR/PVC-free monitor (except for cables), helping you make a greener choice without compromising on cost, performance or reliability
  - Help make the monitor easy to recycle and will help to lower power consumption
  - Arsenic-free glass, mercury-free LED panel
  - More than 25% post-consumer recycled plastics in its chassis
- **PowerNap[6] software** — Helps to dim the monitor to its minimum brightness level or puts it into sleep mode when not in use — designed to help save energy
- **Dynamic dimming[7] software** — Adjusts onscreen brightness when images displayed consist of predominantly large bright and white areas — designed to help save energy
- **Environmental compliance** — Meets the latest environmental standards such as ENERGY STAR®, EPEAT Gold, TCO Certified Displays, and CEL
- **Eco-conscious packaging** — Environmentally responsible packaging includes corrugated cardboard and is free of expanded polystyrene form (EPS). Packaging and corrugated cardboard are easy to recycle and help reduce environmental waste.

Designed for comfort, convenience and ease-of-use



Height adjustment

Tilt

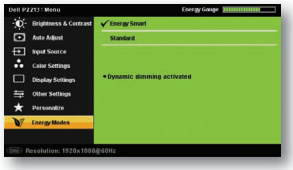


Swivel


Pivot


Connectors

Power-saving features


Dynamic Dimming automatically dims onscreen brightness when displayed images consist of predominantly large bright and white areas

PowerNap dims the monitor to the minimum brightness level or puts it into sleep mode based on user preference

Dell recommends that customers dispose used computer hardware, including monitors, in an environmentally sound manner. Potential methods include reuse of parts or whole products and recycling of product, components and/or materials. For more information, please visit http://dell.com/recycling_programs and www.dell.com/environment

	Dell Professional Series P2213 22" monitor with LED	Dell Professional Series P1913 19" monitor with LED	Dell Professional Series P1913S 19" monitor with LED
Display			
Viewable image size (diagonal)	55.88 cm (22 inches)	48.26 cm (19 inches)	48.26 cm (19 inches)
Preset display area Horizontal Vertical	140,292 sq-mm (217 sq-inches) 473.8 mm (18.65 inches) 296.1 mm (11.66 inches)	104,162 sq-mm (161.5 sq-inches) 408.2 mm (16.07 inches) 255.2 mm (10.05 inches)	113,304 sq-mm (176 sq-inches) 376.3 mm (14.81 inches) 301.1 mm (11.85 inches)
Maximum resolution	1680 x 1050 at 60 Hz	1440 x 900 at 60 Hz	1280 x 1024 at 60 Hz
Pixel pitch	0.282 mm	0.248 mm	0.277 mm
Brightness (typical)	250cd/m^2		
Color gamut (typical)	83%[4]		
Color depth	16.7 million colors		
Contrast ratio (typical) Dynamic contrast ratio (typical)	1,000:1 2 million:1		
Viewing angle (typical) (vertical/horizontal)	160°/170°		
Response time (typical)	5ms (black to white)		
Panel type	TN (active matrix – TFT LCD)		
Backlight	LED		
Connectivity			
Connectors	DVI-D (HDCP), VGA, DisplayPort (vr 1.2)[3], 2 x USB 2.0 ports		
Design Features			
Stand	Height adjustable stand (130 mm) with tilt, swivel and pivot features, built-in cable management, VESA mount support		
Security	Security lock slot and stand lock (security lock and M3x6mm screw for stand lock not included)		
Power			
AC input voltage/frequency/current	100 to 240 VAC/50 or 60 Hz ± 3 Hz/1.5 A (typical)		
Power consumption (typical)	25 W	17 W	
Power consumption active-off mode	<0.3 W		
Dimensions (with stand)			
Height (compressed ~ extended)	368.9 mm ~ 497.4 mm (14.52 inches ~ 19.58 inches)	356.9 mm ~ 476.4 mm (14.05 inches ~ 18.76 inches)	370.1 mm ~ 500.1 mm (14.57 inches ~ 19.69 inches)
Width	510.4 mm (20.09 inches)	43.8 mm (17.47 inches)	411.9 mm (16.22 inches)
Depth	183.3 mm (7.22 inches)		
Weight			
Weight without stand assembly (For wall mount or VESA mount considerations – no cables)	3.43 kg (7.55 lbs)	2.52 kg (5.54 lbs)	2.95 kg (6.49 lbs)
Weight with stand assembly and cables	5.71 kg (12.56 lbs)	4.75 kg (10.45 lbs)	5.23 kg (11.51 lbs)
Weight with packaging	7.43 kg (16.35 lbs)	5.87 kg (12.91 lbs)	6.75 kg (14.85 lbs)

Service & Warranty

- 3 Years Advanced Exchange Service[8] & Limited Hardware Warranty[5]
- Premium Panel Guarantee – 100% replacement of Professional Series monitors sold if any bright pixel is found, valid within the warranty period.

*Registered in US and Canada only.

[1] Based on Dell 2010 internal usability study on US population.
[2] Enabled when PowerNap feature is enabled.
[3] Cable not included.
[4] Color gamut (typical) is based on CIE1976 (83% of NTSC) and CIE1931 (72%) test standards.
[5] For a copy of Limited Hardware Warranty, write to Dell USA LP, Attn: Warranties, One Dell Way, Round Rock, TX 78682 or see www.dell.com/warranty.
[6] Dims the monitor to its minimum brightness or puts it in to sleep mode when not in use.
[7] When enabled, reduces on screen brightness when displayed images consist of predominantly large bright and white areas.
[8] Advanced Exchange Service: Replacement part/unit dispatched, if needed, following completion of phone/online diagnosis. Fee charged for failure to return defective unit. Availability varies. Other conditions apply.

Product availability varies by country.

For more information about Dell monitors, visit www.dell.com/monitors or contact your commercial channel partner.

Ad#G12001014
v.2 07/2012

This Page Left Intentionally Blank

WALL MOUNTED MONITOR BRACKET

Operations & Maintenance Manual
December 2015

VideoSecu TV Wall Mount Articulating Arm Tilt Swivel Bracket for most 15-27″ TV Monitor Display VESA 100X100 75X75 up to 33LBS ML15B A28 description

This adjustable articulating arm swing LCD TV monitor wall mount can extend out up to 14 inch, and folds flat against the wall. Aluminum alloy construction supports LCD monitor up to 33 lbs. Its classic black finish, 3 pivot points provides 0-20 degrees forward tilt, 180 degree swivel, and max 14 inch extends for virtually limitless adjustment. The VESA plate can be taken off to attach the display for easy installation. This two-link arm design offer elegantly look for offices, conference rooms, merchandising displays, hotel rooms or any room in the house. VideoSecu brand new design mount.

- Brand: VideoSecu
- Model: ML15B

Features

- Fits most 15″, 17″, 19″, 20″, 22″, 23″, 24″ and some up to 27″ TV and monitors
- Load capacity up to 33 lbs; Compatible with VESA 75x75mm/100x100mm
- The mount plate can be taken off easily to attach the display; Two piece “slide-in” installation for easy mounting
- Extend out up to 14″ from wall, and 1.6 inch profile when folds flat
- Tilt forward up to 20 degrees;3 pivot points for virtually limitless adjustment

This Page Left Intentionally Blank

ETHERNET MICRO RTU CONTROLLER, 12 DI, 8 DO

Operations & Maintenance Manual
December 2015

ioLogik E2200 Series

Ethernet micro RTU controllers

- Active communication with patented Active OPC Server
- Smart alarm management with e-mail, SNMP Trap, TCP, UDP
- Save time and wiring costs with peer-to-peer communication
- Front-end intelligence with patented Click&Go control logic, up to 24 rules
- Simplify I/O management with MXIO library for Windows or Linux
- Friendly configuration with web browser
- Supports SNMPv1/v2c/v3 protocol
- Wide operating temperature range of -40 to 75°C (-40 to 167°F)

Introduction

Moxa's ioLogik E2200 is a new type of Ethernet micro RTU controller, which is a PC-based data acquisition and control device that uses proactive, event-based reporting to control I/O devices. Unlike traditional RTUs, which are passive and must poll for data, Moxa's ioLogik E2200 series with Active OPC Server makes seamless connection with SCADA systems a reality. In addition, SNMP is used for communicating with an NMS (Network Management System) for IT field users. The I/O status of an Ethernet micro RTU controller can be reported and controlled automatically on-site based on user specified conditions. This report-by-exception approach, which is new to PC-based monitoring, requires far less bandwidth than traditional polling methods.

ioLogik E2200 Series Selection Table

Models	I/O Combinations							
	Digital Inputs	Digital Outputs	Analog Inputs	Analog Outputs	RTD Inputs	TC Inputs	Relay Outputs	Configurable DIOs
ioLogik E2210	12	8	–	–	–	–	–	–
ioLogik E2212	8	8	–	–	–	–	–	4
ioLogik E2214	6	–	–	–	–	–	6	–
ioLogik E2240	–	–	8	2	–	–	–	–
ioLogik E2242	–	–	4	–	–	–	–	12
ioLogik E2260	–	4	–	–	6	–	–	–
ioLogik E2262	–	4	–	–	–	8	–	–

ioLogik E2210 Specifications

Inputs and Outputs

Digital Inputs: 12 channels
Digital Outputs: 8 channels
Isolation: 3K VDC or 2K Vrms

Digital Input

Sensor Type: Wet Contact (NPN), Dry Contact
I/O Mode: DI or Event Counter
Dry Contact:
• On: short to GND
• Off: open
Wet Contact (DI to GND):
• On: 0 to 3 VDC
• Off: 10 to 30 VDC
Common Type: 12 points per COM
Counter Frequency: 900 Hz
Digital Filtering Time Interval: Software selectable

Digital Output

Type: Sink
I/O Mode: DO or Pulse Output
Pulse Output Frequency: 1 kHz
Over-voltage Protection: 45 VDC
Over-current Protection: 2.6 A (4 channels @ 650 mA)
Over-temperature Shutdown: 175°C (min.)
Current Rating: 200 mA per channel

Power Requirements

Power Consumption: 203 mA @ 24 VDC

MTBF (mean time between failure)

Time: 213,673 hrs
Database: Telcordia (Bellcore)

ioLogik E2212 Specifications

Inputs and Outputs
Digital Inputs: 8 channels
Digital Outputs: 8 channels
Configurable DIOs: 4 channels
Isolation: 3K VDC or 2K Vrms

Digital Input
Sensor Type: Wet Contact (NPN or PNP) and Dry Contact
I/O Mode: DI or Event Counter
Dry Contact:
• On: short to GND
• Off: open
Wet Contact (GI to GND):
• On: 0 to 3 VDC
• OFF: 10 to 30 VDC
Common Type: 6 points per COM
Counter Frequency: 900 Hz, power off storage
Digital Filtering Time Interval: Software selectable

Digital Output
Type: Sink
I/O Mode: DO or Pulse Output
Pulse Output Frequency: 1 kHz
Over-voltage Protection: 45 VDC
Over-current Protection: 2.6 A (4 channels @650 mA)
Over-temperature Shutdown: 175°C (min.)
Current Rating: 200 mA per channel

Power Requirements
Power Consumption: 136 mA @ 24 VDC

MTBF (mean time between failure)
Time: 217,722 hrs
Database: Telcordia (Bellcore)

ioLogik E2214 Specifications

Inputs and Outputs
Digital Inputs: 6 channels
Relay Outputs: 6 channels
Isolation: 3K VDC or 2K Vrms

Digital Input
Sensor Type: Wet Contact (NPN or PNP) and Dry Contact
I/O Mode: DI or Event Counter
Dry Contact:
• On: short to GND
• Off: open
Wet Contact:
• On: 0 to 3 VDC
• Off: 10 to 30 VDC
Common Type: 3 points per COM
Counter Frequency: 900 Hz, power off storage
Digital Filtering Time Interval: Software selectable

Relay Output
Type: Form A (N.O.) power relay
Contact Current Rating:
• Inductive Load: 2 A @ 30 VDC, 250 VAC, 110 VAC
• Resistive Load: 5 A @ 30 VDC, 250 VAC, 110 VAC
Minimum permitted load: 1 A @ 5 VDC
Initial Insulation Resistance: 1000 M ohms (min.) @ 500 VDC
Mechanical endurance: 1,000,000 operations
Electrical endurance: 100,000 operations @ 5 A resistive load
Contact Resistance: 100 m ohms (max.)
Pulse Output: 0.3 Hz at rated load

Power Requirements
Power Consumption: 170 mA @ 24 VDC

MTBF (mean time between failure)
Time: 307,239 hrs
Database: Telcordia (Bellcore)

ioLogik E2240 Specifications

Inputs and Outputs
Analog Inputs: 8 channels
Analog Outputs: 2 channels

Analog Input
Type: Differential input
Resolution: 16 bits
I/O Mode: Voltage / Current
Input Range: ±150 mV, ±500 mV, ±5 V, ±10 V, 0 to 20 mA, 4 to 20 mA
Accuracy:
±0.1% FSR @ 25°C
±0.3% FSR @ -10 and 60°C
±0.5% FSR @ -40 and 75°C
Sampling Rate:
All channels:
• 10 samples/sec for voltage
• 6 samples/sec for current
Per channel:
• 1.25 samples/sec for voltage
• 0.75 samples/sec for current
Single channel:
• 1.25 samples/sec for voltage
• 0.75 samples/sec for current
Input Impedance: 900K ohms (min.)
Built-in Resistor for Current Input: 120 ohms
Isolation: 3K VDC or 2K Vrms

Analog Output
Resolution: 12 bits
Output Range: 0 to 10 V, 4 to 20 mA
Drive Voltage: 15 VDC for current output
Accuracy:
±0.1% FSR @ 25°C,
±0.3% FSR @ -10 and 60°C
Load Resistor: Less than 250 ohms

Power Requirements
Power Consumption: 198 mA @ 24 VDC

MTBF (mean time between failure)
Time: 155,941 hrs
Database: Telcordia (Bellcore)

ioLogik E2242 Specifications

Inputs and Outputs
Analog Inputs: 4 channels
Configurable DIOs: 12 channels

Analog Input
Type: Differential input
Resolution: 16 bits
I/O Mode: Voltage / Current
Input Range: ±150 mV, 0 to 150 mV, ±500 mV, 0 to 500 mV, ±5 V, 0 to 5 V, ±10 V, 0 to 10 V, 0 to 20 mA, 4 to 20 mA
Accuracy:
±0.1% FSR @ 25°C
±0.3% FSR @ -10 and 60°C
±0.5% FSR @ -40 and 75°C
Sampling Rate:
All channels:
• 32 samples/sec
Per channel:
• 8 samples/sec
Single channel:
• 100 samples/sec
Input Impedance: 200K ohms (min.)
Built-in Resistor for Current Input: 120 ohms

Digital Input
Sensor Type: Wet Contact (NPN or PNP) and Dry Contact
I/O Mode: DI or event counter
Dry Contact:
• On: short to GND
• Off: Open
Wet Contact:
• On: 0 to 3 VDC
• Off: 10 to 30 VDC
Common Type: 6 points per COM
Isolation: 3K VDC or 2K Vrms
Counter Frequency: 900 Hz, power off storage
Digital Filtering Time Interval: Software selectable

Digital Output
Type: Sink
I/O Mode: DO or Pulse Output
Pulse Output Frequency: 1 kHz
Over-voltage Protection: 45 VDC
Over-current Protection: 2.6 A (4 channels @ 650 mA)
Over-temperature Shutdown: 175°C (min.)
Current Rating: 200 mA per channel
Isolation: 3K VDC or 2K Vrms

Power Requirements
Power Consumption: 178 mA @ 24 VDC

MTBF (mean time between failure)
Time: 204,391 hrs
Database: Telcordia (Bellcore)

ioLogik E2260 Specifications

Inputs and Outputs
RTD Inputs: 6 channels
Digital Outputs: 4 channels
Isolation: 3K VDC or 2K Vrms

RTD Inputs
Input Type: PT50, PT100, PT200, PT500, PT1000; JPT100, JPT200, JPT500, JPT1000; NI100, NI120, NI200, NI500, NI1000; Resistance of 310, 620, 1250, and 2200 ohms
Sampling Rate: 12 samples/sec (all channels)
Resolution: 0.1°C or 0.1 ohm
Accuracy:
±0.1% FSR @ 25°C
±0.3% FSR @ -10 and 60°C
±0.5% FSR @ -40 and 75°C
Input Impedance: 625K ohms

Digital Output
Type: Sink
I/O Mode: DO or Pulse Output
Pulse Output Frequency: 100 Hz
Over-voltage Protection: 45 VDC
Over-current Protection: 2.6 A (4 channels @ 650 mA)
Over-temperature Shutdown: 175°C
Current Rating: 200 mA per channel

Power Requirements
Power Consumption: 95 mA @ 24 VDC

MTBF (mean time between failure)
Time: 327,282 hrs
Database: Telcordia (Bellcore)

ioLogik E2262 Specifications

Inputs and Outputs
Thermocouple Inputs: 8 channels
Digital Outputs: 4 channels

Thermocouple Input
Sensor Type: J (0 to 750°C), K (-200 to 1250°C), T (-200 to 350°C), E (-200 to 900°C), R (-50 to 1600°C), S (-50 to 1760°C), B (600 to 1700°C), N (-200 to 1300°C)
Millivolt Type:
• Mode: ±78.126 mV, ±39.062 mV, ±19.532 mV
• Fault and over-voltage protection: -35 to +35 VDC (power off); -25 to +30 VDC (power on)
Sampling Rate: 12 samples/sec (all channels)
Resolution: 16 bits
Accuracy:
±0.1% FSR @ 25°C
±0.3% FSR @ -10 and 60°C
±0.5% FSR @ -40 and 75°C
Input Impedance: 1 M ohms

Digital Output
Type: Sink
I/O Mode: DO or Pulse Output
Pulse Output Frequency: 100 Hz
Over-voltage Protection: 45 VDC
Over-current Protection: 2.6 A (4 channels @ 650 mA)
Over-temperature Shutdown: 175°C
Current Rating: 200 mA per channel
Isolation: 3K VDC or 2K Vrms

Power Requirements
Power Consumption: 160 mA @ 24 VDC

MTBF (mean time between failure)
Time: 341,063 hrs
Database: Telcordia (Bellcore)

Common Specifications

LAN
Ethernet: 1 x 10/100 Mbps, RJ45
Protection: 1.5 kV magnetic isolation
Protocols: Modbus/TCP, TCP/IP, UDP, DHCP, Bootp, SNMP, HTTP, CGI, SNTP, SMTP

Serial Communication
Interface: RS-485-2w: Data+, Data-, GND (3-contact terminal block)
Serial Line Protection: 15 kV ESD for all signals

Serial Communication Parameters
Parity: None
Data Bits: 8
Stop Bits: 1
Flow Control: None
Baudrate: 1200 to 115200 bps
Protocol: Modbus/RTU

Power Requirements
Power Input: 24 VDC nominal, 12 to 36 VDC

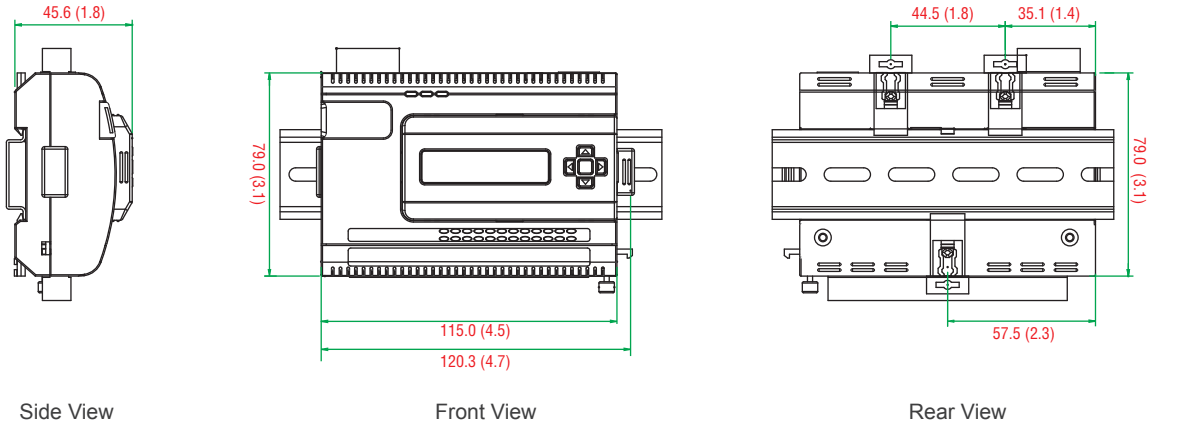
Physical Characteristics
Wiring: I/O cable max. 14 AWG
Dimensions: 115 x 79 x 45.6 mm (4.53 x 3.11 x 1.80 in)
Weight: under 250 g
Mounting: DIN-rail or wall

Environmental Limits
Operating Temperature:
• Standard Models: -10 to 60°C (14 to 140°F)
• Wide Temp. Models: -40 to 75°C (-40 to 167°F)
Storage Temperature: -40 to 85°C (-40 to 185°F)
Ambient Relative Humidity: 5 to 95% (non-condensing)
Altitude: Up to 2000 m
Note: Please contact Moxa if you require products guaranteed to function properly at higher altitudes.

Standards and Certifications
Safety: UL 508
EMI:
EN 61000-3-2; EN 61000-3-3; EN 61000-6-4;
FCC Part 15, Subpart B, Class A
EMS:
EN 61000-4-2, EN 61000-4-3, EN 61000-4-4,
EN 61000-4-5, EN 61000-4-6, EN 61000-4-8,
EN 61000-4-11, EN 61000-6-2
Shock: IEC 60068-2-27
Freefall: IEC 60068-2-32
Vibration: IEC 60068-2-6
Green Product: RoHS, CRoHS, WEEE
Note: Please check Moxa's website for the most up-to-date certification status.

Warranty
Warranty Period: 5 years (excluding ioLogik E2214*)
*Because of the limited lifetime of power relays, products that use that component are covered by a 2-year warranty.
Details: See www.moxa.com/warranty

Dimensions
Unit: mm (inch)



Side View | Front View | Rear View

Ordering Information

Available Models
ioLogik E2210: Ethernet micro RTU controller with 12 DIs, 8 DOs, -10 to 60°C operating temperature
ioLogik E2212: Ethernet micro RTU controller with 8 DIs, 8 DOs, 4 DIOs, -10 to 60°C operating temperature
ioLogik E2214: Ethernet micro RTU controller with 6 DIs, 6 relays, -10 to 60°C operating temperature
ioLogik E2240: Ethernet micro RTU controller with 8 AIs, 2 AOs, -10 to 60°C operating temperature
ioLogik E2242: Ethernet micro RTU controller with 4 AIs, 12 DIOs, -10 to 60°C operating temperature
ioLogik E2260: Ethernet micro RTU controller with 6 RTDs, 4 DOs, -10 to 60°C operating temperature
ioLogik E2262: Ethernet micro RTU controller with 8 TCs and 4 DOs, -10 to 60°C operating temperature
ioLogik E2210-T: Ethernet micro RTU controller with 12 DIs, 8 DOs, -40 to 75°C operating temperature
ioLogik E2212-T: Ethernet micro RTU controller with 8 DIs, 8 DOs, 4 DIOs, -40 to 75°C operating temperature
ioLogik E2214-T: Ethernet micro RTU controller with 6 DIs, 6 relays, -40 to 75°C operating temperature
ioLogik E2240-T: Ethernet micro RTU controller with 8 AIs, 2 AOs, -40 to 75°C operating temperature
ioLogik E2242-T: Ethernet micro RTU controller with 4 AIs, 12 DIOs, -40 to 75°C operating temperature
ioLogik E2260-T: Ethernet micro RTU controller with 6 RTDs, 4 DOs, -40 to 75°C operating temperature
ioLogik E2262-T: Ethernet micro RTU controller with 8 TCs and 4 DOs, -40 to 75°C operating temperature

Optional Accessories (can be purchased separately)
LDP1602: LCD module with 16 x 2 text and 5 buttons

Package Checklist
- ioLogik E2200 series device
- Documentation and software CD

This Page Left Intentionally Blank

ioLogik E2210 User's Manual

Second Edition, August 2006

www.moxa.com/product

MOXA Technologies Co., Ltd.
Tel: +886-2-8919-1230
Fax: +886-2-8919-1231
Web: www.moxa.com

MOXA Technical Support
Worldwide: support@moxa.com.tw
The Americas support@moxa.com

ioLogik E2210 User's Manual

Copyright Notice

Trademarks

Disclaimer

Information in this document is subject to change without notice, and does not represent a commitment on the part of MOXA.

MOXA provides this document "as is," without warranty of any kind, either expressed or implied, including, but not limited to, its particular purpose. MOXA reserves the right to make improvements, and/or changes to this manual, or to the products, and/or the programs described in this manual, at any time.

Information provided in this manual is intended to be accurate, and reliable. However, MOXA assumes no responsibility for its use, or for any infringements on the rights of third parties that may result from its use.

This manual might include unintentional technical or typographical errors. Changes are made periodically to the information herein to correct such errors, and these changes are incorporated into new editions of the manual.

Table of Contents

1

Introduction

The ioLogik E2210 is a stand-alone Active Remote I/O Server that can connect sensors and on/off switches for automation applications over Ethernet and IP-based networks.

The following topics are covered in this chapter:

- **Overview**
  - Traditional Remote I/O
  - Active Remote I/O
  - Click&Go
  - Optional Liquid Crystal Display Module (LCM)
- **Product Features**
- **Packing List**
- **Product Specifications**
- **Physical Dimensions**
- **Hardware Reference**
  - Panel Guide
  - LED Indicators

Overview

(shown with and without optional LCM)

The ioLogik E2210 is part of the E2000 series of ioLogik Active Remote I/O servers, which are designed for intelligent, pro-active status reporting of attached sensors, transmitters, transducers, and valves over a network. As an Easy View device, the ioLogik E2210 supports an optional hot-pluggable Liquid Crystal Display Module (LCM), as shown above, to view and configure device settings.

Traditional Remote I/O

Ethernet remote I/O solutions have been on the market for a long time. Traditional solutions are "passive," in the sense that I/O servers wait passively to be polled by a host computer. The response time in this type of setup, however, tends to be on the order of seconds. The "passive" remote I/O structure is simply inadequate for Data Acquisition and Control (DAC) systems that require an efficient, real-time I/O solution with a response time on the order of hundredths of seconds.

Active Remote I/O

Moxa's **Active Remote I/O** line was developed specifically to address the limitations of the traditional passive approach. Rather than having the host computer poll the I/O device server over the network for the status of each I/O device, the **Active Remote I/O server** intelligently sends the host computer status information only under specified conditions. This is a **report by exception** approach, which greatly reduces the load on CPU and network resources. Network packets are far fewer in number and far smaller in size, since I/O information is only sent when necessary, and only information from the specified I/O device is sent. Based on field tests of an ioLogik E2000 series server used in an RFID system, 50 ms is the typical response time over a 100 Mbps Ethernet network. Moxa's active I/O messaging system uses TCP or UDP for I/O messaging and supports sending messages to up to ten host computers simultaneously.

In addition to providing intelligent status reporting, Active Remote I/O servers are backwards compatible, with all of the functions and capabilities of traditional passive remote I/O servers.

Click&Go

Moxa developed the Click&Go logic control interface for easy configuration and deployment of Active Remote I/O. Click&Go's intuitive, graphical interface lets administrators use simple IF/THEN statements as rules to determine how the Active Remote I/O server responds to different I/O conditions. For example, the Active Remote I/O server could be programmed to turn on an attached switch as well as send an e-mail or SNMP trap when an attached event counter reaches a certain value. Click&Go makes it easy to define a set of these rules, which will become the basis for your Active Remote I/O system.

Optional Liquid Crystal Display Module (LCM)

As a Moxa Easy View product, the ioLogik E2210 supports an optional hot-pluggable Liquid Crystal Display Module (LCM) for field management and configuration. The LCM can display network and I/O settings such as digital input mode and value. The ioLogik E2210's IP address and netmask may also be configured using the LCM, and one LCM can be used to maintain and configure all your Easy View devices.

Product Features

- Click&Go logic builder for easy configuration of your Active Remote I/O system
- High-speed active I/O messaging
- 12-channels of 24 Vdc digital input (DI) with DI/Event Counter mode and software selectable filtering time
- 8-channels of 24 Vdc digital output (DO) with Pulse Output mode and software selectable pulse width
- 10/100 Mbps Ethernet with Modbus/TCP protocol connecting up 10 hosts
- Bundled Windows utility and quick programming library for VB, VC++, BCB (coming soon)
- Support for SCADA software such as Wonderware InTouch and GE Intellution iFix32
- SNMP for system management and I/O status
- Remote management over the network including firmware updates
- Configurable DO power-on and safe status settings
- Optional hot-pluggable LCM for status display and configuration

Packing List

The ioLogik E2210 is shipped with the following items:

Standard Accessories

- ioLogik E2210 Active Remote I/O Server
- Document & Software CD

Optional Accessories

- LDP1602 ioLogik Liquid Crystal Display Module (LCM)

NOTE: Notify your sales representative if any of the above items are missing or damaged.

Product Specifications

LAN

Ethernet	10/100 Mbps, RJ45
Protection	1.5 KV magnetic isolation
Protocols	Modbus/TCP, TCP/IP, UDP, DHCP, Bootp, SNMP(MIB for I/O and Network), HTTP, Active I/O Messaging, IP filtering

Serial (reserved)

Interface	RS-485 (2-wire): Data+, Data-, GND
Serial line protection	15 KV ESD for all signals

Serial Communication Parameters (reserved)

Parity	None
Data bits	8
Stop bits	1
Flow control	None
Speed	1200 to 115200 bps
Protocol	Modbus/RTU
Built-in RTC	Yes

Digital Input

Inputs	12, source type
I/O Mode	DI or Event Counter (input frequency: 100 Hz)
Dry Contact	Logic 0: short to GND, Logic 1: open
Wet Contact	Logic 0: 0 to 3 VDC, Logic 1: 10 to 30 VDC (DI COM to DI)
Common type	12 points / 1 COM
Isolation	2 KV rms

Digital Output

Outputs	8, sink type
On-state voltage	24 VDC nominal
Output current rating:	Max. 200 mA per channel
Optical isolation	3K VDC
Protection	Over temperature shutdown: 170°C Over current limit: 750 mA/channel (typical)

Power Requirements

Power input	24 VDC nominal, 12 to 48 VDC
Power consumption	282 mA @ 24 VDC (typical)
Field power	24 VDC nominal, up to 48 VDC

Mechanical Specifications

Wiring	I/O cable max. 14 AWG

Environmental

Operating temperature	-10 to 60ºC (14 to 140ºF), 5 to 95%RH
Storage temperature	-40 to 85ºC (-4 to 185ºF), 5 to 95%RH
Shock	IEC60068-2-27
Freefall	IEC60068-2-32
Vibration	IEC60068-2-6

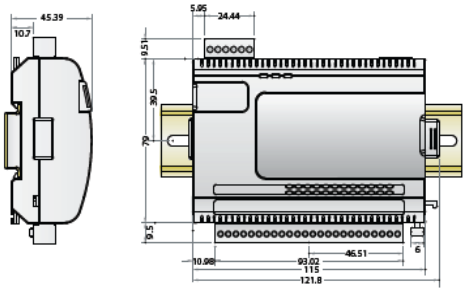
Agency Approvals

EMI	FCC Part 15, CISPR (EN55022) Class A
EMS	IEC61000-4-2 (ESD), level 2/3,

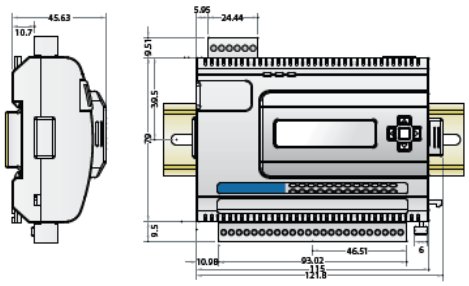
	IEC61000-4-3 (RS), level 2, IEC61000-4-4 (EFT), level 2, IEC61000-4-5 (Surge), level 3, IEC61000-4-6 (CS), level 2, IEC61000-4-8 (PM), level 1, IEC61000-4-11 (Dip)
Safety	UL 508 (pending)
Warranty	2 years

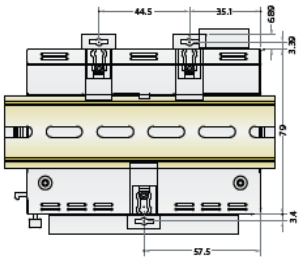
Physical Dimensions

Without LCD Display Module (unit: mm)



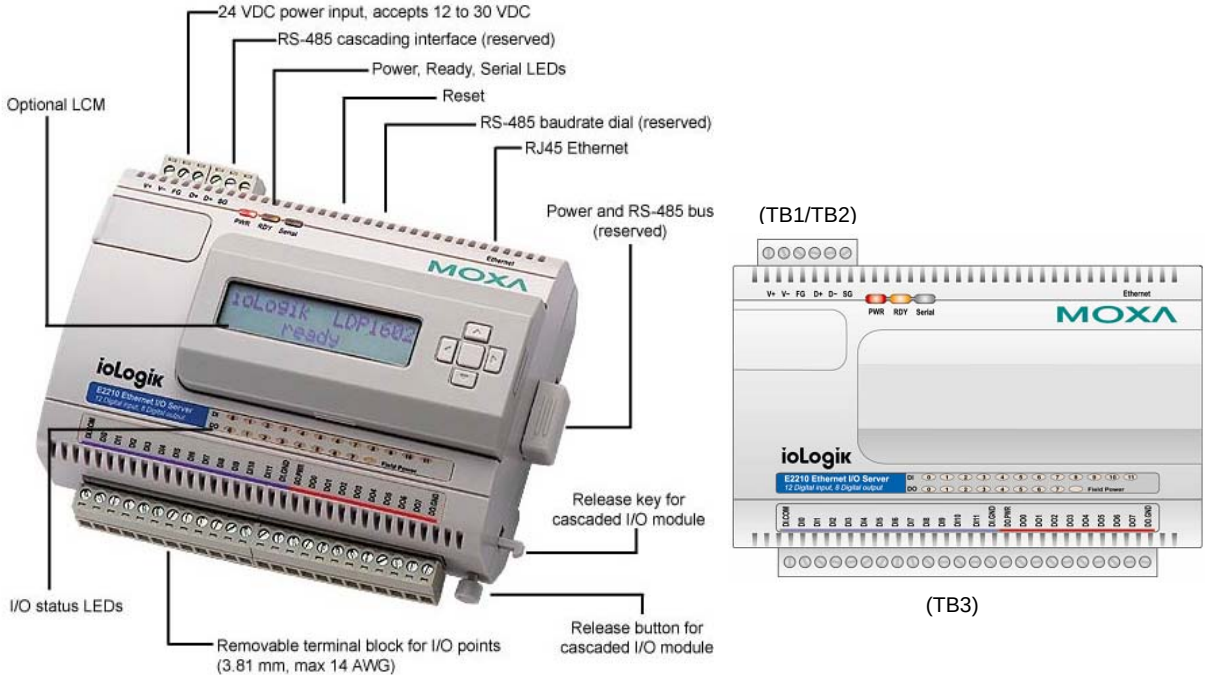
With LCD Display Module (unit: mm)





Hardware Reference

Panel Guide



NOTE – The reset button restarts the server and resets all settings to factory defaults. Use a pointed object such as a straightened paper clip to hold the reset button down for 5 sec. The RDY LED will turn red as you are holding the reset button down. The factory defaults will be loaded once the RDY LED turns green again. You may then release the reset button.

LED Indicators

Ethernet		
Ethernet	orange	Connected to a 10 Mbps Ethernet connection.
	green	Connected to a 100 Mbps Ethernet connection.
	(flashing)	Transmitting or receiving data
System		
PWR	red	Power is on
	off	Power is off
RDY	red	System error
	green (steady)	ioLogik E2210 is functioning normally
	green (flashing)	Click&Go ruleset is active
	green & red (flashing)	ioLogik E2210 is in Safe Status
	off	Power is off or there is a power problem.
Serial	(flashing)	Serial port is receiving/transmitting data
I/O		
DI x12 pins DO x8 pins Field PWR	green	ON status
	off	OFF status

2

Initial Setup

This chapter describes how to install the ioLogik E2210.

The following topics are covered:

- **Hardware Installation**
  - Connecting the Power
  - Grounding the ioLogik E2210
  - Connecting to the Network
  - Setting the RS-485 Baudrate
- **Software Installation**

Hardware Installation

Connecting the Power

Connect the 12 to 48 VDC power line to the ioLogik E2210's terminal block (TB1). If power is properly supplied, the Power LED will glow a solid red color until the system is ready

ATTENTION

Disconnect the power before installing and wiring
Disconnect the power cord before installing and/or wiring your ioLogik E2210.

Do not exceed the maximum current for the wiring
Determine the maximum possible current for each power wire and common wire. Observe all electrical codes dictating the maximum current allowable for each wire size.
If the current exceeds the maximum rating, the wiring could overheat, causing serious damage to your equipment.

Grounding the ioLogik E2210

The ioLogik E2210 is equipped with two grounding points, one on the wall mount hole and the other on the DIN-rail mount.

Connecting to the Network

1. Connect the ioLogik E2210 to the host PC with an Ethernet cable. For initial setup of the ioLogik E2210, it is recommended that the ioLogik E2210 be configured using a direct connection to a host computer rather than remotely over the network.
2. Configure the host PC's IP address to 192.168.127.*xxx*. (*xxx*: from 001 to 253). In Windows, you will need to do this through the Control Panel.

ioLogik E2210 Default IP Address	Default Netmask	Default Gateway
192.168.127.254	255.255.255.0	None

3. Use ioAdmin or the web console to detect the ioLogik E2210. Once the ioLogik E2210 has been detected, modify the settings as needed for your network environment, then restart the server.

Setting the RS-485 Baudrate

The RS-485 port on the ioLogik E2210 is reserved to chain another RS-485 I/O server. The RS-485 port can run Modbus/RTU or I/O command sets. The baudrate is set by a physical dial on the back of the ioLogik R2210. The default settings are baudrate = 115200, parity check = N, data bits = 8, and stop bit = 1.

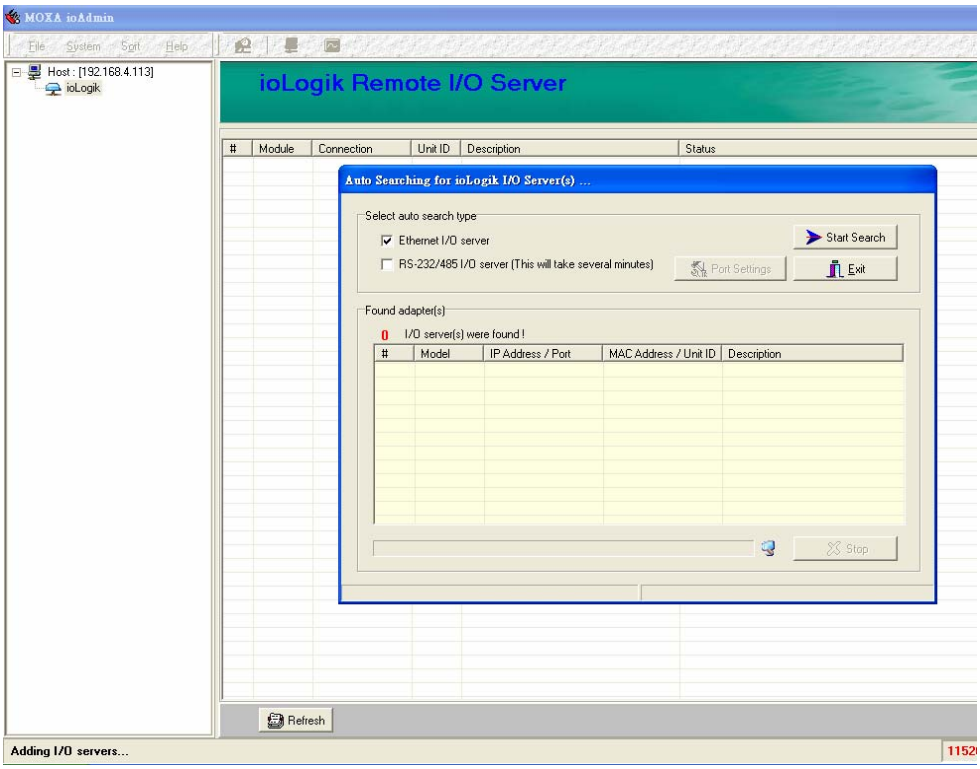
Baudrate for RS-485 (parameters are N, 8, 1)	Dial setting and corresponding baudrate:			
	0:115200	1:57600	2:38400	3:19200
	4:9600	5:4800	6:2400	7:1200

For RS-485 cascading interface, the RS-485 Unit ID = 1.

Software Installation

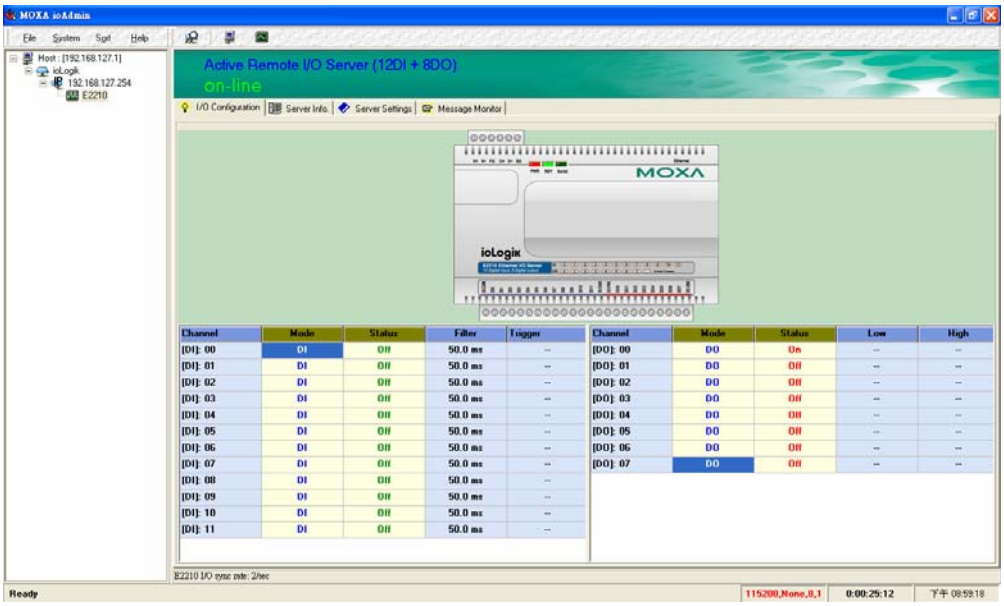
ioAdmin is a Windows utility provided for the configuration and management of the ioLogik E2210 and attached I/O devices. It may be used from anywhere on the network to monitor and configure the ioLogik E2210. You may also configure some of the settings through the web console or optional LCM.

1. **Installation from CD-ROM**: Insert the Software CD into the host computer. Run SETUP.EXE, which is located in the root directory. The installation program will guide you through the installation process and install the ioAdmin utility along with the MXIO DLL library.
2. **Open ioAdmin**: After installation is finished, run **ioAdmin** from **Start → Program Files → ioLogik → Utility → ioAdmin**.
3. **Search the network for the server**: On the menu bar, select **System → Auto Scan Remote I/O Server**. A dialog window will pop up. Click **Start Search** to begin searching for the ioLogik2000.



If ioAdmin is unable to find the ioLogik E2210, there may be a problem with your network settings.

4. **Monitoring I/O status**: Once the ioLogik E2210 is found by ioAdmin, you may view the status of all I/O devices on ioAdmin's main screen.



You may now use ioAdmin to setup or configure your the ioLogik E2210.

3

Using ioAdmin

This chapter goes over the functions available in ioAdmin, the ioLogik E2210's main configuration and management utility.

The following topics are covered:

- **Introduction to ioAdmin**
- **Features of ioAdmin**
- **ioAdmin Main Screen**
  - Main Screen Overview
  - Wiring Guide
  - I/O Configuration Tab (General)
  - Server Info Tab
  - Server Settings Tab (General)
  - Message Monitor Tab
- **ioAdmin Administrator Functions**
  - I/O Configuration Tab (Administrator)
  - Server Settings Tab (Administrator)
  - Network Tab
  - Firmware Update Tab
  - Watchdog Tab
  - Click&Go Logic Tab
  - Server Context Menu

Introduction to ioAdmin

All ioLogik remote I/O Servers may be managed and configured over the Ethernet by ioAdmin, a Windows 2000/XP utility provided with your ioLogik E2210. ioAdmin's graphical-user interface gives you easy access to all status information and settings.

The ioLogik E2210 also supports configuration by web console and by optional LCM, but full configuration and management is only available through ioAdmin.

ioAdmin also includes Click&Go logic control for the configuration of your Active Remote I/O system.

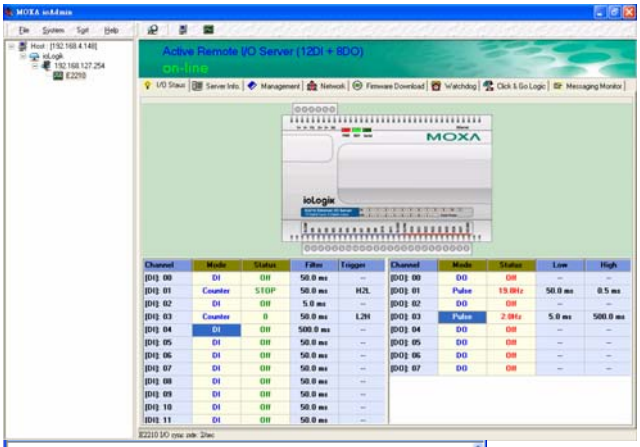
ioAdmin consists of following software:

- **ioAdmin with Click&Go Logic**
- **ioLogik 2000 Wiring Guide**
- **MXIO DLL library** (coming soon)

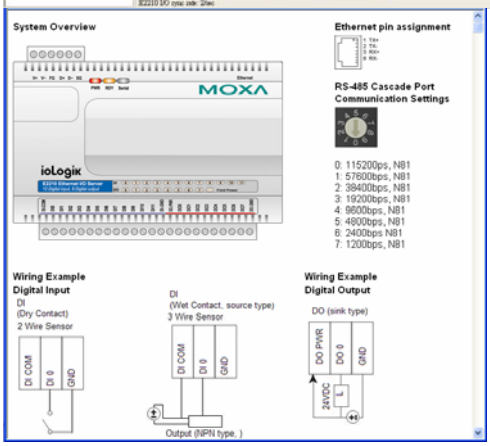
Features of ioAdmin

Remote Management
Over the Ethernet network, ioAdmin allows users to

- find and configure multiple ioLogik servers.
- monitor and configure attached I/O devices.
- test I/O devices.
- reset the server.

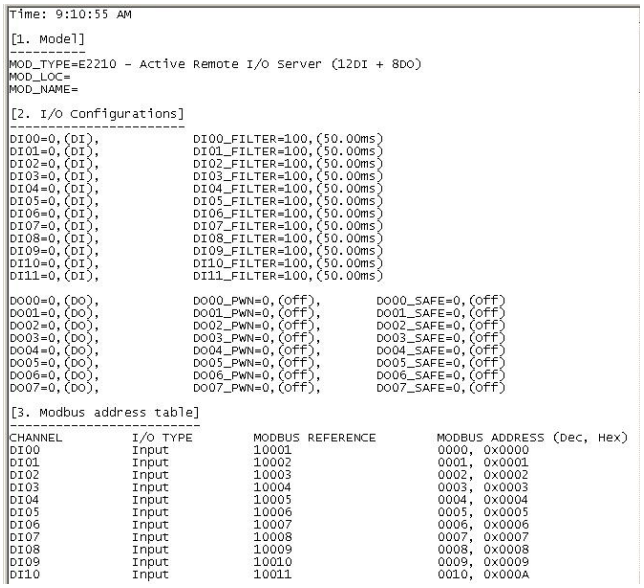


On-line Wiring Guide
An on-line wiring guide can be opened from within ioAdmin for your convenience. The easily accessible wiring guide can save administrators much time while planning or troubleshooting.



Configuration File
ioAdmin allows the entire configuration of the ioLogik E2210 to be saved as a file. The file is viewable as text and can serve three purposes:

- as a record or backup of configuration
- as a template for the configuration of other servers
- as a quick reference guide for you to configure Modbus drivers in a SCADA system

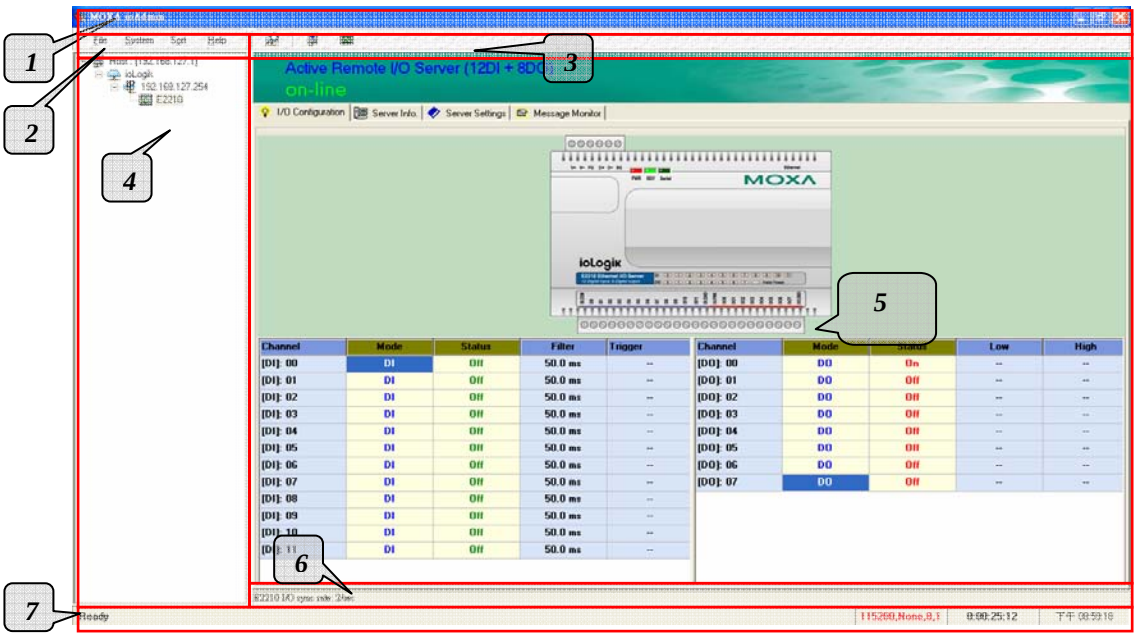


```
Time: 9:10:55 AM

[1. Model]
----------
MOD_TYPE=E2210 - Active Remote I/O Server (12DI + 8DO)
MOD_LOC=
MOD_NAME=

[2. I/O Configurations]
-----------------------
DI00=0,(DI),            DI00_FILTER=100,(50.00ms)
DI01=0,(DI),            DI01_FILTER=100,(50.00ms)
DI02=0,(DI),            DI02_FILTER=100,(50.00ms)
DI03=0,(DI),            DI03_FILTER=100,(50.00ms)
DI04=0,(DI),            DI04_FILTER=100,(50.00ms)
DI05=0,(DI),            DI05_FILTER=100,(50.00ms)
DI06=0,(DI),            DI06_FILTER=100,(50.00ms)
DI07=0,(DI),            DI07_FILTER=100,(50.00ms)
DI08=0,(DI),            DI08_FILTER=100,(50.00ms)
DI09=0,(DI),            DI09_FILTER=100,(50.00ms)
DI10=0,(DI),            DI10_FILTER=100,(50.00ms)
DI11=0,(DI),            DI11_FILTER=100,(50.00ms)

DO00=0,(DO),            DO00_PWN=0,(Off),       DO00_SAFE=0,(Off)
DO01=0,(DO),            DO01_PWN=0,(Off),       DO01_SAFE=0,(Off)
DO02=0,(DO),            DO02_PWN=0,(Off),       DO02_SAFE=0,(Off)
DO03=0,(DO),            DO03_PWN=0,(Off),       DO03_SAFE=0,(Off)
DO04=0,(DO),            DO04_PWN=0,(Off),       DO04_SAFE=0,(Off)
DO05=0,(DO),            DO05_PWN=0,(Off),       DO05_SAFE=0,(Off)
DO06=0,(DO),            DO06_PWN=0,(Off),       DO06_SAFE=0,(Off)
DO07=0,(DO),            DO07_PWN=0,(Off),       DO07_SAFE=0,(Off)

[3. Modbus address table]
-------------------------
CHANNEL         I/O TYPE        MODBUS REFERENCE        MODBUS ADDRESS (Dec, Hex)
DI00            Input           10001                   0000, 0x0000
DI01            Input           10002                   0001, 0x0001
DI02            Input           10003                   0002, 0x0002
DI03            Input           10004                   0003, 0x0003
DI04            Input           10005                   0004, 0x0004
DI05            Input           10006                   0005, 0x0005
DI06            Input           10007                   0006, 0x0006
DI07            Input           10008                   0007, 0x0007
DI08            Input           10009                   0008, 0x0008
DI09            Input           10010                   0009, 0x0009
DI10            Input           10011                   0010, 0x000A
```

ioAdmin Main Screen

Main Screen Overview

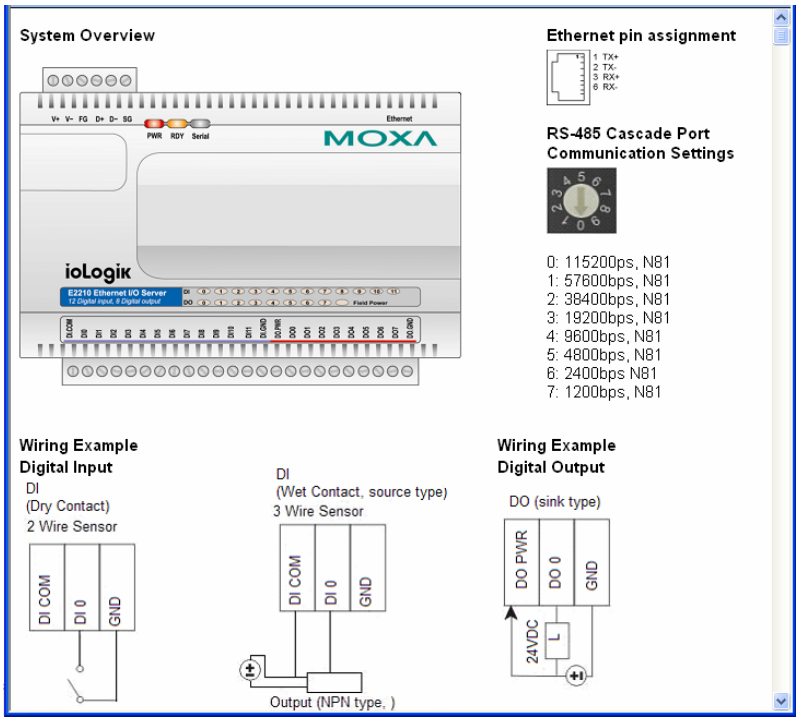
This is ioAdmin's main screen. The main window defaults to the I/O Configuration tab, which displays a figure of the ioLogik E2210 and the status of every I/O channel below it. The other tabs in the main window take you to server and network settings, and further functions are available when you log on as an administrator. Note that configuration options are not available until you log on as an administrator.



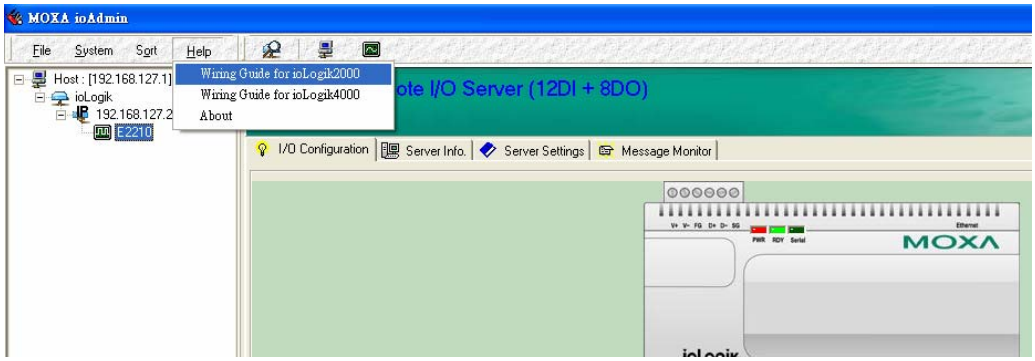
ioAdmin Main Screen	
1.	Title
2.	Menu bar
3.	Quick link
4.	Navigation panel
5.	Main window
6.	Sync. rate status
7.	Status bar

Wiring Guide

ioAdmin provides a wiring guide to the ioLogik E2210. You may access the wiring guide by right-clicking the figure of the ioLogik E2210 in the I/O Configuration tab. Select "Wiring Guide" in the submenu to open a help file showing the wiring information and electrical characteristics of the ioLogik E2210.

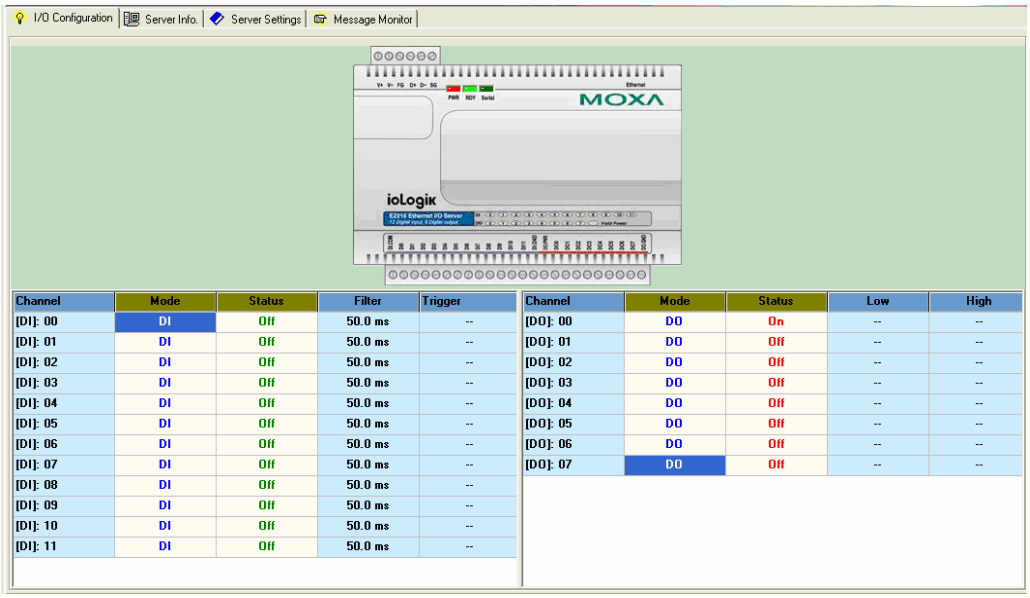


You may also access the On-line Wiring Guide through the Help menu on the menu bar.



I/O Configuration Tab (General)

The I/O Configuration tab shows the status of every I/O channel underneath the ioLogik E2210 figure. This is the default tab when you first open ioAdmin.

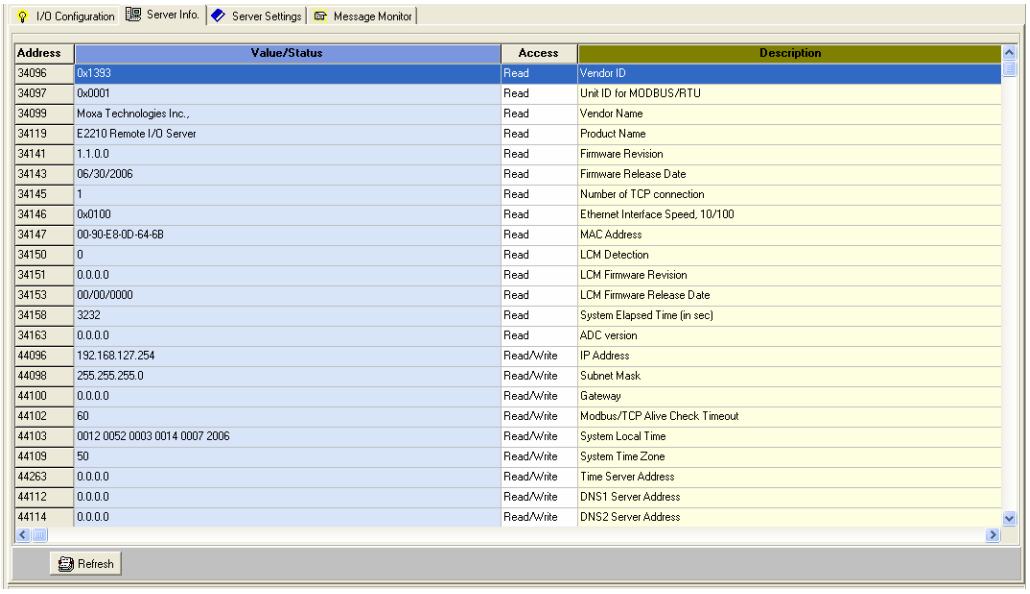


Channel	Mode	Status	Filter	Trigger
[DI]: 00	DI	Off	50.0 ms	--
[DI]: 01	DI	Off	50.0 ms	--
[DI]: 02	DI	Off	50.0 ms	--
[DI]: 03	DI	Off	50.0 ms	--
[DI]: 04	DI	Off	50.0 ms	--
[DI]: 05	DI	Off	50.0 ms	--
[DI]: 06	DI	Off	50.0 ms	--
[DI]: 07	DI	Off	50.0 ms	--
[DI]: 08	DI	Off	50.0 ms	--
[DI]: 09	DI	Off	50.0 ms	--
[DI]: 10	DI	Off	50.0 ms	--
[DI]: 11	DI	Off	50.0 ms	--

Channel	Mode	Status	Low	High
[DO]: 00	DO	On	--	--
[DO]: 01	DO	Off	--	--
[DO]: 02	DO	Off	--	--
[DO]: 03	DO	Off	--	--
[DO]: 04	DO	Off	--	--
[DO]: 05	DO	Off	--	--
[DO]: 06	DO	Off	--	--
[DO]: 07	DO	Off	--	--

Server Info Tab

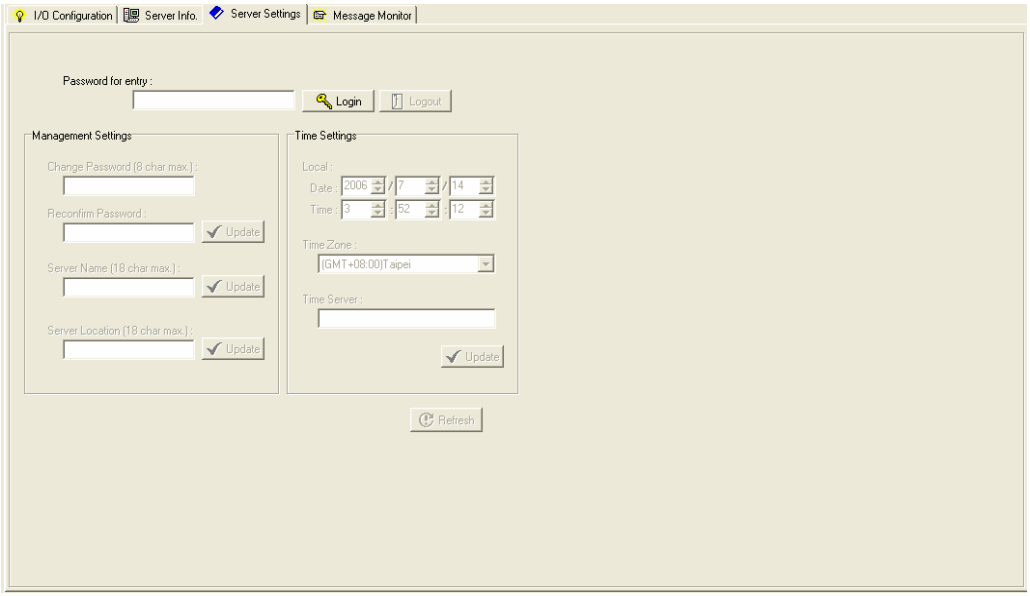
Server information, such as firmware version, is displayed in the Server Info tab.



Address	Value/Status	Access	Description
34096	0x1393	Read	Vendor ID
34097	0x0001	Read	Unit ID for MODBUS/RTU
34099	Moxa Technologies Inc.,	Read	Vendor Name
34119	E2210 Remote I/O Server	Read	Product Name
34141	1.1.0.0	Read	Firmware Revision
34143	06/30/2006	Read	Firmware Release Date
34145	1	Read	Number of TCP connection
34146	0x0100	Read	Ethernet Interface Speed, 10/100
34147	00-90-E8-0D-64-6B	Read	MAC Address
34150	0	Read	LCM Detection
34151	0.0.0.0	Read	LCM Firmware Revision
34153	00/00/0000	Read	LCM Firmware Release Date
34158	3232	Read	System Elapsed Time (in sec)
34163	0.0.0.0	Read	ADC version
44096	192.168.127.254	Read/Write	IP Address
44098	255.255.255.0	Read/Write	Subnet Mask
44100	0.0.0.0	Read/Write	Gateway
44102	60	Read/Write	Modbus/TCP Alive Check Timeout
44103	0012 0052 0003 0014 0007 2006	Read/Write	System Local Time
44109	50	Read/Write	System Time Zone
44263	0.0.0.0	Read/Write	Time Server Address
44112	0.0.0.0	Read/Write	DNS1 Server Address
44114	0.0.0.0	Read/Write	DNS2 Server Address

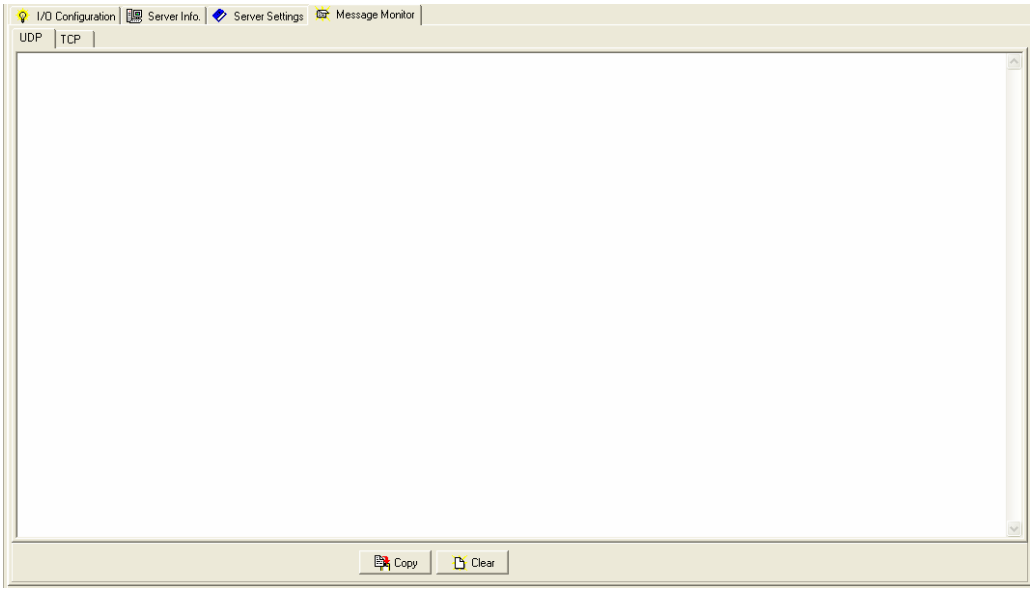
Server Settings Tab (General)

The Server Settings tab is where you log in as an administrator. This is required in order to gain access to the ioLogik E2210 configuration options. If no administrator password has been set up, simply click on **Login** and leave the **Password for entry** field blank. Please refer to the *ioAdmin Administrator Functions* section later on in this chapter for more detail.



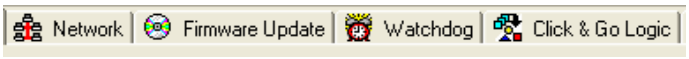
Message Monitor Tab

The Message Monitor tab will display any TCP/UDP I/O messages received from the ioLogik E2210. When you install the ioLogik E2210 for the first time, the active I/O messaging ruleset will not have been defined yet, so there will be no messages in the Message Monitor Tab. Please refer to Chapter 5: *Click&Go Logic* for information on how to program the ioLogik E2210's active I/O messaging system. Once the active I/O messaging system has been configured and activated, TCP/UDP messages sent from the ioLogik E2210 will be viewable in the Message Monitor tab.



ioAdmin Administrator Functions

For full access to all configuration options, log in as an administrator in the Server Settings tab. This is required whenever you start up ioAdmin or boot up/restart the ioLogik E2210. When you install the ioLogik E2210 for the first time, the password will be blank and you may simply click on **Login**. Additional functions will available after logging in, including the following new tabs:



When making configuration changes, you will need to click on **Update** or on **Apply** to save the changes. Some changes will require a restart of the ioLogik E2210 in order to take effect, and you will be given the option to restart the computer if necessary.

ATTENTION

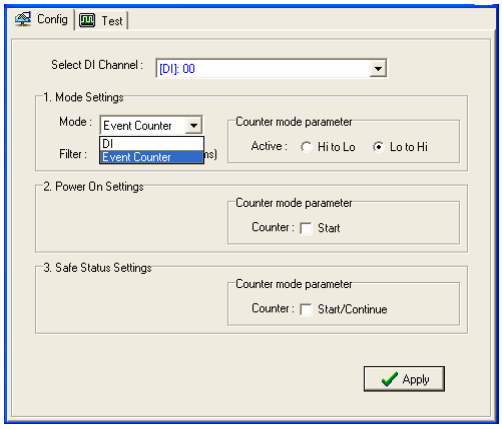
You MUST log in to access any administrator function, including Network, Communication Watchdog Timer, and Firmware Update tabs. If you forget the password, you may hold down the Reset button to clear the password and load factory defaults. **This will result in the loss of all configuration settings and your Click&Go Logic active I/O messaging program!**

I/O Configuration Tab (Administrator)

When logged on as an administrator, you may double click on a channel in the I/O Configuration tab to configure that channel's settings.

Configuring Digital Input Channels

E2210 equipped with 12 DI (digital input) channels that can be separately set to "DI" or "Event Counter Mode." In DI mode, the specification is as follows.



In DI mode, the specifications are as follows:

Type	Logic 0 (OFF)	Logic 1 (ON)
Dry contact	close to GND	open
Wet contact	0-3 V	10-30 V

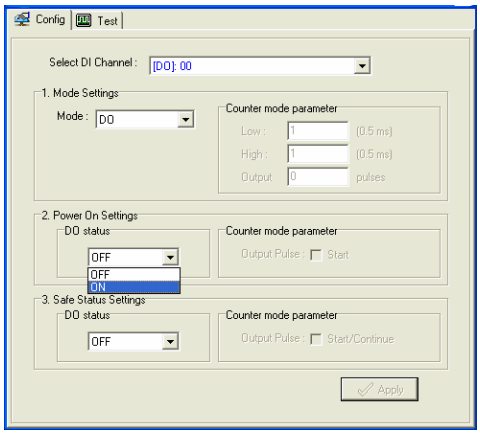
In Event Counter mode, the ioLogik E2210's DI channel accepts limit or proximity switches and counts events according to the ON/OFF status. You may select from two modes, "Lo to Hi" or "Hi to Lo." When "Lo to Hi" is selected, the counter value increases while the switch is pushed. When "Hi to Lo" is selected, the counter value increases when the switch is push and released.

To control switch bounces, the ioLogik E2210 provides software filtering. It is configurable in multiples of 0.5 ms. For example, a setting of **2** would mean a 10 ms filter (2 x 0.5 ms). The maximum value allowed by the software filter is 65535.

NOTE: Setting the filter to "0" causes the system to filter all signals.

Configuring Digital Output Channels

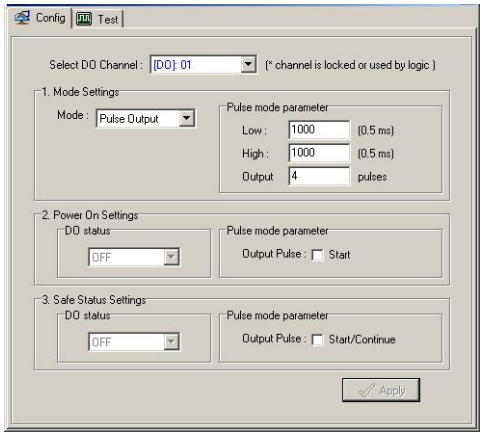
The ioLogik E2210 is equipped with 2 DO (digital output or sink) channels that can be set individually to "DO" or "Pulse Output" mode.



In DO mode, the specification is as follows.

Type	Logic 0 (OFF)	Logic 1 (ON)
DO mode	Open	short

In Pulse Output mode, the selected digital output channel will generate a square wave as specified in the pulse mode parameters. The low and high level widths are entered in multiples of 0.5ms. To set the low level width for 500 ms, you would enter 1000 (because 1000 x 0.5 ms = 500 ms). If the low width is 5000 and the high width is 5000, the pulse output would be a square wave with a 5-second pulse cycle.



Power On Settings

Use this field to set the initial behavior of the DI/O channel when the ioLogik E2210 is powered on. For DI channels in Event Counter mode, you may configure whether or not counting begins at power up. For DO channels in DO mode, you may configure whether or not the DO is set to OFF or ON at power up. For DO channels in Output Pulse mode, you may configure whether or not the pulse output commences at power up.

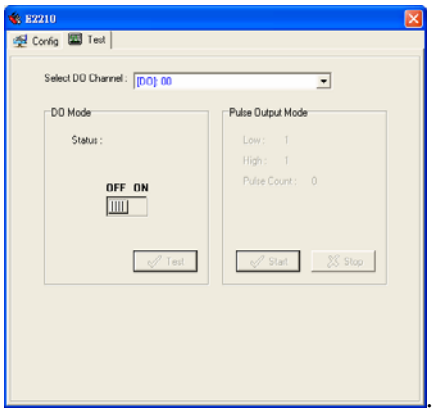
Safe Status Settings

Use this field to specify how the DI/O channel behaves when the network connection is lost. When the network connection is lost for the amount of time specified in the Host Connection Watchdog, the ioLogik E2210 enters Safe Status, and each DI/O channel's Safe Status settings will go into effect. Note that the Host Connection Watchdog is disabled by default. If the Host Connection Watchdog is disabled, the ioLogik E2210 will never enter Safe Status and the Safe Status settings will have no effect.

For DI channels in Event Counter mode, you can configure whether or not counting starts or continues when Safe Status has been activated. For DO channels in DO mode, you can configure whether or not the DO is set to OFF or ON at Safe Status. For DO channels in Output Pulse mode, you can configure whether or not the output pulse commences or continues at Safe Status.

Test I/O

You may test the DI/O channel by using ioAdmin.



DI-DI: depends on the device

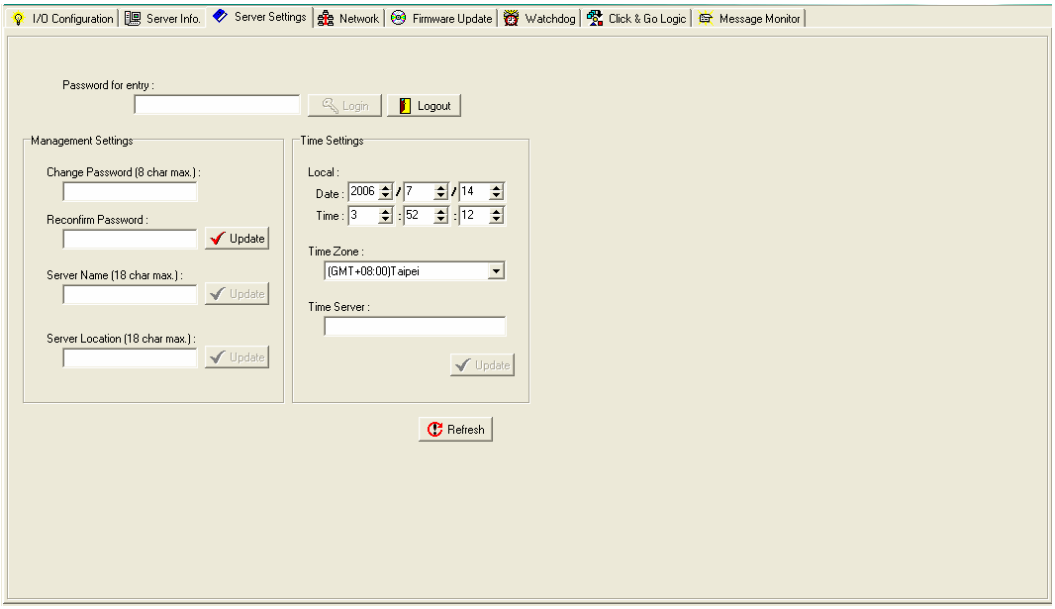
DI-Counter: start or stop the counter

DO-DO: set the DO to "ON" or "OFF"

DO-Pulse: activate or stop pulse generation.

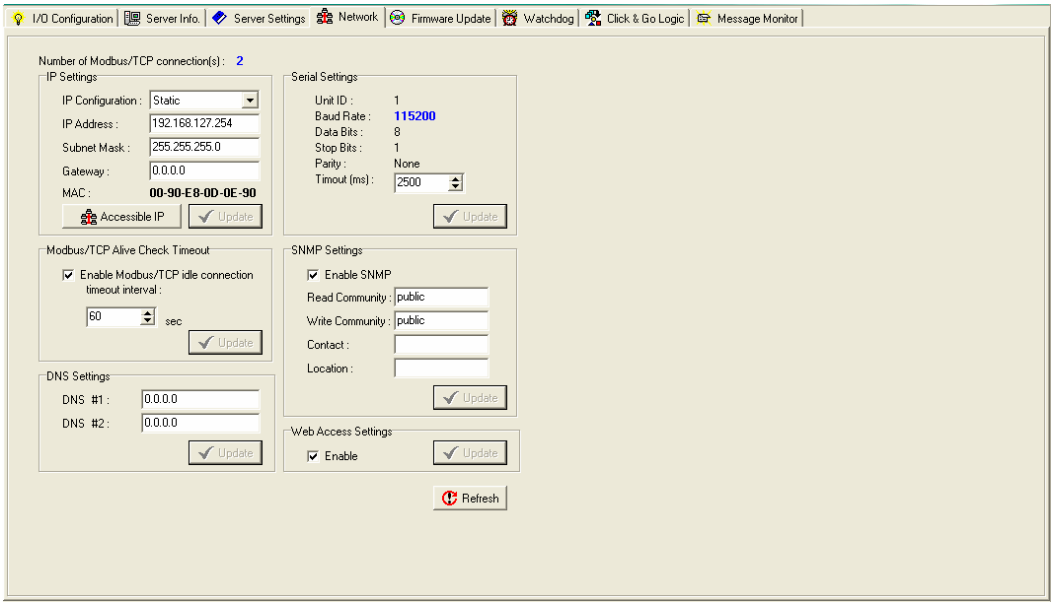
Server Settings Tab (Administrator)

You may set up a password, server name, location, date, time, and area in the Server Settings tab.



Network Tab

The Network tab is where you configure IP settings, Modbus/TCP Alive Check Timeout settings, DNS settings, Serial settings, SNMP settings, and Web Access settings for the ioLogik E2210.



IP Settings: You can set up a static or dynamic IP address for the ioLogik E2210, as well as the subnet mask and gateway address. The **Accessible IP** screen can be used to control network access to the ioLogik E2210 and attached sensors. Network requests that originate from sources that are not listed in the accessible IP list will be unable to use Modbus/TCP or ioAdmin to access the ioLogik E2210.

Modbus/TCP Alive Check Timeout Settings: The Modbus/TCP Alive Check Timeout is designed to avoid TCP connection failure. When the host is down, the ioLogik 2210 will continue to wait for a response from the host. This will cause the TCP port to be indefinitely occupied by the host. When the Modbus/TCP idle connection timeout interval is enabled, the ioLogik E2210 will close the TCP connection automatically if there is no TCP activity for the specified time. Please note that Modbus/TCP connections will be blocked when setting up Accessible IP.

DNS Settings: Use this field to specify up the IP addresses of up to 2 DNS servers. These two DNS servers may be used to automatically find available e-mail addresses when configuring for Active Remote I/O e-mail messaging.

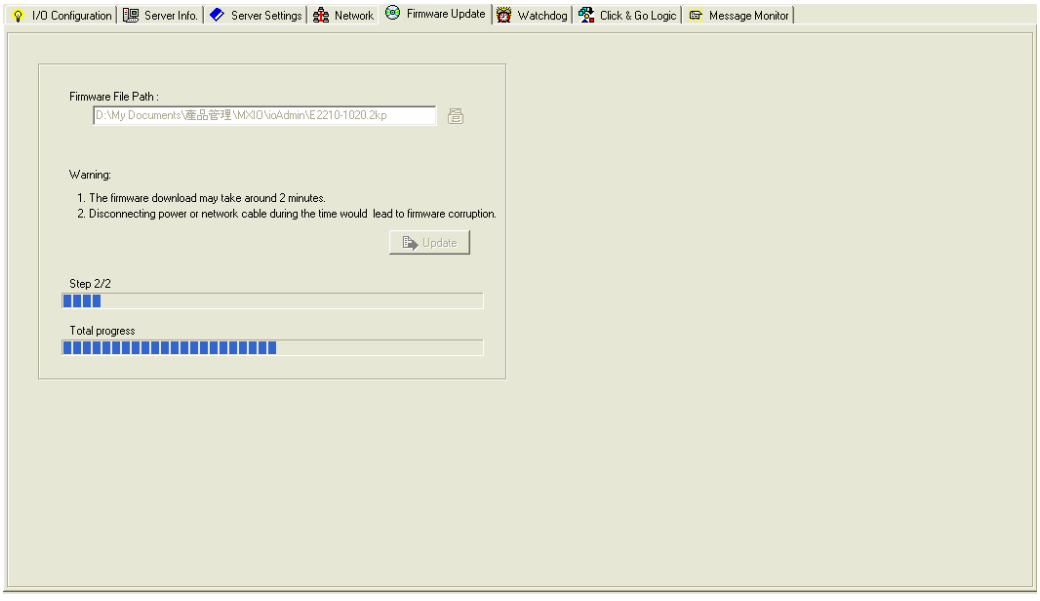
Serial Settings: You may view the reserved RS-485 communication parameters here, and you may set the timeout value for breaks in RS-485 communication. Note that the other serial communication parameters cannot be modified. If you wish to adjust the baudrate, you will need to use the physical dial on the back panel of the ioLogik E2210.

SNMP Settings: The ioLogik E2210 provides SNMP v2 (Simple Network Management Protocol) to allow monitoring of network and I/O devices with SNMP Network Management software. It is useful in building automation and telecom applications. Use these fields to enable SNMP and set the read and write community strings.

Web Access Settings: This field enables and disables the ioLogik E2210's web console. The web console allows the configuration of many settings using a web browser that is directed to the server's IP address. If the web console is not enabled in this field, you will not be able to access the web console.

Firmware Update Tab

The ioLogik E2210 supports remote firmware updates through the Firmware Update tab. Enter the path to the firmware file or click on the icon to browse for the file. Click on **Update** to update the firmware. The wizard will lead you through the process until the server is restarted.



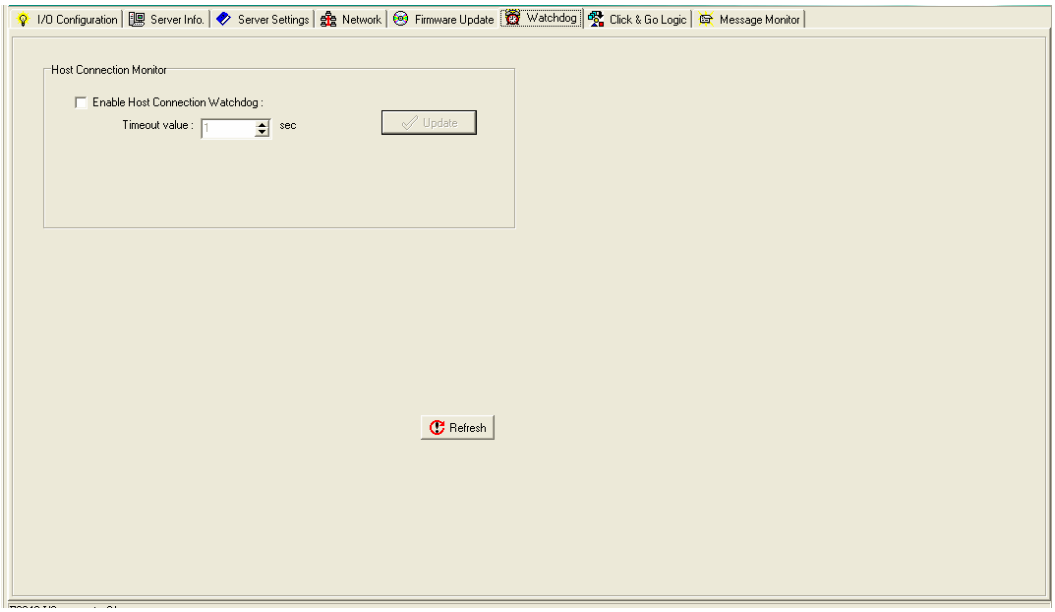
WARNING

Do not interrupt the firmware update process! An interruption in the process may result in your device becoming unrecoverable.

After the firmware is updated, the ioLogik will restart and you will have to log in again to access administrator functions.

Watchdog Tab

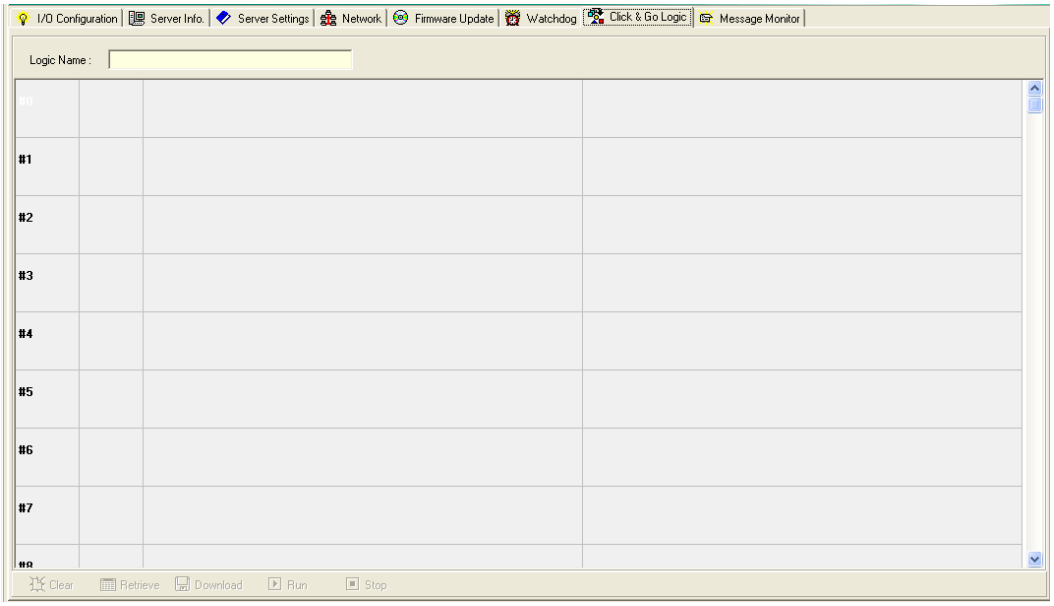
The Watchdog tab is where you configure the Host Connection Watchdog, which is used with the Safe Status settings to define each DI/O channel's response to a lost network connection. When the ioLogik E2210 loses its network connection for the amount of time specified in the timeout, the Host Connection Watchdog will switch the ioLogik E2210 to Safe Status and the DI/O channels will reset to their Safe Status settings. By default, the Watchdog is disabled. To enable the Watchdog, make sure **Enable Host Connection Watchdog** is checked, set the Timeout value, then click the **Update** button.



After the Watchdog is enabled, the ioLogik E2210 will enter safe status if the network connection is lost. Once the connection has been restored, you will need to return to the Watchdog Tab in order to exit safe status. There will be a message saying "Host Connection Lost", indicating that the server is in safe status. Click **Clear Alarm** to exit safe status and return to normal operation.

Click&Go Logic Tab

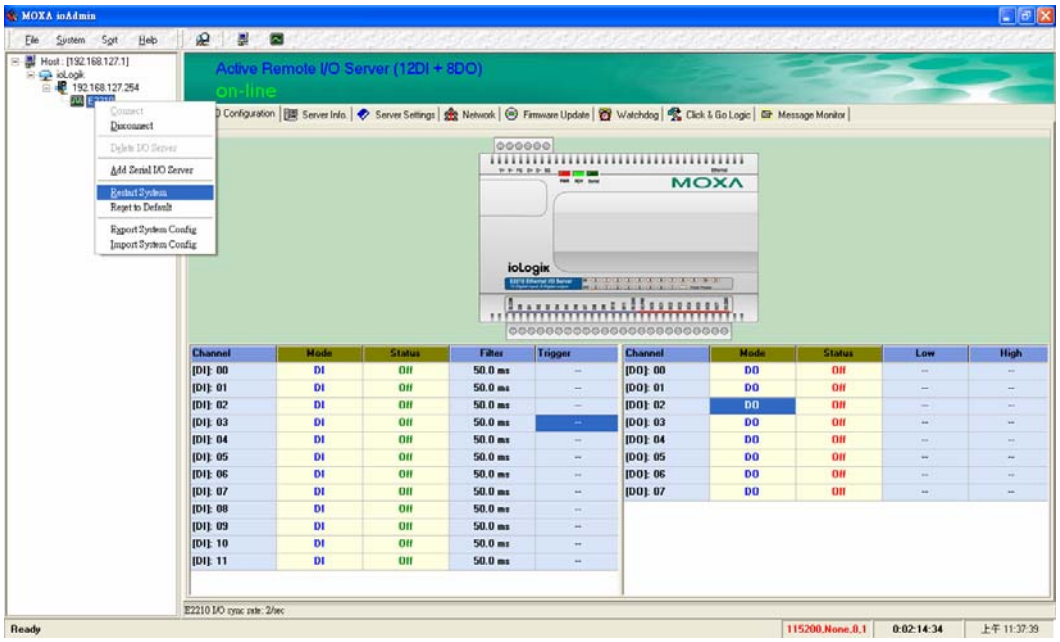
The Click&Go Logic tab is where administrators set up the ioLogik E2210's active I/O messaging program. Instead of the server reacting passively to repeated polling request from a host for I/O data, the ioLogik E2210 is able to actively send I/O information to the host when an I/O channel satisfies conditions that you specify. Click&Go Logic was developed by Moxa to provide a powerful and easy-to-use tool for defining the conditions under which I/O information will be sent over the network. Please refer to Chapter 5: *Click&Go Logic* for more detailed information.



Changes made in the Click&Go Logic tab are not effective until the ioLogik E2210 is restarted, just like changes made in other tabs. Note that when Click&Go Logic is being used, the range and units of I/O channel being used in Click&Go Logic may not be modified.

Server Context Menu

The Server context menu is accessed by right clicking on the server model name in the navigation panel.



Connect

Select this command to have ioAdmin attempt a re-connection over the network to the selected ioLogik server.

Disconnect

Select this command to have ioAdmin drop the network connection with the selected ioLogik server.

Delete I/O Server

Select this command to have ioAdmin remove the selected server.

Add Serial I/O Server

Select this command to manually add a server by using its Unit ID.

Restart System

Select this command to restart your ioLogik E2210 from a remote site

Reset to Default

Select this command to reset all settings, including console password, to factory default values.

Export System Config

Select this command to export the configuration of the ioLogik E2210 to a text file. It is strongly recommended you use this method to back up your configuration after you have finished configuring the ioLogik E2210 for your application.

Below is an example of the exported configuration file

```
Time: 9:10:55 AM

[1. Model]
----------
MOD_TYPE=E2210 - Active Remote I/O Server (12DI + 8DO)
MOD_LOC=
MOD_NAME=

[2. I/O Configurations]
-----------------------
DI00=0,(DI),            DI00_FILTER=100,(50.00ms)
DI01=0,(DI),            DI01_FILTER=100,(50.00ms)
DI02=0,(DI),            DI02_FILTER=100,(50.00ms)
DI03=0,(DI),            DI03_FILTER=100,(50.00ms)
DI04=0,(DI),            DI04_FILTER=100,(50.00ms)
DI05=0,(DI),            DI05_FILTER=100,(50.00ms)
DI06=0,(DI),            DI06_FILTER=100,(50.00ms)
DI07=0,(DI),            DI07_FILTER=100,(50.00ms)
DI08=0,(DI),            DI08_FILTER=100,(50.00ms)
DI09=0,(DI),            DI09_FILTER=100,(50.00ms)
DI10=0,(DI),            DI10_FILTER=100,(50.00ms)
DI11=0,(DI),            DI11_FILTER=100,(50.00ms)

DO00=0,(DO),            DO00_PWN=0,(off),       DO00_SAFE=0,(off)
DO01=0,(DO),            DO01_PWN=0,(off),       DO01_SAFE=0,(off)
DO02=0,(DO),            DO02_PWN=0,(off),       DO02_SAFE=0,(off)
DO03=0,(DO),            DO03_PWN=0,(off),       DO03_SAFE=0,(off)
DO04=0,(DO),            DO04_PWN=0,(off),       DO04_SAFE=0,(off)
DO05=0,(DO),            DO05_PWN=0,(off),       DO05_SAFE=0,(off)
DO06=0,(DO),            DO06_PWN=0,(off),       DO06_SAFE=0,(off)
DO07=0,(DO),            DO07_PWN=0,(off),       DO07_SAFE=0,(off)

[3. Modbus address table]
-------------------------
CHANNEL         I/O TYPE        MODBUS REFERENCE        MODBUS ADDRESS (Dec, Hex)
DI00            Input           10001                   0000, 0x0000
DI01            Input           10002                   0001, 0x0001
DI02            Input           10003                   0002, 0x0002
DI03            Input           10004                   0003, 0x0003
DI04            Input           10005                   0004, 0x0004
DI05            Input           10006                   0005, 0x0005
DI06            Input           10007                   0006, 0x0006
DI07            Input           10008                   0007, 0x0007
DI08            Input           10009                   0008, 0x0008
DI09            Input           10010                   0009, 0x0009
DI10            Input           10011                   0010, 0x000A
```

Import System Config

Select this command to reload a configuration that was exported to a text file. You will need to restart the ioLogik E2210 in order for the new configuration to take effect. This command may be used to restore a configuration after loading the factory defaults, or to duplicate a configuration to multiple ioLogik E2210's.

4

Using the Web Console

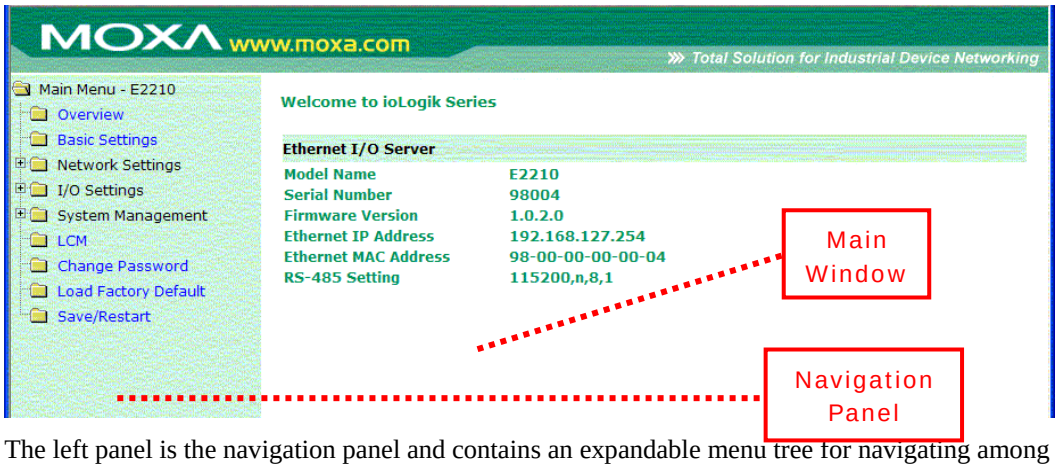
You may use the ioLogik E2210's built in web console to configure many options.

The following topics are covered:

- **Introduction to the Web Console**
- **Basic Settings**
- **Network Settings**
  - General Settings
  - Ethernet Configuration
  - RS-485 Settings
- **I/O Settings**
  - DI Channels
  - DO Channels
- **System Management**
  - Accessible IP Settings
  - SNMP Agent
  - Network Connection
- **LCM**
- **Change Password**
- **Load Factory Default**
- **Save/Restart**

Introduction to the Web Console

The ioLogik E2210 web console is a browser-based configuration utility. When the ioLogik E2210 is connected to your network, you may enter the server's IP address in your web browser to access the web console. Note that although most configuration options are available in the web console, some settings are only available through ioAdmin. Furthermore, the web console can be disabled under Web Access Settings in ioAdmin. If you are unable to access the web console, check the Web Access Settings in ioAdmin.



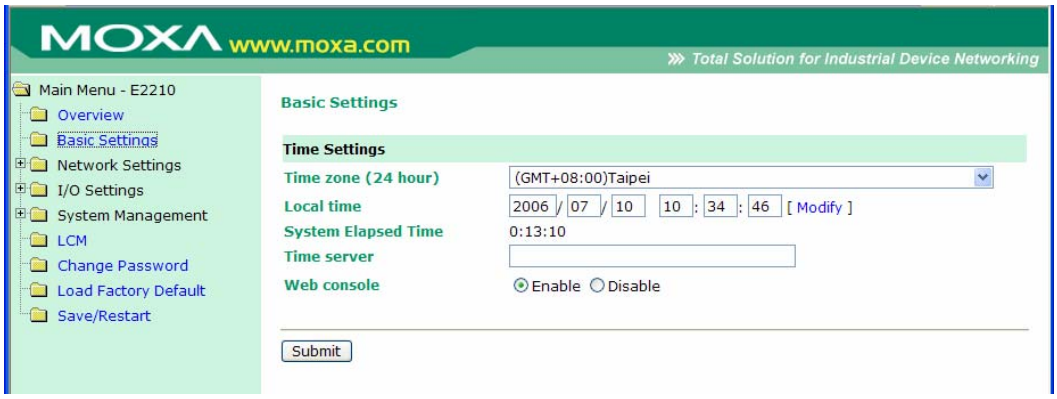
The left panel is the navigation panel and contains an expandable menu tree for navigating among the various settings and categories. When you click on a menu item in the navigation panel, the main window will display the corresponding options for that item. Configuration changes can then be made in the main window. For example, if you click on **Basic Settings** in the navigation panel, the main window will show a page of basic settings that you can configure.

You must click on the **Submit** button after making configuration changes. The **Submit** button will be located at the bottom of every page that has configurable settings. If you navigate to another page without clicking the **Submit** button, your changes will not be retained.

Submitted changes will not take effect until they are saved and the ioLogik E2210 is restarted! You may save and restart the server in one step by clicking on the **Save/Restart** button after you submit a change. If you need to make several changes before restarting, you may save your changes without restarting by selecting **Save/Restart** in the navigation panel. If you restart the ioLogik E2210 without saving your configuration, the ioLogik E2210 will discard all submitted changes.

Basic Settings

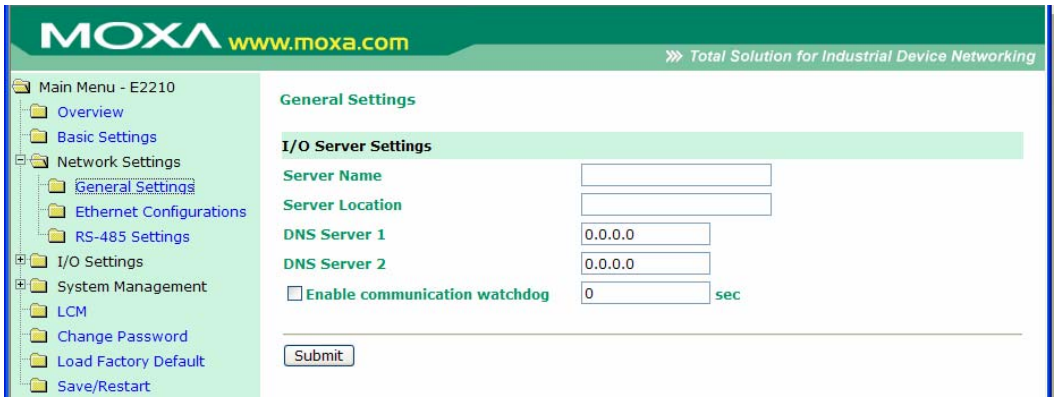
On the Basic Settings page, you may set the ioLogik E2210's system time or provide the IP address of a time server for time synchronization.



Network Settings

General Settings

On the General Settings page, you may assign a server name and location to assist you in differentiating between different I/O servers. You may also enable the Host Communication Watchdog and define the timeout value.

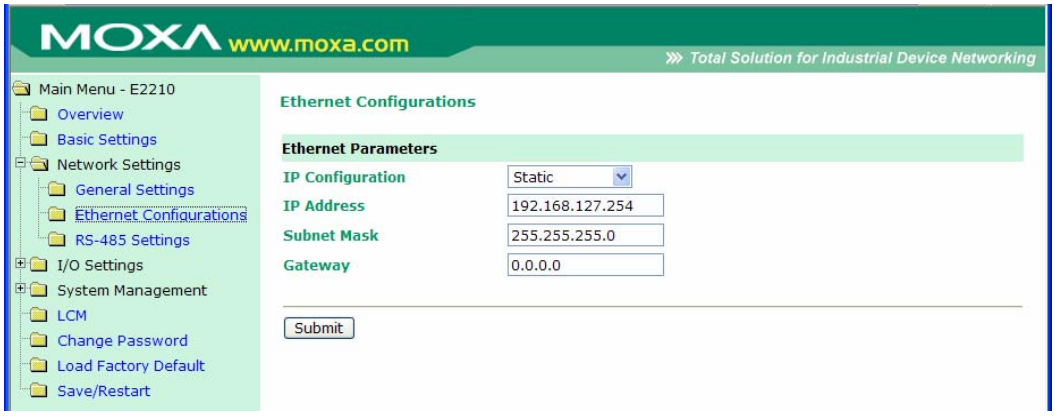


The Host Connection Watchdog activates Safe Status when the ioLogik E2210 loses its network connection for the specified amount of time. By default, the Watchdog is disabled. When the Watchdog is enabled and a timeout occurs, the ioLogik E2210 will enter Safe Status. You may use ioAdmin to configure how each DO channel responds in that channel's Safe Status settings.

To enable the Watchdog, check off **Enable connection watchdog**, set the timeout value, and restart the server. With Watchdog enabled, the ioLogik E2210 will enter Safe Status after there is disruption in communication that exceeds the time specified.

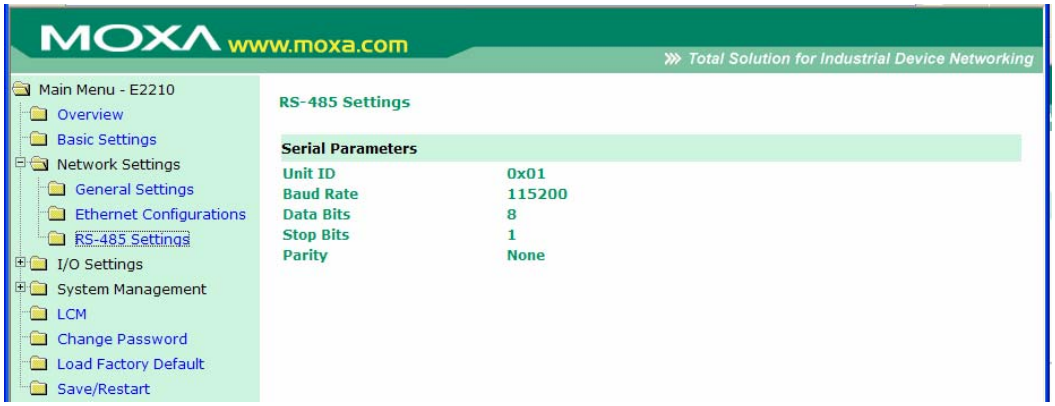
Ethernet Configuration

On the Ethernet Configuration page, you may set up a static or dynamic IP address for the ioLogik E2210, as well as the subnet mask and gateway address.



RS-485 Settings

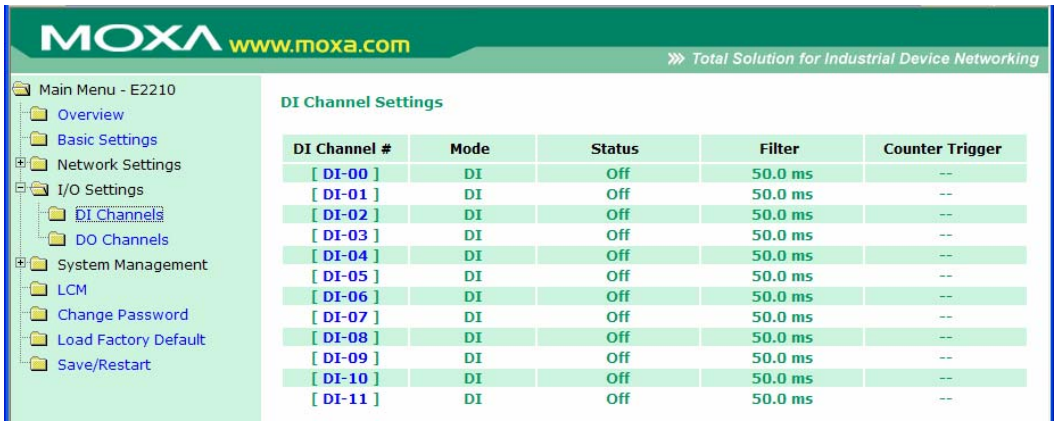
On the RS-485 Settings page, you may view the serial communication parameters, but no configuration changes are allowed. The baudrate may only be configured by the physical dial on the back of the ioLogik E2210. This is a reserved function.



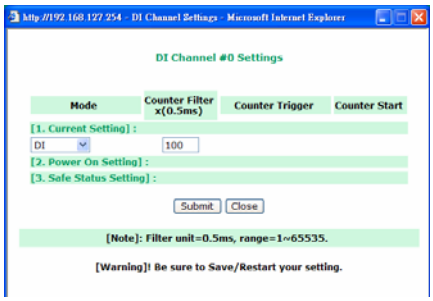
I/O Settings

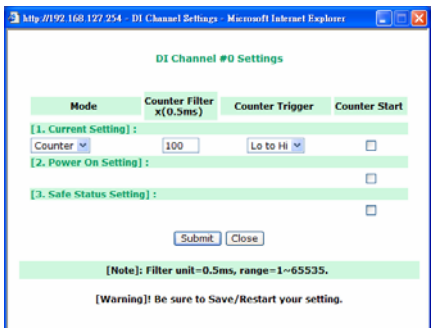
DI Channels

On the DI Channels page, you may view the status of each DI (digital input) channel.



You may also configure each channel's digital input mode and parameters by clicking on the channel. DI channels can operate in DI mode or Event Counter mode.



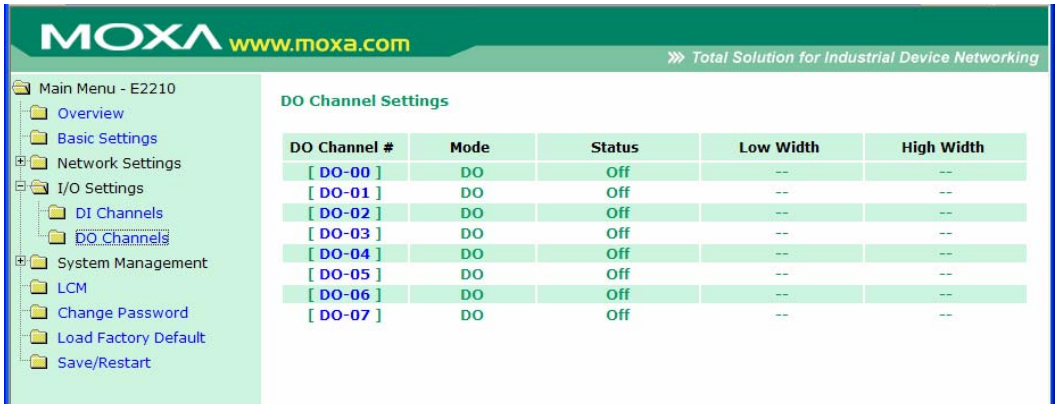


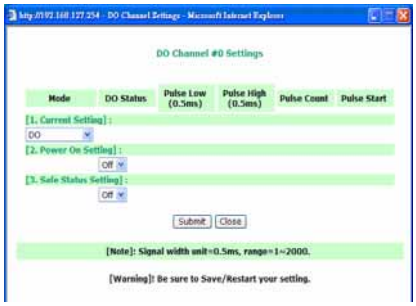
For DI mode, the maximum value of the filter is 65535.

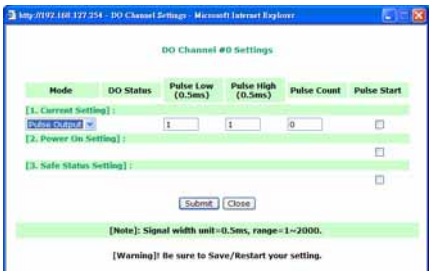
For Event Counter mode, you may configure the low width and high width in multiples of 0.5 ms. The counter should be set to either **start**, or **stop**. If it is in **stop** mode, the counter can be activated by the Modbus command. You may use the **Power On Setting** field to specify the channel's setting when the ioLogik E2210 is powered on, and the **Safe Status Setting** field to specify channel's setting when the ioLogik E2210 enters Safe Status. Note that Safe Status is controlled by the Host Connection Watchdog, which is disabled by default. If the Host Connection Watchdog is disabled, the ioLogik E2210 will never enter Safe Status and your Safe Status settings will have no effect.

DO Channels

On the DO Channels page, you may configure each DO (digital output) channel by clicking on the channel. DO Channels can operate in DO mode or Pulse Output mode. In DO mode, output is either on or off. In Pulse Output mode, a configurable square wave is generated.





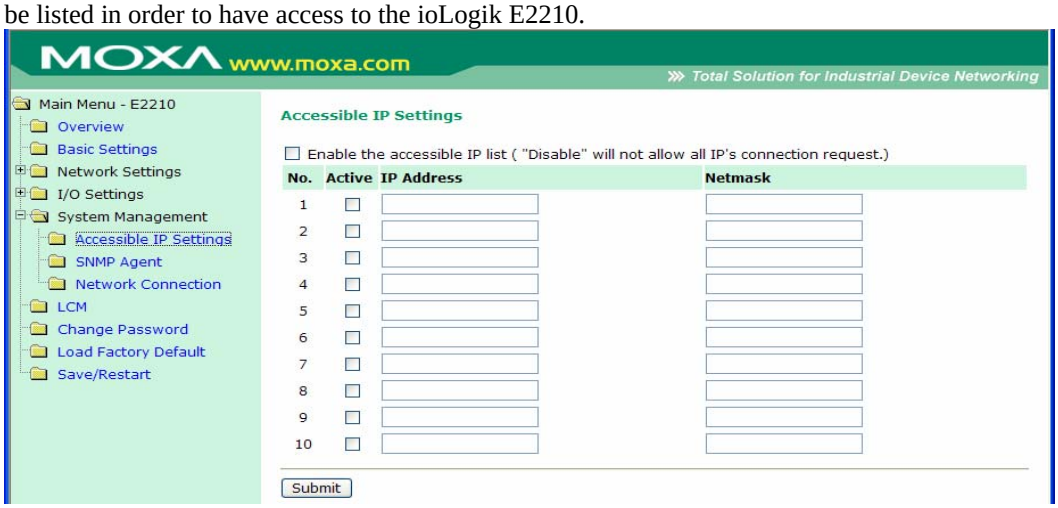


You may use the **Power On Setting** field to specify the channel's setting when the ioLogik E2210 is powered on, and the **Safe Status Setting** field to specify channel's setting when the ioLogik E2210 enters Safe Status. Note that Safe Status is controlled by the Host Connection Watchdog, which is disabled by default. If the Host Connection Watchdog is disabled, the ioLogik E2210 will never enter Safe Status and your Safe Status settings will have no effect.

System Management

Accessible IP Settings

On the Accessible IP Settings page, you may control network access to the ioLogik E2210 by allowing only specified IP addresses. When the accessible IP list is enabled, a host's IP address must be listed in order to have access to the ioLogik E2210.



You may add a specific address or range of addresses by using a combination of IP address and netmask, as follows:

To allow access to a specific IP address
Enter the IP address in the corresponding field; enter **255.255.255.255** for the netmask.

To allow access to hosts on a specific subnet
For both the IP address and netmask, use **0** for the last digit (e.g., **192.168.1.0** and **255.255.255.0**).

To allow unrestricted access
Deselect the **Enable the accessible IP list** option.

Refer to the following table for additional configuration examples.

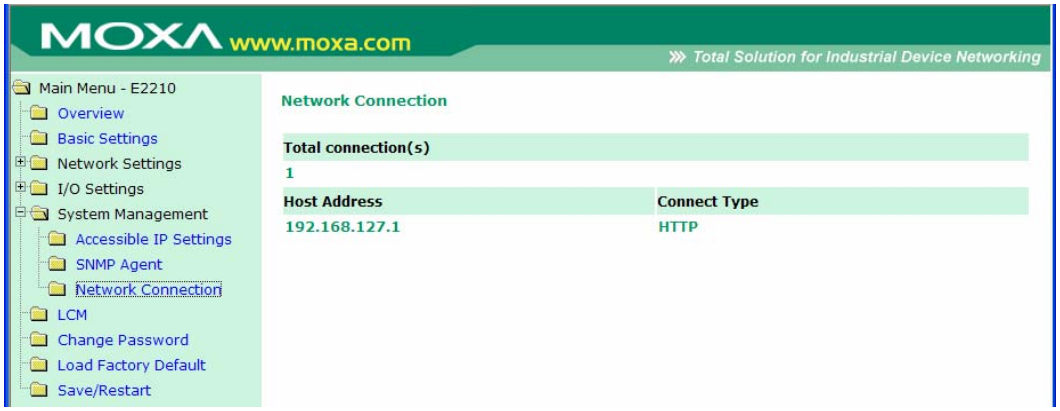
Allowed Hosts	IP address/Netmask
Any host	Disable
192.168.1.120	192.168.1.120 / 255.255.255.255
192.168.1.1 to 192.168.1.254	192.168.1.0 / 255.255.255.0
192.168.0.1 to 192.168.255.254	192.168.0.0 / 255.255.0.0
192.168.1.1 to 192.168.1.126	192.168.1.0 / 255.255.255.128
192.168.1.129 to 192.168.1.254	192.168.1.128 / 255.255.255.128

SNMP Agent

On the SNMP Agent page, you may enable SNMP and set the read and write community strings. The ioLogik E2210 provides SNMP v2 (Simple Network Management Protocol) to allow monitoring of network and I/O devices with SNMP Network Management software. It is useful in building automation and telecom applications.

Network Connection

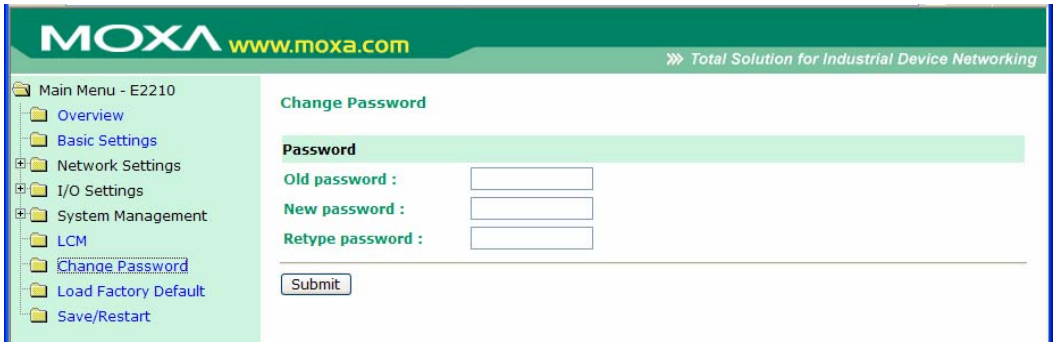
On the Network Connection page, you may view the TCP connections from other hosts. This may assist you in the management of your devices.



LCM

If you have installed the optional LCM, you may view the status and firmware details on the LCM page.

Change Password



For all changes to the ioLogik E2210's password protection settings, you will first need to enter the old password. Leave this blank if you are setting up password protection for the first time. To set up a new password or change the existing password, enter your desired password under both **New password** and **Confirm password**. To remove password protection, leave the **New password** and **Confirm password** fields blank.

ATTENTION

If you forget the password, the ONLY way to configure the ioLogik E2210 is by using the reset button to load the factory defaults.

Before you set a password for the first time, it is a good idea to export the configuration to a file when you have finished setting up your ioLogik E2210. Your configuration can then be easily imported back into the ioLogik E2210 if you need to reset the ioLogik E2210 due to a forgotten password or for other reasons.

Load Factory Default

This function will reset all of the ioLogik E2210's settings to the factory default values. All previous settings including the console password will be lost.

Save/Restart

If you change the configuration, do not forget to reboot the system.

5

Click&Go Logic

Click&Go Logic was developed by Moxa to provide an easy way to program your ioLogik E2210 for active I/O messaging. In the chapter, we will show you how Click&Go Logic works and how to use it to develop your active I/O messaging program.

The following topics are covered in this chapter:

- **Overview**
- **Features**
- **Click&Go Logic Basics**
- **Working with Click&Go Rules**
  - IF conditions
  - THEN actions
- **Working with Click&Go Rulesets**
  - Activating the Ruleset
  - Ruleset Management Bar
  - Ruleset Import/Export
- **Click&Go Logic Demo**
  - Scenario 1
  - Scenario 2

Overview

The ioLogik E2210's Active Remote I/O system eliminates the need for host computers to continually poll I/O devices for status. Instead, the server itself is able to monitors the status of each I/O device and take the appropriate action when the I/O status satisfies a user-defined condition. For example, the ioLogik E2210 could be configured to send a TCP/UDP message only when the temperature sensor attached to DI(0) exceeds a certain level. This structure results in a much improved response time and a much reduced load on the host computer's CPU and on network bandwidth.

Click&Go Logic was developed by Moxa to easily and intuitively configure when and how I/O information is transmitted over the network. Using simple If – Then statements, you may set the conditions that need to be satisfied on one side and the resulting actions on the other side. Up to three conditions and three actions can be combined in any one rule, and you may define up to 16 rules. SNMP traps and TCP/UDP messages may be configured for transmission to up to 10 computers simultaneously.

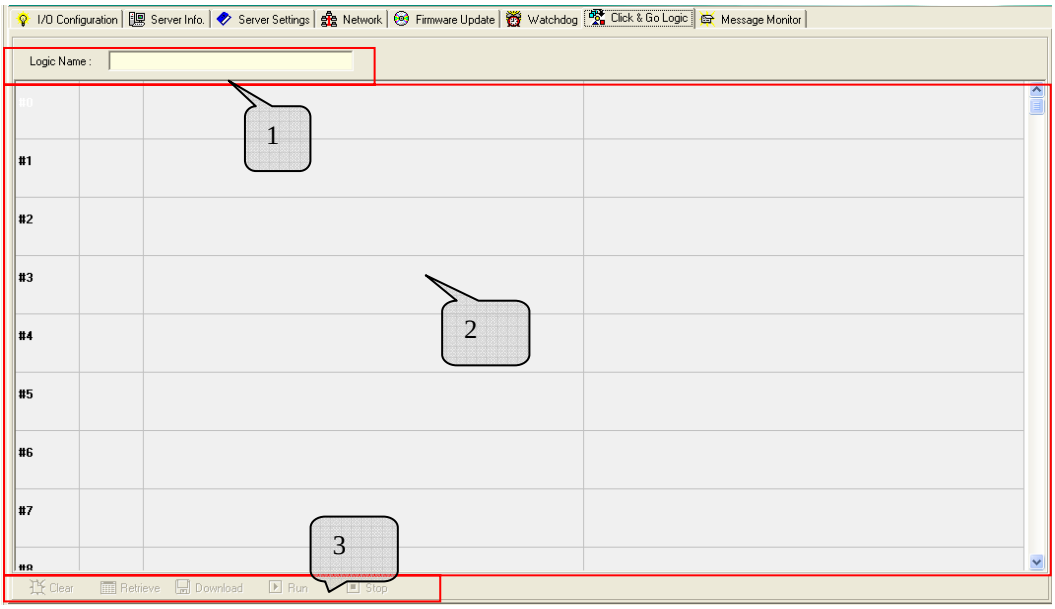
Features

Click&Go Logic's key features are as follows:

- Easy local logic control using intuitive IF/THEN style construction
- Up to 16 user-defined rules
- Up to 3 I/O-based conditions and 3 DO or network actions per rule
- Choice of email, TCP, UDP, or SNMP Trap for active I/O messaging
- Customizable message content with dynamic fields for time, date, IP address, and more
- Support multi-destination active I/O messaging up to 10 host computers for TCP/UDP.

Click&Go Logic Basics

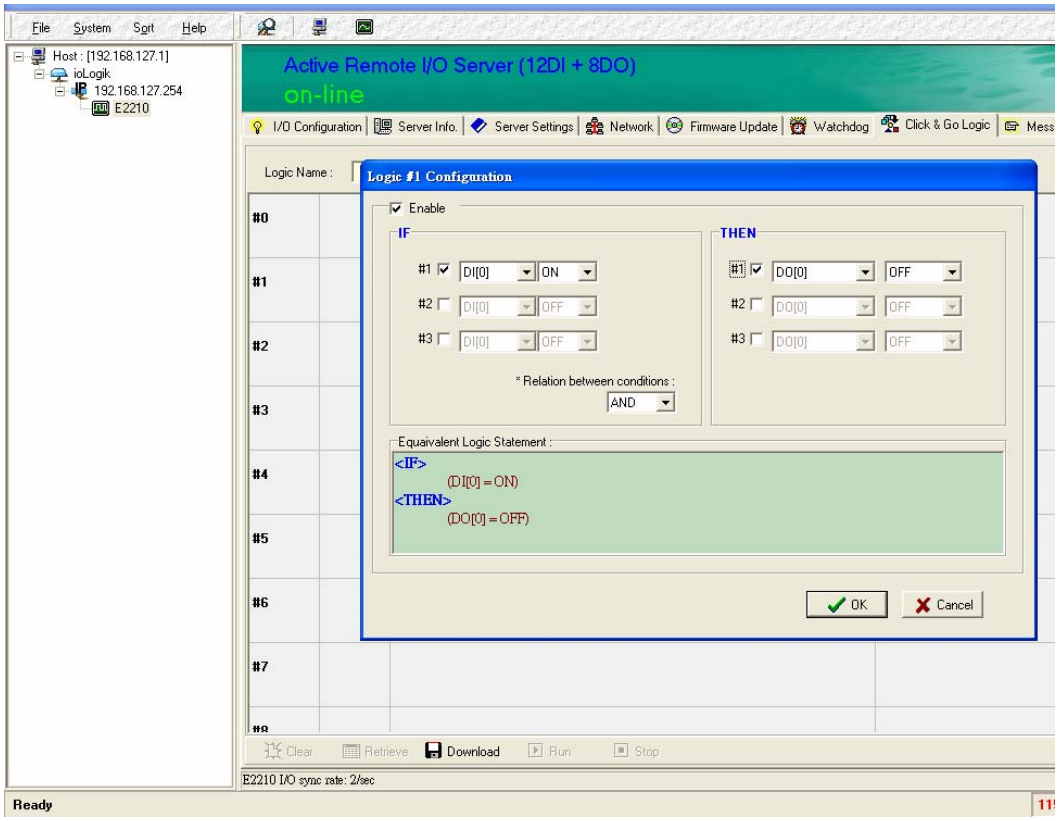
To use Click&Go Logic, open ioAdmin and log on as an administrator on the **Server Settings** tab. Once you are logged on, go to the **Click&Go Logic** tab. It should appear as below:



Click&Go Logic Tab
1. **Logic Name**: In this field, you may assign a name for the set of rules.
2. **Rules List**: In this area, each rule's conditions, actions, and status are displayed.
3. **Ruleset Management Bar**: In this area, you manage the ruleset

Working with Click&Go Rules

Rules are the building blocks of your active I/O system. In the main screen, you will see a list of the rules in the current ruleset. Double click on a rule to open that rule's configuration window, or double click on an empty rule to start a new rule.



The screen is divided into three parts: IF, THEN, and Equivalent Logic Statement. The IF and THEN areas are where you define the rule. The **Equivalent Logic Statement** shows a real-time text-based summary of the rule. It can be a useful way to make sure that the rule is designed as you intended.

ATTENTION

When configuring input or output control or response values, **you must select the unit of measurement before entering a value**. If you select a unit of measurement after entering a value, the value will not be retained. Also, when an I/O channel is being used in a Click&Go Logic rule, the channel's range and units may not be modified.

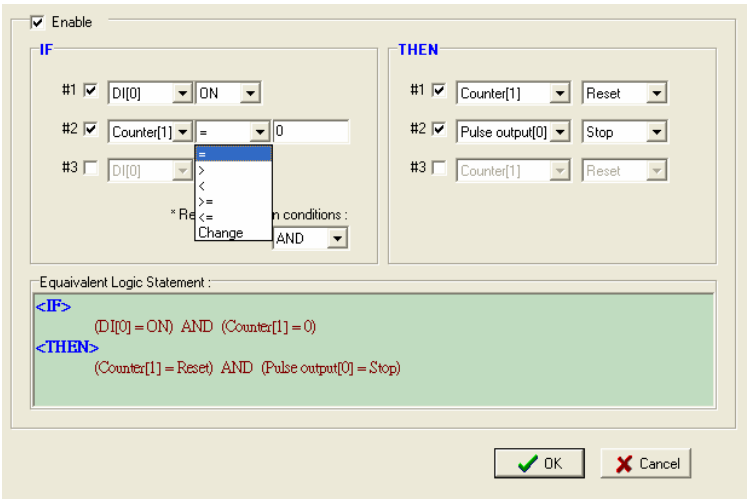
IF conditions

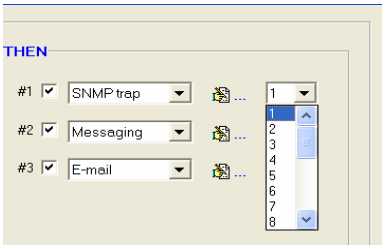
Under the **IF** column, you may set up to 3 sensor conditions that must be satisfied for the actions under the **THEN** column to take place. Use the pull downs to specify the conditions and units of measurement (e.g. DI(0)=OFF). The available operators are =,<,>,<=,>=.

Under **Relation between condition**, select **AND** to specify that all conditions must satisfied for the action to take place; select **OR** to specify that any one of the conditions may be satisfied for the action to take place.

THEN actions

Under the **THEN** column, you may set up to 3 actions that will be performed if the conditions under the **IF** column are satisfied. The 3 actions may be any combination of DI/O setting, SNMP trap, Messaging (by TCP/UDP), or Email. Additional parameters may be configured for SNMP trap, Messaging, and Email actions by clicking the memo icon: 





Counter(*x*)

Select **Counter(*x*)** to have the corresponding DI channel reset the counter.

Pulse output(*x*)

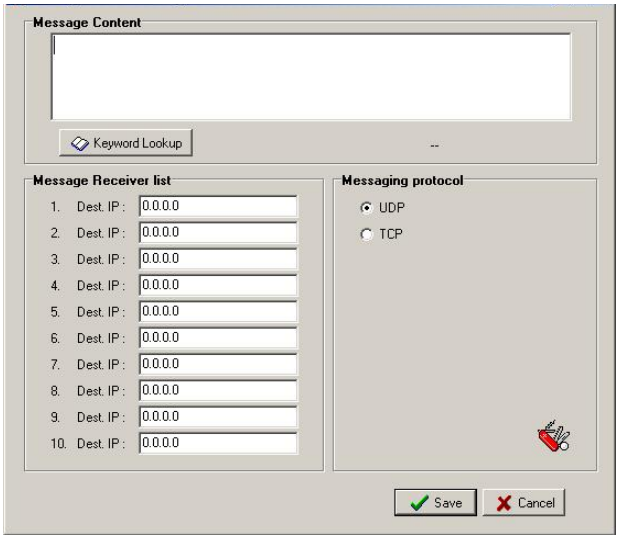
Select **Pulse output(*x*)** to have the corresponding DO channel either start or stop output pulsing.

DO(*x*)

Select **DO(*x*)** to have the corresponding DO channel either turn on or off.

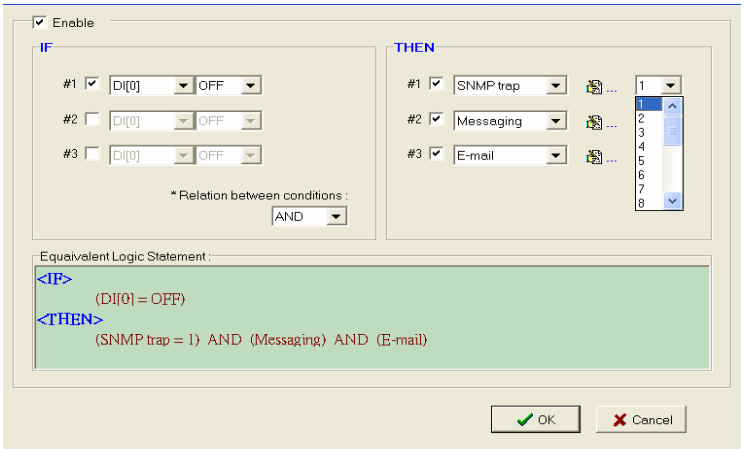
Active I/O Messaging

Select **Messaging** for active I/O messaging via TCP/UDP. This option allows you to select either TCP or UDP as the protocol to send the I/O message. Note that TCP and UDP cannot be used at the same time within a ruleset. In the additional parameters, you may edit the message and set the IP address of up to 10 destinations. Dynamic fields such as time, date, IP address, and I/O status may be inserted in your message by clicking on the **Keyword Lookup** button.

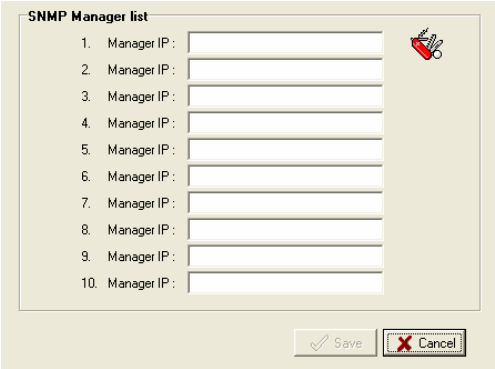


SNMP trap

Select **SNMP trap** and select a trap number between 1 and 20 to be sent. You may need to consult with your network administrator to determine how trap numbers will be used and defined in your network.



In the additional parameters, you may specify up to 10 IP addresses to receive the SNMP trap.

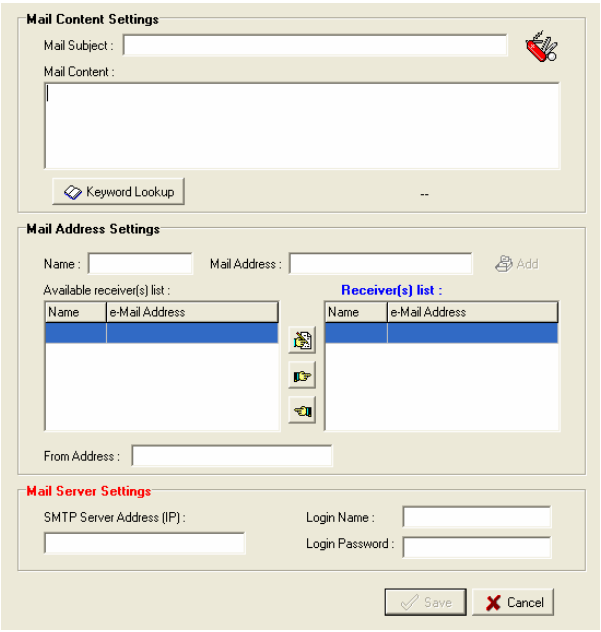


Email

Select **E-mail** to send a user-defined email to the specified addresses. In the additional parameters, you may edit the message and define the recipients of the e-mail. Dynamic fields such as time, date, IP address, and I/O status may be inserted in your message by clicking on the **Keyword Lookup** button.

To add a recipient, you must first add the recipient's e-mail address to the **Available receivers list**. You may then use the finger icons to move e-mail addresses to and from the **Receivers list**. To edit an e-mail address, click on the memo icon. Note that the Available Receivers list will already contain a list of names if you provided the DNS server information in the Network Settings tab.

Under **Mail Server Settings**, you must configure the IP address of the SMTP server with your username and password. Since the ioLogik E2210 supports DNS, you may enter the domain name of the SMTP server.



Working with Click&Go Rulesets

Activating the Ruleset

A Click&Go Logic ruleset is simply the set of rules that you have defined. The rules that are listed on the Click&Go Logic tab make up the current ruleset. The ruleset is the brain of your active I/O system and determines what I/O information is sent, who it is sent to, how it is sent, and under what I/O conditions it is sent. This simple but powerful tool is significantly more efficient with network and CPU resources than traditional blanket polling methods.

In order to start working as an Active Remote I/O server rather than a passive remote I/O server, the ioLogik E2210 will need to download the ruleset into its memory, reboot, and activate the ruleset.

1. The ruleset must first be downloaded from ioAdmin onto the ioLogik E2210. You may do so by clicking on **Download** in the Ruleset Management bar.
2. Now that the ruleset has been downloaded, you must restart the ioLogik E2210 in order for the new ruleset to be made effective. You may do this by right clicking on the server name in the navigation panel in ioAdmin and selecting **Restart**. Do not use the reset button, as that will load all factory defaults and erase your ruleset from memory.
3. After the ioLogik E2210 has restarted, the active I/O message system will be ready for activation with the new ruleset in place. First, you will need to log in as an administrator again in ioAdmin's Server Setting tab. Once you have logged in, click **Run** in the Ruleset Management bar on the Click&Go Logic tab. This will activate the ruleset and the ioLogik E2210 will begin working as an Active Remote I/O server. Note that the ioLogik E2210 can run the ruleset independently of the host computer and network connection.

Ruleset Management Bar

- **Clear**: The Clear command erases the ruleset in both ioAdmin and in the ioLogik E2210.
- **Retrieve**: The Retrieve command copies the ruleset from the ioLogik E2210 into ioAdmin.
- **Download**: The Download command copies the ruleset from ioAdmin onto the ioLogik E2210.
- **Run**: The Run command starts the active I/O messaging system using the ruleset that the ioLogik E2210 booted up with.
- **Stop**: The Stop command stops the active I/O messaging system.

Ruleset Import/Export

Although rulesets alone cannot be imported and exported, the entire system configuration including the current ruleset may be imported and exported. As you make changes to a ruleset, you may export the system configuration in order to save that ruleset.

Click&Go Logic Demo

Scenario 1

In this scenario, we have two switches, one attached to DI(0) and one attached to DO(0). Very simply, we want DO(0) to automatically mirror DI(0)'s setting. Once the ruleset is downloaded onto the ioLogik E2210 and activated, the server handles all processing locally and there is no usage of network or host resources.

Rule 0: IF DI(0)=ON, THEN DO(0)=ON

Rule 1: IF DI(0)=OFF, THEN DO(0)=OFF.

1. In ioAdmin, make sure that you have logged in on the **Server Settings** tab. Go to the **Click&Go Logic** tab.
2. Double click on **#0** in the **Rules List**. The rule configuration window will appear.
3. Make sure that **Enable Click&Go Logic** in the upper left hand corner is checked.
4. Select **DI(0)** as your condition in the first **IF field**, and set its value to **ON**.
5. Select **DO(0)** as your action in the first **THEN field**, and set its value **ON**.
6. Click on **OK**.
7. Double click on **#1** in the **Rules List**.
8. Make sure that **Enable Click&Go Logic** in the upper left hand corner is checked.
9. Select **DI(0)** as your condition in the first **IF field**, and set its value to **OFF**.
10. Select **DO(0)** as your action in the first **THEN field**, and set its value **OFF**.
11. Click on **OK**.
12. Click on **Download** on the **Ruleset Management Bar**.
13. Select **Yes** when asked to restart and wait until the server has restarted and is back on-line.
14. Log in on the **Server Settings** tab, then go to the **Click&Go Logic** tab.
15. Click on **Run** on the **Ruleset Management Bar**. The RDY LED will be flashing green, showing that the server is now operating as an Active Remote I/O server, using the ruleset that was just defined.

Scenario 2

In this scenario, we have a switch attached to DI(0). We want the server to send a TCP message that indicates the exact time that the switch is turned on.

Rule 0: IF DI(0)=ON, THEN Message

1. In ioAdmin, make sure that you have logged in on the **Server Settings** tab. Go to the **Click&Go Logic** tab.
2. Double click on **#0** in the **Rules List**. The rule configuration window will appear.
3. Make sure that **Enable Click&Go Logic** in the upper left hand corner is checked.
4. Select **DI(0)** as your condition in the first **IF field**, and set its value to **ON**.
5. Select **Message** as your action in the first **THEN field**.
6. Click the memo button. The Message parameters window will appear.
7. Click on **Keyword Lookup**. In the dialog box that pops up, click on **<time>**.

8. Click on **Save**.
9. Click on **Download** on the **Ruleset Management Bar**.
10. Select **Yes** when asked to restart and wait until the server has restarted and is back on-line.
11. Log in on the **Server Settings** tab, then go to the **Click&Go Logic** tab.
12. Click on **Run** on the **Ruleset Management Bar**. The RDY LED will be flashing green, showing that the server is now operating as an Active Remote I/O server, using the ruleset that was just defined.

A

Liquid Crystal Display Module (LCM)

As an *Easy View* device, the ioLogik E2210 supports an optional detachable Liquid Crystal Display Module (LCM) for easier field maintenance. The LCM is hot-pluggable and can be used to configure the network settings or display other settings. When plugged in, the LCM displays the ioLogik E2210 "home page," and pressing any button takes you into the settings and configuration.

LCM Controls

The up and down buttons navigate between the current options. The right and left buttons enter and exit the submenus. On the ioLogik E2210, the center button is used only when restarting the server.

Button	Function
Up	go to the previous item
Down	go to the next item
Left	exit the current submenu and return to the previous menu (go up one level)
Right	enter the selected submenu (go down one level)
Center	enter/exit editing mode

If you see an "e" in the upper right hand corner of the display, the current field is editable using the LCM.

LCM Options

Display	Explanation / Actions
`<ioLogik E2210>`	This is the default "home page" showing the IP address. Press the down button to view the submenus.
`<ioLogik E2210>` `server`	Enter this submenu to display information about the specific server you are viewing: • serial number • name • location • E2210 f/w ver • lcm f/w ver • model name

Display	Explanation / Actions
<ioLogik E2210> network	Enter this submenu to display information and settings for the network: ● Ethernet link ● MAC address ● IP mode ● IP address ● netmask ● gateway ● DNS server-1 ● DNS server-2
<ioLogik E2210> click&go	Enter this submenu to display information about the ruleset being used by the active I/O system. ● name ● status
<ioLogik E2210> serial port	Enter this submenu to display the RS-485 cascade port settings.
<ioLogik E2210> i/o setting	Enter this submenu to access I/O channel status. Here are examples of settings that you might see: ● DI-00 [di]=off ● DO-00 [pulse]=stop Press up or down to navigate through the different I/O channels without having to go back to the previous menu.
<ioLogik E2210> console	Enter this submenu to see if the web console is enabled or disabled.
<ioLogik E2210> ping	Select this option to enter an IP address to ping. If you get a "timeout" error, it indicates that the E2210 cannot reach that IP address. Otherwise, the display will show the response time.
<ioLogik E2210> save/restart	Enter this submenu, then enter the **restart now** submenu to display the **restart** option. You may press the center button at that point in order to reboot the ioLogik E2210. For this device, no other options are currently available for this set of submenus.

WARNING

Any configuration changes that are made through the LCM will not take effect until the ioLogik E2210 is restarted.

B

Modbus/TCP Address Mappings

E2210 Modbus Mapping

0xxxx Read/Write Coils (Support Functions 1, 5, 15)

Reference	Address	Data Type	Description
00001	0x0000	1 bit	CH0 DO Value 0: Off 1: On
00002	0x0001	1 bit	CH1 DO Value 0: Off 1: On
00003	0x0002	1 bit	CH2 DO Value 0: Off 1: On
00004	0x0003	1 bit	CH3 DO Value 0: Off 1: On
00005	0x0004	1 bit	CH4 DO Value 0: Off 1: On
00006	0x0005	1 bit	CH5 DO Value 0: Off 1: On
00007	0x0006	1 bit	CH6 DO Value 0: Off 1: On
00008	0x0007	1 bit	CH7 DO Value 0: Off 1: On
00009	0x0008	1 bit	CH0 DO Power-On Value 0: Off 1: On
00010	0x0009	1 bit	CH1 DO Power-On Value 0: Off 1: On
00011	0x000A	1 bit	CH2 DO Power-On Value 0: Off 1: On
00012	0x000B	1 bit	CH3 DO Power-On Value 0: Off 1: On
00013	0x000C	1 bit	CH4 DO Power-On Value 0: Off 1: On
00014	0x000D	1 bit	CH5 DO Power-On Value 0: Off 1: On
00015	0x000E	1 bit	CH6 DO Power-On Value 0: Off 1: On
00016	0x000F	1 bit	CH7 DO Power-On Value 0: Off 1: On
00017	0x0010	1 bit	CH0 DO Safe Value 0: Off 1: On
00018	0x0011	1 bit	CH1 DO Safe Value 0: Off 1: On
00019	0x0012	1 bit	CH2 DO Safe Value 0: Off 1: On
00020	0x0013	1 bit	CH3 DO Safe Value 0: Off 1: On
00021	0x0014	1 bit	CH4 DO Safe Value 0: Off 1: On
00022	0x0015	1 bit	CH5 DO Safe Value 0: Off 1: On
00023	0x0016	1 bit	CH6 DO Safe Value 0: Off 1: On
00024	0x0017	1 bit	CH7 DO Safe Value 0: Off 1: On
00025	0x0018	1 bit	CH0 DO Pulse Operate Status 0: Off 1: On
00026	0x0019	1 bit	CH1 DO Pulse Operate Status 0: Off 1: On
00027	0x001A	1 bit	CH2 DO Pulse Operate Status 0: Off 1: On
00028	0x001B	1 bit	CH3 DO Pulse Operate Status 0: Off 1: On
00029	0x001C	1 bit	CH4 DO Pulse Operate Status 0: Off 1: On

Reference	Address	Data Type	Description
00030	0x001D	1 bit	CH5 DO Pulse Operate Status 0: Off 1: On
00031	0x001E	1 bit	CH6 DO Pulse Operate Status 0: Off 1: On
00032	0x001F	1 bit	CH7 DO Pulse Operate Status 0: Off 1: On
00033	0x0020	1 bit	CH0 DO Power-On Pulse Operate Status 0: Off 1: On
00034	0x0021	1 bit	CH1 DO Power-On Pulse Operate Status 0: Off 1: On
00035	0x0022	1 bit	CH2 DO Power-On Pulse Operate Status 0: Off 1: On
00036	0x0023	1 bit	CH3 DO Power-On Pulse Operate Status 0: Off 1: On
00037	0x0024	1 bit	CH4 DO Power-On Pulse Operate Status 0: Off 1: On
00038	0x0025	1 bit	CH5 DO Power-On Pulse Operate Status 0: Off 1: On
00039	0x0026	1 bit	CH6 DO Power-On Pulse Operate Status 0: Off 1: On
00040	0x0027	1 bit	CH7 DO Power-On Pulse Operate Status 0: Off 1: On
00041	0x0028	1 bit	CH0 DO Safe Pulse Operate Status 0: Off 1: On
00042	0x0029	1 bit	CH1 DO Safe Pulse Operate Status 0: Off 1: On
00043	0x002A	1 bit	CH2 DO Safe Pulse Operate Status 0: Off 1: On
00044	0x002B	1 bit	CH3 DO Safe Pulse Operate Status 0: Off 1: On
00045	0x002C	1 bit	CH4 DO Safe Pulse Operate Status 0: Off 1: On
00046	0x002D	1 bit	CH5 DO Safe Pulse Operate Status 0: Off 1: On
00047	0x002E	1 bit	CH6 DO Safe Pulse Operate Status 0: Off 1: On
00048	0x002F	1 bit	CH7 DO Safe Pulse Operate Status 0: Off 1: On
00049	0x0030	1 bit	CH0 DI Counter Status 0: Off 1: On
00050	0x0031	1 bit	CH1 DI Counter Status 0: Off 1: On
00051	0x0032	1 bit	CH2 DI Counter Status 0: Off 1: On
00052	0x0033	1 bit	CH3 DI Counter Status 0: Off 1: On
00053	0x0034	1 bit	CH4 DI Counter Status 0: Off 1: On
00054	0x0035	1 bit	CH5 DI Counter Status 0: Off 1: On
00055	0x0036	1 bit	CH6 DI Counter Status 0: Off 1: On
00056	0x0037	1 bit	CH7 DI Counter Status 0: Off 1: On
00057	0x0038	1 bit	CH8 DI Counter Status 0: Off 1: On
00058	0x0039	1 bit	CH9 DI Counter Status 0: Off 1: On
00059	0x003A	1 bit	CH10 DI Counter Status 0: Off 1: On
00060	0x003B	1 bit	CH11 DI Counter Status 0: Off 1: On
00061	0x003C	1 bit	CH0 DI Clear Counter Value read always: 0 Write: 1: Clear counter value 0: return Illegal Data Value
00062	0x003D	1 bit	CH1 DI Clear Counter Value read always: 0 Write: 1: Clear counter value 0: return Illegal Data Value
00063	0x003E	1 bit	CH2 DI Clear Counter Value read always: 0 Write: 1: Clear counter value 0: return Illegal Data Value
00064	0x003F	1 bit	CH3 DI Clear Counter Value read always: 0 Write: 1: Clear counter value 0: return Illegal Data Value

Reference	Address	Data Type	Description
00065	0x0040	1 bit	CH4 DI Clear Counter Value read always: 0 Write: 1: Clear counter value 0: return Illegal Data Value
00066	0x0041	1 bit	CH5 DI Clear Counter Value read always: 0 Write: 1: Clear counter value 0: return Illegal Data Value
00067	0x0042	1 bit	CH6 DI Clear Counter Value read always: 0 Write: 1: Clear counter value 0: return Illegal Data Value
00068	0x0043	1 bit	CH7 DI Clear Counter Value read always: 0 Write: 1: Clear counter value 0: return Illegal Data Value
00069	0x0044	1 bit	CH8 DI Clear Counter Value read always: 0 Write: 1: Clear counter value 0: return Illegal Data Value
00070	0x0045	1 bit	CH9 DI Clear Counter Value read always: 0 Write: 1: Clear counter value 0: return Illegal Data Value
00071	0x0046	1 bit	CH10 DI Clear Counter Value read always: 0 Write: 1: Clear counter value 0: return Illegal Data Value
00072	0x0047	1 bit	CH11 DI Clear Counter Value read always: 0 Write: 1: Clear counter value 0: return Illegal Data Value
00073	0x0048	1 bit	CH0 DI Counter Overflow Status Read: 0: Normal 1: Overflow Write: 0: clear overflow status 1: return Illegal Data Value
00074	0x0049	1 bit	CH1 DI Counter Overflow Status Read: 0: Normal 1: Overflow Write: 0: clear overflow status 1 : return Illegal Data Value
00075	0x004A	1 bit	CH2 DI Counter Overflow Status Read: 0: Normal 1: Overflow Write: 0: clear overflow status 1: return Illegal Data Value
00076	0x004B	1 bit	CH3 DI Counter Overflow Status Read: 0: Normal 1: Overflow Write: 0 : clear overflow status 1: return Illegal Data Value

Reference	Address	Data Type	Description
00077	0x004C	1 bit	CH4 DI Counter Overflow Status Read: 0: Normal 1: Overflow Write: 0: clear overflow status 1: return Illegal Data Value
00078	0x004D	1 bit	CH5 DI Counter Overflow Status Read: 0: Normal 1: Overflow Write: 0: clear overflow status 1: return Illegal Data Value
00079	0x004E	1 bit	CH6 DI Counter Overflow Status Read: 0: Normal 1: Overflow Write: 0: clear overflow status 1: return Illegal Data Value
00080	0x004F	1 bit	CH7 DI Counter Overflow Status Read: 0: Normal 1: Overflow Write: 0: clear overflow status 1: return Illegal Data Value
00081	0x0050	1 bit	CH8 DI Counter Overflow Status Read: 0: Normal 1: Overflow Write: 0: clear overflow status 1: return Illegal Data Value
00082	0x0051	1 bit	CH9 DI Counter Overflow Status Read: 0: Normal 1: Overflow Write: 0: clear overflow status 1: return Illegal Data Value
00083	0x0052	1 bit	CH10 DI Counter Overflow Status Read: 0: Normal 1: Overflow Write: 0: clear overflow status 1: return Illegal Data Value
00084	0x0053	1 bit	CH11 DI Counter Overflow Status Read: 0: Normal 1: Overflow Write: 0: clear overflow status 1: return Illegal Data Value
00085	0x0054	1 bit	CH0 DI Counter Trigger : 0=Low to High, 1=High to Low
00086	0x0055	1 bit	CH1 DI Counter Trigger : 0=Low to High, 1=High to Low
00087	0x0056	1 bit	CH2 DI Counter Trigger : 0=Low to High, 1=High to Low
00088	0x0057	1 bit	CH3 DI Counter Trigger : 0=Low to High, 1=High to Low

Reference	Address	Data Type	Description
00089	0x0058	1 bit	CH4 DI Counter Trigger : 0=Low to High, 1=High to Low
00090	0x0059	1 bit	CH5 DI Counter Trigger : 0=Low to High, 1=High to Low
00091	0x005A	1 bit	CH6 DI Counter Trigger : 0=Low to High, 1=High to Low
00092	0x005B	1 bit	CH7 DI Counter Trigger : 0=Low to High, 1=High to Low
00093	0x005C	1 bit	CH8 DI Counter Trigger : 0=Low to High, 1=High to Low
00094	0x005D	1 bit	CH9 DI Counter Trigger : 0=Low to High, 1=High to Low
00095	0x005E	1 bit	CH10 DI Counter Trigger : 0=Low to High, 1=High to Low
00096	0x005F	1 bit	CH11 DI Counter Trigger : 0=Low to High, 1=High to Low
00097	0x0060	1 bit	CH0 DI Counter Power-On Status 0: Off 1: On
00098	0x0061	1 bit	CH1 DI Counter Power-On Status 0: Off 1: On
00099	0x0062	1 bit	CH2 DI Counter Power-On Status 0: Off 1: On
00100	0x0063	1 bit	CH3 DI Counter Power-On Status 0: Off 1: On
00101	0x0064	1 bit	CH4 DI Counter Power-On Status 0: Off 1: On
00102	0x0065	1 bit	CH5 DI Counter Power-On Status 0: Off 1: On
00103	0x0066	1 bit	CH6 DI Counter Power-On Status 0: Off 1: On
00104	0x0067	1 bit	CH7 DI Counter Power-On Status 0: Off 1: On
00105	0x0068	1 bit	CH8 DI Counter Power-On Status 0: Off 1: On
00106	0x0069	1 bit	CH9 DI Counter Power-On Status 0: Off 1: On
00107	0x006A	1 bit	CH10 DI Counter Power-On Status 0: Off 1: On
00108	0x006B	1 bit	CH11 DI Counter Power-On Status 0: Off 1: On
00109	0x006C	1 bit	CH0 DI Counter Safe Status 0: Off 1: On
00110	0x006D	1 bit	CH1 DI Counter Safe Status 0: Off 1: On
00111	0x006E	1 bit	CH2 DI Counter Safe Status 0: Off 1: On
00112	0x006F	1 bit	CH3 DI Counter Safe Status 0: Off 1: On
00113	0x0070	1 bit	CH4 DI Counter Safe Status 0: Off 1: On
00114	0x0071	1 bit	CH5 DI Counter Safe Status 0: Off 1: On
00115	0x0072	1 bit	CH6 DI Counter Safe Status 0: Off 1: On
00116	0x0073	1 bit	CH7 DI Counter Safe Status 0: Off 1: On
00117	0x0074	1 bit	CH8 DI Counter Safe Status 0: Off 1: On
00118	0x0075	1 bit	CH9 DI Counter Safe Status 0: Off 1: On
00119	0x0076	1 bit	CH10 DI Counter Safe Status 0: Off 1: On
00120	0x0077	1 bit	CH11 DI Counter Safe Status 0: Off 1: On

1xxxx Read Only Coils (Support Function 2)

Reference	Address	Data Type	Description
10001	0x0000	1 bit	CH0 DI Value
10002	0x0001	1 bit	CH1 DI Value
10003	0x0002	1 bit	CH2 DI Value
10004	0x0003	1 bit	CH3 DI Value
10005	0x0004	1 bit	CH4 DI Value
10006	0x0005	1 bit	CH5 DI Value
10007	0x0006	1 bit	CH6 DI Value
10008	0x0007	1 bit	CH7 DI Value

Reference	Address	Data Type	Description
10009	0x0008	1 bit	CH8 DI Value
10010	0x0009	1 bit	CH9 DI Value
10011	0x000A	1 bit	CH10 DI Value
10012	0x000B	1 bit	CH11 DI Value

3xxxx Read Only Registers (Support Function 4)

Reference	Address	Data Type	Description
30001	0x0000	word	CH0 DI Counter Value Hi-Word
30002	0x0001	word	CH0 DI Counter Value Lo-Word
30003	0x0002	word	CH1 DI Counter Value Hi-Word
30004	0x0003	word	CH1 DI Counter Value Lo-Word
30005	0x0004	word	CH2 DI Counter Value Hi-Word
30006	0x0005	word	CH2 DI Counter Value Lo-Word
30007	0x0006	word	CH3 DI Counter Value Hi-Word
30008	0x0007	word	CH3 DI Counter Value Lo-Word
30009	0x0008	word	CH4 DI Counter Value Hi-Word
30010	0x0009	word	CH4 DI Counter Value Lo-Word
30011	0x000A	word	CH5 DI Counter Value Hi-Word
30012	0x000B	word	CH5 DI Counter Value Lo-Word
30013	0x000C	word	CH6 DI Counter Value Hi-Word
30014	0x000D	word	CH6 DI Counter Value Lo-Word
30015	0x000E	word	CH7 DI Counter Value Hi-Word
30016	0x000F	word	CH7 DI Counter Value Lo-Word
30017	0x0010	word	CH8 DI Counter Value Hi-Word
30018	0x0011	word	CH8 DI Counter Value Lo-Word
30019	0x0012	word	CH9 DI Counter Value Hi-Word
30020	0x0013	word	CH9 DI Counter Value Lo-Word
30021	0x0014	word	CH10 DI Counter Value Hi-Word
30022	0x0015	word	CH10 DI Counter Value Lo-Word
30023	0x0016	word	CH11 DI Counter Value Hi-Word
30024	0x0017	word	CH11 DI Counter Value Lo-Word

4xxxx Read/Write Registers (Support Functions 3, 6, 16)

Reference	Address	Data Type	Description
40001	0x0000	word	CH0 DO Pulse Output Count Value Hi-Word
40002	0x0001	word	CH0 DO Pulse Output Count Value Lo-Word
40003	0x0002	word	CH1 DO Pulse Output Count Value Hi-Word
40004	0x0003	word	CH1 DO Pulse Output Count Value Lo-Word
40005	0x0004	word	CH2 DO Pulse Output Count Value Hi-Word
40006	0x0005	word	CH2 DO Pulse Output Count Value Lo-Word
40007	0x0006	word	CH3 DO Pulse Output Count Value Hi-Word
40008	0x0007	word	CH3 DO Pulse Output Count Value Lo-Word
40009	0x0008	word	CH4 DO Pulse Output Count Value Hi-Word

Reference	Address	Data Type	Description
40010	0x0009	word	CH4 DO Pulse Output Count Value Lo-Word
40011	0x000A	word	CH5 DO Pulse Output Count Value Hi-Word
40012	0x000B	word	CH5 DO Pulse Output Count Value Lo-Word
40013	0x000C	word	CH6 DO Pulse Output Count Value Hi-Word
40014	0x000D	word	CH6 DO Pulse Output Count Value Lo-Word
40015	0x000E	word	CH7 DO Pulse Output Count Value Hi-Word
40016	0x000F	word	CH7 DO Pulse Output Count Value Lo-Word
40017	0x0010	word	CH0 DO Pulse Low Signal Width
40018	0x0011	word	CH1 DO Pulse Low Signal Width
40019	0x0012	word	CH2 DO Pulse Low Signal Width
40020	0x0013	word	CH3 DO Pulse Low Signal Width
40021	0x0014	word	CH4 DO Pulse Low Signal Width
40022	0x0015	word	CH5 DO Pulse Low Signal Width
40023	0x0016	word	CH6 DO Pulse Low Signal Width
40024	0x0017	word	CH7 DO Pulse Low Signal Width
40025	0x0018	word	CH0 DO Pulse High Signal Width
40026	0x0019	word	CH1 DO Pulse High Signal Width
40027	0x001A	word	CH2 DO Pulse High Signal Width
40028	0x001B	word	CH3 DO Pulse High Signal Width
40029	0x001C	word	CH4 DO Pulse High Signal Width
40030	0x001D	word	CH5 DO Pulse High Signal Width
40031	0x001E	word	CH6 DO Pulse High Signal Width
40032	0x001F	word	CH7 DO Pulse High Signal Width
40033	0x0020	word	CH0 DO Mode 0: DO 1: Pulse
40034	0x0021	word	CH1 DO Mode 0: DO 1: Pulse
40035	0x0022	word	CH2 DO Mode 0: DO 1: Pulse
40036	0x0023	word	CH3 DO Mode 0: DO 1: Pulse
40037	0x0024	word	CH4 DO Mode 0: DO 1: Pulse
40038	0x0025	word	CH5 DO Mode 0: DO 1: Pulse
40039	0x0026	word	CH6 DO Mode 0: DO 1: Pulse
40040	0x0027	word	CH7 DO Mode 0: DO 1: Pulse
40041	0x0028	word	CH0 DI / Counter Filter
40042	0x0029	word	CH1 DI / Counter Filter
40043	0x002A	word	CH2 DI / Counter Filter
40044	0x002B	word	CH3 DI / Counter Filter

Reference	Address	Data Type	Description
40045	0x002C	word	CH4 DI / Counter Filter
40046	0x002D	word	CH5 DI / Counter Filter
40047	0x002E	word	CH6 DI / Counter Filter
40048	0x002F	word	CH7 DI / Counter Filter
40049	0x0030	word	CH8 DI / Counter Filter
40050	0x0031	word	CH9 DI / Counter Filter
40051	0x0032	word	CH10 DI / Counter Filter
40052	0x0033	word	CH11 DI / Counter Filter
40053	0x0034	word	CH0 DI Mode 0: DI 1: Counter Others: return Illegal Data Value
40054	0x0035	word	CH1 DI Mode 0: DI 1: Counter Others: return Illegal Data Value
40055	0x0036	word	CH2 DI Mode 0: DI 1: Counter Others: return Illegal Data Value
40056	0x0037	word	CH3 DI Mode 0: DI 1: Counter Others: return Illegal Data Value
40057	0x0038	word	CH4 DI Mode 0: DI 1: Counter Others: return Illegal Data Value
40058	0x0039	word	CH5 DI Mode 0: DI 1: Counter Others: return Illegal Data Value
40059	0x003A	word	CH6 DI Mode 0: DI 1: Counter Others: return Illegal Data Value
40060	0x003B	word	CH7 DI Mode 0: DI 1: Counter Others: return Illegal Data Value
40061	0x003C	word	CH8 DI Mode 0: DI 1: Counter Others: return Illegal Data Value
40062	0x003D	word	CH9 DI Mode 0: DI 1: Counter Others: return Illegal Data Value
40063	0x003E	word	CH10 DI Mode 0: DI 1: Counter Others: return Illegal Data Value
40064	0x003F	word	CH11 DI Mode 0: DI 1: Counter Others: return Illegal Data Value

Function 8

Sub-function	Data Field (Request)	Data Field (Response)	Description
0x0001	0x0000	Echo Request Data	Reboot
0x0001	0xFF00	Echo Request Data	Reset to Factory defaults

C

Used Network Port Numbers

E2210/E2210 Network Port Usage

Port	Type	Usage
80	TCP	Web Server
502	TCP	Modbus Communication
161	TCP	SNMP
68	UDP	BOOTPC
68	UDP	DHCP
4800	UDP	Auto search

D

SNMP Agents with MIB II & RS-232 like groups

RFC1213 MIB II Supported SNMP Variables

The ioLogik E2210 has built-in SNMP (Simple Network Management Protocol) agent software that supports RFC1317 RS-232 like groups and RFC 1213 MIB-II, I/O status MIB.

System MIB	Interfaces MIB	IP MIB	ICMP MIB
SysDescr	ifNumber	ipForwarding	IcmpInMsgs
SysObjectID	ifIndex	ipDefaultTTL	IcmpInErrors
SysUpTime	ifDescr	ipInreceives	IcmpInDestUnreachs
SysContact	ifType	ipInHdrErrors	IcmpInTimeExcds
SysName	ifMtu	ipInAddrErrors	IcmpInParmProbs
SysLocation	ifSpeed	ipForwDatagrams	IcmpInSrcQuenchs
SysServices	ifPhysAddress	ipInUnknownProtos	IcmpInRedirects
	ifAdminStatus	ipInDiscards	IcmpInEchos
	ifOperStatus	ipInDelivers	IcmpInEchoReps
	ifLastChange	ipOutRequests	IcmpInTimestamps
	ifInOctets	ipOutDiscards	IcmpTimestampReps
	ifInUcastPkts	ipOutNoRoutes	IcmpInAddrMasks
	ifInNUcastPkts	ipReasmTimeout	IcmpOutMsgs
	ifInDiscards	ipReasmReqds	IcmpOutErrors
	ifInErrors	ipReasmOKs	IcmpOutDestUnreachs

System MIB	Interfaces MIB	IP MIB	ICMP MIB
SysServices	ifInUnknownProtos	ipReasmFails	IcmpOutTimeExcds
	ifOutOctets	ipFragOKs	IcmpOutParmProbs
	ifOutUcastPkts	ipFragFails	IcmpOutSrcQuenchs
	ifOutNUcastPkts	ipFragCreates	IcmpOutRedirects
	ifOutDiscards	ipAdEntAddr	IcmpOutEchos

System MIB	Interfaces MIB	IP MIB	ICMP MIB
	ifOutErrors	ipAdEntIfIndex	IcmpOutEchoReps
	ifOutQLen	ipAdEntNetMask	IcmpOutTimestamps
	ifSpecific	ipAdEntBcastAddr	IcmpOutTimestampReps
		ipAdEntReasmMaxSize	IcmpOutAddrMasks
		ipRouteDest	IcmpOutAddrMaskReps
		ipRouteIfIndex	
		ipRouteMetric1	
		ipRouteMetric2	
		ipRouteMetric3	
		ipRouteMetric4	
		ipRouteNextHop	
		ipRouteType	
		ipRouteProto	
		ipRouteAge	
		ipRouteMask	
		ipRouteMetric5	
		ipRouteInfo	
		IpNetToMediaIfIndex	
		IpNetToMediaPhysAddress	
		IpNetToMediaNetAddress	
		IpNetToMediaType	
		IpRoutingDiscards	

UDP MIB	TCP MIB	SNMP MIB
UdpInDatagrams	tcpRtoAlgorithm	snmpInPkts
UdpNoPorts	tcpRtoMin	snmpOutPkts
UdpInErrors	tcpRtoMax	snmpInBadVersions
UdpOutDatagrams	tcpMaxConn	snmpInBadCommunityNames
UdpLocalAddress	tcpActiveOpens	snmpInBadCommunityUses
UdpLocalPort	tcpPassiveOpens	snmpInASNParseErrs
	tcpAttempFails	snmpInTooBigs
	tcpEstabResets	snmpInNoSuchNames
Address Translation MIB	tcpCurrEstab	snmpInBadValues
AtIfIndex	tcpInSegs	snmpInReadOnlys
AtPhysAddress	tcpOutSegs	snmpInGenErrs
AtNetAddress	tcpRetransSegs	snmpInTotalReqVars
AtNetAddress	tcpConnState	snmpInTotalSetVars
	tcpConnLocalAddress	snmpInGetRequests
	tcpConnLocalPort	snmpInGetNexts
	tcpConnRemAddress	snmpInSetRequests
	tcpConnRemPort	snmpInGetResponses
	tcpInErrs	snmpInTraps
	tcpOutRsts	snmpOutTooBigs
		snmpOutNoSuchNames
		snmpOutBadValues
		snmpOutGenErrs
		snmpOutGetRequests
		snmpOutGetNexts
		snmpOutSetRequests
		snmpOutGetResponses
		snmpOutTraps
		snmpEnableAuthenTraps

MOXA-IO-MIB	MOXA-IO-MIB	MOXA-IO-MIB
totalChannelNumber	AI03-Index	AI07-Index
serverMode	AI03-Type	AI07-Type
systemTime	AI03-Range	AI07-Range
firmwareVersion	AI03-Value	AI07-Value
AI00-Index	AI03-Min	AI07-Min
AI00-Type	AI03-Max	AI07-Max
AI00-Range	AI04-Index	AO00-Index
AI00-Value	AI04-Type	AO00-Type

MOXA-IO-MIB	MOXA-IO-MIB	MOXA-IO-MIB
AI00-Min	AI04-Range	AO00-Range
AI00-Max	AI04-Value	AO00-Value
AI01-Index	AI04-Min	AO01-Index
AI01-Type	AI04-Max	AO01-Type
AI01-Range	AI05-Index	AO01-Range
AI01-Value	AI05-Type	AO01-Value
AI01-Min	AI05-Range	
AI01-Max	AI05-Value	
AI02-Index	AI05-Min	
AI02-Type	AI05-Max	
AI02-Range	AI06Index	
AI02-Value	AI06-Type	
AI02-Min	AI06-Range	
AI02-Max	AI06-Value	
	AI06-Min	
	AI06-Max	

E

Factory Default Settings

The ioLogik E2210 is configured with the following factory defaults:

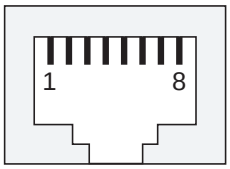
Default IP address:	**192.168.127.254**
Default Netmask:	**255.255.255.0**
Default Gateway:	**0.0.0.0**
Communication watchdog:	**Disable**
Modbus TCP alive check Timeout:	**60 secs**
DI Mode:	**DI**
Filter time:	**100 × 0.5 ms**
Trigger for counter:	**Lo to Hi**
Counter status:	**Stop**
DO Mode:	**DO**
DO Safe Status:	**Off**
Power on status:	**Off**
Low width for pulse:	**1 × 0.5 ms**
Hi width for pulse:	**1 × 0.5 ms**
Output pulses:	**0 (continuous)**
Password:	**NONE**
Module Name:	**NONE**
Module Location:	**NONE**
SNMP:	**Enable**
Community:	**Public**
Contact:	**NONE**
Location:	**NONE**
Click&Go	**NONE**

F

Pinouts and Cable Wiring

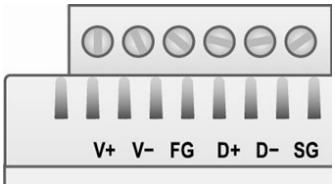
Ethernet Port Pinouts

Pin	Signal
1	Tx+
2	Tx-
3	Rx+
6	Rx-

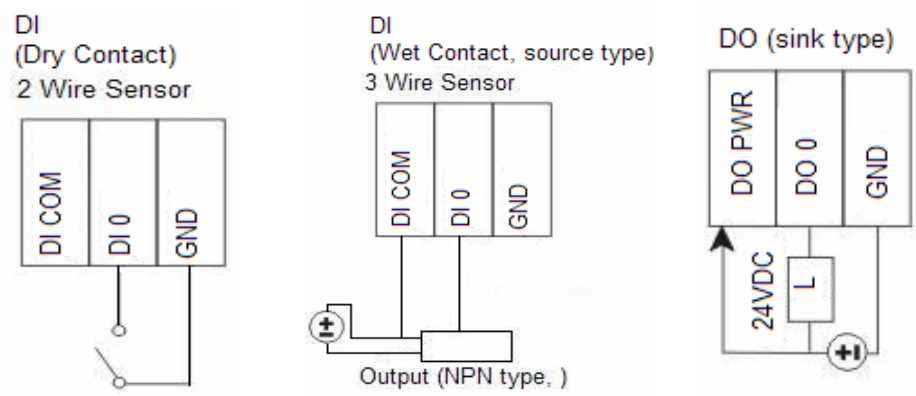


Serial Port Pinouts

E2210 RS-485 Network Adapter Pin Assignment



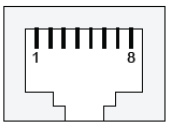
I/O Device Wiring



* DO PWR is for powering up the ***field Power*** LED.

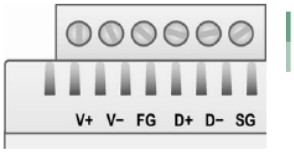
Pin Assignment of Terminal Blocks

Ethernet



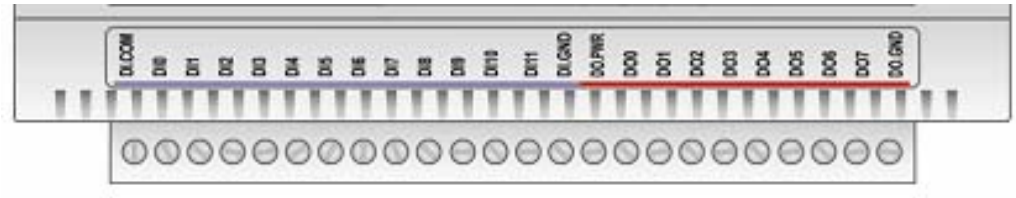
PIN	Signals
1	Tx+
2	Tx-
3	Rx+
6	Rx-

Power / RS-485 (TB1 / TB2)



I/O (left to right) (TB3)

Pin	1	2	3	4	5	6	7	8	9	10	11	12
Signal	DI COM	DI0	DI1	DI2	DI3	DI4	DI5	DI6	DI7	DI8	DI9	DI10
Pin	13	14	15	16	17	18	19	20	21	22	23	24
Signal	DI11	DI. GND	DO.PWR	DO0	DO1	DO2	DO3	DO4	DO5	DO6	DO7	DO.GND



G

Service Information

This appendix shows you how to contact MOXA for information about the ioLogik E2210, and other products, and how to report problems.

In this appendix, we cover the following topics.

- **MOXA Internet Services**
- **Problem Report Form**
- **Product Return Procedure**

MOXA Internet Services

Customer satisfaction is our top priority. To ensure that customers receive the full benefit of our products, MOXA Internet Services has been set up to provide technical support, driver updates, product information, and user's manual updates.

The following services are provided

Technical Support E-mail Address

support@moxa.com

Website for Product Information

http://www.moxa.com

Problem Report Form

MOXA ioLogik E2210 Active Remote I/O Server

Customer name:	
Company:	
Tel:	**Fax:**
Email:	**Date:**

MOXA Product: ioLogik E2210

Serial Number: _____

Problem Description: Please describe the symptoms of the problem as clearly as possible, including any error messages you see. A clearly written description of the problem will allow us to reproduce the symptoms, and expedite the repair of your product.

Product Return Procedure

For product repair, exchange, or refund, the customer must complete each of the following:

- Provide evidence of original purchase.
- Obtain a Product Return Agreement (PRA) from the sales representative or dealer.
- Fill out the Problem Report Form (PRF) with as much detail as possible to minimize repair time.
- Carefully pack the product in an anti-static package and send it, pre-paid, to the dealer. The PRA should be visible on the outside of the package and should include a description of the problem along with the return address and telephone number.

This Page Left Intentionally Blank

UNINTERRUPTABLE POWER SOURCE (UPS), 1000W, RACK MOUNT, CCTV HEAD END EQUIPMENT

Operations & Maintenance Manual
December 2015

Smart-UPS 120 V

Advanced line interactive power protection for servers and network equipment

The world's most popular network and server UPS

The award-winning Smart-UPS™ unit from APC™ by Schneider Electric™ is the most popular UPS in the world for servers, storage, and networks. Trusted to protect critical data and equipment from power problems, the UPS supplies clean and reliable network-grade power. In addition to Legendary Reliability and manageability, Smart-UPS units have extremely high efficiency at low, medium, and high load levels, making them ideal for today's multi-core or virtualized servers that have varying load consumption. Available in a variety of form factors (tower, rack-mount, rack/tower convertible), there is a model for every application and budget.

Intelligent and efficient network power protection from entry level to scaleable runtime. Ideal for servers, point-of-sale, routers, switches, hubs, and other network devices.

- Reliable
- Intelligent
- Efficient
- Manageable

APC by Schneider Electric

Smart-UPS Tower and Rack-mount 750 – 3,000 VA

Application-optimized standard models, ideal for servers, storage, point-of-sale, and other network devices

[SMT1500RM1U]

[SMT1500RM2U]

[SMT750]

[SMT1500RM2U]

[SMT750]

Standard Features

High-efficiency Green Mode:
Optimum efficiency which saves utility and cooling costs

Emergency Power Off (EPO):
Provides for remote UPS shut-off in the event of a fire or other emergency (2,200 VA and above)

Alphanumeric LCD Display:
Intuitive interface provides detailed and accurate information with ability to configure locally

Battery Disconnect:
Convenient way to disconnect battery for transport

Network-grade Power:
Provides most stable power conditions by filtering noise, automatic voltage regulation (AVR), and surge protection

Communication Ports:
Serial, USB, and SmartSlot™ for accessory cards

Advanced Battery Management:
Temperature-compensated charging extends life and advanced algorithms recommend replacement date

Smart-UPS Extended Run 750 – 3,000 VA

Convertible extended run models ideal for
critical servers and voice/data switches

[SMX3000LV]

[SMX1500RM2U]

[SMX1500RM2UNC]

[SMX3000RMLV2U]

Additional Features

Slim 2U Rack/Tower and 4U Short Depth Convertible Forms:

Display rotates easily for use in or out of a rack

High-frequency Design:

Reduces size of (or eliminates) bulky transformers making installation even easier

Low-voltage Models:

(2 – 3 kVA)
Configurable output from 100 V – 127 V on low-voltage models

Models Available with Pre-installed Network Cards:

Models with “NC” suffix have pre-installed AP9631 network cards with environmental monitoring

Smart External Battery Connector:

Accepts external batteries and increases runtime automatically to increase availability

Switched Outlet Groups:

Reboot hung devices, shed non-critical loads to conserve runtime, and sequence start-up/turn off

Smart-UPS Display

Intuitive, easy-to-use LCD interface

Standard Features

LCD Display Screen
Clear, consistent, and detailed information in your choice of basic or advanced menus

Power Status:
- Operating mode and efficiency
- Load VA/Watts/Amps
- Input/Output voltage and frequency
- Battery capacity and runtime
- Energy meter and more

Control:
UPS and outlet group settings

Configuration:
- Language
- Power quality settings
- Alarm, delay, and threshold settings

Test and Diagnostics:
Initiate battery and runtime calibration tests

Logs:
See explanation of last 10 transfers and faults

About:
UPS and replacement battery part numbers, serial numbers, battery install, and suggested replacement dates

About:
UPS and replacement battery part numbers, serial numbers, battery install, and suggested replacement dates

Quick Status Indicators
Online, on battery, fault, and replace battery LEDs for quick status identification

Escape:
Exits to the previous menu or screen

Return:
Used to enter or confirm settings

Navigation Arrows:
Allow for quick adjustment of settings

Product Services and Accessories

Schneider Electric Critical Power & Cooling Services (CPCS) provides the highest quality services and solutions by trained and trusted professionals. Our world-class services offer a smart way to build, operate, and maintain your critical applications, ensuring the right people, in the right place, at the right time.

Management Cards

AP9630: UPS Network Management Card

AP9631: UPS Network Management Card with Environmental Monitoring

AP9620: Legacy Communications SmartSlot Card

Battery Packs

SMX48RMBP2U: APC Smart-UPS 48 V External Battery Pack Rack/Tower

SMX120RMBP2U: APC Smart-UPS 120 V External Battery Pack Rack/Tower

Additional Accessories

AP9625: APC Smart-UPS Two-post Rail Kit

SMX039-2: APC Smart-UPS 48V Battery Extension Cable

SMX040: APC Smart-UPS 120V Battery Extension Cable

Service Bypass Panels

SBP1500RM: APC Service Bypass PDU, 120 V; 15 AMP W/ (8) NEMA 5-15R

SBP3000RM: APC Service Bypass PDU, 120 V; 30 AMP W/ (4) NEMA 5-20R and (1) L5-30R

SBP3000: APC Service Bypass Panel- 100 – 240 V; 30 A; BBM; Hard-wire Input/Output

SBP3000RMHW: APC Service Bypass Panel- 100 – 240 V; 30 A; BBM; Hard-wire Input/Output

AP9631

SBP3000RM

Standard Tower models

Product feature	SMT750	SMT1000	SMT1500	SMT2200	SMT3000
Output					
Power capacity	500 W/750 VA	700 W/1,000 VA	1,000 W/1,440 VA	1,980 W/2,200 VA	2,700 W/3,000 VA
Nominal output voltage	120 V				
Output frequency	57 – 63 Hz				
Waveform type	Sine wave				
Output connections (NEMA)	(6) 5-15R	(8) 5-15R		(8) 5-15R (2) 5-20R	
Switched outlet groups	-	1			
Input					
Nominal input voltage	120 V				
Input voltage range for main operations (Max adjustable range)	82 – 144 V (75 – 154 V)				
Input frequency	50/60 Hz +/- 3 Hz (auto sensing)				
Input connection	5-15P, 6 ft. cord			5-20P	L5-30P
Batteries and runtime					
Battery type	Maintenance-free sealed lead-acid battery with suspended electrolyte; leak proof				
Replacement battery	RBC48	RBC6	RBC7	RBC55	
Runtime estimates					
200 W	:22	:45	1:24	2:17	2:29
500 W	:05	:10	:23	:51	:55
700 W		:06	:12	:34	:37
1,000 W			:07	:21	:23
1,400 W				:13	:14
1,600 W				:10	:12
Full load	:05	:06	:07	:07	:06
Communication and management					
Interface ports	Serial (RJ45), USB, and SmartSlot				
Control panel and audible alarms	Alpha-numeric LCD display with LED status indicators; alarm on battery, distinctive low battery alarm and configurable delays				
Emergency power off (EPO)	Optional			Yes	
Surge protection and filtering					
Surge energy rating	459 J	480 J			
Filtering meets	Full-time multi-pole noise filtering: 0.3% IEEE surge let-through, zero clamping response time, meets UL 1449				
Physical					
Maximum height (inches)	6.2	8.5	8.5	17.0	17.0
Maximum width (inches)	5.4	6.7	6.7	7.7	7.7
Maximum depth (inches)	14.1	17.3	17.3	21.5	21.5
Net weight (pounds)	29	42	53	112	116
Conformance					
Regulatory	UL 1778, CSA				
Warranty and equipment protection policy	3-year electronics, 2-years battery, and $150,000 lifetime EPP				

Standard Rack-mount models

Product feature	SMT750RM2U	SMT1000RM2U	SMT1500RM1U	SMT1500RM2U	SMT2200RM2U	SMT3000RM2U
Output						
Power capacity	500 W/750 VA	700 W/1,000 VA	1,000 W/1,440 VA	1,000 W/1,440 VA	1,980 W/2,200 VA	2,700 W/3,000 VA
Nominal output voltage	120 V					
Output frequency	57 – 63 Hz					
Waveform type	Sine wave					
Output connections (NEMA)	(6) 5-15R	(6) 5-15R	(4) 5-15R	(6) 5-15R	(6) 5-15R (2) 5-20R	
Switched outlet groups	1					
Input						
Nominal input voltage	120 V					
Input voltage range for main operations (Max adjustable range)	82 – 144 V (75 – 154 V)					
Input frequency	50/60 Hz +/- 3 Hz (auto sensing)					
Input connection (NEMA, 8 ft. cord)	5-15P				5-20P	L5-30P
Batteries and runtime						
Battery type	Maintenance-free sealed lead-acid battery with suspended electrolyte; leak proof					
Replacement battery	APCRBC123	APCRBC132	APCRBC88	APCRBC133	RBC43	
Runtime estimates						
200 W	:24	1:10	1:32	:27	1:24	1:26
500 W	:05	:17	:26	:12	:35	:38
600 W		:12	:19	:09	:28	:31
700 W		:09	:14	:07	:24	:26
1,000 W			:07	:04	:15	:17
1,400 W					:09	:11
1,600 W					:07	:09
Full load	:06	:09	:07	:04	:05	:03
Communication and management						
Interface ports	Serial (RJ45), USB, and SmartSlot					
Control panel and audible alarms	Alpha-numeric LCD display with LED status indicators; alarm on battery, distinctive low-battery alarm and configurable delays					
Emergency power off (EPO)	Optional				Yes	
Surge protection and filtering						
Surge energy rating	459 J		540 J	459 J	480 J	
Filtering meets	Full-time multi-pole noise filtering: 0.3% IEEE surge let-through, zero clamping response time, meets UL 1449					
Physical						
Maximum height (inches)	3.5	3.5	1.75 (1U)	3.5	3.5	3.5
Maximum width (inches)	17.0	17.0	17.0	17.0	19.0	19.0
Maximum depth (inches)	16.0	18.0	26.0	18.0	26.0	26.0
Net weight (pounds)	38.0	62.0	53	63.0	96.0	96.0
Conformance						
Regulatory	UL 1778, CSA					
Warranty and equipment protection policy	3-year electronics, 2-years battery, and $150,000 lifetime EPP					

Extended Run Rack/Tower Convertible 2U models

Product feature	SMX750	SMX1000	SMX1500RM2U*	SMX2000RMLV2U*	SMX2200RMLV2U	SMX3000RMLV2U*
Output						
Power capacity	600 W/750 VA	800 W/1,000 VA	1,200 W/1,440 VA	1,800 W/2,000 VA	1,980 W/2,200 VA	2,700 W/3,000 VA
Nominal output voltage	120 V			100/110/120/127 V		
Output frequency	57 – 63 Hz					
Waveform type	Sine wave					
Output connections (NEMA)	(8) 5-15R			(3) 5-15R (3) 5-20R (1) L5-20R	(6) 5-15R (2) 5-20R	(3) 5-15R (3) 5-20R (1) L5-30R
Switched outlet groups	1	2	3			
Input						
Nominal input voltage	120 V			100 – 127 V		
Input voltage range for main operations (Max adjustable range)	82 – 143 V (75 – 153 V)			70 – 153 V		
Input frequency	50/60 Hz +/- 3 Hz (auto sensing)					
Input connection (NEMA)	5 - 15P 8 ft. cord			5-20P	L5-30P	
Batteries and runtime						
Battery type	Maintenance-free sealed lead-acid battery with suspended electrolyte; leak proof					
Replacement battery (UPS)	APCRBC116		APCRBC115	APCRBC117		
External Battery Pack	SMX48RMBP2U			SMX120RMBP2U		
Replacement battery (XBP)	APCRBC115			APCRBC118		
Typical back up time at other load conditions, and with external battery packs	Please refer to www.apc.com for runtime charts					
Communication and management						
Interface ports	Serial (RJ45), USB and Smartslot (Note: models denoted with asterisk * are also available in “NC” version with pre-installed AP9631 network management card.)					
Control panel and alarms	Alphanumeric LCD display with LED status indicators; alarm on battery, distinctive low battery alarm, and configurable delays					
Emergency power off (EPO)	Yes					
Surge protection						
Surge energy rating	540 J					
Filtering	Full-time multi-pole noise filtering: 0.3% IEEE surge let-through, zero clamping response time, meets UL 1449					
Physical						
Maximum height (inches)	3.5 (2U)					
Maximum width (inches)	17					
Maximum depth (inches)	19			6		
Net weight (pounds)	49	50	55	85		
Conformance						
Regulatory	UL 1778, CSA					
Warranty and equipment protection policy	3-years electronics, 2-years battery, and $150,000 lifetime EPP					

Extended Run Rack/Tower Convertible 4U Short Depth models

Product feature	SMX2000LV*	SMX3000LV*	SMX3000HVT
Output			
Power capacity	1,800 W/2,000 VA	2,700 W/3,000 VA	2,700 W/3,000 VA
Nominal output voltage	120 V (user selectable 100 – 127 V)		
Output frequency	57 – 63 Hz		
Waveform type	Sine wave		
Output connections (NEMA)	(6) 5-15R (3) 5-20R (1) L5-20R	(6) 5-15R (3) 5-20R (1) L5-30R	(2) L6-20R (4) IEC 320 C13 (2) IEC 320 C19
Switched outlet groups	3		
Input			
Nominal input voltage	120 V (user selectable 100 – 127 V)		
Input voltage range for main operations (Max adjustable range)	70 – 153 V		
Input frequency	50/60 Hz +/- 3 Hz (auto sensing)		
Input connection (NEMA)	5-20P, 8 ft. cord	L5-30P, 8 ft. cord	L6-20P, 8 ft. cord
Batteries and runtime			
Battery type	Maintenance-free sealed lead-acid battery with suspended electrolyte; leak proof		
Replacement battery (UPS)	APCRBC143		
External Battery Pack	SMX120BP		
Replacement battery (XBP)	APCRBC143		
Typical back up time at other load conditions, and with external battery packs	Please refer to www.apc.com for runtime charts		
Communication and management			
Interface ports	Serial (RJ45), USB and SmartSlot (Note: models denoted with asterisk * are also available in “NC” version with pre-installed AP9631 network management card.)		
Control panel and alarms	Alphanumeric LCD display with LED status indicators; alarm on battery, distinctive low battery alarm, and configurable delays		
Emergency power off (EPO)	Yes		
Surge protection			
Surge energy rating	540 J		
Filtering	Full-time multi-pole noise filtering: 0.3% IEEE surge let-through, zero clamping response time, meets UL 1449		
Physical			
Maximum height (inches)	17		
Maximum width (inches)	7.0 (4U)		
Maximum depth (inches)	19		
Net weight (pounds)	85		
Conformance			
Regulatory	UL 1778, CSA		
Warranty and equipment protection policy	3-years electronics, 2-years battery, and $150,000 lifetime EPP		

This Page Left Intentionally Blank

by Schneider Electric

Operation Manual

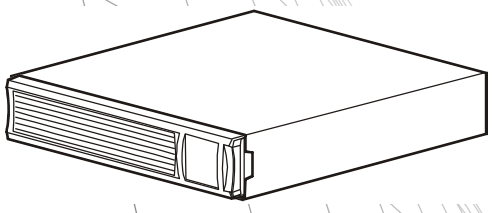
Smart-UPS™
Uninterruptible Power Supply

Rack-Mount 2U

750/1000/1500 VA
120/230 Vac

2200 VA
120 Vac

3000 VA
100/120/208/230 Vac



CCTV - 1,560

Product Description

The APC™ by Schneider Electric Smart-UPS™ is a high performance uninterruptible power supply (UPS). The UPS provides protection for electronic equipment from utility power blackouts, brownouts, sags, and surges, small utility power fluctuations and large disturbances. The UPS also provides battery backup power for connected equipment until utility power returns to safe levels or the batteries are fully discharged.

This user manual is available on the enclosed CD and on the APC by Schneider Electric Web site, www.apc.com.

Important Safety Messages

Read the instructions carefully to become familiar with the equipment before trying to install, operate, service or maintain it. The following special messages may appear throughout this manual or on the equipment to warn of potential hazards or to call attention to information that clarifies or simplifies a procedure.

The addition of this symbol to a Caution product safety label indicates that a hazard exists that can result in injury and product damage if the instructions are not followed.

The following safety messages may appear throughout this manual to warn of potential hazards.

⚠ CAUTION
CAUTION indicates a potentially hazardous situation which, if not avoided, **can result in** equipment damage and minor or moderate injury.

CAUTION
CAUTION indicates a potentially hazardous situation which, if not avoided, **can result in** equipment damage.

Safety and General Information

Inspect the package contents upon receipt. Notify the carrier and dealer if there is any damage.

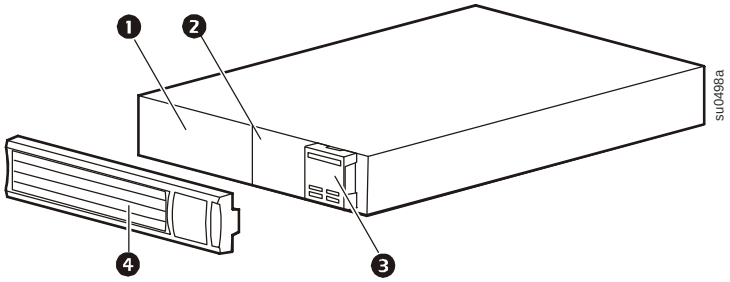
Read the Safety Guide supplied with this unit before installing the UPS.

- Adhere to all national and local electrical codes.
- This UPS is intended for indoor use only.
- Do not operate this UPS in direct sunlight, in contact with fluids, or where there is excessive dust or humidity.
- Be sure the air vents on the UPS are not blocked. Allow adequate space for proper ventilation.
- The battery typically lasts for two to five years. Environmental factors impact battery life. Elevated ambient temperatures, poor quality utility power, and frequent short duration discharges will shorten battery life.
- Connect the UPS power cable directly to a wall outlet. Do not use surge protectors or extension cords.
- The equipment is heavy. Always practice safe lifting techniques adequate for the weight of the equipment.
- The batteries are heavy. Remove the batteries before installing the UPS and XLBP in a rack.
- Always install external battery packs (XLBPs) at the bottom in rack-mount or stack configurations. The UPS must be installed above the XLBPs.
- Always install peripheral equipment above the UPS in rack-mount or stack configurations.
- The UPS will recognize as many as 10 external battery packs connected to the UPS. However there is no limit to the number of XLBPs that can be used with the UPS.
- The model and serial numbers are located on a small, rear panel label. For some models, an additional label is located on the chassis under the front bezel.
- Always recycle used batteries.
- Recycle the package materials or save them for reuse.

Front and Rear Panel Features

Front panel features

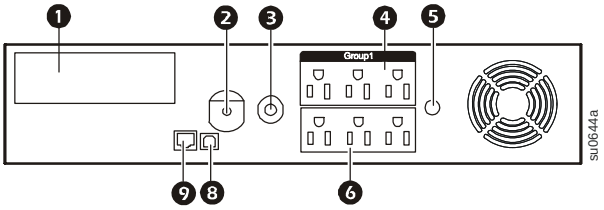
1. Battery
2. Battery connector
3. Display interface
4. Bezel



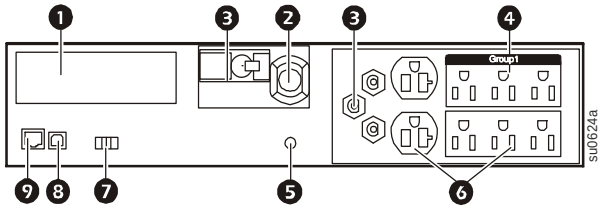
Rear panel features

1. SmartSlot for optional NMC accessory card
2. UPS input
3. Circuit breaker/Overload protection
4. Controlled outlet group
5. Chassis ground screw
6. Outlets
7. EPO connector
8. USB port
9. RJ45 connector - UPS monitoring serial port

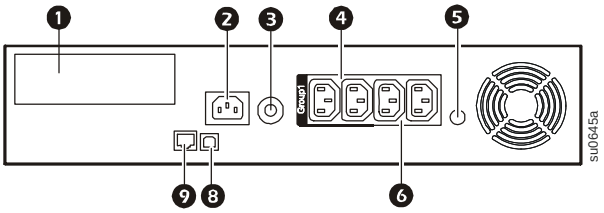
750/1000 VA 120 Vac
1500 VA 100/120 Vac



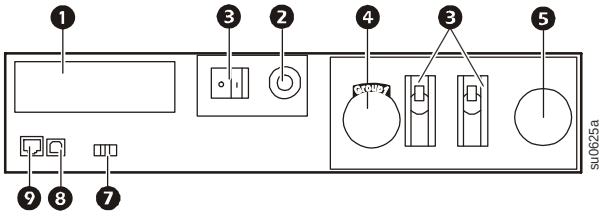
3000 VA 100/120 Vac



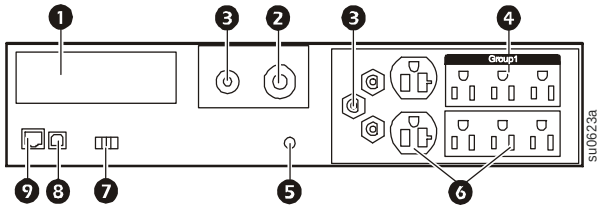
750/1000/1500 VA 230 Vac



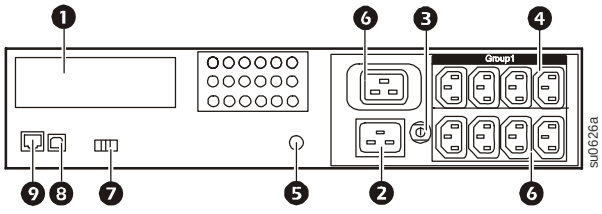
3000 VA 208 Vac



2200 VA 120 Vac



3000 VA 230 Vac



Specifications

For additional specifications, refer to the APC by Schneider Electric Web site at www.apc.com.

Environmental Specifications

Temperature	**Operating**	0° to 40° C (32° to 104° F)
	Storage	-15° to 45° C (5° to 113° F) charge UPS battery every six months
Maximum Elevation	**Operating**	3,000 m (10,000 ft)
	Storage	15,000 m (50,000 ft)
Humidity	0% to 95% relative humidity, non-condensing	

Installation

UPS

For UPS installation information, refer to the Smart-UPS Installation Guide that is included with the UPS. The guide is also available on the enclosed CD and the APC by Schneider Electric Web site at www.apc.com.

Network Management Card

For installation information, refer to the user manual provided with the Network Management Card (NMC). The user manual is also available on the APC by Schneider Electric Web site at www.apc.com.

Operation

Connect Equipment to UPS

⚠ CAUTION

DAMAGE TO EQUIPMENT OR PERSONNEL

- When installing equipment in a rack, always install the UPS at the bottom of the rack with the peripheral equipment above the UPS.
- The UPS should always be installed below peripheral equipment in rack or stack configurations.

Failure to follow these instructions can result in equipment damage and minor or moderate injury

CAUTION

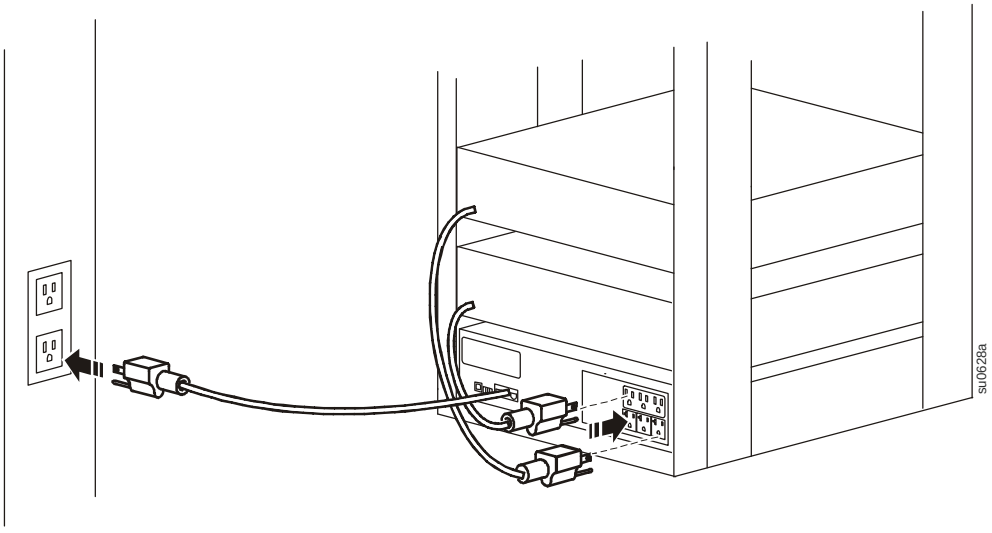
RISK OF EQUIPMENT DAMAGE

- Adhere to all national and local electrical codes.
- Wiring should be performed by qualified electrician.
- Always connect the UPS to a grounded outlet.

Failure to follow these instructions can result in equipment damage

Note: The UPS will charge to 90% capacity in the first three hours of normal operation. **Do not expect full battery runtime capability during this initial charge period.**

1. Connect equipment to the outlets on the rear panel of the UPS.
2. Connect the UPS to the building utility power.
   Always connect the UPS to a two pole, three wire, grounded source.
3. To use the UPS as a master ON/OFF switch, turn on all the equipment that is connected to the UPS.
4. Press the ON/OFF button on the front panel of the UPS to turn on the UPS and all connected equipment.
5. See “UPS Settings” on page 1 for information on how to configure the outlet groups.



Rear panel connectors

Serial port: Connect to a computer to use power management software.

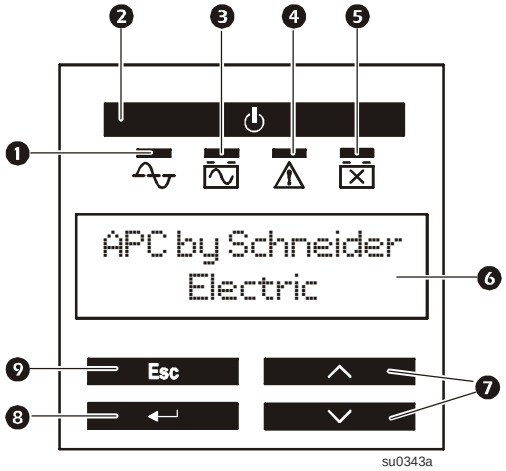
USB port: Connect to a computer to use power management software.

Note: Serial and USB communication can not be used simultaneously.

Ground Screw: The UPS features a ground screw for connecting the ground leads on transient voltage devices. Prior to connecting a ground lead, disconnect the UPS from utility power.

Display Panel Features

1. **Online** LED
2. UPS ON/OFF key
3. **On Battery** LED
4. **Site Wiring Fault** LED
5. **Replace Battery** LED
6. Display interface
7. UP/DOWN arrow keys
8. ENTER key
9. ESCAPE key



Display Interface Menus

Use the UP/DOWN arrow keys to scroll through the main menu options. Press ENTER to view the submenus under each main menu option. Press ESCAPE to exit a submenu and return to a main menu.

Standard menus

The Standard menus are the most commonly used menus for the UPS.

Menu	General Functions
Status	View basic information about the UPS: • Operating mode • Efficiency of the UPS • Information about the load • Battery capacity • Estimated runtime • Input and output voltage and frequency • Information about the last transfer to battery power • Self-test results
Configuration	Configure the settings for the UPS: • Language • Local power quality: Good, Fair, Poor • Choose Standard or Advanced menus • UPS Test settings • Reset to Factory Defaults • Battery installation date • Display: Always On, Auto Off, Auto Dim
Test & Diags	Use the Test & Diags menu to have the UPS perform a Self-Test, UPS Alarms Test or Calibration Test
About	Display information about this unit: • Unit model number • Serial number • Battery information •Model number •Installation date •Suggested battery replacement date •UPS firmware version

Advanced menus

The Advanced menus provide additional options for the UPS and are available only if the display interface is configured to use the Advanced menus.

Menu	General Functions
Status	View detailed information about the UPS: • Energy meter • Load current • Status of the Switched Outlet Group • Battery voltage • Operation mode • Efficiency • SmartSlot Card (if applicable)
Configuration	Configure advanced settings for the UPS: • Main and Switched Outlet Group—delays and settings • High and lower transfer points • Sensitivity settings • Date of last battery replacement • Output voltage • Battery settings • Number of battery packs (not available on all models) • Reset energy meter • UPS test settings • Display: Always On, Auto Off, Auto Dim
Control	Control the Main and Switched Outlet Group to turn on, turn off, shutdown, or reboot.
Test & Diags	Perform UPS test and diagnostic functions such as user interface testing, battery tests, and battery calibration.
Log	View the event and error logs for information about any changes to the UPS and any faults.
About	View information about the unit: • Hardware version • Software version • NMC information, if applicable • SmartSlot Card information, if applicable

Configuration

UPS Settings

Start up Settings

Configure these settings at initial start up, using the display interface or PowerChute™ software.

Note: During start up, use the display interface to configure these settings. If nothing is selected, the unit will use the default settings.

Function	Factory Default	Options	Description
Language	English	• English • French* • German* • Spanish* • Italian* • Portuguese* • Japanese*	The language for the display interface. *Language options will vary by model.
Local Power Quality	Good	• Good • Fair • Poor	Select the quality of input utility power. • If Good is selected, the unit will go on battery power more often to provide the cleanest power supply to the connected equipment. • If Poor is selected, the UPS will tolerate more fluctuations in power and will go on battery power less often. If unsure of the local power quality, select Good.
Menu Type	Standard	Standard or Advanced	The Standard menus display a limited set of menus and options. The Advanced menus include all parameters.

General Settings

Configure these settings at any time, using the display interface or PowerChute software.

Function	Factory Default	Options	Description
High Transfer Point	100 Vac: 108 Vac	• 108 Vac • 110 Vac • 112 Vac • 114 Vac	To avoid unnecessary battery usage, set the transfer point higher if the utility voltage is chronically high and the connected equipment is known to work under this condition. The POWER QUALITY setting will automatically change this setting. **Note:** Use the Advanced Menus to configure this setting.
	120 Vac: 127 Vac	• 127 Vac • 130 Vac • 133 Vac • 136 Vac	
	208 Vac: 225 Vac	• 225 Vac • 229 Vac • 233 Vac • 237 Vac	
	230 Vac: 253 Vac	• 253 Vac • 257 Vac • 261 Vac • 265 Vac	
Low Transfer Point	100 Vac: 92 Vac	• 86 Vac • 88 Vac • 90 Vac • 92 Vac	Set the transfer point lower if the utility voltage is chronically low and the connected equipment can tolerate this condition.This setting may also be adjusted using the power quality setting. **Note:** Use the Advanced Menus to configure this setting.
	120 Vac: 106 Vac	• 97 Vac • 100 Vac • 103 Vac • 106 Vac	
	208 Vac: 182 Vac	• 170 Vac • 174 Vac • 178 Vac • 182 Vac	
	230 Vac: 208 Vac	• 196 Vac • 200 Vac • 204 Vac • 208 Vac	
Nominal Output Voltage	100 Vac	N/A	Set the nominal output voltage of the UPS on battery. This is available on 230 Vac models only.
	120 Vac	N/A	
	230 Vac	208-252 Vac	
Transfer Sensitivity	High	High, Reduced, Low	Select the level of sensitivity to power events that the UPS will tolerate. • High: The UPS will go on battery power more often to provide the cleanest power supply to the connected equipment. • Low: The UPS will tolerate more fluctuations in power and will go on battery power less often. If the connected load is sensitive to power disturbances, set the sensitivity to High.
Low Battery Warning	120 sec	Set the value in seconds	The UPS will emit an audible alarm when the remaining runtime has reached this level.

Function	Factory Default	Options	Description
Date of Last Battery Replacement	Date set at factory	Reset this date when the battery module is replaced.	
Audible Alarm	On	On/Off	The UPS will mute all audible alarms if this is set to Off or when the display keys are pressed.
Battery Self-Test Interval Setting	On start-up and every 14 days since the last test	• Never • Start-up only • Frequency of test (every 7 to 14 days)	The interval at which the UPS will execute a self-test.
Reset to Factory Default	No	Yes/No	Restore the UPS factory default settings.

Main Outlet Group and Controlled Outlet Group

Overview

The Main Outlet Group and the Controlled Outlet Group can be configured to independently turn off, turn on, shut down, and reboot connected equipment. (These features are not available on the 750 VA tower units.)

The Main and Controlled Outlet Groups can be configured to do the following:

- Turn off: Disconnect from power immediately and restart only with a manual command.
- Turn on: Connect to power immediately.
- Shutdown: Disconnect power in sequence, and automatically reapply power in sequence when utility power becomes available.
- Reboot: Shut down and restart.

In addition, the Main Outlet Group and the Controlled Outlet Group can be configured to do the following:

- Turn on or off in a specified sequence
- Automatically turn off or shut down when various conditions occur

Note: If the Main and Controlled Outlet Groups are not configured, all of the outlets on the unit will still provide battery backup power.

Using the Main and Controlled Outlet Groups

The Main Outlet Group functions as a master switch. It will turn on first when power is applied, and shut off last when there is a power outage and battery runtime has been exhausted.

The Main Outlet Group must be turned on for the Controlled Outlet Group to turn on.

1.Connect critical equipment to the Main Outlet Group.

2. Connect peripheral equipment to the Controlled Outlet Group.
   - Nonessential equipment that should shut off quickly in the event of a power outage to conserve battery runtime can be added to a short power off delay
   - If equipment has dependent peripherals that must restart or shut down in a specific order, such as an ethernet switch that must restart before a connected server, connect the devices to separate groups
   - Equipment that needs to reboot independently from other equipment should be added to a separate group
3. Use the Configuration menus to configure how the Controlled Outlet Group will react in the event of a power outage.

Customize the Main and Controlled Outlet Groups

Use the **Control** menus to change the Main Outlet Group and the Controlled Outlet Group settings.

Function	Factory Default	Options	Description
Name String Outlet Group	Outlet Group 1	Edit these names using an external interface, such as the Network Management Card Web interface.	
UPS Name String	UPS Outlets		
Turn On Delay	0 sec	Set the value in seconds	The amount of time the UPS or the Controlled Outlet Group will wait between receiving the command to turn on and the actual startup.
Turn Off Delay	• 0 sec (UPS Outlets) • 90 sec (Controlled Outlet Groups)	Set the value in seconds	The amount of time that the UPS or the Controlled Outlet Group will wait between receiving the command to turn off and the actual shut down.
Reboot Duration	8 sec	Set the value in seconds	The amount of time that the UPS or the Controlled Outlet Group must remain off before it will restart.
Minimum Return Time	0 sec	Set the value in seconds	The amount of battery runtime that must be available before the UPS or the Controlled Outlet Group will turn on.
Load Shed On Battery	Disabled	• Shutdown with Delay • Shutdown immediately • Turn off immediately • Turn off with delay • Disabled	When the unit switches to battery power, the UPS can disconnect power to the Controlled Outlet Group to save runtime. Configure this delay time, use the LOAD SHED TIME WHEN ON BATTERY setting.
Load Shed Time when On Battery	Disabled	Set the value in seconds	The amount of time the outlets will function on battery power before they will turn off.
Load Shed On Runtime	Disabled	• Shutdown with delay • Shutdown immediately • Turn off immediately • Turn off with delay • Disabled	When the battery runtime falls below the specified value, the Controlled Outlet Group will turn off. Configure this time using the LOAD SHED RUNTIME REMAINING setting.
Load Shed On Runtime Remaining	Disabled	Set the value in seconds	When the remaining runtime reaches this level, the Controlled Outlet Group will turn off.
Load Shed on Overload	Disabled	• Disabled • Enabled	In the event of an overload (greater than 100% output), the Controlled Outlet Group will immediately turn off to conserve power for critical loads. The ControlledOutlet Group will only turn on again with a manual command.

Network Management Card Settings

These settings are available only on units that have a Network Management Card (NMC) and are set in the factory. These settings can only be modified using an external interface, like the NMC web interface.

- NMC IP Address Mode
- NMC IP Address
- NMC Subnet Mask
- NMC Default Gateway

Emergency Power Off

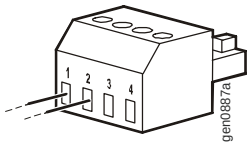
EPO Overview

The Emergency Power Off (EPO) option is a safety feature that will immediately disconnect all connected equipment from utility power. The UPS will immediately shut down and will not switch to battery power.

The UPS must be manually restarted to reapply power to connected equipment. Press ON/OFF on the front panel of the unit.

Adhere to all national and local electrical codes. All wiring must be performed by a qualified electrician.

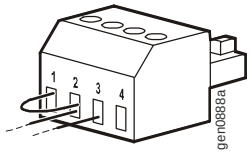
Normally open contacts



1. If the EPO switch or relay contacts are normally open, insert the wires from the switch or contacts at pins 1 and 2 of the EPO terminal block. Use 16-28 AWG wire.
2. Secure the wires by tightening the screws.

If the contacts are closed, the UPS will turn OFF and power will be removed from the load.

Normally closed contacts



1. If the EPO switch or relay contacts are normally closed, insert the wires from the switch or contacts at pins 2 and 3 of the EPO terminal block. Use 16-28 AWG wire.
2. Insert a wire jumper between pins 1 and 2. Secure the wires by tightening the three screws at positions 1, 2, and 3.

If the contacts are opened, the UPS will turn OFF and power will be removed from the load.

Note: The power for operating the EPO circuit is sourced from pin 1. This is an isolated 24 V which can source only a few milliamperes.

If the normally closed (NC) EPO configuration is used, the EPO switch or relay should be rated for dry circuit applications, the rating should be for low voltage and low current applications. This normally implies the contacts are gold-plated.

The EPO interface is a Safety Extra Low Voltage (SELV) circuit. Connect the EPO interface only to other SELV circuits. The EPO interface monitors circuits that have no determined voltage potential. SELV circuits are controlled by a switch or relay properly isolated from utility power. To avoid damage to the UPS, do not connect the EPO interface to any circuit other than a SELV circuit.

Use one of the following cable types to connect the UPS to the EPO switch.

- CL2: Class 2 cable for general use.
- CL2P: Plenum cable for use in ducts, plenums, and other spaces used for environmental air.
- CL2R: Riser cable for use in a vertical run in a floor-to-floor shaft.
- CLEX: Limited use cable for use in dwellings and for use in raceways.
- Installation in Canada: Use only CSA certified, type ELC, (extra-low voltage control cable).
- Installation in countries other than Canada and the USA: Use standard low-voltage cable in accordance with national and local regulations.

Troubleshooting

Problem and Possible Cause	Solution
The UPS will not turn on or there is no output	
The unit has not been turned on.	Press the ON key once to turn on the UPS.
The UPS is not connected to utility power.	Be sure the power cable is securely connected to the unit and to the utility power supply.
The input circuit breaker has tripped.	Reduce the load on the UPS. Disconnect nonessential equipment and reset the circuit breaker.
The unit shows very low or no input utility voltage.	Check the utility power supply to the UPS by plugging in a table lamp. If the light is very dim, check the utility voltage.
The battery connector plug is not securely connected.	Be sure that all battery connections are secure.
There is an internal UPS fault.	Do not attempt to use the UPS. Unplug the UPS and have it serviced immediately.
The UPS is operating on battery, while connected to utility power	
The input circuit breaker has tripped.	Disconnect nonessential equipment and reset the circuit breaker.
There is very high, very low, or distorted input line voltage.	Move the UPS to a different outlet on a different circuit. Test the input voltage with the utility voltage display. If acceptable to the connected equipment, reduce the UPS sensitivity.
UPS emits intermittent beeps	
The UPS is operating normally.	None. The UPS is protecting the connected equipment.
UPS does not provide expected backup time	
The UPS battery is weak due to a recent power outage or is near the end of its service life.	Charge the battery. Batteries require recharging after extended outages and wear out faster when put into service often or when operated at elevated temperatures. If the battery is near the end of its service life, consider replacing the battery even if the replace battery LED is not illuminated.
The UPS is experiencing an overload condition.	Check the UPS load display. Unplug unnecessary equipment, such as printers.
Display interface LEDs flash sequentially	
The UPS has been shut down remotely through software or an optional accessory card.	None. The UPS will restart automatically when utility power is restored.

Problem and Possible Cause	Solution
The Fault LED is illuminated The UPS displays a fault message and emits a constant beeping sound	
Internal UPS fault.	Do not attempt to use the UPS. Turn the UPS off and have it serviced immediately.
All LEDs are illuminated and the UPS is plugged into a wall outlet	
The UPS has shut down and the battery has discharged from an extended outage.	None. The UPS will return to normal operation when the power is restored and the battery has a sufficient charge.
The Replace Battery LED is illuminated	
The battery has a weak charge.	Allow the battery to recharge for at least four hours. Then, perform a self-test. If the problem persists after recharging, replace the battery.
The replacement battery is not properly connected.	Be sure the battery connector is securely connected.
The UPS displays a site wiring fault message	
Wiring faults detected include missing ground, hot-neutral, polarity reversal, and overloaded neutral circuit.	If the UPS indicates a site wiring fault, have a qualified electrician inspect the building wiring. Applicable for 120 V units only.

Service

If the unit requires service, do not return it to the dealer. Follow these steps:

1. Review the *Troubleshooting* section of the manual to eliminate common problems.
2. If the problem persists, contact APC by Schneider Electric Customer Support through the APC by Schneider Electric Web site, **www.apc.com**.
    a. Note the model number and serial number and the date of purchase. The model and serial numbers are located on the rear panel of the unit and are available through the LCD display on select models.
    b. Call APC by Schneider Electric Customer Support and a technician will attempt to solve the problem over the phone. If this is not possible, the technician will issue a Returned Material Authorization Number (RMA#).
    c. If the unit is under warranty, the repairs are free.
    d. Service procedures and returns may vary internationally. Refer to the APC by Schneider Electric Web site for country specific instructions.
3. Pack the unit in the original packaging whenever possible to avoid damage in transit. Never use foam beads for packaging. Damage sustained in transit is not covered under warranty.
    a. **Always DISCONNECT THE UPS BATTERIES before shipping. The United States Department of Transportation (DOT), and the International Air Transport Association (IATA) regulations require that UPS batteries be disconnected before shipping.** The internal batteries may remain in the UPS.
    b. External Battery Pack products are deenergized when disconnected from the associated UPS product. It is not necessary to disconnect the internal batteries for shipping. Not all units utilize an external battery pack.
4. Write the RMA# provided by Customer Support on the outside of the package.
5. Return the unit by insured, prepaid carrier to the address provided by Customer Support.

Transport the unit

1. Shut down and disconnect all connected equipment.
2. Disconnect the unit from utility power.
3. Disconnect all internal and external batteries (if applicable).
4. Follow the shipping instructions outlined in the *Service* section of this manual.

Two Year Limited Factory Warranty

Schneider Electric IT Corporation (SEIT), warrants its products to be free from defects in materials and workmanship for a period of three (3) years excluding the batteries, which are warranted for two (2) years from the date of purchase. The SEIT obligation under this warranty is limited to repairing or replacing, at its own sole option, any such defective products. Repair or replacement of a defective product or parts thereof does not extend the original warranty period.

This warranty applies only to the original purchaser who must have properly registered the product within 10 days of purchase. Products may be registered online at warranty.apc.com.

SEIT shall not be liable under the warranty if its testing and examination disclose that the alleged defect in the product does not exist or was caused by end user's or any third person's misuse, negligence, improper installation, testing, operation or use of the product contrary to SEIT's recommendations or specifications. Further, SEIT shall not be liable for defects resulting from: 1) unauthorized attempts to repair or modify the product, 2) incorrect or inadequate electrical voltage or connection, 3) inappropriate on site operation conditions, 4) Acts of God, 5) exposure to the elements, or 6) theft. In no event shall SEIT have any liability under this warranty for any product where the serial number has been altered, defaced, or removed.

EXCEPT AS SET FORTH ABOVE, THERE ARE NO WARRANTIES, EXPRESS OR IMPLIED, BY OPERATION OF LAW OR OTHERWISE, APPLICABLE TO PRODUCTS SOLD, SERVICED OR FURNISHED UNDER THIS AGREEMENT OR IN CONNECTION HEREWITH.

SEIT DISCLAIMS ALL IMPLIED WARRANTIES OF MERCHANTABILITY, SATISFACTION AND FITNESS FOR A PARTICULAR PURPOSE.

SEIT EXPRESS WARRANTIES WILL NOT BE ENLARGED, DIMINISHED, OR AFFECTED BY AND NO OBLIGATION OR LIABILITY WILL ARISE OUT OF, SEIT'S RENDERING OF TECHNICAL OR OTHER ADVICE OR SERVICE IN CONNECTION WITH THE PRODUCTS.

THE FOREGOING WARRANTIES AND REMEDIES ARE EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES AND REMEDIES. THE WARRANTIES SET FORTH ABOVE CONSTITUTE SEIT'S SOLE LIABILITY AND PURCHASER'S EXCLUSIVE REMEDY FOR ANY BREACH OF SUCH WARRANTIES. SEIT WARRANTIES EXTEND ONLY TO ORIGINAL PURCHASER AND ARE NOT EXTENDED TO ANY THIRD PARTIES.

IN NO EVENT SHALL SEIT, ITS OFFICERS, DIRECTORS, AFFILIATES OR EMPLOYEES BE LIABLE FOR ANY FORM OF INDIRECT, SPECIAL, CONSEQUENTIAL OR PUNITIVE DAMAGES, ARISING OUT OF THE USE, SERVICE OR INSTALLATION OF THE PRODUCTS, WHETHER SUCH DAMAGES ARISE IN CONTRACT OR TORT, IRRESPECTIVE OF FAULT, NEGLIGENCE OR STRICT LIABILITY OR WHETHER SEIT HAS BEEN ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH DAMAGES. SPECIFICALLY, SEIT IS NOT LIABLE FOR ANY COSTS, SUCH AS LOST PROFITS OR REVENUE, WHETHER DIRECT OR INDIRECT, LOSS OF EQUIPMENT, LOSS OF USE OF EQUIPMENT, LOSS OF SOFTWARE, LOSS OF DATA, COSTS OF SUBSTITUANTS, CLAIMS BY THIRD PARTIES, OR OTHERWISE.

NOTHING IN THIS LIMITED WARRANTY SHALL SEEK TO EXCLUDE OR LIMIT SEIT'S LIABILITY FOR DEATH OR PERSONAL INJURY RESULTING FROM ITS NEGLIGENCE OR ITS FRAUDULENT MISREPRESENTATION OF TO THE EXTENT THAT IT CANNOT BE EXCLUDED OR LIMITED BY APPLICABLE LAW.

To obtain service under warranty you must obtain a Returned Material Authorization (RMA) number from customer support. Customers with warranty claims issues may access the SEIT worldwide customer support network through the SEIT Web site: **www.apc.com**. Select your country from the country selection drop down menu. Open the Support tab at the top of the web page to obtain information for customer support in your region. Products must be returned with transportation charges prepaid and must be accompanied by a brief description of the problem encountered and proof of date and place of purchase.

APC by Schneider Electric
Worldwide Customer Support

Customer support for this or any other APC by Schneider Electric product is available at no charge in any of the following ways:

- Visit the APC by Schneider Electric Web site to access documents in the APC by Schneider Electric Knowledge Base and to submit customer support requests.
  - **www.apc.com** (Corporate Headquarters)
    Connect to localized APC by Schneider Electric Web sites for specific countries, each of which provides customer support information.
  - **www.apc.com/support/**
    Global support searching APC by Schneider Electric Knowledge Base and using e-support.
- Contact the APC by Schneider Electric Customer Support Center by telephone or e-mail.
  - Local, country specific centers: go to **www.apc.com/support/contact** for contact information.
  - For information on how to obtain local customer support, contact the APC by Schneider Electric representative or other distributors from whom you purchased your APC by Schneider Electric product.

Select models are ENERGY STAR® qualified.
For more information go to www.apc.com/site/recycle/index.cfm/energy-efficiency/energy-star/

This Page Left Intentionally Blank

Installation Guide Smart-UPS™ 750/1000/1500/2200/3000 VA 100/120/230 Vac Rack-Mount 2U

Important Safety Messages

Read the instructions carefully to become familiar with the equipment before trying to install, operate, service or maintain it. The following special messages may appear throughout this manual or on the equipment to warn of potential hazards or to call attention to information that clarifies or simplifies a procedure.

The addition of this symbol to a Caution product safety label indicates that an electrical hazard exists which will result in personal injury if the instructions are not followed.

The following safety messages may appear throughout this manual to warn of potential hazards.

⚠ CAUTION
CAUTION indicates a potentially hazardous situation which, if not avoided, **can result in** equipment damage and minor or moderate injury.

CAUTION
CAUTION indicates a potentially hazardous situation which, if not avoided, **can result in** equipment damage.

Safety and General Information

Inspect the package contents upon receipt. Notify the carrier and dealer if there is any damage.

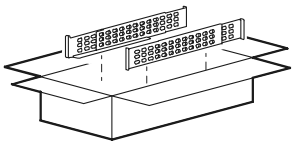
Read the Safety Guide supplied with this unit before installing the UPS.

- Adhere to all national and local electrical codes.
- This UPS is intended for indoor use only.
- Do not operate this UPS in direct sunlight, in contact with fluids, or where there is excessive dust or humidity.
- Be sure the air vents on the UPS are not blocked. Allow adequate space for proper ventilation.
- The battery typically lasts for two to five years. Environmental factors impact battery life. Elevated ambient temperatures, poor quality utility power, and frequent short duration discharges will shorten battery life.
- Connect the UPS power cable directly to a wall outlet. Do not use surge protectors or extension cords.
- The equipment is heavy. Always practice safe lifting techniques adequate for the weight of the equipment.
- The batteries are heavy. Remove the batteries before installing the UPS and XLBP in a rack.
- Always install external battery packs (XLBPs) at the bottom in rack-mount or stack configurations. The UPS must be installed above the XLBPs.
- Always install peripheral equipment above the UPS in rack-mount or stack configurations.
- The UPS will recognize as many as 10 external battery packs connected to the UPS. However there is no limit to the number of XLBPs that can be used with the UPS.
- The model and serial numbers are located on a small, rear panel label. For some models, an additional label is located on the chassis under the front bezel.
- Always recycle used batteries.
- Recycle the package materials or save them for reuse.

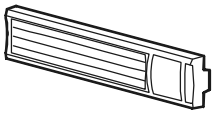
Inventory

All models

(1)

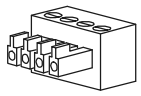


(1)



(1)

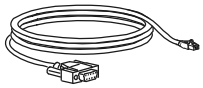
2200/3000 VA models



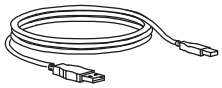
(1)

120/208/230 Vac models

(1)

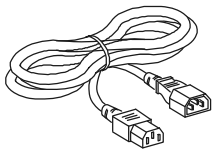


(1)

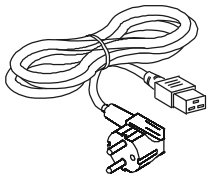


(1)

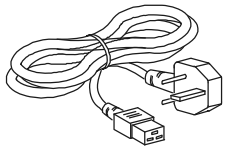
230 Vac models



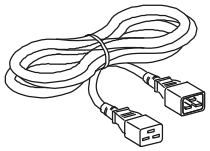
(2)



(1)
2200/3000 VA models



(1)
2200/3000 VA models



(1)
2200/3000 VA models

Installation

⚠ CAUTION

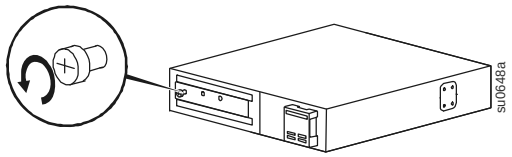
DAMAGE TO EQUIPMENT OR PERSONNEL

- The equipment is heavy. Always practice safe lifting techniques adequate for the weight of the equipment.
- Remove the battery before installing the UPS in a rack.
- When installing equipment in a rack, always install the UPS at the bottom of the rack with the peripheral equipment above the UPS.
- The UPS should always be installed below peripheral equipment in stack or rack configurations.

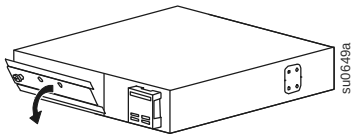
Failure to follow these instructions can result in equipment damage and minor or moderate injury

750 VA models

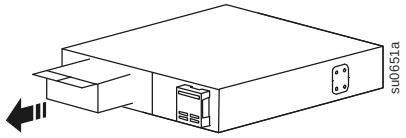
❶



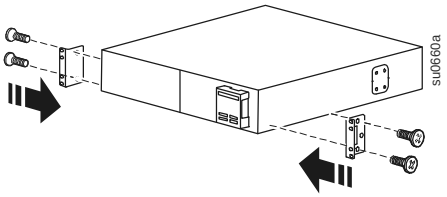
❷



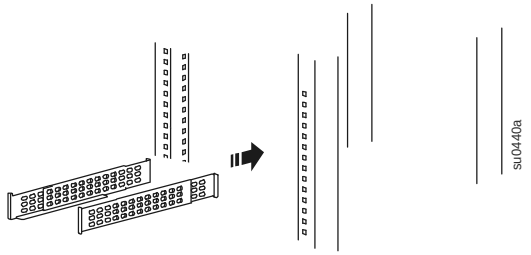
❸



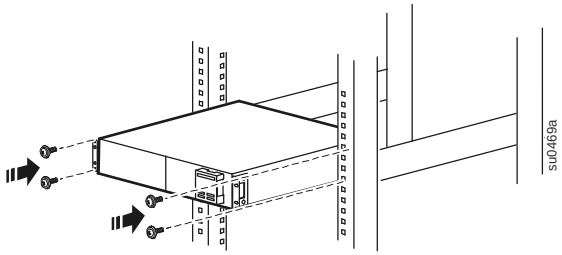
❹



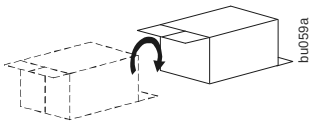
❺



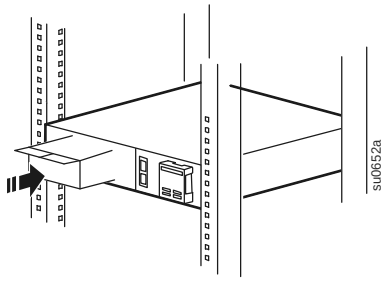
❻



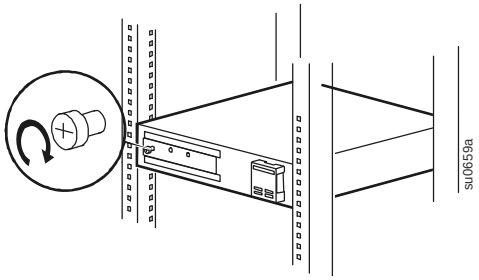
❼



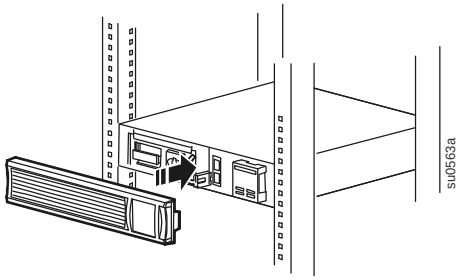
❽



❾

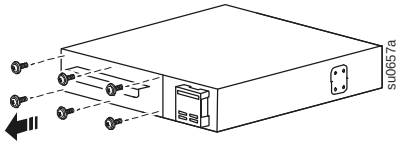


❿

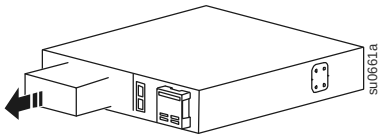


1000/1500 VA models

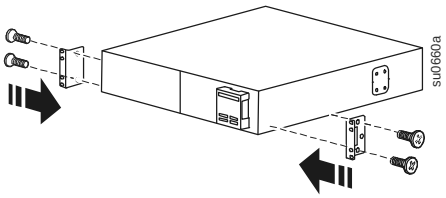
❶



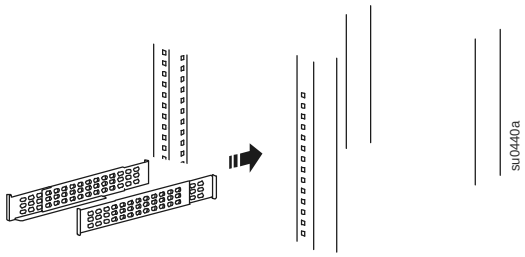
❷



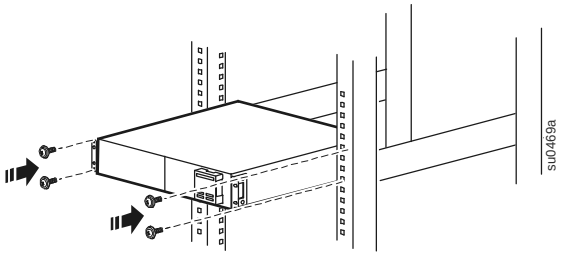
❸



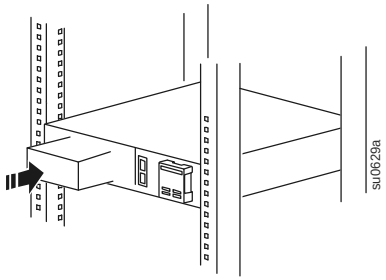
❹



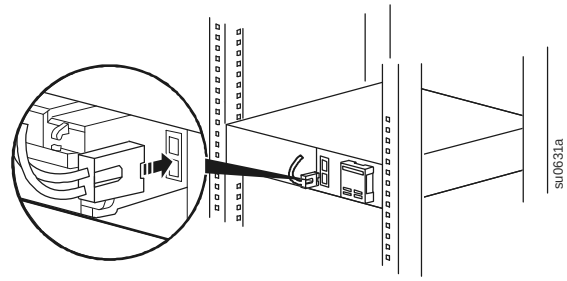
❺



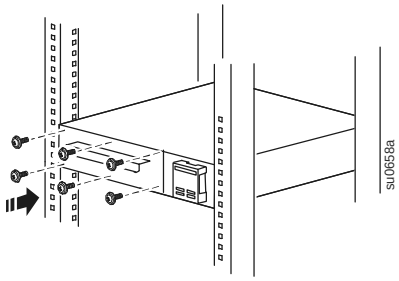
❻



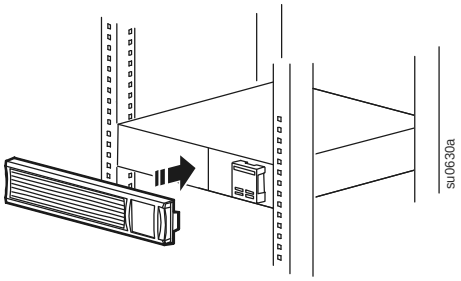
❼



❽

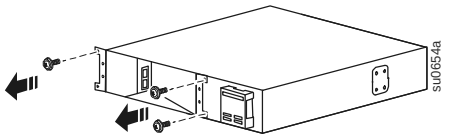


❾

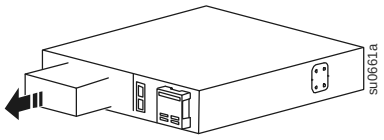


2200/3000 VA models

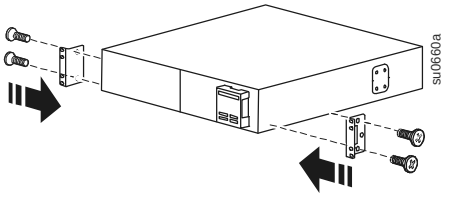
❶



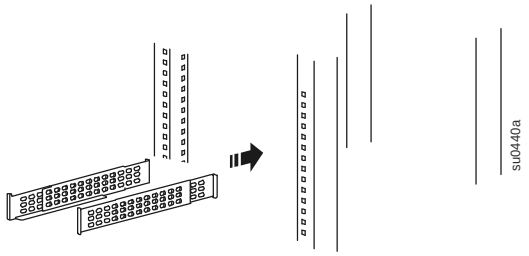
❷



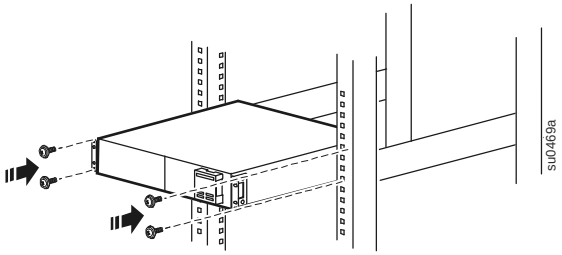
❸



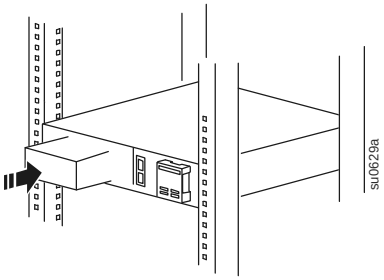
❹



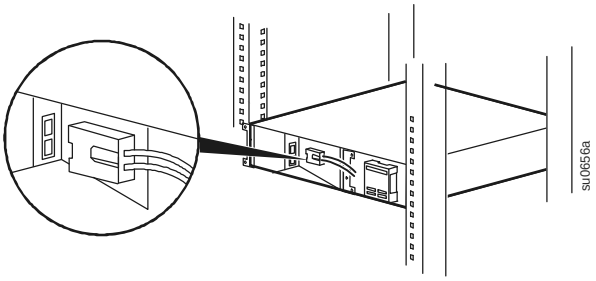
❺



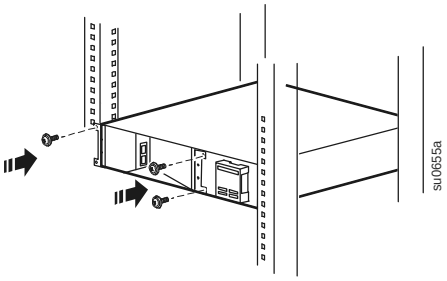
❻



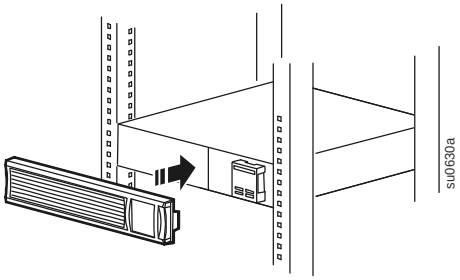
❼



❽



❾

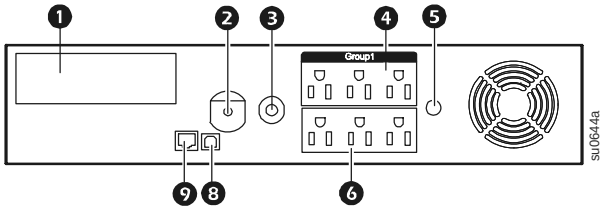


Overview and Start Up

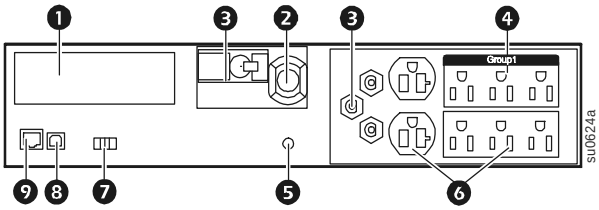
Rear panel features

1. SmartSlot for optional NMC accessory card
2. UPS input
3. Circuit breaker/Overload protection
4. Controlled outlet group
5. Chassis ground screw
6. Outlets
7. EPO connector
8. USB port
9. RJ45 connector - UPS monitoring serial port

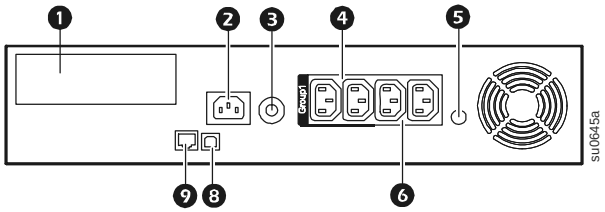
750/1000 VA 120 Vac
1500 VA 100/120 Vac



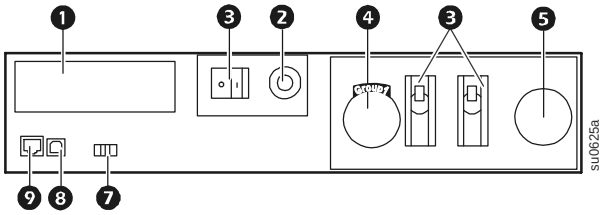
3000 VA 100/120 Vac



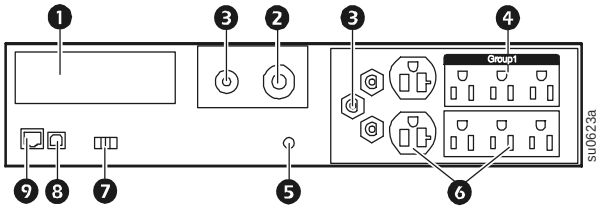
750/1000/1500 VA 230 Vac



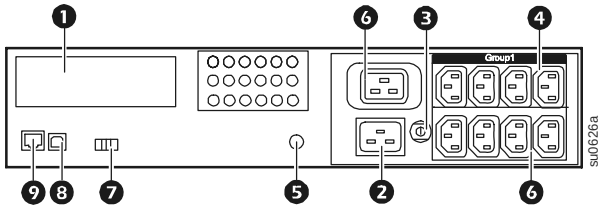
3000 VA 208 Vac



2200 VA 120 Vac



2200/3000 VA 230 Vac



Electrical connections

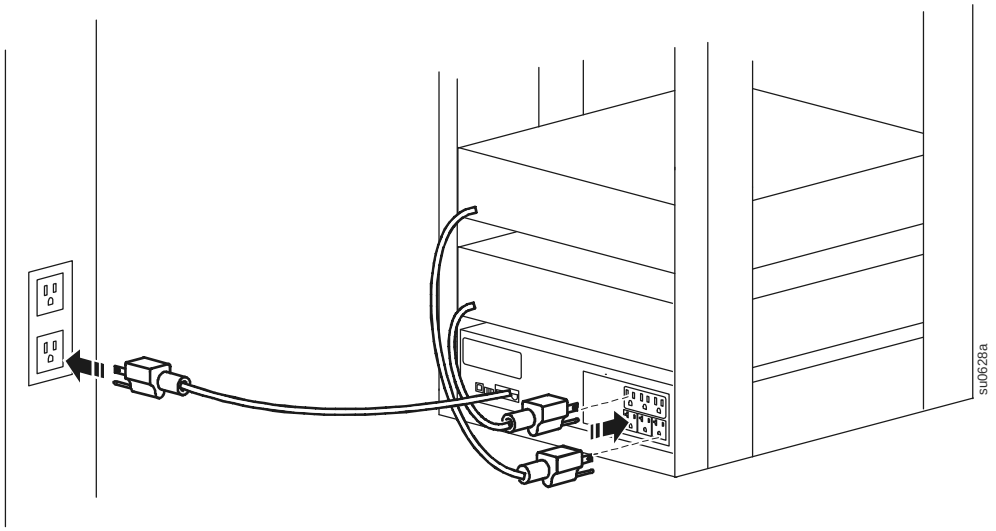
⚠ CAUTION

DAMAGE TO EQUIPMENT OR PERSONNEL

- Adhere to all local and national electrical codes.
- Wiring should be performed by qualified electrician.
- Always connect the UPS to a grounded outlet.

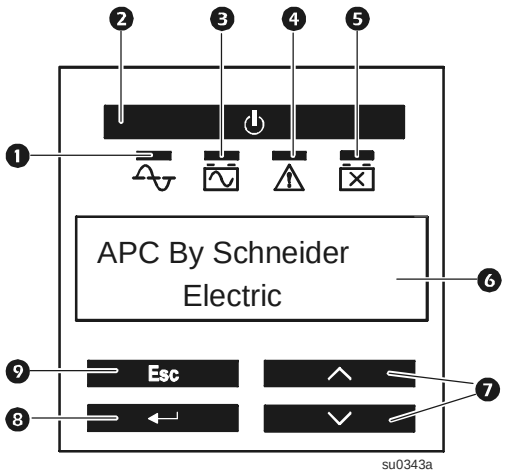
Failure to follow these instructions can result in equipment damage and minor or moderate injury

Plug type and connector locations may vary.



Display panel features

1. **Online** LED
2. UPS ON/OFF key
3. **On Battery** LED
4. **Site Wiring Fault** LED
5. **Replace Battery** LED
6. Display interface
7. UP/DOWN arrow keys
8. ENTER key
9. ESCAPE key



Controlled outlet groups

Some UPS models have one bank of outlets that can function as a controlled group. Use the display interface to configure the controlled outlet features, navigate to:
Main Menu > Control > Outlet1 Control.

Select models are ENERGY STAR® qualified.
For more information go to www.apc.com/site/recycle/index.cfm/energy-efficiency/energy-star/

EN 990-3892C
10/2014

UNINTERRUPTABLE POWER SOURCE (UPS), 865W, CCTV WORKSTATION

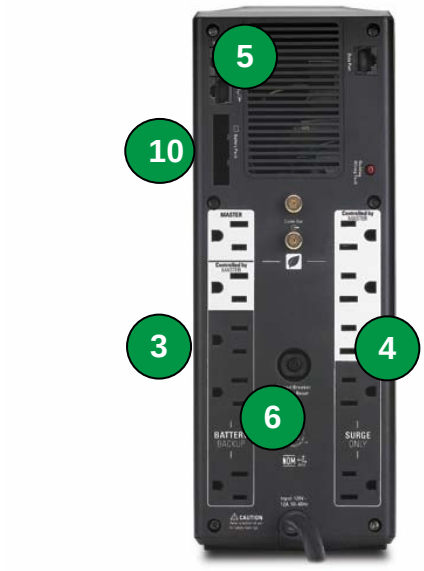
Operations & Maintenance Manual
December 2015

APC Back-UPS® Pro 1300/1500

Power-Saving, high performance power protection for office computers

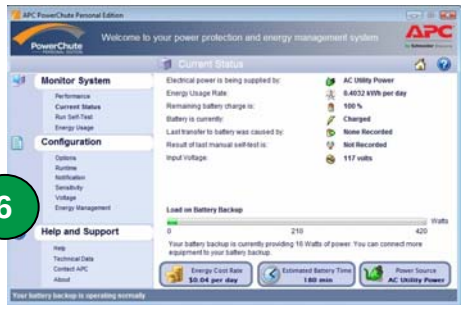
The Back-UPS Pro provides abundant battery backup power, so you can work through medium and extended length power outages. It safeguards your equipment against damaging surges and spikes that travel along utility and data lines. The Back-UPS Pro also features automatic voltage regulation (AVR), which instantly adjusts high and low voltages to safe levels, so you can work indefinitely during brownouts and overvoltages.

The Back-UPS Pro also includes unique “green” features, like power-saving outlets that automatically turn off idle peripherals. A high efficiency charging system and “AVR Bypass” also reduce power consumption. With the rest of the Back-UPS Pro’s standard features, this is the perfect unit to protect your productivity from the constant threat of bad power and lost data.



Product Features:

1. **LCD (Liquid Crystal Display)** gives the status of over 20 different utility and battery backup conditions.
2. **Automatic Voltage Regulation (AVR)** instantly corrects voltage fluctuations so you can work indefinitely through brownouts and overvoltages.
3. **5 “Battery Backup & Surge Protected” Outlets** keep a CPU, monitor and other critical devices running when the power goes out or fluctuates outside safe levels. (Includes one power-saving “*Controlled*” outlet).
4. **5 “Surge Only” Outlets** protect printers, faxes or other equipment without reducing battery capacity. (Includes three power-saving “*Controlled*” outlets).
5. **Data Line Surge Protection** guards against surges and spikes traveling over Ethernet or coax cable lines.
6. **PowerChute Software** lets you use your computer to access additional power protection and management features:
   - Preserves your work, shuts down system during outages
   - Restarts your system, minimizing work disruptions
   - Enables customization of your Back-UPS settings
   - Monitors and displays power and battery status
7. **Push Button Circuit Breaker** enables quick recovery from overloads.
8. **3 Yr Warranty**, $150,000 Equipment Protection Policy, free technical support and data recovery services.
9. **Automatic Diagnostic Testing** ensures your unit is ready when you need it.
10. **External Battery Pack Compatibility** allows you to dramatically increase your run time. (BR1500G only)



by Schneider Electric

Back-UPS Pro 1300 & 1500 Specifications

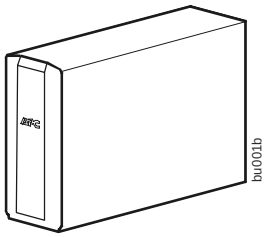
Model Number	BR1300G	BR1500G
Output		
Output Capacity	1300 VA / 780 Watts	1500 VA / 865 Watts
Output Volt., Freq. (on utility)	120V, 50 or 60 Hz, +/- 3Hz (auto sensing)	120V, 50 or 60 Hz, +/- 3Hz (auto sensing)
Output Volt., Freq. (on battery)	115V +/-8%, 50 or 60Hz +/-1Hz (auto sensing)	115V +/-8%, 50 or 60Hz +/-1Hz (auto sensing)
Output Connections	10 total NEMA 5-15R outlets: 5 battery & surge (incl. 1 *Master* & 1 *Controlled)* 5 surge protection only (incl. 3 *Controlled* outlets)	10 total NEMA 5-15R outlets: 5 battery & surge (incl. 1 *Master* & 1 *Controlled*) 5 surge protection only (incl. 3 *Controlled* outlets)
Waveform Type	Stepped Approximation to Sine Wave	Stepped Approximation to Sine Wave
Input		
Input Voltage, Frequency	120V, 50 or 60 Hz, +/- 3 Hz	120V, 50 or 60 Hz, +/- 3 Hz
Input Connection	6 ft cord with NEMA 5-15 plug	6 ft cord with NEMA 5-15 plug
Surge Protection		
AC Power Surge Protection	All outlets	All outlets
Data Line Surge Protection	Network: 10/100/1000 Base-T (gigabit) Ethernet Coax cable (CATV, SATV, modem, A/V)	Network: 10/100/1000 Base-T (gigabit) Ethernet Coax cable (CATV, SATV, modem, A/V)
Physical		
Unit Dimensions (H x W x D)	11.9 x 4.4 x 15.0“ (30.2 x 11.2 x 38.1 cm)	11.9 x 4.4 x 15.0“ (30.2 x 11.2 x 38.1 cm)
Unit Weight	28.3 lbs (12.9 kg)	29.4 lbs (13.4 kg)
Shipping Dims. (H x W x D)	15.0 x 9.25 x 19.0“ (38.1 x 22.9 x 48.3 cm)	15.0 x 9.25 x 19.0“ (38.1 x 22.9 x 48.3 cm)
Shipping Weight	30.8 lbs (14.0 kg)	31.9 lbs (14.5 kg)
Color	Black	Black
UPC Code	731304268765	731304268772
Battery		
Battery Type	Sealed, lead-acid, maintenance-free	Sealed, lead-acid, maintenance-free
Extended run battery pack compatibility	No	Yes p/n: BR24BPG
Management		
Alarms	Visual (LCD) and audible alarms	Visual (LCD) and audible alarms
Auto-Shutdown Software	PowerChute Personal Edition (via USB and serial interface)	PowerChute Personal Edition (via USB and serial interface)
Safety		
Certification/Approvals	FCC Part 15 Class B, NOM, TUV, UL1778	FCC Part 15 Class B, NOM, TUV, UL1778

APC *by Schneider Electric*
132 Fairgrounds Rd
West Kingston, RI 02892
Tel: 800-800-4272
www.apc.com

This Page Left Intentionally Blank

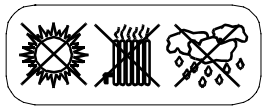
Back-UPS®Pro 1300/1500 Installation and Operation

Inventory



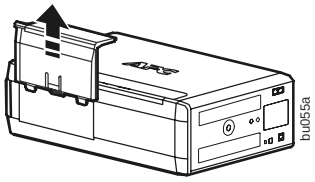
Safety

Do not install the Back-UPS in direct sunlight, in excessive heat, humidity, or in contact with fluids.

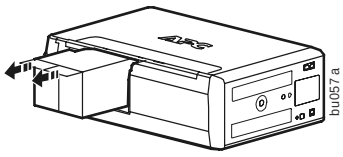


Connect the battery

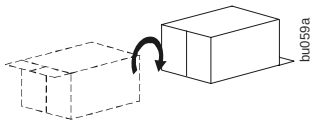
❶



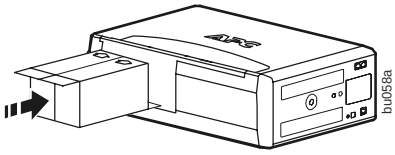
❷



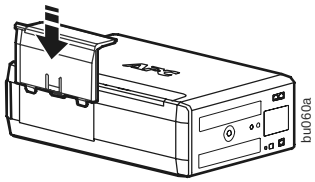
❸



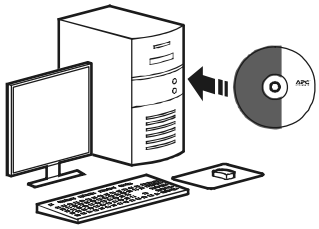
❹



❺



Install PowerChute® Personal Edition Software



APC PowerChute Personal Edition software provides automatic file saving and shutdown of your computer in the event of a power failure. Use the cable supplied with the Back-UPS to connect the data port on the Back-UPS to the USB port on your computer. Place the CD into your computer, and follow the on-screen instructions.

Connect the equipment

Battery Backup and Surge Protected outlets

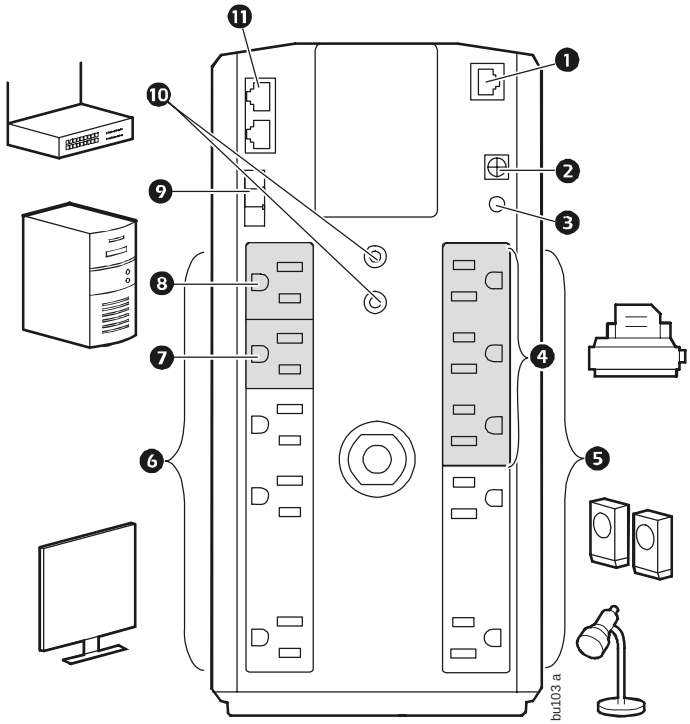
When the Back-UPS is receiving input power, the Battery Backup with Surge Protection outlets will supply power to connected equipment. During a power outage or other utility problems, the Battery Backup outlets receive power for a limited time from the Back-UPS.

Connect equipment such as printers, fax machines, scanners, or other peripherals that do not need battery backup power to the Surge Protection Only outlets. These outlets provide full-time protection from surges even if the Back-UPS is switched OFF.

Master and Controlled outlets

To conserve electricity, when the device connected to Master Outlet goes into Sleep or Standby mode, or turns Off, the Controlled device(s) will shut down as well, saving electricity.

Connect a master device, such as a desktop computer or audio/visual receiver to the Master outlet. Connect peripheral devices such as a printer, speakers, or a scanner to the Controlled outlets.



❶	**USB and Serial Data port**	To use PowerChute Personal Edition, connect a serial cable or USB cable.
❷	**Ground screw**	Connect the ground lead of additional surge suppression devices such as network and data line surge protectors.
❸	**Building Wiring Fault indicator**	If this indicator is illuminated, there is a problem with the wiring in the building. Contact an electrician immediately and do not use the Back-UPS.
❹	**Surge Protected outlets, controlled by the Master outlet**	These outlets are protected from electrical surges, and will disconnect from utility power during a power outage, or if the Master device goes into Sleep or Standby mode.
❺	**Surge Protected outlets**	These outlets provide full-time protection from surges, even if the Back-UPS is off. Connect equipment such as printers and scanners that do not require battery backup protection.
❻	**Battery Backup outlets with Surge Protection**	During a power outage or other utility problems, the Battery Backup outlets receive power for a limited time from the Back-UPS. Connect critical equipment such as desktop computer, computer monitor, modem or other data sensitive devices into these outlets.
❼	**Battery Backup outlets with Surge Protection, controlled by the Master outlet**	These outlets will supply battery power to the connected equipment during a power outage. Power will be disconnected to these outlets if the Master device goes into Sleep or Standby mode. Connect equipment such as a computer monitor to these outlets.
❽	**Master outlet**	Connect the master device to this outlet, in most scenarios, this will be the main computer.
❾	**External Battery Pack connector**	Connect an external battery pack to provide additional battery backup runtime (Back-UPS RS 1500 only).
❿	**Co-axial ports with surge protection**	Connect a cable modem or other equipment with coaxial jacks.
⓫	**In & Out Ethernet surge-protected ports**	Use an ethernet cable to connect a cable modem to the IN port, and connect a computer to the OUT port.

Operation

Power-Saving Function

To conserve electricity, configure the Back-UPS to recognize a Master device, such as a desktop computer or an A/V receiver, and Controlled peripheral devices, such as a printer, speakers, or a scanner. When the Master device goes into Sleep or Standby mode, or is switched OFF, the Controlled device(s) will be switched off as well, saving electricity.

Enable the Power-Saving function. Press and hold MUTE and DISPLAY simultaneously for two seconds. The Back-UPS will beep to indicate that the feature is enabled. The leaf icon on the display will illuminate.

Disable the Power-Saving function. Press and hold MUTE and DISPLAY simultaneously for two seconds. The Back-UPS will beep to indicate that the feature is disabled. The leaf icon on the display will darken.

Setting the threshold. The amount of power used by a device in Sleep or Standby mode varies between devices. It may be necessary to adjust the threshold at which the Master outlet signals the Controlled outlets to shut down.

1. Ensure a master device is connected to the Master outlet. Put that device into Sleep or Standby mode, or turn it OFF.
2. Press DISPLAY and MUTE simultaneously and hold for six seconds, until the leaf icon flashes three times and the Back-UPS beeps three times.
3. The Back-UPS will now recognize the threshold level of the Master device and save it as the new threshold setting.

Power-Saving Display

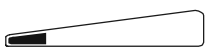
The display interface can be configured to be continuously illuminated, or to save energy, it can be configured to darken after a period of inactivity.

1. Full Time Mode: Press and hold DISPLAY for two seconds. The display will illuminate and the Back-UPS will beep to confirm the Full-Time mode.
2. Power-Saving Mode: Press and hold DISPLAY for two seconds. The display will darken and the Back-UPS will beep to confirm the Power-Saving mode. While in Power-Saving Mode, the display will illuminate if a button is pressed, it then darkens after 60 seconds of no activity.

Unit sensitivity

Adjust the sensitivity of the Back-UPS to control when it will switch to battery power; the higher the sensitivity, the more often the Back-UPS will switch to battery power.

1. Ensure the Back-UPS is connected to utility power, but is OFF.
2. Press and hold the POWER button for six seconds. The LOAD CAPACITY bar will flash on and off, indicating that the Back-UPS is in programming mode.
3. Press POWER again to rotate through the menu options. Stop at selected sensitivity. The Back-UPS will beep to confirm the selection.

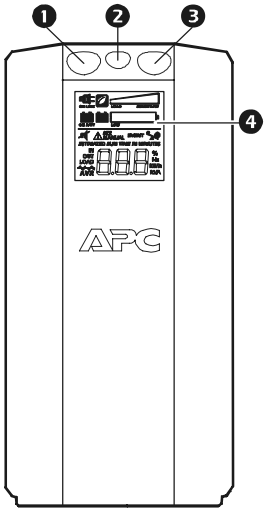
Generator Sensitivity	Default	Sensitive Loads
		
Low sensitivity	Medium sensitivity (Default)	High sensitivity
78-142 Vac	88-139 Vac	88-136 Vac
Input voltage is extremely low or high. (Not recommended for computer loads.)	*The Back-UPS frequently switches to battery power.*	*The connected equipment is sensitive to voltage fluctuations.*

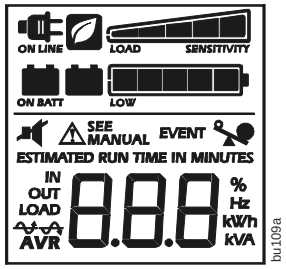
Front Panel Buttons and Display Interface

Use the three buttons on the front panel of the Back-UPS and the display interface to configure the Back-UPS.

Front panel

1. Mute button
2. Power On/Off button
3. Display button
4. Display interface





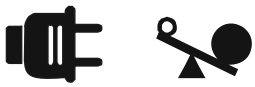
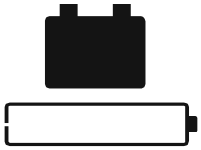
	**On Line—**The Back-UPS is supplying conditioned utility power to connected equipment
	**Power-Saving—**Master and Controlled outlets are enabled, saving power when the master device goes into sleep or standby mode
	**Load Capacity—**The load is indicated by the number of sections illuminated, one to five. Each bar represents 20% of the load.
	**Battery Charge—**The battery charge level is indicated by the number of sections illuminated. When all five blocks are illuminated, the Back-UPS is at full charge. When one block is filled, the Back-UPS is near the end of its battery capacity, the indicator will flash and the Back-UPS will beep continuously.
	**Overload—**The power demand from the load has exceeded the capacity of the Back-UPS.
EVENT	**Event—**The event counter shows the number of events that occurred that caused the Back-UPS to switch to on-battery operation.
	**Automatic Voltage Regulation**—The Back-UPS can compensate for high or low input voltage.  When illuminated, the Back-UPS is compensating for low input voltage.  When illuminated, the Back-UPS is compensating for high input voltage.
IN OUT	**In—**Input voltage. **Out—**Output voltage.
	**System Faults—**The system has a fault. The fault number will illuminate on the display interface. See “System Faults” on page 5.
	**Mute—**If the line through the speaker icon is illuminated, the audible alarm has been turned off.
	**Replace Battery—**The battery is not connected or is nearing the end of its useful life. Replace the battery.
	**On Battery—**The Back-UPS is supplying battery backup power to the connected equipment, it will beep four times every 30 seconds.

Warnings and System Faults

Audible Warnings

Four Beeps Every 30 Seconds	Back-UPS is running on battery. You should consider saving any work in progress.
Continuous Beeping	Low battery condition and battery run-time is very low. Promptly save any work in progress, exit all open applications, and shut down the operating system.
Continuous tone	Battery Backup outputs are overloaded.
Chirps for 1 Minute every 5 hours	Battery fails the automatic diagnostic test and should be replaced.

Warning Icons

If these icons are illuminated...	This may be the problem.
	The Back-UPS is operating on utility power, but is overloaded. Disconnect one of the items connected to the Back-UPS. If the Overload icon stops flashing, the Back-UPS is no longer overloaded and will continue to operate normally.
	The Back-UPS is operating on battery power, but is overloaded. Disconnect one of the items connected to the Back-UPS. If the Overload icon stops flashing, the Back-UPS is no longer overloaded and will continue to operate normally.
	The Back-UPS is operating on utility power, but the battery is not functioning properly. Contact APC Customer Service to order a replacement battery. See “Replacement Battery” on page 8.
	The Back-UPS is operating on battery power and the battery power is getting low. Shut down all connected equipment to avoid losing an unsaved data. When possible, connect the Back-UPS to utility power to recharge the batter.

System Faults

The Back-UPS will display these fault messages. For faults F01 and F02, contact APC Technical Support.

F01	On-Battery Overload	Turn the Back-UPS off. Disconnect non-essential equipment from the Battery Backup outlets and the turn Back-UPS on.
F02	On-Battery Output Short	Turn the Back-UPS off. Disconnect non-essential equipment from the Battery Backup outlets and the turn Back-UPS on.
F03	On-Battery Xcap Overload	Faults F03-F09 cannot be corrected by the user, contact APC Technical Support for assistance.
F04	Clamp Short	
F05	Charge Fault	
F06	Relay Welding	
F07	Temperature	
F08	Fan Fault	
F09	Internal Fault	

Function Button Quick-Reference

Function	Button	Timing (seconds)	UPS Status	Description
Power				
Power On		0.2	Off	Press POWER to start receiving input utility power. If A/C input power is not available, the Back-UPS will run on battery power.
Power Off		2	On	The Back-UPS is not receiving input utility power, but is providing surge protection.
Display				
Status Inquiry		0.2	On	Verify the status or condition of the Back-UPS. The LCD will illuminate for 60 seconds.
Full-Time/Power-Saving mode		2	On	The LCD will illuminate and the Back-UPS will beep to confirm the Full-Time mode. The LCD will darken and the Back-UPS will beep to confirm the Power-Saving mode. While in Power-Saving Mode, the LCD will illuminate if a button is pressed, then darkens after 60 seconds of no activity.
Mute				
Event Specific		0.2	On	Disable any audible alarms caused by an event.
General Status Enable/ Disable		2	On	Enable or disable the audible alarms. The Mute icon will illuminate and the Back-UPS will beep one time. The Mute function will not activate unless the Back-UPS is operating on battery power.
Sensitivity		6	Off	The Load Capacity icon will blink, indicating that the Back-UPS is in programming mode. Use the POWER button to scroll through Low, Medium, and High, stop at selected sensitivity. The Back-UPS will beep to confirm selection. See Configuration for details.
Master/Controlled outlet Enable/Disable		2	On	The leaf icon will darken indicating that the Master Outlet feature is disabled or illuminate to indicate the Master Outlet feature is enabled. The Back-UPS will beep once.
Master/Enable Threshold Calibration		6	On	While calibrating the threshold setting, the device connected to the Master Outlet should be turned off or placed in Standby or Sleep mode. Upon completion, Power-Saving icon will flash 3 and beep 3 times.
Self-Test (manual)		6	On	The Back-UPS will perform a test of the internal battery. Note: This will happen automatically when the Back-UPS is turned ON.
Event Reset		0.2	On	When the Event screen is visible, press and hold DISPLAY, then press POWER, to clear the utility failure event counter.
Fault Reset		2	Fault	After a fault has been identified, press POWER to remove the visual indication and return to standby status.

Troubleshooting

Problem	Possible Cause	Corrective Action
Back-UPS will not switch on.	The Back-UPS is not connected to utility power.	Ensure that the Back-UPS is securely connected to an AC outlet.
	The circuit breaker has been tripped.	Disconnect non-essential equipment from the Back-UPS. Reset the circuit breaker. Re-connect equipment one item at a time. If the circuit breaker is tripped again, disconnect the device that caused the trip.
	The internal battery is not connected.	Connect the battery.
	The utility input voltage is out of range.	Adjust the transfer voltage and sensitivity range.
The Back-UPS does not provide power during a utility power outage.	Ensure that essential equipment is **not** plugged into a SURGE ONLY outlet.	Disconnect equipment from the SURGE ONLY outlet and re-connect to a Battery Backup outlet.
The Back-UPS is operating on battery power, while connected to utility power.	The plug has partially pulled out of the wall outlet, the wall outlet is no longer receiving utility power, or the circuit breaker has been tripped.	Ensure that the plug is fully inserted into the wall outlet. Ensure that the wall outlet is receiving utility power by checking it with another device.
	The Back-UPS is performing an automatic self test.	No action is necessary.
	The utility input voltage is out of range, the frequency is out of range, or the waveform is distorted.	Adjust the transfer voltage and sensitivity range.
The Back-UPS does not provide the expected amount of backup time.	Battery Backup outlets may be fully or improperly loaded.	Disconnect non-essential equipment from the Battery Backup outlets and connect the equipment to SURGE ONLY outlets.
	The battery was recently discharged due to a power outage and has not fully recharged.	Charge the battery cartridge for 16 hours.
	The battery has reached the end of its useful life.	Replace the battery.
The REPLACE BATTERY **indicator is illuminated.**	The battery has reached the end of its useful life.	Replace the battery.
The OVERLOAD indicator is illuminated.	The equipment connected to the Back-UPS is drawing more power than the Back-UPS can provide.	Disconnect non-essential equipment from the Battery Backup outlets and connect the equipment to SURGE ONLY outlets.
The SYSTEM FAULT **indicator is illuminated, all the front panel indicators are flashing.**	There is an internal fault.	Determine which internal fault message is displayed by matching the number displayed on the LCD with the corresponding Fault Message (see System Faults) and contact APC Technical Support.
Power is not supplied to some outlets.	Power to the Controlled outlets has intentionally been turned off.	Confirm that the correct peripherals are connected to Controlled outlets. If this feature is not desired, disable the Power-Saving Master and Controlled outlets.
The Controlled outlets are not supplying power, even though the Master device is not in sleep mode.	The Master Outlet threshold may be incorrectly set.	Adjust the threshold when the Master outlet signals the Controlled outlets to shut down.

Specifications

VA	1300 VA / 1500 VA
Maximum Load	780 W / 865 W
Nominal Input Voltage	120 V
Online Input Voltage Range	88 - 139V
Automatic Voltage Regulation	(94-107) +11.5% (126-141) -11/5%
Frequency Range	50/60 Hz ± 1 Hz
On-battery Waveshape	Step-approximated sine-wave
Typical Recharge Time	8 hours
Transfer Time	8 ms, maximum
Operating Temperature	32° to 104°F (0° to 40°C)
Storage Temperature	23° to 113°F (-5° to 45°C)
Unit Dimensions	11.9 × 4.4 × 15.0 in (30.1 × 11.2 × 38.2 cm)
Unit Weight	22.8 lbs (10.4 kg)
Interface	USB and Serial
On-Battery Runtime	Go to: http://www.apc.com/product
EMI Classification	FCC / DOC Class B Certified
Approvals	TUV C-US, NOM

Replacement Battery

The battery cartridge typically lasts 3 to 6 years, a shorter period if subjected to frequent outages or elevated temperatures. For the BR1300G or BR1500G, order part **APCRBC124**. Please recycle spent battery cartridges.

Service

If the Back-UPS arrived damaged, notify the carrier.

If the Back-UPS requires service, do not return it to the dealer.

1. Consult the Troubleshooting section to eliminate common problems.
2. If the problem persists, go to http:// www.apc.com/support/.
3. If the problem still persists, contact APC Technical Support.

Have the Back-UPS model number, serial number and date of purchase available. Be prepared to troubleshoot the problem with an APC Technical Support representative. If this is not successful, APC will issue a Return Merchandise

Authorization (RMA) number and a shipping address.

Warranty

The standard warranty is three (3) years from the date of purchase. APC's standard procedure is to replace the original unit with a factory reconditioned unit. Customers who must have the original unit back due to the assignment of asset tags and set depreciation schedules must declare such a need at first contact with an APC Technical Support representative. APC will ship the replacement unit once the defective unit has been received by the repair department, or cross-ship upon the receipt of a valid credit card number. The customer pays for shipping the unit to APC. APC pays ground freight transportation costs to ship the replacement unit to the customer.

APC Worldwide Customer Support

Internet	http://www.apc.com
Worldwide	+1 800 800 4272

Customer support and warranty information is available at the APC Web site, **www.apc.com**.

This Page Left Intentionally Blank

FLOOR MOUNTED RACK,

24-1/4” W x 32-5/8” D X 83-1/8” H

Operations & Maintenance Manual
December 2015

Middle Atlantic Products

EXCEPTIONAL SUPPORT & PROTECTION™

WRK-SA Series Enclosure

EIA/TIA Compliant | SEISMIC CERTIFIED | c UL us LISTED

Wide stand-alone design ideal for accommodating large cable bundles

Features

- Fully welded construction provides the following weight capacities - UL Listed load capacity: 2,500 lbs - Static load capacity: 10,000 lbs. - Seismic certified load capacity: 900 lbs.
- Pre-configured WRK-24MDK presentation enclosure system available
- Seismic certified (when used with WRK-Z4 option) with an Ip value of 1.5
- 24-1/4" OD width, available 27-5/8" or 32-5/8" OD depth
- 1/2", 3/4", 1" & 1-1/2" electrical knockouts on split rear plates top & bottom, easily removable for cable pass-through, top plates additionally include UHF/VHF knockouts
- 2 extra-wide pairs of 11-gauge 10-32 threaded rackrail with numbered rackspace increments
- Keylocked solid rear door standard, optional vented rear doors available
- Open top with configurable top panel options
- Durable black textured powder coat finish
- UL Listed in the US and Canada

WRK-44SA-32

WRK-24MDK

Architects' and Engineers' Specifications

Stand-alone equipment rack shall be Middle Atlantic Products model # WRK-__ (see chart for available models). Overall dimensions of rack shall be __"H x __"W x __"D (refer to chart). Useable height shall be __ rackspaces, useable depth shall be __" (refer to chart). Fully welded construction shall provide a static load capacity of 10,000 lbs. and a UL Listed 2,500 lb. weight capacity. Top and bottom shall be 14-gauge steel, horizontal braces shall be 16-gauge steel welded to integral structural side panels of 16-gauge steel giving an 1/8" thick structure, all structural elements shall be finished in a durable black powder coat. Rack shall include a locking, latching rear door. Rack shall come equipped with two pairs of 11-gauge steel rackrail with tapped 10-32 mounting holes in universal EIA spacing. Rackrail shall be finished in black e-coat with numbered rackspaces. Top and bottom of rack shall have a vertical slotted vent pattern. The WRK shall have a solid locking rear door. Rack shall have removable split rear knockout panels with 1/2", 3/4", 1", and 1-1/2" electrical knockouts installed in base, and removable split rear knockout panels with electrical knockouts and BNC knockouts for UHF/VHF antennae installed in top. Fully welded sides shall feature vertical vent pattern at top and bottom. Grounding and bonding stud shall be 1/4-20 threaded, installed in base of enclosure. WRK-24MDK shall additionally include a 3/4" thick, graphite-marbled laminate top, skirted wheel-base, latching front plexi door, latching vented rear door and front and rear rackrail. WRK-SA Series enclosures shall satisfy the 2007 & 2010 CBC; 2006, 2009 & 2012 IBC; ASCE 7-05 (2005 Edition) & ASCE 7-10 (2010 Edition) and the 2006 & 2009 editions of NFPA 5000 for use in areas of high seismicity, Seismic Use Group III, Zone 4 or Seismic Design Category (SDC) "D" with lateral force requirements for protecting 900 lbs. of essential equipment in locations with the highest level of seismicity and top floor or rooftop installations with an Importance factor (Ip) of 1.5 when used with WRK-Z4 seismic floor anchor bracket. WRK shall be UL Listed in the US and Canada. WRK shall be GREENGUARD Indoor Air Quality Certified for Children and Schools. WRK shall be RoHS EU Directive 2002/95/EC compliant. WRK shall be manufactured by an ISO 9001 and ISO 14001 registered company. Rack shall be warrantied to be free from defects in material or workmanship under normal use and conditions for the lifetime of the product.

OPTIONS

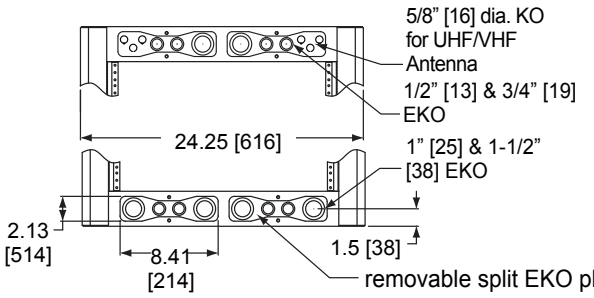
- Front doors shall be 16-gauge reinforced steel, model # FD-XX (solid), VFD-XX (vented, 25% open area), LVFD-XX (vented, 64% open area), PFD- XX(plexi), PVFD-44 (vented plexi) (X=# of rackspaces of WRK rack)
- Vented rear doors shall be 16-gauge steel model # MW-VRD-44 (vented, top and bottom), MW-LVRD-XX (vented 64% open area-excludes 24 and 37 space rack), (X= # of rackspaces of WRK rack), MW-CLVRD-44 (split rear door, vented, 79% open area)
- Top panels multiple styles available in model # MW-ST (solid), #MW-10FT (10" fan), MW-4FT (four 4-1/2" fans), MW-6FT (three 6" fans), MW-VT (vented) and MW-LA (accepts 6" & 12" wide cable ladders). See A&E spec 96-01063 for more details
- Caster base, four casters shall have a total weight capacity of 1300 pounds, model # CBS-WRK-YY (Y= cabinet depth) and be UL Listed in the US and Canada
- Inner platform base (inset base w/out casters) model # BS-WRK-YY (Y= cabinet depth)
- Additional rail kit, 11-gauge, 10-32 threaded, sold in pairs, hardware included, model # WRK-RRXX (X= # of rackspaces)
- AXS slide out option available (See AXS Spec sheet 96-052S)

CUSTOMIZABLE SPECIFICATION CLIPS AVAILABLE AT MIDDLEATLANTIC.COM

US: New Jersey • California • Illinois • Voice: 973-839-1011 Fax: 973-839-1976 • middleatlantic.com
Canada: Ontario • British Columbia • Voice: 613-836-2501 Fax: 613-836-2690 • middleatlantic.ca

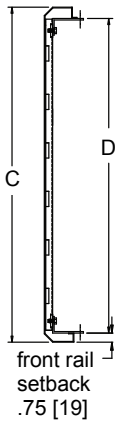
WRK-SA basic dimensions

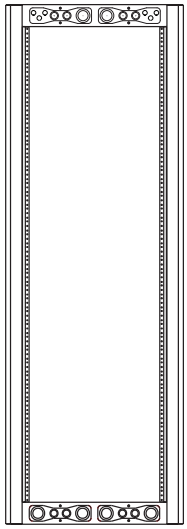
REAR VIEW, TOP & BOTTOM



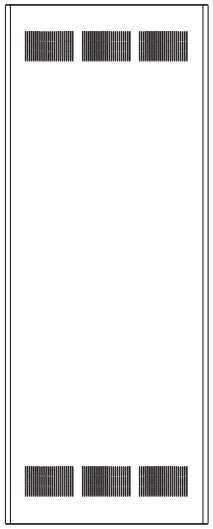
Part #	A OVERALL HEIGHT	B USEABLE HEIGHT	C OVERALL DEPTH	D USEABLE DEPTH	E BASE OPENING DEPTH
WRK-44SA-27	83.125 [2111]	77.125 [1959]	27.625 [702]	25.75 [654]	24.50 [622]
WRK-40SA-27	76.125 [1934]	70.125 [1781]	27.625 [702]	25.75 [654]	24.50 [622]
WRK-37SA-27	70.875 [1800]	64.875 [1648]	27.625 [702]	25.75 [654]	24.50 [622]
WRK-24SA-27	48.125 [1222]	42.125 [1070]	27.625 [702]	25.75 [654]	24.50 [622]
WRK-44SA-32	83.125 [2111]	77.125 [1959]	32.625 [829]	30.75 [781]	29.50 [749]
WRK-40SA-32	76.125 [1934]	70.125 [1781]	32.625 [829]	30.75 [781]	29.50 [749]
WRK-37SA-32	70.875 [1800]	64.875 [1648]	32.625 [829]	30.75 [781]	29.50 [749]
WRK-24SA-32	48.125 [1222]	42.125 [1070]	32.625 [829]	30.75 [781]	29.50 [749]

TOP SIDE SECTIONAL VIEW

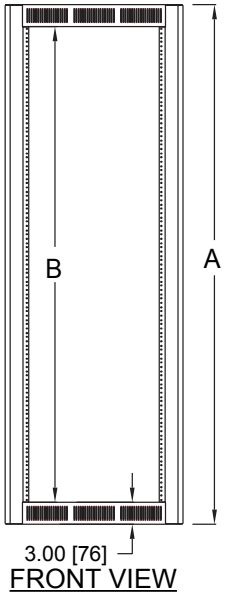




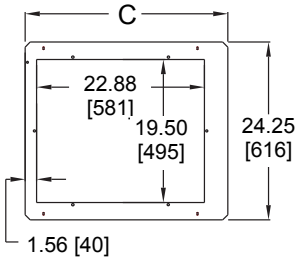
REAR VIEW



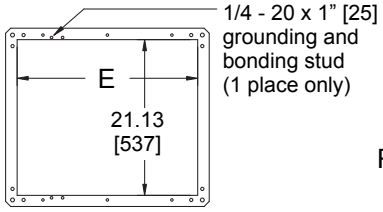
SIDE VIEW



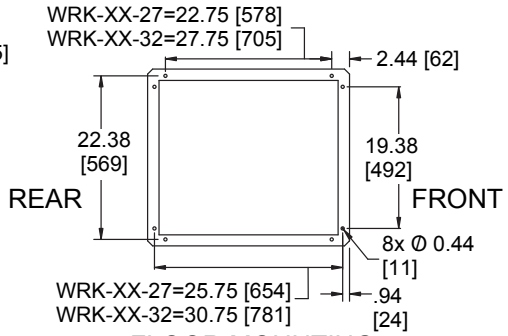
FRONT VIEW



TOP VIEW



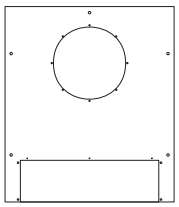
BOTTOM VIEW



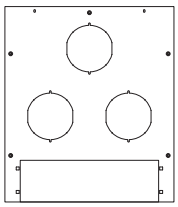
FLOOR MOUNTING LOCATIONS

All dimensions in inches unless otherwise noted [All dimensions in brackets are in millimeters]

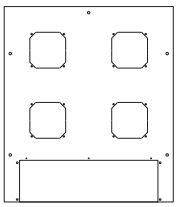
TOP OPTIONS (removable plate opening accommodates 2 space panel)



MW-10FT accepts 10" fan
MW-10FT-550CFM includes 10" fan
MW-10FT-FC includes 10" fan and fan controller

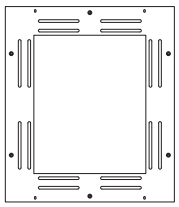


MW-6FT accepts 6" fans
MW-6FT-660CFM includes 6" fans

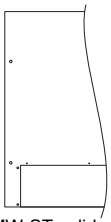


MW-4FT accepts 4-1/2" fans
MW-4FT-380CFM includes 4-1/2" fans MW-4QFT-FC includes 4-1/2" quiet fans and fan controller

accommodates 12" and 6" width cable ladders

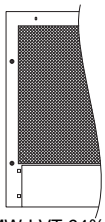


MW-LA accepts 6", 9" and 12" width cable ladder



MW-ST solid

MW-VT slot vent

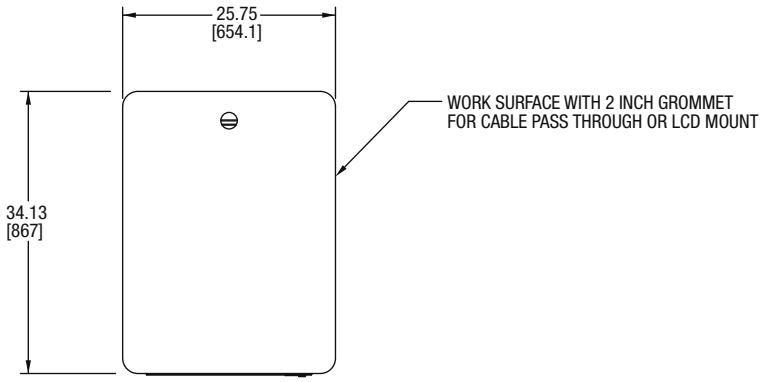


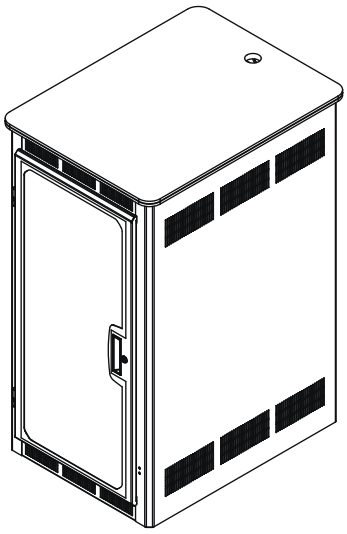
MW-LVT 64% open area

Middle Atlantic Products

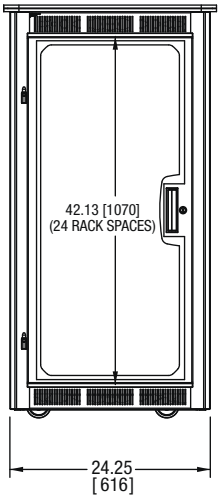
WRK-24MDK basic dimensions

TOP VIEW

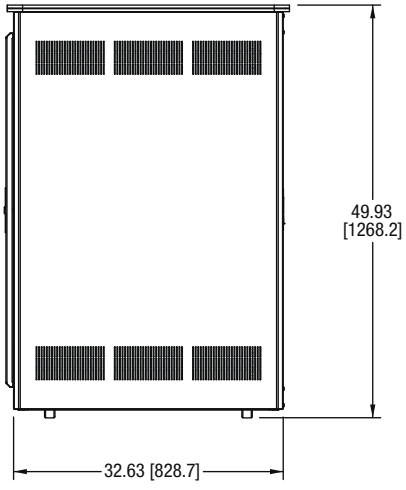




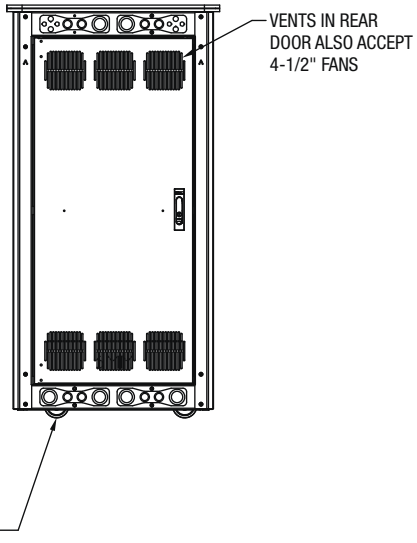
FRONT VIEW



SIDE VIEW



REAR VIEW



All dimensions in inches unless otherwise noted [All dimensions in brackets are in millimeters]

Middle Atlantic Products

This Page Left Intentionally Blank

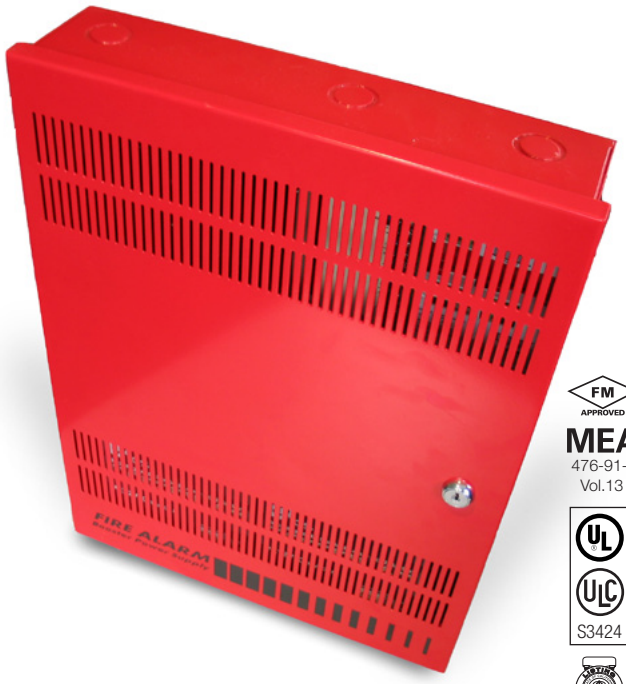
REMOTE BOOSTER POWER SUPPLY, 10 AMP

Operations & Maintenance Manual
December 2015

EST
Life Safety & Communications

Remote Booster Power Supplies

BPS6A, BPS10A



FM APPROVED
MEA 476-91-E Vol.13
UL UL C S3424
7300-1657: 0229

Overview

The Booster Power Supply (BPS) is a UL 864, 9th Edition listed power supply. It is a 24 Vdc filtered-regulated, and supervised unit that can easily be configured to provide additional notification appliance circuits (NACs) or auxiliary power for Mass Notification/ Emergency Communication (MNEC), as well as life safety, security, and access control applications.

The BPS contains the circuitry to monitor and charge internal or external batteries. Its steel enclosure has room for up to two 10 ampere-hour batteries. For access control-only applications, the BPS can support batteries totaling up to 65 ampere-hours in an external enclosure. The BPS has four Class B (convertible to two Class A) NACs. These can be activated in one or two groups from the BPS's unique dual input circuits.

The BPS is available in 6.5 or 10 ampere models. Each output circuit has a capacity of three amperes; total current draw cannot exceed the unit's rating.

The BPS meets current UL requirements and is listed under the following standards:

Standard (CCN)	Description
UL864 9th ed.ition (UOXX)	Fire Alarm Systems
UL636 (ANET, UEHX7)	Holdup Alarm Units and Systems
UL609 (AOTX, AOTX7)	Local Burglar Alarm Units and Systems
UL294 (ALVY, UEHX7)	Access Control Systems
UL365 (APAW, APAW7)	Police Station Connected Burglar Alarm Units and Systems
UL1076 (APOU, APOU7)	Proprietary Burglar Alarm System Units
UL1610 (AMCX)	Central Station Alarm Unit
ULC-S527 (UOXXC)	Control Units, Fire Alarm (Canada)
ULC-S303 (AOTX7)	Local Burglar Alarm Units and Systems (Canada)
C22.2 No. 205	Signaling Equipment (Canada)

Standard Features

- Allows for reliable filtered and regulated power to be installed where needed
- Cost effective system expansion
- Provides for Genesis and Enhanced Integrity notification appliance synchronization
- Supports coded output operation
- Self-restoring overcurrent protection
- Multiple signal rates
- Can be cascaded or controlled independently
- Easy field configuration
- On-board diagnostic LEDs identify wiring or internal faults
- Standard Edwards keyed lockable steel cabinet with removable door
- 110 and 230 Vac models available
- Accommodates 18 to 12 AWG wire sizes
- Optional tamper switch
- Dual battery charging rates
- Optional earthquake hardening: OSHPD seismic pre-approval for component Importance Factor 1.5

Application

The BPS provides additional power and circuits for notification appliances and other 24 Vdc loads. It is listed for indoor dry locations and can easily be installed where needed.

Fault conditions are indicated on the on-board diagnostic LEDs, opening the BPS input sense circuit and the trouble relay (if programmed). While this provides indication to the host system, the BPS can still be activated upon command. A separate AC Fail contact is available on the BPS circuit board, which can be programmed for trouble or AC Fail. There are seven on-board diagnostic LEDs: one for each NAC fault, one for battery fault, one for ground fault, and one for AC power.

The unique dual-input activation circuits of the BPS can be activated by any voltage from 6 to 45 VDC (filtered-regulated) or 11 to 33 Vdc (full-wave rectified, unfiltered). The first input circuit can be configured to activate 1-4 of the four possible outputs. The second input circuit can be configured to control circuits 3 and 4. When outputs are configured for auxiliary operation, these circuits can be configured to stay on or automatically deactivate 30 seconds after AC power is lost. This feature makes these circuits ideal for door holder applications. The BPS also has a separate 200 mA 24 Vdc output that can be used to power internal activation modules.

BPS NACs can be configured for a 3-3-3 temporal or continuous output. California temporal rate outputs are also available on certain models. This makes the BPS ideal for applications requiring signaling rates that are not available from the main system.

In addition to the internally generated signal rates, the BPS can also be configured to follow the coded signal rate of the main system NACs. This allows for the seamless expansion of existing NACs.

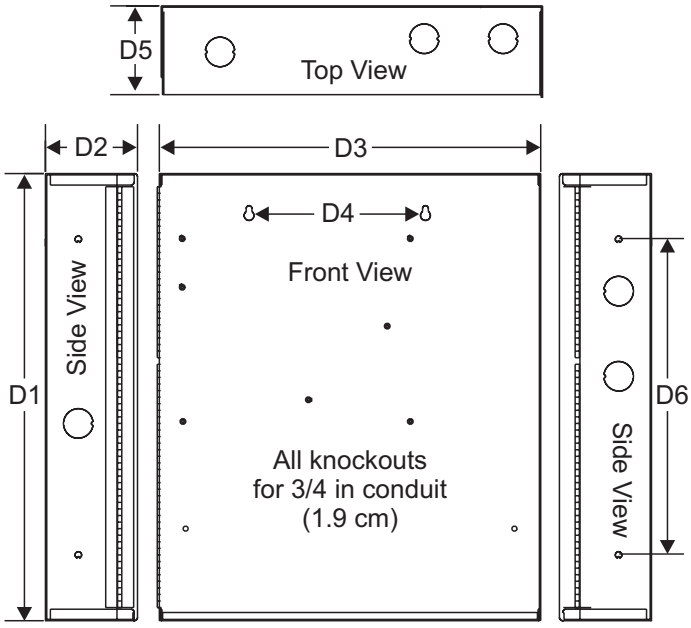
The BPS enclosure has mounting brackets for up to three Signature modules to the right of the circuit board.

Engineering Specification

Supply, where needed, Edwards BPS Series Booster Power Supplies (BPS) that are interconnected to and supervised by the main system. The BPS shall function as a stand-alone auxiliary power supply with its own fully-supervised battery compliment. The BPS battery compliment shall be sized to match the requirements of the main system. The BPS shall be capable of supervising and charging batteries having the capacity of 24 ampere-hours for Mass Notification/Emergency Communication (MNEC), life safety and security applications, and the capacity of 65 ampere-hours for access control applications.

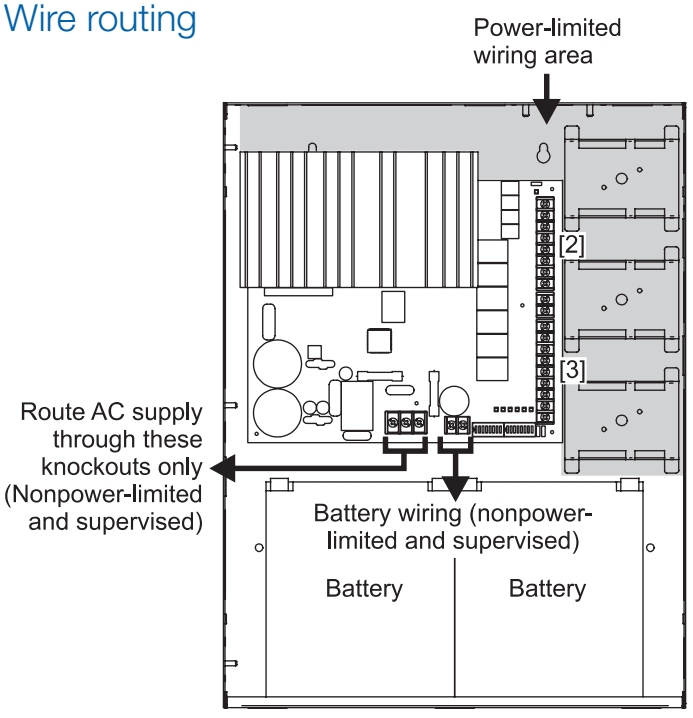
<<The BPS shall be capable of installation for a seismic component Importance Factor of 1.5.>> The BPS shall provide a minimum of four independent, fully supervised Class B circuits that can be field configurable for notification appliance circuits or auxiliary 24 Vdc power circuits. BPS NACs shall be convertible to a minimum of two Class A NACs. Each BPS output circuit shall be rated at 3 amperes at 24 Vdc. Each output circuit shall be provided with automatically restoring overcurrent protection. The BPS shall be operable from the main system NAC and/or Edwards Signature Series control modules. BPS NACs shall be configurable for continuous, 3-3-3 temporal or optionally, California rate. Fault conditions on the BPS shall not impede operation of main system NAC. The BPS shall be provided with ground fault detection circuitry and a separate AC fail relay.

Dimensions



D1	D2	D3	D4	D5	D6
17.0 in (43.2 cm)	3.5 in (8.9 cm)	13.0 in (33.0 cm)	6.5 in (16.5 cm)	3.375 in (8.6 cm)	12.0 in (30.4 cm)

Wire routing



Notes

1. Maintain 1/4-inch (6 mm) spacing between power-limited and nonpower-limited wiring or use type FPL, FPLR, or FPLP cable per NEC.

[2] Power-limited and supervised when not configured as auxiliary power. Non-supervised when configured as auxiliary power.

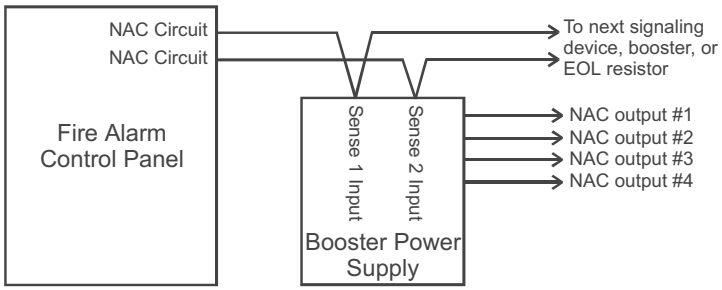
[3] Source must be power-limited. Source determines supervision.

4. When using larger batteries, make sure to position the battery terminals towards the door.

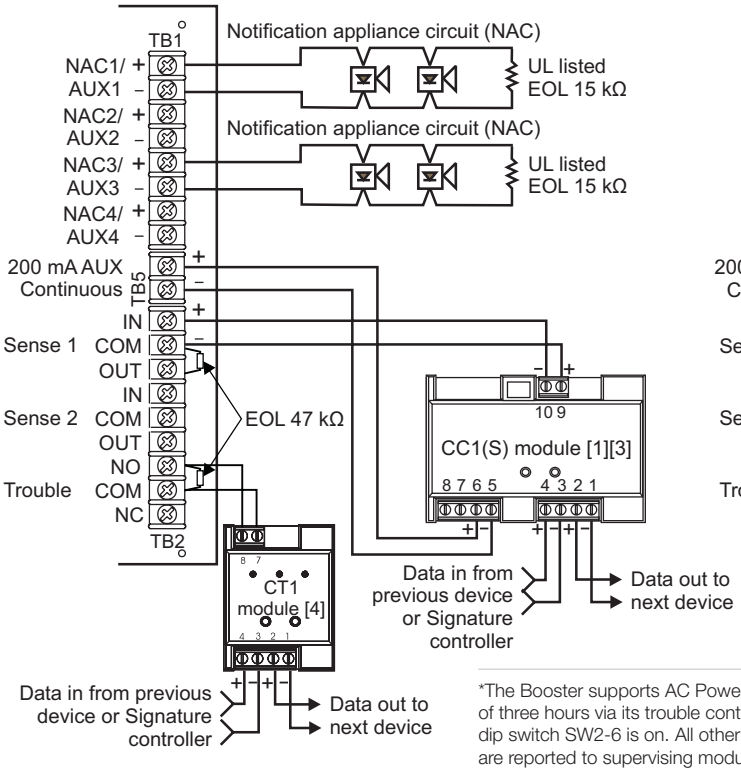
Typical Wiring

Single or cascaded booster anywhere on a notification appliance circuit

Existing NAC end-of-line resistors are not required to be installed at the booster's terminals. This allows multiple boosters to be driven from a single NAC circuit without the need for special configurations.

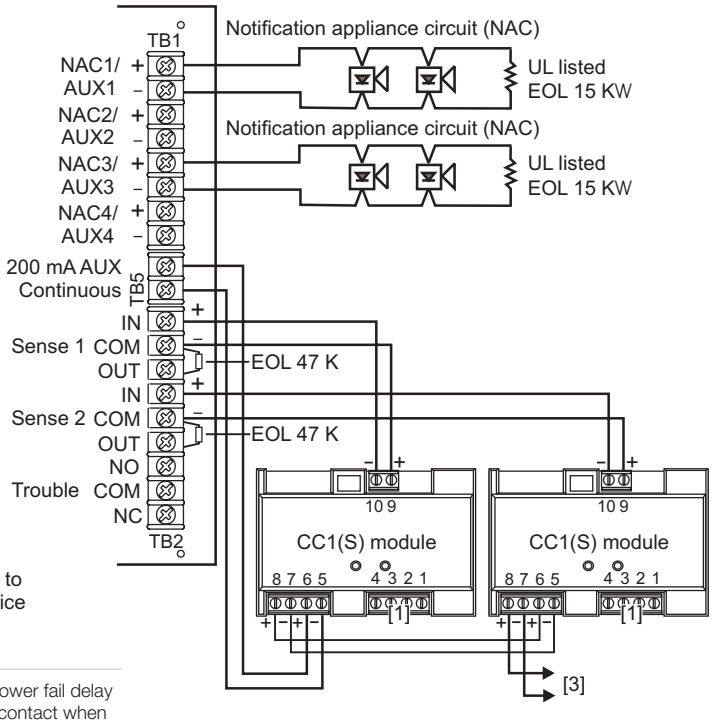


Configuring the Booster for AC Power Fail delay operation*

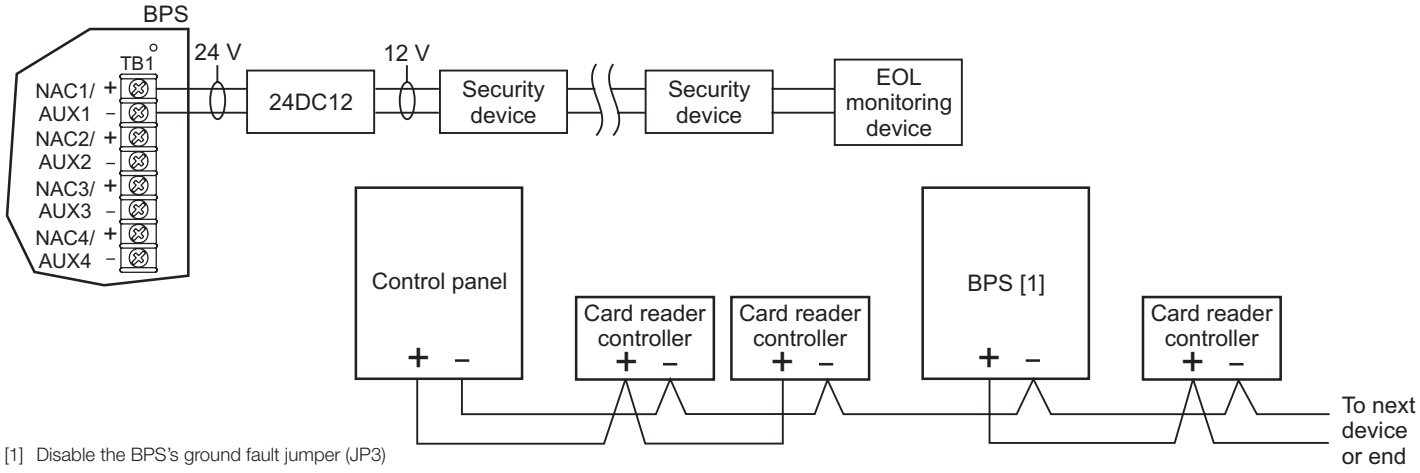


*The Booster supports AC Power fail delay of three hours via its trouble contact when dip switch SW2-6 is on. All other troubles are reported to supervising module or panel without delay via Sense inputs.

Multiple CC1(S) modules using the BPS's sense inputs



Security and access



[1] Disable the BPS's ground fault jumper (JP3)

Contact us...

Email: edwards.fire@fs.utc.com
Web: *www.est-fire.com*

EST is an **EDWARDS** brand.

1016 Corporate Park Drive
Mebane, NC 27302

In Canada, contact Chubb Edwards...
Email: inquiries@chubbedwards.com
Web: *www.chubbedwards.com*

Specifications

Model	6.5 amp Booster	10 amp Booster
AC Line Voltage	120VAC or 220-240VAC 50/60Hz 390 watts	120VAC or 220-240VAC 50/60Hz 580 watts
Notification Appliance Circuit Ratings	3.0A max. per circuit @ 24Vdc nominal 6.5A max total all NACs	3.0A max. per circuit @ 24Vdc nominal 10A max total all NACs
Trouble Relay	2 Amps @ 30Vdc	
Auxiliary Outputs	Four configurable outputs replace NACs 1, 2, 3 or 4. as auxiliary outputs and 200 mA dedicated auxiliary. (See note 2.)	
Input Current (from an existing NAC)	3mA @ 12Vdc, 6mA @ 24Vdc	
Booster Internal Supervisory Current	70mA + 35 mA for each circuit set to AUX	
Booster Internal Alarm Current	270mA	
Signature Mounting Space	Accomodates three two-gang modules.	
Maximum Battery Size	10 Amp Hours (2 of 12V10A) in cabinet up to 24 Amp hours with external battery cabinet for fire and security applications; up to 65 Amp hours for access control applications in external battery box.	
Terminal Wire Gauge	18-12 AWG	
Relative Humidity	0 to 93% non condensing @ 32°C	
Temperature Rating	32° to 120°F (0° to 49°C)	
NAC Wiring Styles	Class A or Class B	
Output Signal Rates	Continuous, California rate, 3-3-3 temporal, or follow installed panel's NAC. (See note 1.)	
Ground Fault Detection	Enable or Disable via jumper	
Agency Listings	UL, ULC, CSFM	

1. Model BPS*CAA provides selection for California rate, in place of temporal.
2. Maximum of 8 Amps can be used for auxiliary output.

Ordering Information

Catalog Number	Description	Shipping Wt. lb (kg)
BPS6A	6.5 Amp Booster Power Supply	13 (5.9)
BPS6AC	6.5 Amp Booster Power Supply (ULC)	13 (5.9)
BPS6A/230	6.5 Amp Booster Power Supply (220V)	13 (5.9)
BPS6CAA	6.5 Amp Booster Power Supply with California rate	13 (5.9)
BPS10A	10 Amp Booster Power Supply	13 (5.9)
BPS10AC	10 Amp Booster Power Supply (ULC)	13 (5.9)
BPS10A/230	10 Amp Booster Power Supply (220V)	13 (5.9)
BPS10CAA	10 Amp Booster Power Supply with California rate	13 (5.9)
Related Equipment		
12V6A5	7.2 Amp Hour Battery, two required	3.4 (1.6)
12V10A	10 Amp Hour Battery, two required	9.5 (4.3)
3-TAMP	Tamper switch	
BC-1EQ	Seismic Kit for BC-1. Order BC-1 separately. See note 3.	
BPSEQ	Seismic kit for BPS6A or BPS10 Booster Power Supplies. See note 3	
BC-1	Battery Cabinet (up to 2 - 40 Amp Hour Batteries)	58 (26.4)
BC-2	Battery Cabinet (up to 2 - 17 Amp Hour Batteries)	19 (8.6)
12V17A	18 Amp Hour Battery, two required (see note 1)	13 (5.9)
12V24A	24 Amp Hour Battery, two required (see note 1)	20 (9.07)
12V40A	40 Amp Hour Battery, two required (see notes 1, 2)	32 (14.5)
12V50A	50 Amp Hour Battery, two required (see notes 1, 2)	40 (18.14)
12V65A	65 Amp Hour Battery, two required (see notes 1, 2)	49 (22.2)

1. Requires installation of separate battery cabinet.
2. BPS supports batteries greater than 24 Amp hours for access control applications only.
3. For earthquake anchorage, including detailed mounting weights and center of gravity detail, refer to Seismic Application Guide 3101676. Approval of panel anchorage to site structure may require local AHJ, structural or civil engineer review.

This Page Left Intentionally Blank

SEALED LEAD ACID BATTERY, 18AH

Operations & Maintenance Manual
December 2015

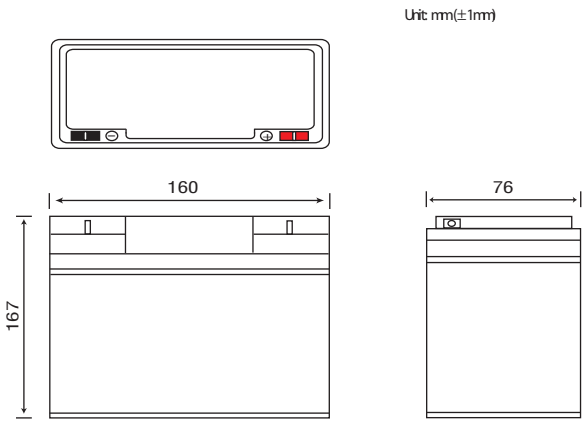
Power Patrol® Batteries

Specification Sheet

Sealed Lead-Acid Batteries — SLA1116

Technical Specifications

Nominal Voltage		12V
Nominal Capacity		18.0 Ah (20 Hr Rate)
Dimensions	Length:	180 mm (7.20 in)
	Width:	76 mm (3.00 in)
	Height:	167 mm (6.60 in)
Total Height w/ Teminal:		167 mm (6.60 in)
Weight		Approx 6.2 Kg (13.85 Lbs.)
Terminal Type		Nut & Bolt (w/faston adapter)



Capacity Characteristics

Cut Off Voltage	20 Hr Rate (0.90A)	18.0AH
1.75 v/c @ 25°C	10 Hr Rate (1.60A)	16.0AH
1.70 v/c	5 Hr Rate (2.9A)	14.5AH
1.55 v/c	1 Hr Rate (9.8A)	9.8AH

Charge Voltage (constant)

	Bloc	Per Cell
Float	13.5~13.8	2.25~2.30
Cycle	14.4~14.7	2.40~2.45

Discharge Current Amps *(5 seconds maximum)*	250
Discharge Current Amps *(maximum continuous)*	80
Max. Charge Current	5.1A
Approx Final Charge Current *(2.25 v/c Float)*	0.03 (30 mA)
Approx Final Charge Current *(2.45 v/c Cycle)*	0.15 (150 mA)
Self Discharge	9 months@21°C
Case Material	ABS - *Gray or Black

Due to changes in the manufacturing process, specifications may change without notice.
*Gray option is Flame Retardent ABS.

Actual Wattage / Ampere Capacity at Various Discharge Times (Volt per Cell @ 25° C)

Cut Off Wattage \ Time		5 Min	10 Min	15 Min	30 Min	45 Min	60 Min
1.75 v/c	W	107.4	72.33	55.6	33.79	24.68	19.78
25°C	A	61.37	41.33	31.77	19.31	14.1	11.3
1.67 v/c	W	104.79	72.16	55.31	33.48	25.05	20.04
25°C	A	62.75	43.21	33.12	20.05	15.0	12.0
1.60 v/c	W	116.8	73.76	54.72	32.19	24.37	19.33
25°C	A	73.0	46.1	34.2	20.12	15.23	12.08

This Page Left Intentionally Blank

SEALED LEAD ACID BATTERY, 10AH

Operations & Maintenance Manual
December 2015

SLA1097
General Purpose Battery
Battery Specification Sheet

Technical

Nominal Voltage	12 V
Nominal Capacity (20HR)	10.0Ah
Chemistry	Lead Acid (AGM)

Charging

Initial Charging Current	3.0 A
Cycle Use	14.4V~15.0V at 25°C(77°F)
Standby Use	13.5V~13.8V at 25°C(77°F)

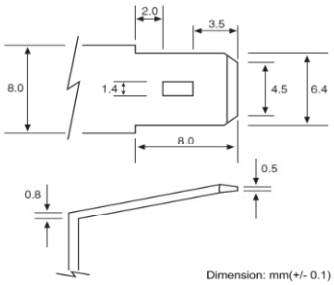
Physical

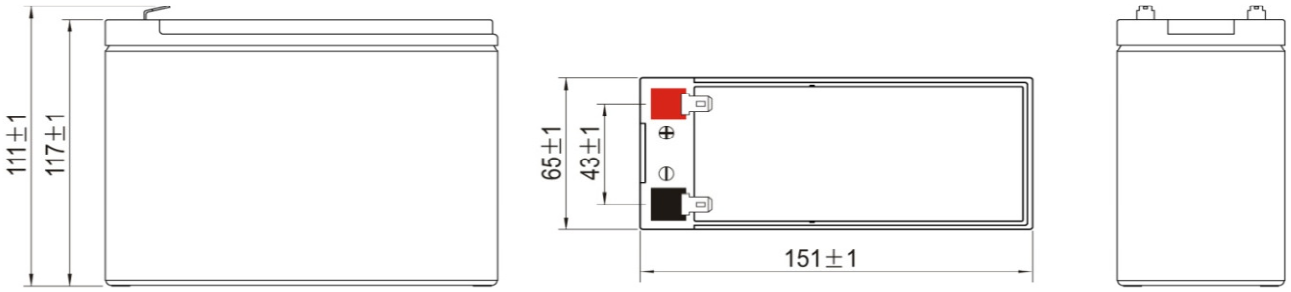
Length	151 mm	5.95 in.
Width	65 mm	2.56 in.
Height	111 mm	4.37 in.
Total Height (w/ terminals)	117 mm	4.61 in.
Weight	3.2 kg	7.06 lbs
Terminal Type		.250" Faston
Case Material		Black ABS

Capacity

20HR, 1.80V/cell, 25°C/77°F	10.0Ah	0.50A
10HR, 1.80V/cell, 25°C/77°F	9.30Ah	0.93A
5HR, 1.75V/cell, 25°C/77°F	8.10Ah	1.70A
3HR, 1.75V/cell, 25°C/77°F	7.65Ah	2.55A
1HR, 1.60V/cell, 25°C/77°F	6.28Ah	6.28A
Maximum Discharge Current		150A (5 seconds)
Self Discharge to 80%		6 months @ 25°C
Internal Resistance		~22 mΩ

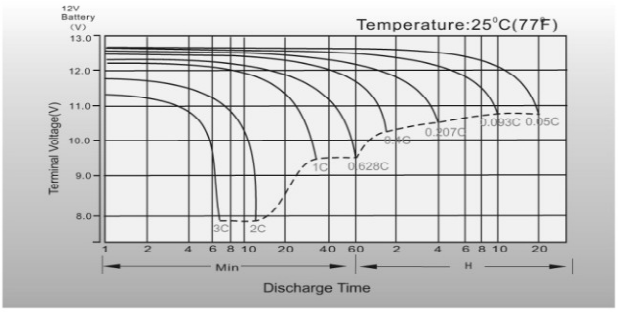
BAZR2.MH18830



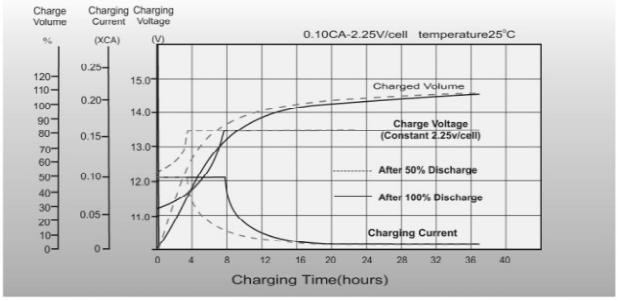


SLA1097
General Purpose Battery
Battery Specification Sheet

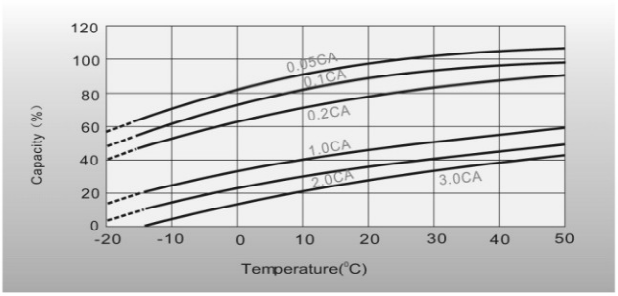
Discharge Characteristics



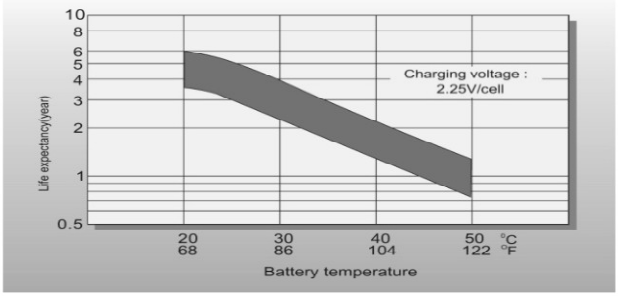
Float Charging Characteristics



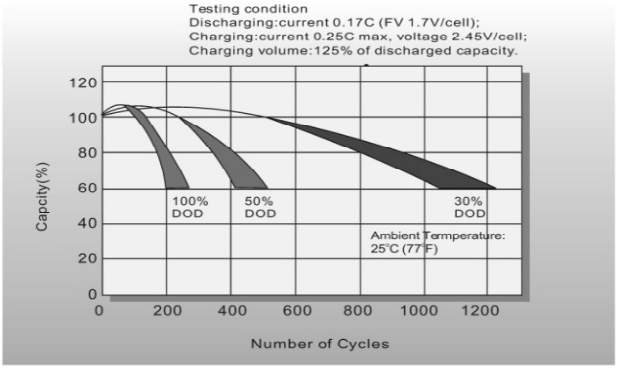
Temperature Effects in Relation to Battery Capacity



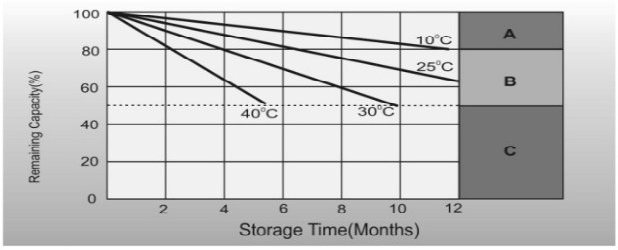
Effect of Temperature on Long Term Float Life



Cycle Life in Relation to Depth of Discharge



Self Discharge Characteristics



A No supplementary charge required
(Carry out supplementary charge before use if 100% capacity is required.)

B Supplementary charge required before use.Optional charging way as below:
1.Charged for above 3 days at limted current 0.25CA and constant volatge 2.25V/cell.
2.Charged for above 20hours at limted current 0.25CA and constant volatge 2.45V/cell.
3.Charged for 8~10hours at limted current 0.05CA .

C Supplementary charge may often fail to recover the capacity.
The battery should never be left standing till this is reached.

This Page Left Intentionally Blank

TEMPCO STRIP HEATER, 120vAC, 125W

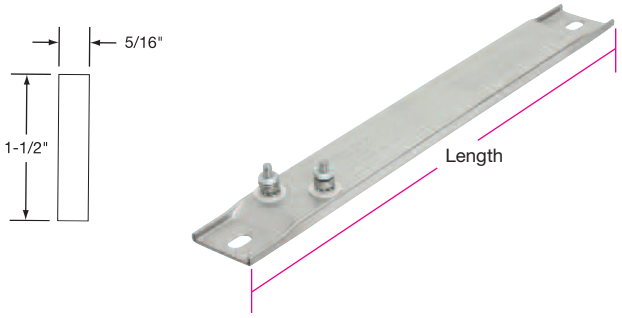
Operations & Maintenance Manual
December 2015

Standard (Non-Stock) Sizes and Ratings

1-1/2" × 5/16" (38.1 × 7.94 mm) Channel Strip Heaters with T4 Terminals and Mounting Tabs

Stock Items Are Shown In RED

Length in	Length mm	Wattage	Watt Density W/in²	Watt Density W/cm²	Part Number 120V	Part Number 240V
5¼	133.4	125	34	5	**CSH00338**	CSH00339
5¾	???.4	300	55	8	**CSH01596**	**CSH01595**
6	152.4	150	24	4	**CSH00318**	**CSH00321**
7½	190.5	150	15	2	CSH00054	CSH00055
7½	190.5	200	20	3	CSH00056	CSH00057
8	203.2	150	13	2	**CSH00058**	**CSH00059**
8	203.2	175	15	2	CSH00060	CSH00061
8	203.2	250	21	3	**CSH00062**	**CSH00063**
8	203.2	400	31	5	CSH00064	CSH00065
8	203.2	500	42	7	**CSH00066**	**CSH00067**
10½	266.7	250	12	2	**CSH00068**	**CSH00069**
10½	266.7	350	17	3	CSH00070	CSH00071
10½	266.7	400	19	3	CSH00072	CSH00073
12	304.8	250	10	1	CSH00074	CSH00075
12	304.8	350	13	2	**CSH00076**	**CSH00077**
12	304.8	500	19	3	**CSH00078**	**CSH00079**
14	355.6	300	9	1	CSH00080	CSH00081
14	355.6	500	15	2	**CSH00082**	**CSH00083**
15¼	387.4	325	9	1	CSH00084	CSH00085
15¼	387.4	500	13	2	CSH00086	CSH00087
17⅞	454.2	350	7	1	CSH00088	CSH00089
17⅞	454.2	375	8	1	CSH00090	CSH00091
17⅞	454.2	500	11	2	CSH00092	CSH00093
17⅞	454.2	750	16	2	**CSH00094**	**CSH00095**
17⅞	454.2	1000	23	3	CSH00096	CSH00097
19½	495.3	350	7	1	CSH00098	CSH00099
19½	495.3	500	9	1	CSH00100	CSH00101
19½	495.3	750	14	2	CSH00102	CSH00103
19½	495.3	1000	19	3	CSH00104	CSH00105
19½	495.3	1200	23	4	CSH00329	**CSH00333**
21	533.4	500	8	1	CSH00106	CSH00107
21	533.4	750	13	2	CSH00108	CSH00109
23¾	603.3	500	7	1	CSH00110	CSH00111
23¾	603.3	750	11	2	**CSH00112**	**CSH00113**

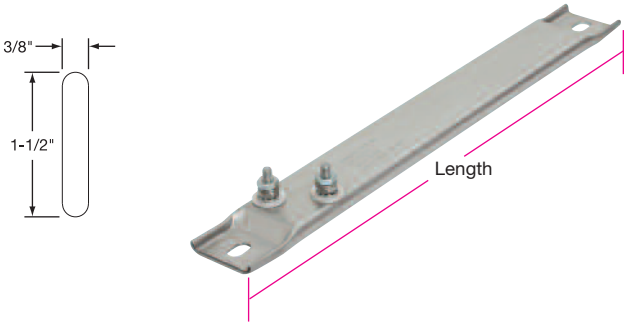


Stock Items Are Shown In RED

Length in	Length mm	Wattage	Watt Density W/in²	Watt Density W/cm²	Part Number 120V	Part Number 240V
23¾	603.3	1000	15	2	CSH00114	CSH00115
23¾	603.3	1500	22	3	CSH00116	CSH00117
25½	647.7	500	7	1	CSH00118	CSH00119
25½	647.7	750	10	2	CSH00120	CSH00121
25½	647.7	1000	13	2	CSH00122	CSH00123
26¾	679.5	700	9	1	CSH00124	CSH00125
26¾	679.5	750	9	1	CSH00126	CSH00127
26¾	679.5	1000	13	2	CSH00128	**CSH00129**
29¼	743.0	750	8	1	CSH00130	**CSH00131**
30½	774.7	750	8	1	CSH00132	CSH00133
30½	774.7	1000	11	2	CSH00134	CSH00135
30½	774.7	1250	13	2	—	CSH00136
33½	850.9	750	7	1	CSH00137	CSH00138
34⅝	879.5	1000	9	1	CSH00139	**CSH00140**
35⅞	911.4	1000	9	1	CSH00141	**CSH00142**
35⅞	911.4	1500	13	2	CSH00143	CSH00144
37¼	946.2	1500	13	2	**CSH00145**	**CSH00146**
38½	977.9	800	7	1	CSH00147	CSH00148
38½	977.9	1000	8	1	CSH00149	CSH00150
38½	977.9	1500	12	2	CSH00151	CSH00152
42½	1079.5	1250	9	1	CSH00153	CSH00154
42½	1079.5	1500	11	2	CSH00155	CSH00156
47⅞	1216.2	1350	9	1	—	CSH00157
47⅞	1216.2	2250	14	2	—	CSH00158

1-1/2" × 3/8" (38.1 × 9.53 mm) Channel Strip Heaters with T4 Terminals and Mounting Tabs

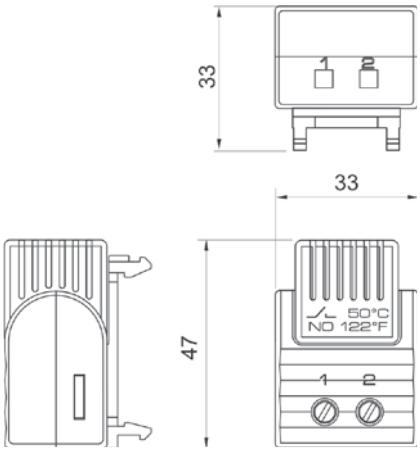
Length in	Length mm	Wattage	Watt Density W/in²	Watt Density W/cm²	Part Number 120V	Part Number 240V
7½	190.5	200	19	3	—	CSH00294
9	228.6	500	31	5	—	CSH00295
10½	266.7	250	12	2	CSH00296	—
10½	266.7	400	19	3	CSH00297	—
12	304.8	500	18	3	—	CSH00298
15¼	387.4	500	13	2	—	CSH00299
17	431.8	1000	22	3	—	CSH00300
17⅞	454.0	350	7	1	—	CSH00301
17⅞	454.0	500	10	2	—	CSH00302
18	457.2	1000	20	3	—	CSH00303
18½	469.9	500	10	2	—	CSH00304
22½	571.5	1000	15	2	—	CSH00305
24	609.6	1000	14	2	—	CSH00306
25½	647.7	1000	13	2	—	CSH00307
26	660.4	1600	20	3	—	CSH00308
26½	673.1	1500	18	3	—	CSH00309

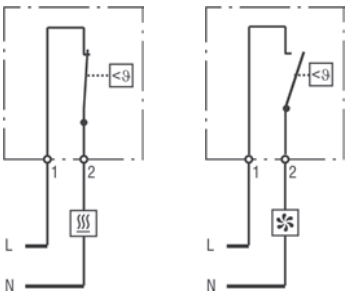


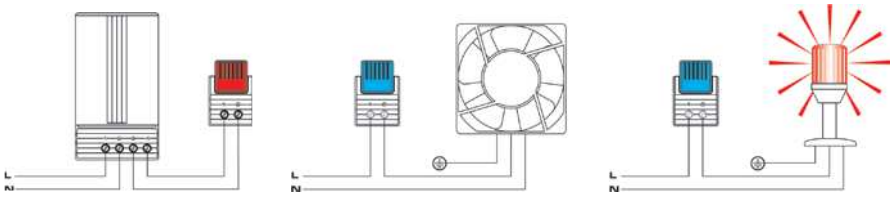
Length in	Length mm	Wattage	Watt Density W/in²	Watt Density W/cm²	Part Number 120V	Part Number 240V
30½	774.7	750	8	1	—	CSH00310
31½	800.1	800	8	1	—	CSH00311
35⅞	911.2	1000	9	1	—	CSH00312
36	914.4	1000	9	1	—	CSH00313
50	1270.0	1000	6	1	—	CSH00314
62	1574.8	1500	7	1	—	CSH00315

This Page Left Intentionally Blank


15°C
NC 59°F
1 2
50°C
NO 122°F
1 2


33
1 2
33
47
50°C
NO 122°F
1 2


1
2
L
N
1
2
L
N


L
N
L
N
L
N

Compact design
Wide adjustment range
Color coded temperature dials
DIN rail mountable

Thermostat NC (normally closed)

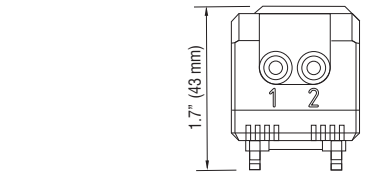
Thermostat opens on temperature rise - for regulating heaters or for switching signal devices. Comes with **red** temperature dial.

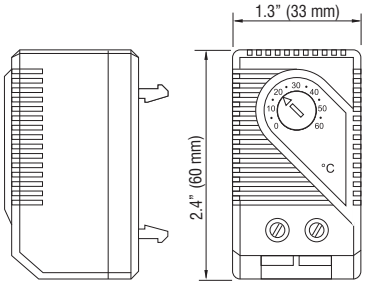
Thermostat NO (normally open)

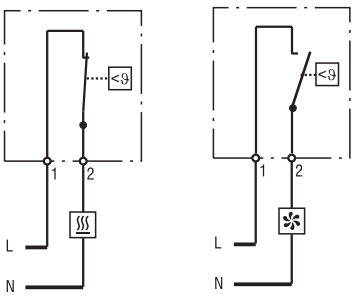
Thermostat closes on temperature rise - for regulating filter fans and heat exchangers or for switching signal devices. Comes with **blue** temperature dial.

Technical Data

Switching difference	12.6°F ± 7°F tolerance (7K ± 4K)
Sensor element	thermostatic bimetal
Contact type	snap-action contact
Contact resistance	< 10mΩ
Service life	> 100,000 cycles
Max. switching capacity	15A resistive / 2A inductive @ 120VAC
	10A resistive / 2A inductive @ 250VAC
	DC 30W
Minimum load	20mA (all voltages)
EMC	acc. to EN 55014-1-2, EN 61000-3-2, EN 61000-3-3
Connection	2-pole terminal, clamping torque 0.5Nm max.:
	solid wire - AWG 14 max. (2.5mm²)
	stranded wire (with wire end ferrule) - AWG 16 (1.5mm²)
Housing	plastic, UL 94V-0, light grey
Mounting	clip for 35mm DIN rail, EN 60 715
	(or for Exhaust Filter EF 118 Series)
Mounting position	vertical
Operating / Storage temperature	-49 to +176°F (-45 to +80°C)
Dimensions	2.4 x 1.3 x 1.7" (60 x 33 x 43mm)
Weight	approx. 1.4 oz. (40g)
Protection type	IP20

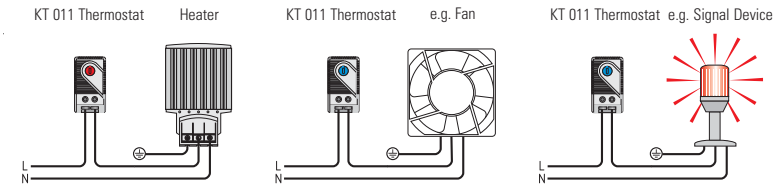






NC (red)

NO (blue)



Wiring examples

Setting range	Part No. (NC)	Part No. (NO)	Approvals
+32 to +140°F	01140.9-00	01141.9-00	UL File No. E164102, CSA
0 to +60°C	01146.9-00	01147.9-00	UL File No. E164102, CSA
-10 to +50°C	01142.0-00	N/A	UL File No. E164102, CSA, VDE
+10 to +70°C	N/A	01149.9-00	UL File No. E164102, CSA
-15 to +45°C	01157.0-00	01156.0-00	UL File No. E164102, CSA
+20 to +80°C	01159.0-00	01158.0-00	UL File No. E164102, CSA, VDE

STEGO, Inc. · 1395 South Marietta Parkway · Building 800 · Marietta, GA 30067 · Tel: (770) 984-0858 · Fax: (770) 984-0615
Toll free: 1-888-783-4611 (US & Canada only) · www.stegousa.com

This Page Left Intentionally Blank

CCTV DOME CAMERA, 2.0MP, DAY/NIGHT, 20X

Operations & Maintenance Manual
December 2015

2.0 Megapixel Day/Night 20x HD PTZ Pendant Dome Camera

Avigilon's end-to-end surveillance solutions deliver image detail no other system can match. Avigilon Control Center software, featuring High-Definition Stream Management™ (HDSM™) technology combined with our broad range of megapixel cameras (from 1 MP to 29 MP) provide unprecedented clarity—while effectively managing storage and bandwidth requirements. Our components are scalable and can work together in an end-to-end system, or can be customized to create your own powerful and cost-effective solution.

The innovative HD PTZ camera is just one way Avigilon can help provide the very best monitoring and protection.

The HD PTZ camera offers unsurpassed image quality with precise positioning and predictable high-speed tracking. Underpinned by the H3 platform, the HD PTZ camera takes advantage of enhanced High-Definition Stream Management™ technology which lowers bandwidth and storage requirements, and provides incredible low light performance. The camera features a 20x optical zoom with up to 12x digital zoom, and provides continuous 360° degree rotation at up to 450° per second. This indoor and outdoor mounted camera is targeted specifically at expansive areas with manned operations, such as large retail chains, airports, petrochemical, casinos and city surveillance.

*Mount sold separately (MNT-PEND-WALL)

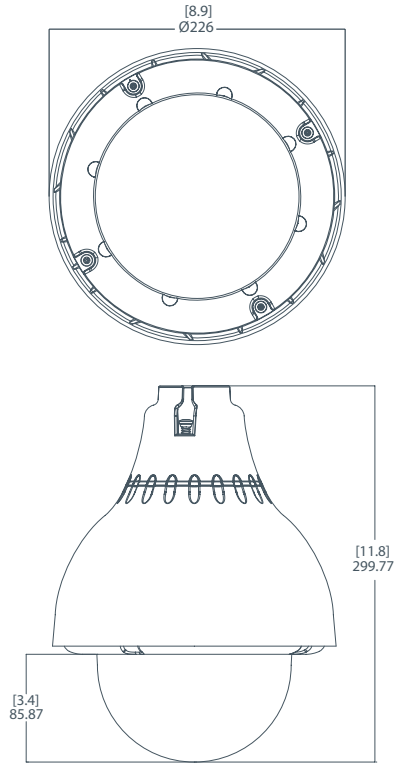
KEY FEATURES

2.0 megapixel progressive scan CMOS sensor
Easily track targets with 360 degree endless rotation
Able to move at up to 450 degrees per second
4.7 - 94mm, F1.6 lens with 20x zoom
Provides smooth operation and captures fluid motion at 30 frames per second
0.4 lux (F1.6) minimum illumination in color mode and 0.04 lux (F1.6) minimum illumination in monochrome mode
H.264 and Motion JPEG compression
ONVIF compliant API
Hide sensitive areas with 3D privacy mask
Automatic exposure control and iris control
Automatic removable IR cut filter for IR sensitivity at night
Power over Ethernet, 24 VAC or 24 VDC power input
Supports broad environmental conditions for challenging outdoor installations
External microphone and speaker support for two-way audio
External I/O interface for connecting alarms and relays

Specifications

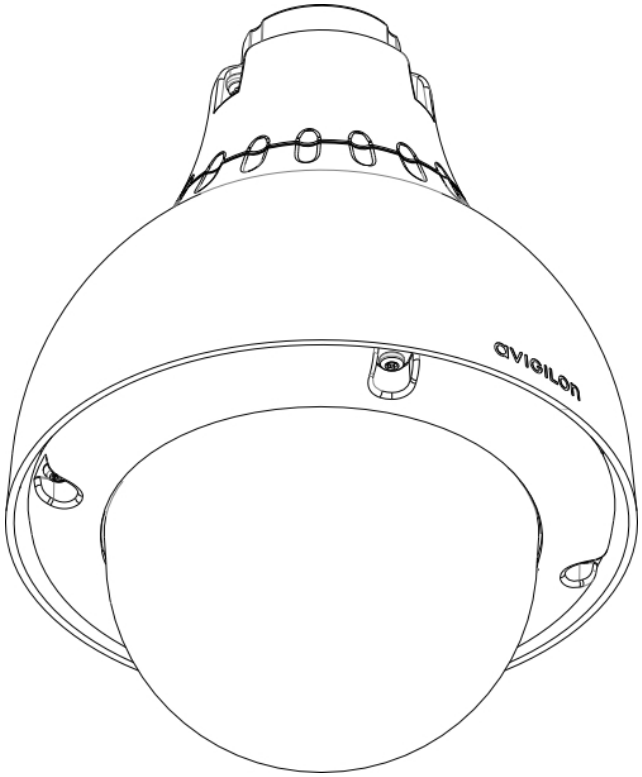
CAMERA	Image Sensor	WDR 1/2.8” progressive scan CMOS		
	Active Pixels	1920 (H) x 1080 (V)		
	Imaging Area	4.8 mm (H) x 2.7 mm (V) (0.189” (H) x 0.106” (V))		
	Minimum Illumination	0.4 lux (F1.6) in color mode; 0.04 lux (F1.6) in monochrome mode		
	Dynamic Range	100dB		
	Lens	4.7-94 mm, 20x zoom, F1.6 and automatic focus		
	Angle of View	2.9° - 55.2°		
	Image Compression Method	H.264 (MPEG-4 Part 10/AVC), Motion JPEG		
	Image Rate	30 (all resolutions)		
	Streaming	Multi-stream H.264 and Motion JPEG		
	Resolution Scaling	Down to 352 x 240		
	Motion Detection	Selectable sensitivity and threshold		
	Electronic Shutter Control	Automatic, Manual (1/6 to 1/8000 sec)		
	Iris Control	Automatic, Manual		
	Day/Night Control	Automatic, Manual		
	Flicker Control	50 Hz, 60 Hz		
	White Balance	Automatic, Manual		
	Privacy Zones	Up to 4 zones, 3D privacy mask supported		
	Presets	100 named presets		
	Tours	10 named guard tours		
	Audio Compression Method	G.711 PCM 8 kHz		
	Audio Input	Line input		
	Audio Output	Line level		
	Video Output	NTSC/PAL		
	External I/O Terminals	2 Alarm In, 2 Alarm Out		
NETWORK	Network	100BASE-TX		
	Cabling Type	CAT5		
	Connector	RJ-45		
	API	ONVIF compliant (www.onvif.org)		
	Security	Password protection, HTTPS encryption, digest authentication, WS authentication, user access log.		
	Protocol	IPv4, HTTP, HTTPS, SOAP, DNS, NTP, RTSP, RTCP, RTP, TCP,UDP, IGMP, ICMP, DHCP, Zeroconf, ARP, LLDP		
	Streaming Protocols	RTP/UDP, RTP/UDP multicast, RTP/RTSP/TCP, RTP/RTSP/HTTP/TCP, RTP/RTSP/HTTPS/TCP, HTTP		
MECHANICAL	Dimensions (ØxH)	226 mm x 299.77 mm (8.9” x 11.8”)		
	Weight	3.9 kg (8.6 lbs)		
	Dome Bubble	Acrylic, clear		
	Body	Aluminum		
	Housing	Pendant mount		
	Finish	Powder coat, cool gray 2		
	Tilt	186°, E-flip, 0.05 - 360°/sec		
	Pan	360°, endless, 0.05 - 450°/sec		
ELECTRICAL	Power Source	VAC: 24 V +/- 10% VDC: 24 V +/- 10%	PoE: IEEE 802.3at Class 4 PoE Plus compliant	
	Power Consumption	55 VA with AC power 44 W with DC power 25.5 W with IEEE 802.3at Class 4 PoE Plus		
	Power Connector	Waterproof 2-pin connector		
ENVIRONMENTAL	Operating Temperature	-45 °C to + 50 °C (-50 °F to 122 °F) with external power -30 °C to + 50 °C (-22 °F to 122 °F) with IEEE 802.3at Class 4 PoE Plus power		
	Storage Temperature	-10 °C to +70 °C (14 °F to 158 °F)		
	Humidity	20 - 80% Relative humidity (non-condensing)		
CERTIFICATIONS	Safety	UL 60950 CSA 60950	CVV C-Tick	CB Scheme
	Environment	IK09 Impact Rating	Meets IP66 Weather Rating	
	Electromagnetic Emission	FCC Part 15 Subpart B Class B IC ICES-003 Class B		EN 55022 Class B
	Electromagnetic Immunity	EN 55024 Class B EN 61000-4-2 EN 61000-4-3	EN 61000-4-4 EN 61000-4-5 EN 61000-4-6	EN 61000-4-11
ORDERING INFORMATION	2.0W-H3PTZ-DP20	2.0 Megapixel Day/Night 20x HD PTZ Pendant Dome Camera		
	MNT-PEND-WALL	Indoor/Outdoor Pendant Mount Bracket		
	H3PTZ-DP-SMOKE	Dome Camera Cover with Smoked Bubble		

Outline Dimensions



[X.X]	INCHES
X	MM

This Page Left Intentionally Blank



Installation Guide

Avigilon™ High Definition H.264 PTZ IP Dome Camera Models:

1.0W-H3PTZ-DP20 and 2.0W-H3PTZ-DP20

Important Safety Information

This manual provides installation and operation information and precautions for the use of this camera. Incorrect installation could cause an unexpected fault. Before installing this equipment read this manual carefully. Please provide this manual to the owner of the equipment for future use.

The Warning symbol indicates the presence of dangerous voltage within and outside the product enclosure that may constitute a risk of electric shock, serious injury or death to persons if proper precautions are not followed.

The Caution symbol alerts the user to the presence of hazards that may cause minor or moderate injury to persons, damage to property or damage to the product itself if proper precautions are not followed.

WARNING — Failure to observe the following instructions may result in severe injury or death.

- Installation must be performed by qualified personnel only, and must conform to all local codes.
- This product is intended to be supplied by a UL Listed Power Unit marked “Class 2” or “LPS” or “Limited Power Source” with output rated 24 VAC +/- 10%, 55 VA min.; 24 VDC +/- 10%, 44 W min. or Power over Ethernet (PoE) Plus IEEE802.3at Type 2 compliant Power Sourcing Equipment (PSE) rated 42.5-57 VDC, 25.5W min.
- Any external power supply connected to this product may only be connected to another Avigilon product of the same model series. External power connections must be properly insulated.
- Do not connect directly to mains power for any reason.

CAUTION — Failure to observe the following instructions may result in injury or damage to the camera.

- Do not install near any heat sources such as radiators, heat registers, stoves, or other sources of heat.
- Do not subject the cables to excessive stress, heavy loads or pinching.
- Do not open or disassemble the device. There are no user serviceable parts.
- Refer all servicing to qualified personnel. Servicing may be required when the device has been damaged (such as from a liquid spill or fallen objects), has been exposed to rain or moisture, does not operate normally, or has been dropped.
- Do not use strong or abrasive detergents when cleaning the device body.
- Use only accessories recommended by Avigilon.

Regulatory Notices

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

This Class B digital apparatus complies with Canadian ICES-003.

FCC Notice

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and the receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Changes or modifications made to this equipment not expressly approved by Avigilon Corporation or parties authorized by Avigilon Corporation could void the user's authority to operate this equipment.

Disposal and Recycling Information

When this product has reached the end of its useful life, please dispose of it according to your local environmental laws and guidelines.

Risk of fire, explosion, and burns. Do not disassemble, crush, heat above 100 °C (212 °F), or incinerate.

European Union:

This symbol means that according to local laws and regulations your product should be disposed of separately from household waste. When this product reaches its end of life, take it to a collection point designated by local authorities. Some collection points accept products for free. The separate collection and recycling of your product at the time of disposal will help conserve natural resources and ensure that it is recycled in a manner that protects human health and the environment.

Legal Notices

Disclaimer

This manual has been compiled and published covering the latest product descriptions and specifications. The contents of this manual and the specifications of this product are subject to change without notice. Avigilon reserves the right to make changes without notice in the specifications and materials contained herein and shall not be responsible for any damages (including consequential) caused by reliance on the materials presented, including but not limited to typographical and other errors relating to the publication.

Avigilon Corporation
http://www.avigilon.com

920-0074A

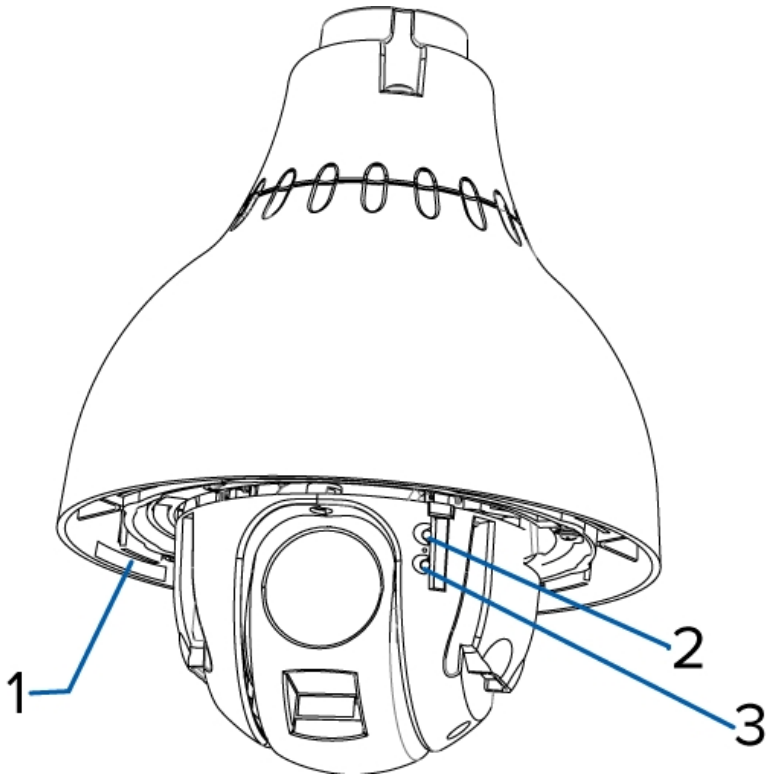
Revision: 5 - EN

2015-01-20

Table of Contents

Overview

Front View



1. **Serial Number Tag**

   Product serial number and part number label.

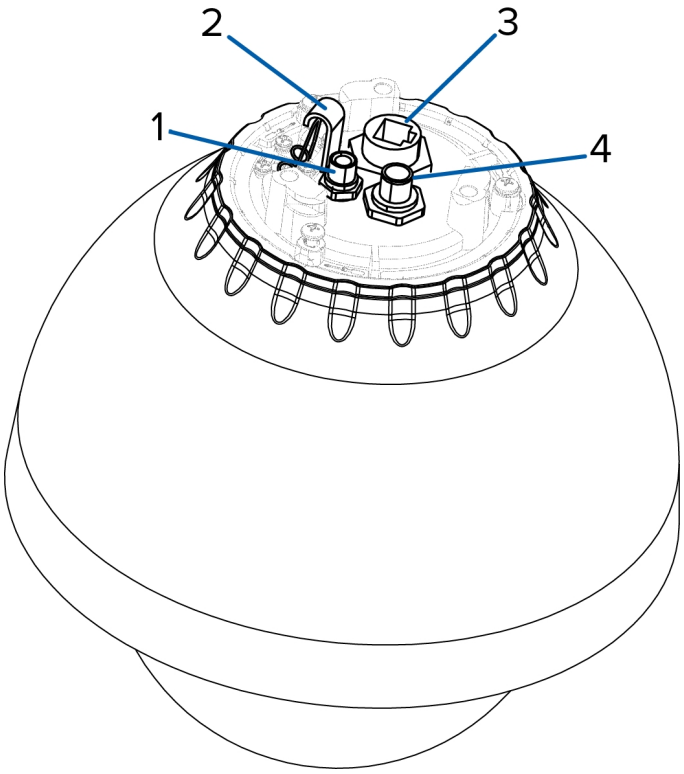
2. **Link LED**

   Indicates if there is an active connection in the Ethernet port.

3. **Connection Status LED**

   Provides information about device operation. For more information, see *LED Indicators* on page 13

Top View



1. **External Power**

   Accepts an external power connection when Power over Ethernet is not available.

2. **Lanyard Anchor**

   The safety lanyard attaches to the anchor to prevent the camera from falling during installation.

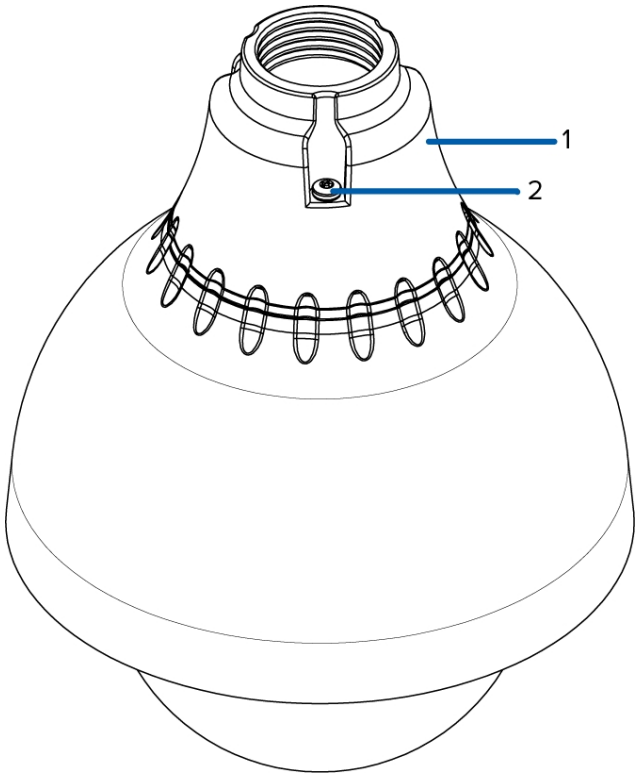
3. **Ethernet Port**

   Accepts an Ethernet connection to a network. Server communication and image data transmission occurs over this connection. Also receives power when it is connected to a network that provides Power over Ethernet.

4. **External I/O**

   Provides connections to external input/output and audio/video devices.

Pendant Mount Adapter



1. **1-1/2” NPT Mount Adapter**

   Standard 1-1/2” NPT adapter for mounting the dome camera to a pendant mount bracket.

2. **Tamper Resistant Screws**

   Torx captive screws to fix the dome camera to the NPT adapter.

Installation

Camera Package Contents

Ensure the package contains the following:

- Avigilon™ High Definition PTZ Dome Camera
- 1 ½" NPT Adapter
- T20 Torx key
- Teflon Sealing Tape
- RJ-45 crimp-on plug and weather-resistant housing
- External Power wiring harness, Avigilon Part #110-0017B
- External I/O wiring harness, Avigilon Part #110-0018B

Precautions for Installing Near Salt Water

Salt environments are hard on camera paint and external appearances but the camera functionality will not be affected if the cameras are installed as described in this guide.

Follow these precautions to avoid camera issues when installing in a salt heavy environment:

- Use mounting accessories offered by Avigilon. All Avigilon accessories are tested to work with Avigilon cameras in the rated environments.
- If you use a third-party accessory, you *must* ensure that the material is compatible with the finish of the camera housing or galvanic corrosion may occur.
- Never pair steel mounting accessories with aluminum camera enclosures. Steel corrodes aluminum when salt is introduced. The corrosion is an electrochemical reaction and will cause the corrosion to spread across the entire camera body.
- Always insulate any camera surface that is in contact with another metal or conductive material. It is recommended that you always isolate the mounting screws from the mounting surface and camera housing with rubber or plastic shoulder washers.

Installation Steps

Complete the following steps to install the device:

Installing the Mount Adapter

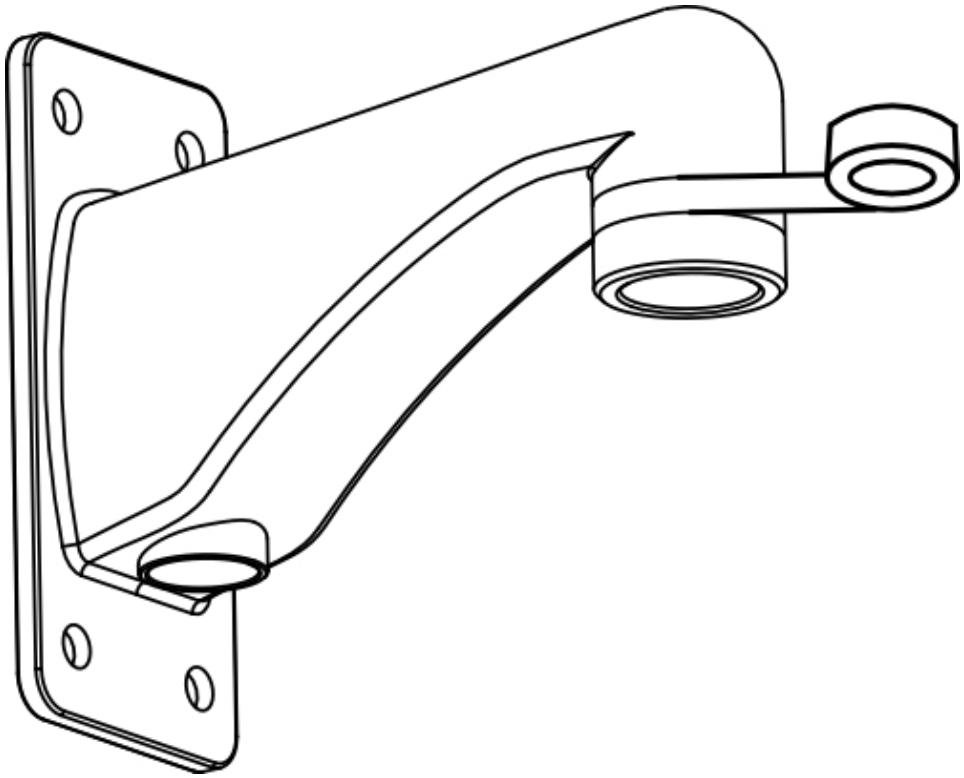
CAUTION — The dome camera must be mounted as instructed below or problems with moisture may arise and will not be covered by the dome camera warranty.

The dome camera must be mounted on a 1-1/2” NPT male threaded wall or ceiling mounting bracket. The mounting bracket is not included in the camera package.

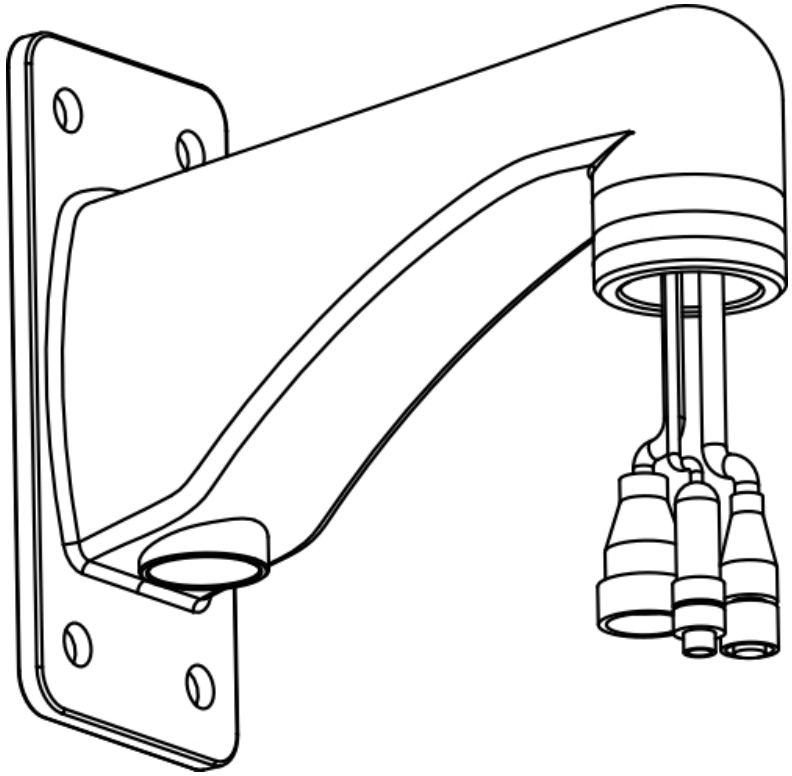
1. Wrap the thread of the mounting bracket with the supplied Teflon sealing tape to create a water tight seal around the camera connection. There should be a minimum of three turns around the entire threaded surface.

   When applying the Teflon sealing tape, be sure to wrap in the same direction that the mount will be tightened. This will ensure the tape does not unravel when installing the mating parts together.

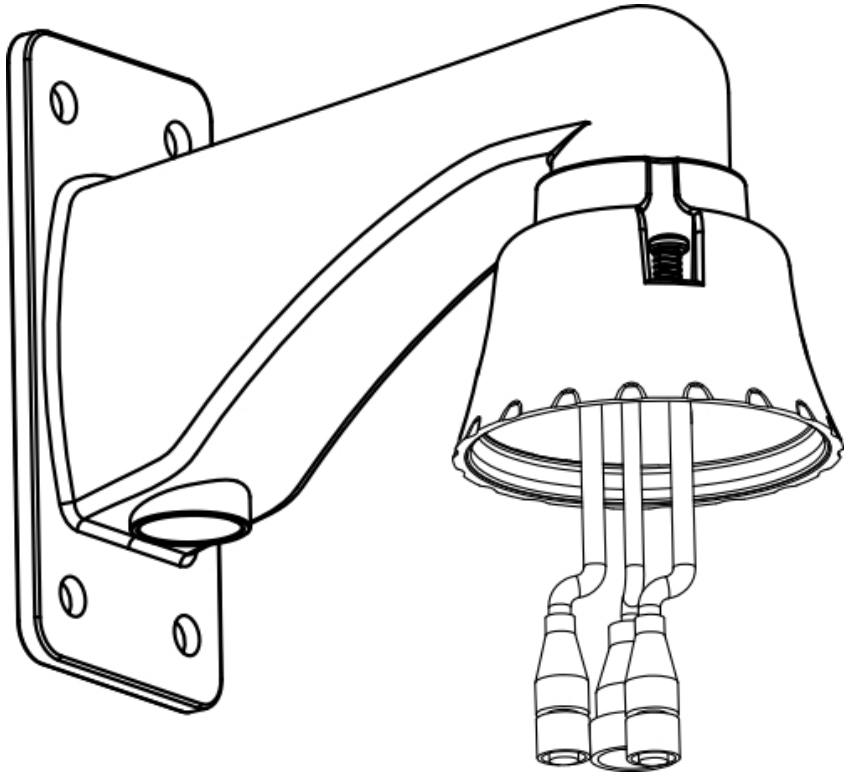
   Tip: Always apply Teflon tape to threaded mounts to help prevent the threads from binding.



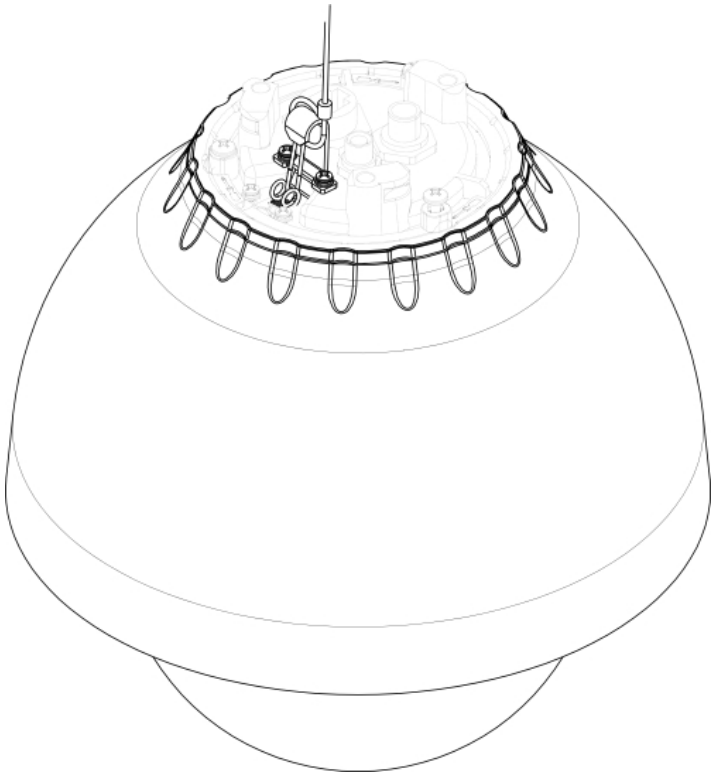
2. Pull the required cables through the mounting bracket then install the supplied connectors and wire assemblies.



3. Install the 1 1/2” NPT mount adapter.



4. Connect the safety lanyard from inside the NPT mount adapter to the anchor on the PTZ dome camera.



Connecting Cables

Refer to the diagrams in the Overview section for the location of the different connectors.

To connect the cables required for proper operation, complete the following:

1. Make sure the safety lanyard is connected to the PTZ dome camera.
2. If there are external input or output devices that need to be connected to the camera (for example: door contacts, relays, analog video, speakers, etc), connect the devices to the camera I/O connector cable.
3. Connect power using one of the following methods:
   - Power over Ethernet (PoE) Plus IEEE 802.3at Class 4 — Connect a PoE Plus compliant injector or switch to the Ethernet network cable.
   - External Power — Connect an external “Class 2” or “LPS” or “Limited Power Source” with output rated 24 VAC +/- 10%, 55 VA minimum or 24 VDC +/- 10%, 44 W minimum.

     For more information, see *Connecting External Power* on page 10.
4. Connect a network cable to the Ethernet Port (RJ-45 connector).

   The Link LED will turn on once a network link has been established.
5. Check that the Connection Status LED indicates the correct state. For more information, see *LED Indicators* on page 13.

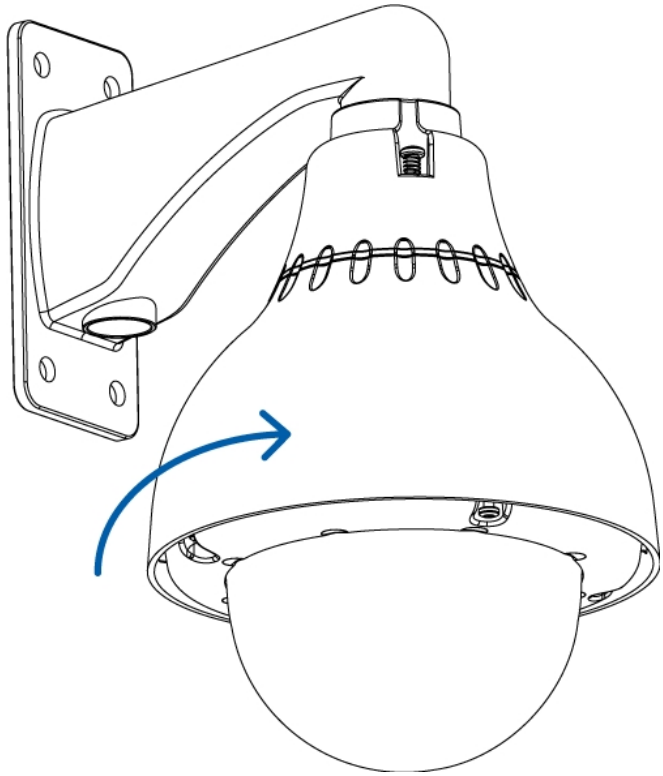
.

Securing the PTZ Dome Camera

After the cable connections have been made, secure the PTZ dome camera to the mount.

1. Push the PTZ dome camera into the 1 1/2” NPT mount adapter then twist until it locks into place.

   NOTE: Be careful not to trap any cables between the dome camera housing and the mount adapter.



2. Use the Torx key included with the dome camera to tighten the three screws in the mount adapter.

Assigning an IP Address

The camera automatically obtains an IP address when it is connected to a network.

NOTE: If the camera cannot obtain an IP address from a DHCP server, it will use Zero Configuration Networking (Zeroconf) to choose an IP address. When set using Zeroconf, the IP address is in the 169.254.0.0/16 subnet.

The IP address settings can be changed using one of the following methods:

- Camera's web browser interface: http://<*camera IP address*>/
- ARP/Ping method. For more information, see *Setting the IP Address Using the ARP/Ping Method* on page 15
- Network Video Management software application (for example, Avigilon™ Control Center).

NOTE: The default camera username is `admin` and the default password is `admin`.

Accessing the Live Video Stream

Live video stream can be viewed using one of the following methods:

- Web browser interface: http://<*IP address*>/
- Network Video Management software application (for example, the Avigilon Control Center software).

NOTE: The default camera username is `admin` and the default camera password is `admin`.

For More Information

Additional information about setting up and using the device is available in the following guides:

- *Avigilon™ Control Center Client User Guide*
- *Avigilon™ High Definition H.264 Web Interface User Guide*

The manuals are available on the Avigilon website: **http://avigilon.com/support-and-downloads**

Cable Connections

Connecting External Power

NOTE: Do not perform this procedure if Power over Ethernet (POE) is used.

If PoE is not available, the dome camera can be powered with 24 VAC or 24 VDC through the removable power connector:

1. Remove as much insulation as required to splice the supplied power connector to the power adapter wires (not included).

   Do not nick or damage the wires.

2. Remove the dummy plug from the power receptacle on the camera. See *Top View* on page 2 for the location of the external power receptacle.
3. Attach the power connector to the receptacle on the camera.

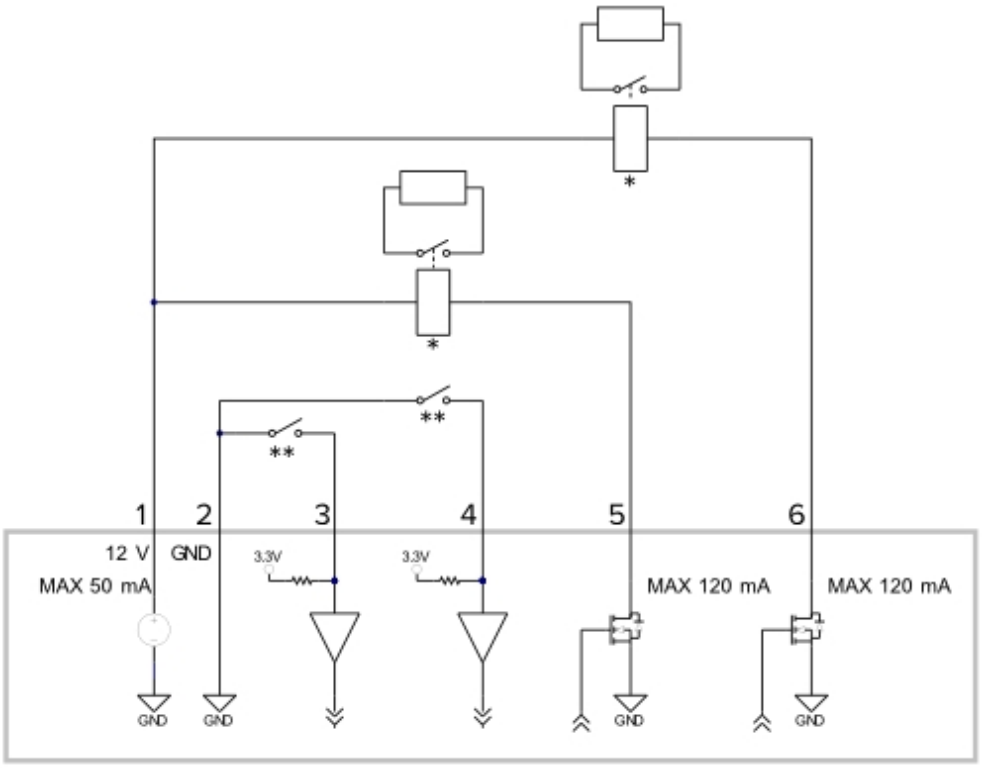
The power connector pin details are:

1. Brown — Power, accepts either polarity
2. Not used
3. Blue — Power, accepts either polarity

WARNING — This product is intended to be supplied by a UL Listed Power Unit marked “Class 2” or “LPS” or “Limited Power Source” with output rated 24 VAC +/- 10%, 55 VA min. or 24 VDC +/- 10%, 44 W min.

Connecting to External Devices

External devices, including audio and video devices, are connected to the camera through the I/O cable. The pinout for the I/O connector is shown here:



1. Dark Red — +12 VDC, 50 mA max. output for relay drive
2. Grey — Relay ground return
3. Red — Relay input 1
4. Orange — Relay input 2
5. Pink — Relay output 1
6. Blue — Relay output 2
7. * — Relay
8. ** — Switch

NOTE: The 12 V connection can be used to energize a relay coil with up to 50 mA. If more than 50 mA is required, an external power supply up to 25 VDC at 120 mA can be used.

- White — Audio/video analog ground return
- Brown — Analog audio input
- Green — Analog audio output
- Yellow — Analog video output
- Black — not connected
- Purple — not connected

The camera can be connected to an external microphone, speaker and video monitor through the I/O connector.

NOTE: The camera only supports line level mono audio input and an NTSC or PAL video output.

The video output signal is determined by the camera flicker control setting. When the camera flicker control is set to 60 Hz, the video output signal is NTSC. When the flicker control is set to 50 Hz, the video output signal is PAL. Use the Camera Installation Tool to configure the camera's flicker control in the Image and Display setup.

LED Indicators

Once connected to the network, the Connection Status LED will display the progress in connecting to the Network Video Management software.

The following table describes what the LEDs indicate:

Connection State	Connection Status LED	Description
Obtaining IP Address	One short flash every second	Attempting to obtain an IP address.
Discoverable	Two short flashes every second	Obtained an IP address but is not connected to the Network Video Management software.
Upgrading Firmware	Two short flashes and one long flash every second	Updating the firmware.
Connected	On	Connected to the Network Video Management software.

Resetting to Factory Default Settings

If the camera no longer functions as expected, you can choose to reset the camera to its factory default settings.

Use the firmware revert button to reset the camera.

NOTE: Be careful not to scratch the dome bubble.

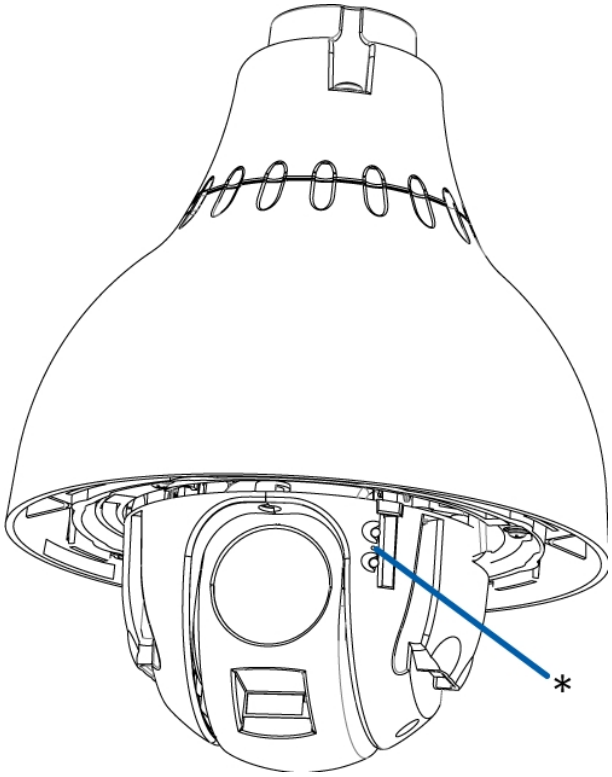


Figure 1: The firmware revert button between the status LEDs.

1. Ensure the camera is powered on.
2. Remove the dome cover by loosening the screws that fix the cover to the base. The Torx key included with the dome camera can be used to loosen the screws
3. Using a straightened paperclip or similar tool, gently press and hold the firmware revert button for two seconds.
4. Re-install the dome cover.

CAUTION — Do not apply excessive force. Inserting the tool too far will damage the device.

Setting the IP Address Using the ARP/Ping Method

Complete the following steps to configure the camera to use a specific IP address:

1. Locate and copy down the MAC Address (MAC) listed on the Serial Number Tag for reference.
2. Open a Command Prompt window and enter the following commands:
   a. `arp -s` *<New Camera IP Address> <Camera MAC Address>*

      For example: `arp -s 192.168.1.10 00-18-85-12-45-78`

   b. `ping -l 123 -t` *<New Camera IP Address>*

      For example: `ping -l 123 -t 192.168.1.10`
3. Reboot the camera.
4. Close the Command prompt window when you see the following message:

   `Reply from <New Camera IP Address>: ...`

Cleaning

Dome Bubble

If the video image becomes blurry or smudged in areas, it may be because the dome bubble requires cleaning.

To clean the dome bubble:

- Use hand soap or a non-abrasive detergent to wash off dirt or finger prints
- Use a microfiber cloth or non-abrasive fabric to dry the dome bubble.

Important: Failure to use the recommended cleaning materials may result in a damaged or scratched dome bubble that will negatively impact image quality and result in unwanted IR light reflecting into the lens.

Body

- Use a dry or lightly dampened cloth to clean the camera body.

  Do not use strong or abrasive detergents.

Specifications

Camera	
Lens	4.7-94mm, 20x zoom, F1.6 and automatic focus
Audio Input/Output	Line level input and output
Video Output	NTSC/PAL
Network	
Network	100Base-TX
Cabling Type	CAT5
Connector	RJ-45
API	ONVIF compliance version 1.02, 2.00, Profile S (www.onvif.org)
Security	Password protection, HTTPS encryption, digest authentication, WS authentication, user access log, 802.1x port based authentication.
Streaming Protocols	IPv4, HTTP, HTTPS, SOAP, DNS, NTP, RTSP, RTCP, RTP, TCP, UDP, IGMP, ICMP, DHCP, Zeroconf, ARP, LLDP, RTP/UDP, RTP/UDP multicast, RTP/RTSP/TCP, RTP/RTSP/HTTP/TCP,RTP/ RTSP/HTTPS/TCP, HTTP
Mechanical	
Dimensions Ø x H	226 mm x 299.77 mm (8.9” x 11.8”)
Weight	3.9 kg (8.6 lbs)
Dome Bubble	Acrylic, clear
Body	Aluminum
Housing	Pendant mount
Finish	Powder coat, cool gray 2
Tilt	186°, E-flip, 0.05 - 360°/sec
Pan	360°, endless, 0.05 - 450°/sec
Electrical	
Power Consumption	55 VA with AC power 44 W with DC power 25.5 W with IEEE 802.3at Class 4 PoE Plus
Power Source	VDC: 24 V +/- 10% VAC: 24 V +/- 10% PoE: IEEE 802.3at Class 4 PoE Plus compliant
Power Connector	Waterproof 2-pin connector
Environmental	
Operating	-30 °C to + 50 °C (-22 °F to 122 °F) with IEEE 802.3at Class 4 PoE Plus power

Temperature	-45 °C to + 50 °C (-50 °F to 122 °F) with external power
Storage Temperature	-10 °C to +70 °C (14 °F to 158 °F)
Humidity	0-95% non-condensing
Certifications	
Safety	UL 60950 CSA 60950 CB Scheme CVV RCM
Environmental	IK10 Impact Rating (with H3PTZ-DP-CLEAR-IK only) Meets IP66 Weather Rating
Electromagnetic Emissions	FCC Part 15 Subpart B Class B EN 55022 Class B IC ICES-003 Class B
Electromagnetic Immunity	EN 55024 Class B EN 61000-4-2 EN 61000-4-3 EN 61000-4-4 EN 61000-4-5 EN 61000-4-6 EN 61000-4-11

Limited Warranty & Technical Support

Avigilon warrants to the original consumer purchaser, that this product will be free of defects in material and workmanship for a period of 3 years from date of purchase. The warranty period shall be limited to a period of 1 year from date of purchase for all moving parts (including but not limited to fans, pan/tilt motors, lens motors, irises and lens assemblies).

The manufacturer's liability hereunder is limited to replacement of the product, repair of the product or replacement of the product with repaired product at the discretion of the manufacturer. This warranty is void if the product has been damaged by accident, unreasonable use, neglect, tampering or other causes not arising from defects in material or workmanship. This warranty extends to the original consumer purchaser of the product only.

AVIGILON DISCLAIMS ALL OTHER WARRANTIES EXPRESSED OR IMPLIED INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, EXCEPT TO THE EXTENT THAT ANY WARRANTIES IMPLIED BY LAW CANNOT BE VALIDLY WAIVED.

No oral or written information, advice or representation provided by Avigilon, its distributors, dealers, agents or employees shall create another warranty or modify this warranty. This warranty states Avigilon's entire liability and your exclusive remedy against Avigilon for any failure of this product to operate properly.

In no event shall Avigilon be liable for any indirect, incidental, special, consequential, exemplary, or punitive damages whatsoever (including but not limited to, damages for loss of profits or confidential or other information, for business interruption, for personal injury, for loss of privacy, for failure to meet any duty including of good faith or of reasonable care, for negligence, and for any other pecuniary or other loss whatsoever) arising from the use of or inability to use the product, even if advised of the possibility of such damages. Since some jurisdictions do not allow the above limitation of liability, such limitation may not apply to you.

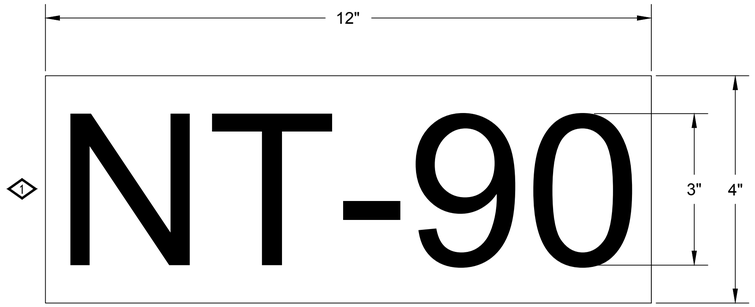
This Limited Warranty gives you specific legal rights and you may also have other rights which vary from jurisdiction to jurisdiction.

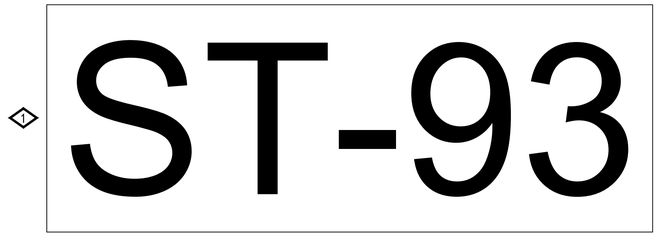
Warranty service and technical support can be obtained by contacting Avigilon Technical Support by phone at 1.888.281.5182 or via email at support@avigilon.com.

This Page Left Intentionally Blank

TUNNEL SIGNAGE

Operations & Maintenance Manual
December 2015





EISENHOWER (NORTH) TUNNEL

NORTH TUNNEL = NT-1 THRU NT-90
WEST PORTAL = NT-1, NT-2, & NT-3
INTERNAL NORTH TUNNEL = NT-4 THRU NT-87
EAST PORTAL = NT-88, NT-89, & NT-90

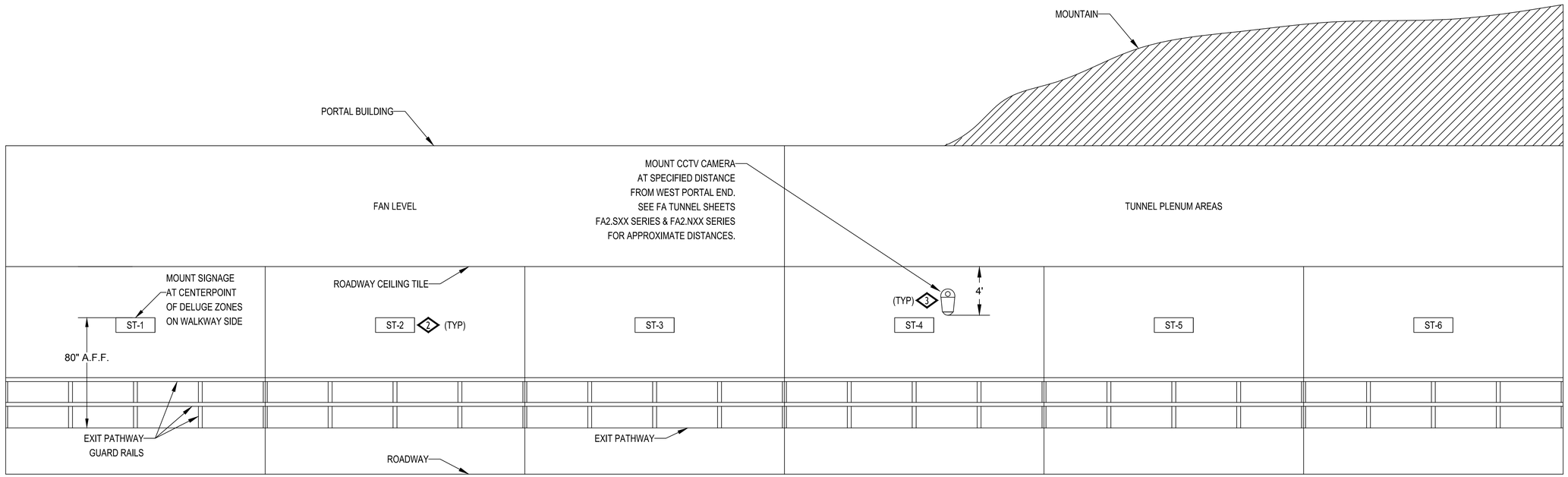
TUNNEL ZONING DELUGE SYSTEM IS FROM WEST TO EAST NUMERICALLY IN BOTH TUNNELS.
ARIAL FONT SHALL BE UTILIZED.

JOHNSON (SOUTH) TUNNEL

SOUTH TUNNEL = ST-1 THRU ST-93
WEST PORTAL = ST-1, ST-2, & ST-3
INTERNAL SOUTH TUNNEL = ST-4 THRU ST-90
EAST PORTAL = ST-91, ST-92, & ST-93

TUNNEL ZONING DELUGE SYSTEM IS FROM WEST TO EAST NUMERICALLY IN BOTH TUNNELS.
ARIAL FONT SHALL BE UTILIZED.

1 SIGNAGE LAYOUT
SCALE: 1 : 1 (IF SHEET IS 34" X 22")



2 TYPICAL TUNNEL - DELUGE SYSTEM ZONES (SOUTH TUNNEL SHOWN)
SCALE: NOT TO SCALE

DETAIL NOTES:

1. SIGN MATERIAL IS 3M REFLECTIVE 280i VINYL, WHITE, WITH BLACK ADHESIVE LETTERING. SIGN BACKER MATERIAL IS 0.032" THICK ALUMINUM.
2. THE BOTTOM OF THE DELUGE ZONE SIGN WILL BE LOCATED APPROXIMATELY 3" ABOVE THE EXISTING TUNNEL SEGMENT SIGN.
3. FIRE ALARM CCTV CAMERAS WILL BE MOUNTED WITH BOTTOM OF LENS AT 4' BELOW THE CEILING TILE. EXISTING TRAFFIC CONTROL CAMERAS ARE MOUNTED WITH THE BOTTOM OF THE LENS AT APPROXIMATELY 7' 6" BELOW THE CEILING TILE.

IF THIS SHEET IS NOT 22"x34" IT IS NOT PLOTTED TO SCALE

BARNARD EJMT TEAM
BARNARD · RONDINELLI · BCER Engineering · Sturgeon Electric · Western States Fire Protection Co. · EYP Consulting Engineers

EISENHOWER/JOHNSON MEMORIAL TUNNEL
FIXED FIRE SUPPRESSION SYSTEM
DESIGN BUILD PROJECT
Project No. C0703-360 Subaccount 17810

RFC DOCUMENTS - 2015-03-27

Revisions
Num | Description | Date

DRAWN BY: B.T.L. | CHECKED BY: AEE,Jr

FIRE ALARM:
DETAILS - SYSTEM
SIGNAGE

Drawing Number
FA6.02

CCTV - 1,655

This Page Left Intentionally Blank

Scotchlite™
Reflective Sheeting Series 280

Description

Advantages

- Designed for imaging and electronic cutting with Gerber Scientific Equipment
- Long term, exterior durability
- Pressure-sensitive adhesive
- Durable, flexible, enclosed-lens, retroreflective film
- Retains 90% of its retroreflectivity when totally wet
- Similar daytime and nighttime appearance
- 3M™ Scotchlite™ Reflective Film 280-85 has a black daytime appearance but reflects white at night
- Resists cracking in cold climates

Applications and Uses

Scotchlite reflective sheeting series 280 is intended for making permanent, durable graphics when used with the listed Compatible Products in the following applications. These applications are warranted by the 3M™ MCS™ Warranty.

- Commercial vehicle graphics, commercial signs and striping

Limitations of Uses

We do not normally warrant other applications, but please contact us to discuss your needs or let us suggest other 3M products.

Specifically, we do not warrant this sheeting for the following:

- Regulated traffic signs
- Application to corrugated surfaces
- Application to stainless steel
- Graphics made for automotive Original Equipment Manufacturers (OEM); contact 3M Automotive Division at 1-800-328-1684, Ext. 444, for alternatives.

Compatible Products

- 3M™ Premask Tape SCPM-3
- 3M™ Prespace Tape SCPS-2
- 3M™ Scotchlite™ Edge Sealer 4433

Product Line

This information is subject to change. Be sure this is the most current Product Bulletin. See 3M Related Literature at the end of this bulletin.

Characteristic	Description
Product number and color	280-10 White 280-14 Orange 280-64 Gold 280-71 Yellow 280-72 Red 280-75 Blue 280-76 Light blue 280-77 Green 280-81 Lemon yellow 280-82 Ruby red 280-85 Black
Thickness (film and adhesive)	0.007 to 0.008 inch (0.18 to 0.20 mm)
Adhesive color and type	Clear, pressure-sensitive
Liner	78 pound, white kraft paper
Application surfaces	Flat, flat with rivets, or moderate curves
Application substrates	Acrylic, aluminum, fiberglass, FRP paint
Application temperature range (for air and substrate)	55° to 100°F (13° to 38°C) flat surface without rivets 60° to 100°F (15° to 38°C) flat surface with rivets
Removability	Permanent

Effective Performance Life

The effective performance life is based on field experience and exposure tests conducted throughout the United States. When the graphics are processed and used according to 3M recommendations, they should have the following performance life. The actual performance depends on the:

- Selection and preparation of the substrate
- Application methods
- Exposure conditions
- Cleaning methods

Effective Performance Life continued on the next page.

Warranted Durability

3M™ Scotchlite™ Reflective Sheeting Series 280	Overprint or Protective Clear	Vertical Exposure *face of graphic is vertical ± 10°* 				Non-Vertical Exposure *face of graphic is 10° to 45° from vertical* 			
		All film colors except 280-85		Film 280-85		All film colors except 280-85		Film 280-85	
		U.S.[1] *years*	S.W[2] *years*	U.S.[1] *years*	S.W[2] *years*	U.S.[1] *years*	S.W[2] *years*	U.S.[1] *years*	S.W[2] *years*
Vehicle Applications									
Unprinted film	None	7	5	5	4	5	-	3	-
Commercial Signs and Non-vehicle Applications									
Unprinted film	None	5	3	4	2	-	-	-	-
Railroad Applications									
Unprinted film	None	5	4	5	4	3	-	3	-

[1] For warranty periods outside the United States, contact the 3M sales organization for that country.

[2] The U.S. Desert Southwest includes Arizona, New Mexico, and the desert areas of California, Nevada, Utah, and Texas. A detailed map is available by request. The warranty for this area is reduced because there is more solar energy. This warranty applies to graphics that are exposed more than 50% of the time in the U.S. Desert Southwest.

Warranty Limitations

- 3M does not warrant sheeting series 280 for non-vertical applications greater than 45° from vertical. Film that is exposed at these angles may have a shorter life. The customer must assume the responsibility for testing and approving non-vertical exposures.
- Long exposure to continuous high heat decreases the effective performance life of this film by 2 years. High heat is a temperature above 150°F (65°C). It may occur in areas such as railroad locomotives, vehicle engine compartments, non-insulated tankers exposed to frequent internal steam cleaning, or compartments that carry hot cargo.

Cutting

⚠ Caution

When using any equipment, always follow the manufacturers' instructions for safe operation.

Recommended Cutting Methods

Sheeeting series 280 can be cut with any Gerber Scientific Products computer-driven cutting equipment. Before starting a cutting operation, consider these factors:

- Cutting and weeding capabilities of your equipment
- Font characteristics
- Physical stresses to which the graphic may be exposed

Design Factors

- Use a minimum letter height of 2 inches (5 cm).
- Use a minimum stroke width of 3/8 inch (1.0 cm).
- For uniform color and brightness when making a graphic with multiple pieces of sheeting series 280 together, be sure the pieces are properly color matched. See Instruction Bulletin 2.1 for details.

Factors That Affect Electronic Cutting Quality and Ability

- **Sharpness of the knife blade.** Dull blades create a serrated look on the edge of the cut film.
- **Weight on the knife blade.** The ideal weight results in a slight scoring of the liner. Too little weight results in incomplete cutting through the film and adhesive. Too much weight cuts the liner. It also causes the blade to drag, which accelerates wear, and eventually creates a serrated cut edge on the film.
- **Weeding.** Weed the film within 24 hours of cutting it. The adhesive may flow after cutting.

Prespacing and Premasking

The application tape to use depends on the type of graphic produced. See Instruction Bulletin 4.3 for details.

- For graphics that have a large amount of exposed liner, and/or small letters and/or narrow stroke width, use prespace tape SCPS-2.
- For graphics that have very little exposed liner, and/or large letters, and/or wide stroke width, use premask tape SCPM-3.

Application

- 3M™ Scotchlite™ Reflective Sheeting Series 280 is not positionable. Refer to Instruction Bulletin 5.5 for applying graphics with a pressure-sensitive adhesive.
- Do not apply graphics if the air or surface temperature is less than 55° F (13°C) on a flat surface without rivets, or 60°F (15°C) on a flat surface with rivets.
- At surface temperatures greater than 80°F (27°C), the film may pre-adhere to the application surface.
- Some substrates such as under-cured polyurethane paint, fiberglass, and some paint systems may continue to outgas for some time. Two-part polyurethane paints and clear coats may stop curing when the air and surface temperatures are below 75°F (24°C). Be aware that outgassing causes this film to bubble.

Edge Sealing

- 3M™ Scotchlite™ Edge Sealer 4433 is recommended for this film.
- Use edge sealer on processed and unprocessed graphics subjected to gasoline vapors or occasional gasoline spillage.
- Edge sealing is not required in the following applications, but it can help prevent edge lifting caused by external sources such as aggressive pressure washing. Use edge sealer 4433.
  - graphics subjected to severe abrasion or high pressure spray cleaners

    Exceeding 3M's pressure washing recommendations, as stated in Instruction Bulletin 6.5, will void the 3M warranty whether or not the graphic has been edge sealed.
  - graphics applied to truck roll-up doors
  - graphics applied to chrome

Removal

⚠ Warning

Solvents may ignite near heat or an open flame. To reduce the risk of a flash fire and serious injury, do not use heat sources near solvents.

Sheeting series 280 is not a removable product. Heat helps take off the top layer, but removing the adhesive requires a solvent-based remover.

Refer to Instruction Bulletin 6.5 for more details.

Shelf Life and Storage

- The shelf life of the sheeting cannot exceed 2 years from the date of receipt from 3M.
- Leave rolls of sheeting in the original shipping carton, or suspend the rolls horizontally.
- Store cut sheets lying flat.
- Store the sheeting in a clean, dry area, away from direct sunlight, and at a temperature less than 100°F (38°C).
- Ship the finished graphics lying flat or in a roll. To roll the graphic, wrap it sheeting-side-out on a minimum 6 inch (15 cm) diameter core. These methods help prevent the sheeting and premask from wrinkling or popping off the liner.

Health and Safety

⚠ Caution

When handling any chemical products, read the manufacturers' container labels and the Material Safety Data Sheets (MSDS) for important health, safety and environmental information.

To obtain MSDS sheets for 3M products:

- By fax, call 1-800-364-0768 in the US and Canada or 1-650-556-8417 for all other locations.
- Electronically, visit us at http://www.3M.com/MSDS.
- By mail, or in case of an emergency, call 1-800-364-3577 or 1-651-737-6501.

When using any equipment, always follow the manufacturers' instructions for safe operation.

Product Data

The values given are typical for sheeting series 280 and are not for use in specifications. The data given below are for sheeting as purchased from 3M.

Retroreflection

At a -4° entrance angle and a 0.2°observation angle, unprinted sheeting series 280i has the following typical coefficient of retroreflection. It is expressed in candlepower per foot-candle per square foot (candela/lux/square meter) per ASTME 810.

The entrance angle is formed by a light beam striking the surface at a point and at a line that is perpendicular to the surface at the same point.

An observation angle is formed by the light beam striking the reflective surface and returning to the observer. From 800 feet (249 meters), a motorist normally views a graphic at a 0.2° angle.

Film and Color		Typical Coefficient of Retroreflection
280-10	White	100
280-14	Orange	25
280-64	Gold	65
280-71	Yellow	60
280-72	Red	20
280-75	Blue	10
280-76	Light blue	10
280-77	Green	15
280-81	Lemon yellow	40
280-82	Ruby red	20
280-85	Black (reflects white)	30

These charts are for 3M™ Scotchlite™ Reflective Film Series 280.

Physical Properties

Property	English Units	Metric Units
Thickness (sheeting and adhesive)	0.007 to 0.008 inch	0.18 to 0.20 mm
Service temperature range	-30° to +200°F	-34° to +93°C
Applied shrinkage	0.015 inch	0.4 mm
Tensile strength	11 pound/inch at 73°F	2.0 kg/cm at 23°C

Adhesion Characteristics

(24 hours after application)

Substrate	English Units *pounds/inch*	Metric Units *kg/cm*
Aluminum, anodized	5.0	0.9
Aluminum, etched	5.0	0.9
FRP	3.9	0.7
Fruehauf prepainted panels	4.5	0.8

Chemical Resistance Characteristics

- Resists mild acids, mild alkalis, and salts
- Excellent water resistance

Warranty and Limited Remedy

The following is made in lieu of all other express or implied warranties, including any implied warranty of ***merchantability*** *or fitness for a particular purpose:* Film series 280 is warranted to be free of defects in materials and manufacture at the time of shipment and to meet the specifications stated in this Product Bulletin. 3M will replace or refund the price of any 3M materials that do not meet this warranty within the specified time periods. See the worldwide 3M™ MCS™ Warranty bulletin, which gives the terms and limitations of the warranty.

These remedies are exclusive. In no case shall 3M be liable for any direct, indirect or consequential damages, including any labor or non-3M material charges.

3M Related Literature

Listed below is related 3M technical literature that may be of interest. You may view and print these Bulletins from our Web site at www.scotchprint.com, or order them via our Fax-on-Demand (FOD) system. Call one of these phone numbers to order the desired bulletins, and specify the FOD document number provided in the chart.

United States or Canada: 1-800-364-0768
International: 1-651-732-6506

Subject	Bulletin No.	FOD No.
Instruction Bulletins		
Design of markings	2.1	5501
Scoring and cutting	4.1	6501
Premasking/prespacing	4.3	6503
Surface preparation -Non vehicular -Vehicular	5.1 5.2	7001 7002
Application to flat and curved surfaces, markings with pressure sensitive adhesive	5.5	7005
Storage, maintenance, removal	6.5	8505
Warranties		
Worldwide 3M MCS Warranty Packet *(includes all Commercial Graphics MCS Warranties)*		9503
Worldwide 3M MCS Warranty Overview-Folder		9504
3M MCS Graphics Warranty for Fleet Vehicle Applications *(includes overview)*		9506
Other 3M Literature		
Multi-Color Graphics Assembly	75-5100-0776-0	

GERBER EDGE is a registered trademark of Gerber Scientific Products.
GerberColor is a trademark of Gerber Scientific Products.

3M

Commercial Graphics Division
3M Center, Building 220-12E−04
PO Box 33220
St. Paul, MN 55133-3220 USA
General Info. 1-800-374-6772
Technical Info. 1-800-328-3908
Fax 1-651-736-4233

3M Canada
P.O. Box 5757
London, Ontario
Canada N6A 4T1
1-800-265-1840
Fax 519-452-6245

3M México, S.A. de C.V.
Av. Santa Fe No. 55
Col. Santa Fe, Del. Alvaro Obregón
México, D.F. 01210
52-55-52-70-04-00
Fax 52-55-52-70-22-77

3M Puerto Rico, Inc.
Puerto Rico Industrial Park
P.O. Box 100
Carolina, PR 00986-0100
787-620-3000
Fax 787-750-3035

Fax-on-Demand 800-364-0768 US/Canada or 650-556-8417 International
Fax-on-Demand document: 2001
www.3M.com/imagegraphics

40% pre-consumer waste paper
10% post-consumer waste paper

Printed in USA
 75-3455-9208-5

This Page Left Intentionally Blank

Certificate of Mill Test Results

PO/Rel

BL BR -000000-000

PART NO.

Attn:

NICHOLS ALUMINUM-NAA
CERTIFIED INSPECTION REPORT

To: O'NEAL FLAT ROLLED METALS
1229 SOUTH FULTON AVE
BRIGHTON, CO 80601
USA

Date: 10/30/14
Ship Date: 10/31/14

Nichols Sales Order Number: 117505
Customer Purchase Order No.: BR-24265
Nichols Part No.: 124621

Line Number: 1
Customer Part No.: NA124621
Bill of Lading No.: NAA42944
Total Net Weight: 39,658.0

Description: .0290X49.000 3105 H24 WHITE(1118)/CLEAR

CHEMICAL INFORMATION:

Coil #	SI	FE	CU	MN	MG	CR	ZN	TI
589501	0.37	0.68	0.19	0.49	0.55	0.08	0.17	0.03
589502	0.37	0.68	0.19	0.49	0.55	0.08	0.17	0.03
589503	0.37	0.68	0.19	0.49	0.55	0.08	0.17	0.03

MECHANICAL INFORMATION:

Coil #	H/T	UTS (KSI)	YTS (KSI)	%EL		
589501	H	26.8	22.6	11	Actual Gauge =	0.0287
589502	H	27.1	23.0	11	Actual Gauge =	0.0289
589503	H	26.8	22.7	10	Actual Gauge =	0.0285

Report approved by Nichols Aluminum Quality Manager

This product conforms to the applicable paragraphs of ASTM B209 (latest revision).

MATERIAL WAS MELTED, ROLLED AND PROCESSED IN THE USA

This Page Left Intentionally Blank

FACCTV SYSTEM PARTS LIST SECTION

Operations & Maintenance Manual
December 2015

This Page Left Intentionally Blank

Eisenhower Johnson Memorial Tunnel - EMJT
Fixed Fire Suppression System Project
Parts List

Part #	Description	Qnty
ACC5.0	Avigilon Control Center Software	3
4MN-HD-RMWS	Avigilon Remote Monitoring Workstation	3
5.0TB-HD-NVR2	HD Network Video Recorder Server, 5.0 TB Storage	2
NS3550-8T-2S	IFS Gigabit Managed Switch	24
S30-2SLC-10	Gigabit 1000Base-SX Fiber SFP Transceiver, SM	48
S30-RJ	Gigabit RJ-45 Transceiver, Cat5e	24
P2213	Dell 22" Video Display Monitor	6
ML15B	Wall Mount Monitor Bracket	6
E2210	Ethernet Micro RTU Controller, 12 DI, 8 DO	16
SMT1500RM2U	Uninterruptable Power Source (UPS), 1000W, Rack Mount, CCTV Head	2
	End Equipment	
BR1500G	Uninterruptable Power Source (UPS), 865W, CCTV Workstation	3
WRK-44SA-32	Floor Mounted Rack, 24-1/4"W x 32-5/8"D x 83-1/8"H *	
	* Racks hold the CCTV head end equipment, the LIOS FOLHD detector,	4
	the WAGO I/O equipment, and the FA System monitoring and control	
	interface equipment.	
MW-ST	Solid Rack Top	4
BPS10A	Remote Booster Power Supply, 10 Amp *	2
	* Shared power supply between Equipment Rack Fire Alarm and	
	FA CCTV Equipment	
BPS10A	Remote Booster Power Supply, 10 Amp *	20
	* Shared power supply between Fire Protection Cabinet Fire Alarm	
	and FA CCTV Equipment	
SLA1116	Sealed Lead Acid Battery, 18AH *	4
	* Shared battery between Equipment Rack Fire Alarm and	
	FA CCTV Equipment	
SLA1097	Selad Lead Acid Battery,10AH *	40
	* Shared battery between Fire Protection Cabinet Fire Alarm	
	and FA CCTV Equipment	
CSH00338	Tempco Strip Heater, 120vAC, 125W	20
	* Shared strip heater between Fire Protection Cabinet Fire Alarm	
	and FA CCTV Equipment	
01160.0-00	Stego Thermostat, 41F - 59F, Heater Start	20
01161.0-02	Stego Thermostat, 77F - 95F, Heater Stop	20
01161.0-00	Stego Thermostat, 104F-122F, High Temp Alarm	20
01142.0-00	Stego Thermostat, -10C (14F) - 50C (122F) , Low Temp Alm	20
	* Shared thermostats between Fire Protection Cabinet Fire Alarm	
	and FA CCTV Equipment	
2.0W-H3PTZ-DP20	CCTV Dome Camera, 2.0 Mp, Day/Night, 20x	24
MNT-PEND-WALL	Indoor/Outdoor Pendant Mount Bracket	24
FA6.02	Tunnel Signage	183

This Page Left Intentionally Blank

FA CCTV SYSTEM RECOMMENDED SPARE PARTS LIST SECTION

Operations & Maintenance Manual
December 2015

This Page Left Intentionally Blank

Eisenhower Johnson Memorial Tunnel - EMJT
Fixed Fire Suppression System Project
Recommend Spare Parts List

Part #	Description	Qnty
ACC5.0	Avigilon Control Center Software	0
4MN-HD-RMWS	Avigilon Remote Monitoring Workstation	0
5.0TB-HD-NVR2	HD Network Video Recorder Server, 5.0 TB Storage	0
NS3550-8T-2S	IFS Gigabit Managed Switch	1
S30-2SLC-10	Gigabit 1000Base-SX Fiber SFP Transceiver, SM	2
S30-RJ	Gigabit RJ-45 Transceiver, Cat5e	2
P2213	Dell 22" Video Display Monitor	0
ML15B	Wall Mount Monitor Bracket	0
E2210	Ethernet Micro RTU Controller, 12 DI, 8 DO	1
SMT1500RM2U	Uninterruptable Power Source (UPS), 1000W, Rack Mount, CCTV Head	0
	End Equipment	
BR1500G	Uninterruptable Power Source (UPS), 865W, CCTV Workstation	0
WRK-44SA-32	Floor Mounted Rack, 24-1/4"W x 32-5/8"D x 83-1/8"H *	
	* Racks hold the CCTV head end equipment, the LIOS FOLHD detector,	0
	the WAGO I/O equipment, and the FA System monitoring and control	
	interface equipment.	
MW-ST	Solid Rack Top	0
BPS10A	Remote Booster Power Supply, 10 Amp *	0
	* Shared power supply between Equipment Rack Fire Alarm and	
	FA CCTV Equipment	
BPS10A	Remote Booster Power Supply, 10 Amp *	0
	* Shared power supply between Fire Protection Cabinet Fire Alarm	
	and FA CCTV Equipment	
SLA1116	Sealed Lead Acid Battery, 18AH *	0
	* Shared battery between Equipment Rack Fire Alarm and	
	FA CCTV Equipment	
SLA1097	Selad Lead Acid Battery,10AH *	0
	* Shared battery between Fire Protection Cabinet Fire Alarm	
	and FA CCTV Equipment	
CSH00338	Tempco Strip Heater, 120vAC, 125W	0
	* Shared strip heater between Fire Protection Cabinet Fire Alarm	
	and FA CCTV Equipment	
01160.0-00	Stego Thermostat, 41F - 59F, Heater Start	0
01161.0-02	Stego Thermostat, 77F - 95F, Heater Stop	0
01161.0-00	Stego Thermostat, 104F-122F, High Temp Alarm	0
01142.0-00	Stego Thermostat, -10C (14F) - 50C (122F) , Low Temp Alm	0
	* Shared thermostats between Fire Protection Cabinet Fire Alarm	
	and FA CCTV Equipment	
2.0W-H3PTZ-DP20	CCTV Dome Camera, 2.0 Mp, Day/Night, 20x	1
MNT-PEND-WALL	Indoor/Outdoor Pendant Mount Bracket	1
FA6.02	Tunnel Signage	0

This Page Left Intentionally Blank

Eisenhower Johnson Memorial Tunnel
Fixed Fire Suppression System
FA CCTV Equipment & Service Providers

Local Equipment & Service Provider

Systems Group
800 East 64th Avenue, Unit 17
Denver, CO 80229

Tunnel Signage Placard

Easter Owens
6692 Fig Street
Arvada, CO 80004

Tunnel Signage Vinyl
A Cut Above Engraving
PO Box 1194
Broomfield, CO 80038-1194

FA CCTV Equipment (Cameras, Workstations, NVR)

Avigilon USA Corporation
700-1717 McKinney Avenue
Dallas, TX 75202

Network Switches

Lenel Systems International, Inc.
Lockbox 223229
Pittsburgh, PA 15251-2229

Network Ethernet RTUs

MOXA
601 Valencia, Suite 100
Brea, CA 92823

This Page Left Intentionally Blank

FA CCTV SYSTEM CONSUMABLE SUPPLIES SECTION

Operations & Maintenance Manual
December 2015

This Page Left Intentionally Blank

Eisenhower Johnson Memorial Tunnel
Fixed Fire Suppression System
FA CCTV System

Consumable Supplies

The FA CCTV System and all associates components have no required consumables for normal operations, nor for any ongoing testing and maintenance operations.

This Page Left Intentionally Blank

FA CCTV SYSTEM TESTING & COMMISSIONING SECTION

Operations & Maintenance Manual
December 2015

This Page Left Intentionally Blank

Eisenhower Johnson Memorial Tunnel
Fixed Fire Suppression System
FA CCTV System

Testing & Maintenance Requirements

The FA CCTV System is essentially maintenance free; however, some general maintenance is required on the system databases to insure that the System stays in optimal operating performance:

The System databases should be copied off routinely, to insure adequate permanent records are maintained for previous incidents; as well as, to allow adequate space for new incidents to be stored for viewing or other activities.

The System databases should subject to a disk clean-up and de-fragmentation process to keep the on-board storage memory in optimal operation. This is similar to what you do with your typical PC database on an ongoing basis.

Additional required testing of the FA CCTV System, as a function of the overall fixed fire suppression system is addressed in the Short Term Operation Plan (STOP) and the Annual Maintenance Plan (AMP), which are provided under separate submittal.