Administrator Console 5.5.2

User Manual

MARCH networks

TRANSFORMING THE WAY YOU VIEW YOUR BUSINESS

About March Networks

March Networks® (TSX:MN) is a global provider of intelligent IP video solutions. For close to a decade, the company has helped some of the world's largest commercial and government organizations transition from traditional CCTV to networked video surveillance used for advanced security, loss prevention and risk mitigation. VideoSphere®, the company's enterprise-class video management portfolio, includes open-platform VMS software complemented by high-definition IP cameras, encoders, video analytics and recording platforms, as well as outstanding professional and managed services. March Networks systems are delivered through an extensive distribution and partner network and currently support over one million channels of video in more than 50 countries.
www.marchnetworks.com.

Our Commitment to a Green Tomorrow

March Networks takes pride in its commitment to social responsibility and environmental sustainability. Our employees, suppliers and valued partners are passionate about designing environmentally friendly solutions for our customers and minimizing the company's carbon footprint.

We embrace environmental sustainability as part of our overall strategy and business values with multiple initiatives to ensure that we do our part to create a cleaner, healthier environment for future generations. The steps we have taken affect all aspects of our organization and involve our senior management team, employees, suppliers, partners and customers. You can receive further details at:
Company General: http://www.marchnetworks.com/resources/default.aspx?id=81
Product Specific: http://www.marchnetworks.com/Files/RoHS-WEEE_Compliance_Statement_EN.pdf

Customer Support and Assistance

North America

Telephone — 613 591 1441
Toll Free (US & Canada) — 1 800 472 0116
Fax — 1 613 591 1858
E-mail — techsupport@marchnetworks.com

EMEA

Telephone — +39 0362 17935 extension 3 (CET)
Fax — +39 0362 17935 90
E-mail — milantechsupport@marchnetworks.com

APAC

For former March Networks Products:

Telephone — 1 613 591 1441
Fax — 1 613 591 1858
E-mail — techsupport@marchnetworks.com

For former Cieffe Products and VMS:

Telephone — +39 0362 17935 extension 3 (CET)
Fax — +39 0362 17935 90
E-mail — milantechsupport@marchnetworks.com

Providing Documentation Feedback

At March Networks, our goal is to produce documentation that is technically accurate and informative. If you have comments or suggestions about our online Help and documentation, you can e-mail us at: techwriters@marchnetworks.com.

Trademarks

Notice of Rights

Part Number

MC-23897 1.0 Most Recent Revision: June 2, 2010

Table of Contents

Welcome to the Administrator Console

The Administrator Console is an integral part of the VideoSphere Visual Intelligence suite that lets security and IT staff customize and maintain recorders in a local or centralized manner. This chapter introduces the Administrator Console as part of the VideoSphere Visual Intelligence suite.

This guide outlines the configuration, maintenance, and administration activities that administrators can perform to set up their system and maintain up-to-date health and status information for recorders.

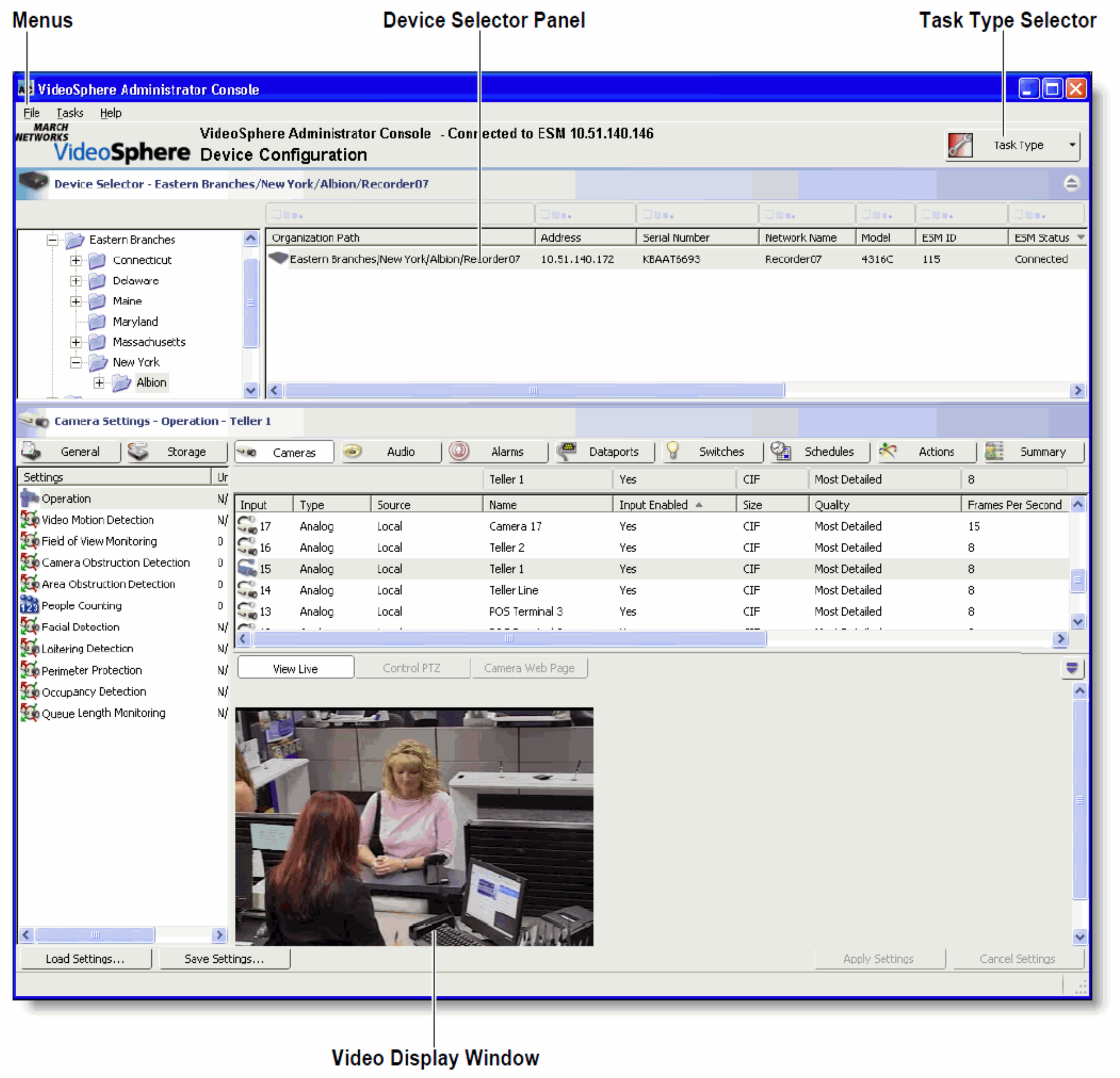
Additional VideoSphere Visual Intelligence suite publications are available in PDF format on your March Networks CD.

The following topics are covered in this chapter:

- “Components of the Administrator Console” on page 2
- “Recorder Installation, Configuration, and Maintenance” on page 3
- “Multi-Site Management of Recorders” on page 3
- “Understanding the Product Suite” on page 4

Components of the Administrator Console

The following figure shows the key components of the Administrator Console.



VideoSphere Administrator Console - Connected to ESM 10.51.140.146

Device Configuration

Device Selector - Eastern Branches/New York/Albion/Recorder07

Organization Path	Address	Serial Number	Network Name	Model	ESM ID	ESM Status
Eastern Branches/New York/Albion/Recorder07	10.51.140.172	KBAAT6693	Recorder07	4316C	115	Connected

Camera Settings - Operation - Teller 1

Settings	Ur
Operation	N/
Video Motion Detection	N/
Field of View Monitoring	0
Camera Obstruction Detection	0
Area Obstruction Detection	0
People Counting	0
Facial Detection	N/
Loitering Detection	N/
Perimeter Protection	N/
Occupancy Detection	N/
Queue Length Monitoring	N/

Input	Type	Source	Name	Input Enabled	Size	Quality	Frames Per Second
			Teller 1	Yes	CIF	Most Detailed	8
17	Analog	Local	Camera 17	Yes	CIF	Most Detailed	15
16	Analog	Local	Teller 2	Yes	CIF	Most Detailed	8
15	Analog	Local	Teller 1	Yes	CIF	Most Detailed	8
14	Analog	Local	Teller Line	Yes	CIF	Most Detailed	8
13	Analog	Local	POS Terminal 3	Yes	CIF	Most Detailed	8

Recorder Installation, Configuration, and Maintenance

All recorders are pre-configured to operate at optimum settings for most environments. In addition, as cameras are added to a recorder, they are automatically enabled and start capturing video.

As part of your system installation, programming, and maintenance tasks, you can:

- Locally or remotely access each connected peripheral and verify that the peripheral is working properly. For example, you can view video or test an alarm.
- Customize the peripheral settings to better meet your organization’s needs. For example, you can specify higher video capture frame rates for cameras monitoring important views.
- Ensure the recorder is functioning properly by reviewing its general status. For example, you can check the network settings, review hard drive temperatures, and assess storage targets.

Multi-Site Management of Recorders

The Administrator Console lets you manage recorders at different sites from one central location. This can be accomplished in two ways:

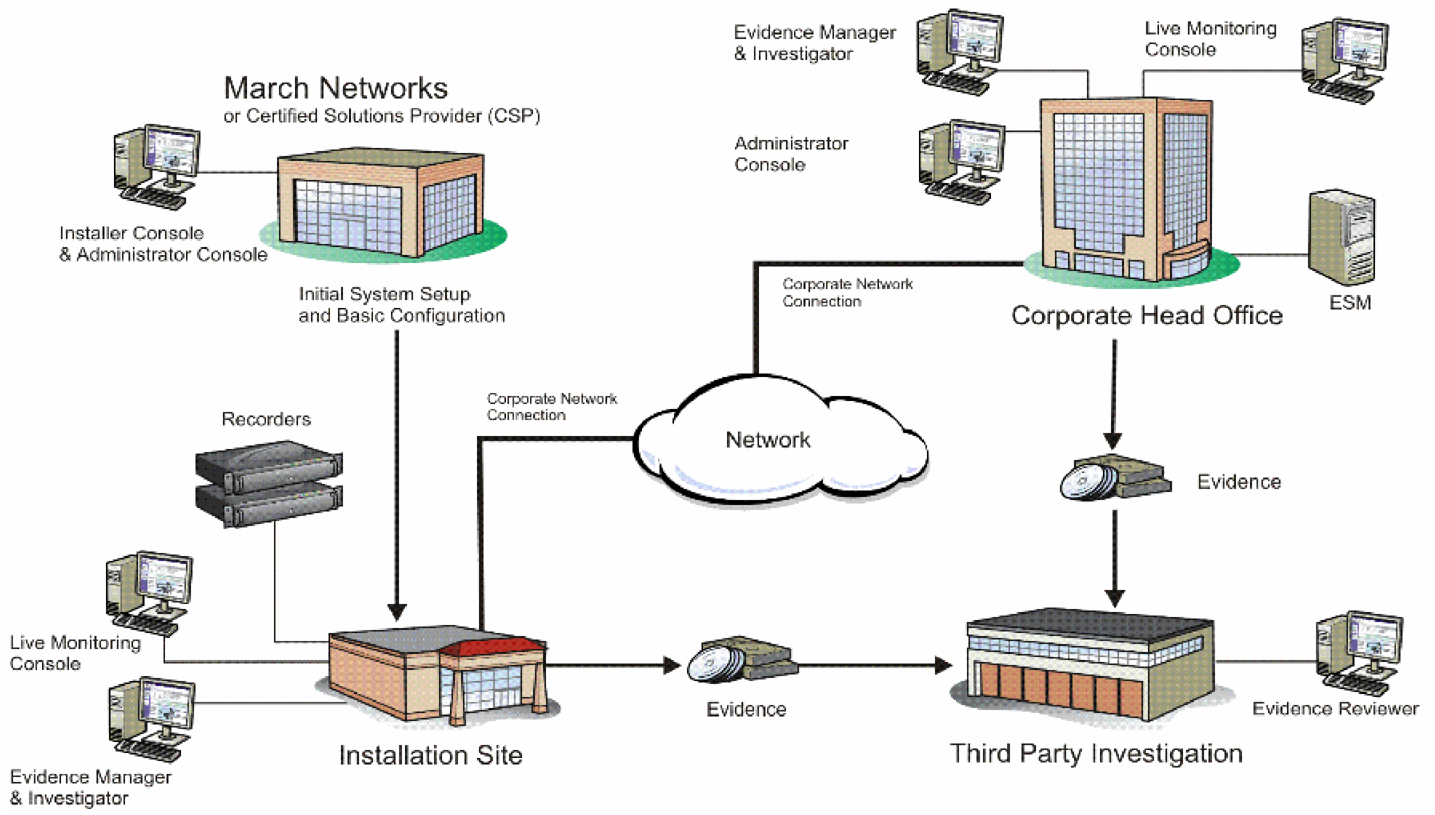
- By directly communicating with each recorder on the network.
- Or, by communicating through an Enterprise Service Manager (ESM), which is in constant communication with each recorder.

From the Administrator Console you can:

- Access a system-wide status of recorders. In addition to this, alerts can be received in real-time to ensure timely resolution of recorder health issues.
- View a summary of users and quickly review their access rights. Access rights can be modified to restrict users from performing certain tasks, and restrict the recorders and peripherals they can access.
- Organize recorders into a hierarchy that matches your organization.
- Centrally configure multiple recorders. This can include upgrading recorders to the latest software release or applying custom changes.

Understanding the Product Suite

The following illustration and table provide an overview of the VideoSphere Visual Intelligence suite. They also highlight the relationship between the components, including the Installer Console, Administrator Console, Evidence Manager and Investigator, Live Monitoring Console, Evidence Reviewer, and ESM.



Component	Description
Recorders	Devices at your site that capture, retain, and stream audio, video, and text data from connected peripherals.
Recorder installation, configuration, and management tools	
Installer Console	A setup tool that lets installers test the peripherals connected to the recorder.
Administrator Console	A configuration and maintenance tool that lets security and IT staff customize and maintain recorders in a central or local manner.

Component	Description
Evidence retrieval and management tools	
Evidence Manager and Investigator	The *Evidence Manager* provides senior loss prevention, security, or operations managers with the tools for building and managing investigation cases. The *Investigator* lets security, theft, and fraud investigators locate video evidence linked to an investigation. The Investigator works alongside the Evidence Manager to allow users to quickly locate video evidence and then organize the evidence for distribution to third-party investigators or law enforcement authorities.
Live video playback tools	
Live Monitoring Console	A monitoring tool that lets individuals view live video and receive real-time notification of alarms.
Evidence and case viewing tools	
Evidence Reviewer	A playback tool that allows third-party investigators or law enforcement authorities to view video captured by the recorder and review cases created with the Evidence Manager. To ensure that others can review evidence copied to CD, the Evidence Reviewer can be included when evidence is burned to CD from the Evidence Manager or Investigator.
Recorder management	
ESM	Enterprise Service Manager. A server application that lets you monitor and maintain recorders on your network, at one or more sites. The ESM can be made up of one or more servers, which form a cluster.

Chapter 2

Installing, Uninstalling, and Starting the Administrator Console

This chapter describes how to install, uninstall, and start the Administrator Console. The following topics are covered in this chapter:

- “System Requirements” on page 8
- “Installing the Administrator Console” on page 8
- “Uninstalling the Administrator Console” on page 9
- “Starting the Administrator Console” on page 9

System Requirements

Before you install the Administrator Console, ensure your system meets the following recommended requirements:

- Computer with 3.0 GHz equivalent (or higher) processor
- One of the following operating systems:
  - Microsoft® Windows® XP Professional SP3
  - Microsoft® Windows® Vista Home Premium SP1
  - Microsoft® Windows® Vista Business SP1
  - Microsoft® Windows® Vista Enterprise SP1
  - Microsoft® Windows® Vista Ultimate SP1
- 2.0 GB (or higher) of system RAM
- Quad-speed (or faster) CD-ROM drive
- 10/100 Mbps Ethernet card
- Sound card with speakers or headphones (only required when working with a recorder that has connected audio inputs, such as microphones)
- 40 MB of space free on hard drive for software
- Screen color depth: 32-bit
- Video card:
  - Video RAM: 64 MB
  - Screen Resolution: 1280 x 1024 (or greater)
- Wheel mouse (for use with PTZ cameras only)

NOTE: Workstations that do not meet the recommendations specified above may be used for lower performance requirements or in environments with small numbers of recorders.

NOTE: For the online Help to function properly, you must enable JavaScript in your Web browser. For more information about enabling JavaScript, see the documentation accompanying your Web browser.

Installing the Administrator Console

Use your March Networks CD to install the Administrator Console.

To install the Administrator Console

1. Insert your March Networks CD into your computer's CD-ROM drive.

   The **Software Installation** page appears automatically. If this page does not appear automatically, use Microsoft Windows Explorer to locate the **setup.exe** file on the CD and then double-click **setup.exe**.
2. On the **Software Installation** page, click the application you want to install. As you move your pointer over each link, a brief description of the application appears.

3. Follow the installation wizard prompts to install the application.

   During the installation you are asked if you will be using an ESM. If your organization has an ESM that centrally monitors and maintains your March Networks recorders, click **Yes** and then type the ESM's IP address in the **Address** box.

   If you indicate that you are using an ESM, you are prompted to enter a user name and password when you start the Administrator Console.

Uninstalling the Administrator Console

If you no longer need the application, you can remove it using the **Add or Remove Programs** option in your computer's control panel. For more information about removing programs, see the documentation accompanying Microsoft Windows.

Starting the Administrator Console

After the installation completes, a shortcut appears on your computer's desktop and is also inserted into the Microsoft Windows Start menu. Use this shortcut to start the application.

If you indicated during installation of the Administrator Console that you are using an ESM, when you start the Administrator Console, you are prompted to enter a user name and password.

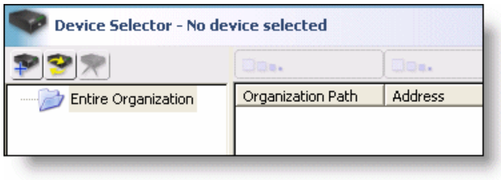
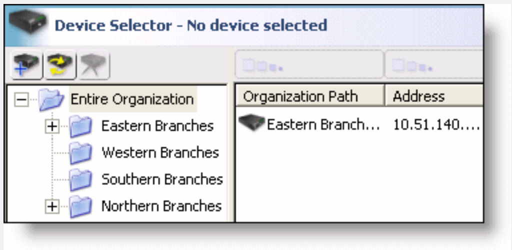
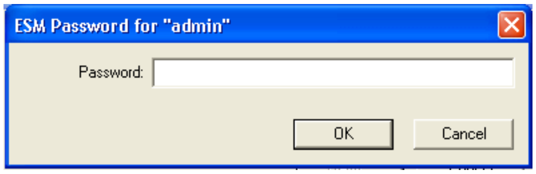
Accessing Recorders

This chapter describes the various ways to access recorders. The following topics are covered:

- "Connecting to Recorders" on page 12
- "Configuring a Dial-Up Recorder" on page 13
- "Accessing a Dial-Up Recorder" on page 15
- "Accessing an Intermittently-Connected Recorder" on page 15
- "Connecting to an ESM" on page 16

Connecting to Recorders

When you start the Administrator Console, one of the scenarios listed in the table below occurs:

Scenario	Example and details
The **Device Selector** panel is empty.	 Organization Path | Address Click **Detect Devices** to automatically add recorders to the list, or click the **Add Device** button to manually add a recorder using its IP address or network name. For details, see "To add a recorder" on page 12.
A list of previously-added recorders appears.	 Device Selector - No device selected Entire Organization Eastern Branches Western Branches Southern Branches Northern Branches Organization Path | Address Eastern Branch... | 10.51.140.... Click a recorder to access it. If you want to access a recorder that is managed by an ESM, you must connect to the ESM before the recorder will appear in the panel. For more information, see "Connecting to an ESM" on page 16.
You are prompted for a password to connect to an ESM.	 Password: Log on to the ESM. For more information, see "Connecting to an ESM" on page 16.

To add a recorder

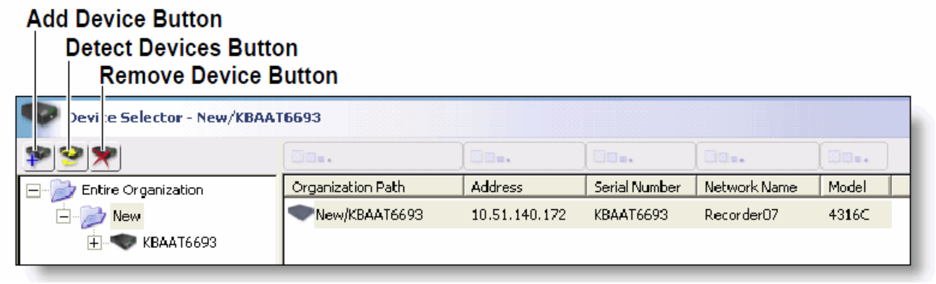
1. Ensure the **Device Installation** task type is selected.
2. Do one of the following tasks:
   - **Manually add a recorder.** Click the **Add Device** button and then type the recorder's IP address or network name.
   - **Detect recorders on your network's subnet.** Click the **Detect Devices** button.

   If this is the first time the recorder is being accessed by the March Networks software, or if it has not yet been organized within a folder, the recorder appears in the **New** folder. If the recorder had been previously deleted and then added again, the recorder is placed in its original folder structure.

   After you add the recorder, you do not need to add it again. It automatically appears in the **Entire Organization** folder each time you start the application.

   When you are connected to an ESM, the recorders managed by the ESM appear automatically — you do not need to add them.

NOTE: You can remove a recorder from the **Device Selector** panel by clicking it and then clicking the **Remove Device** button.



Organization Path	Address	Serial Number	Network Name	Model
New/KBAAT6693	10.51.140.172	KBAAT6693	Recorder07	4316C

Configuring a Dial-Up Recorder

If a recorder is installed in a location that does not have network access, you can configure it to communicate over a dial-up (telephone) connection.

NOTE: This section outlines how to configure a dial-up recorder in an organization that does not use an ESM. If your recorder is managed by an ESM, the steps for accessing a dial-up recorder are slightly different. For more information, see the *Setting Up Units for Dial-up Connection Technical Instructions* included on your March Networks CD.

After you configure the recorder for dial-up connection, you can add it to the March Networks applications, such as the Investigator, and connect to it.

To configure the recorder's dial-up settings, perform the following tasks:

- Connect a USB modem to the recorder. For more information, see the documentation accompanying the recorder.
- Configure the recorder's dial-up settings using the *setppp* command in the unit's built-in provisioning interface. For more information, see the *Provisioning Interface Technical Instructions* included on your March Networks CD. If you are working in a non-managed environment, ensure you choose the server mode when you use the *setppp* command.
- Create a dial-up networking entry on your computer for modem connection. For more information, see "To create a dial-up networking entry for modem connection" on page 14.

After you configure and establish a dial-up connection, the March Networks applications, such as the Investigator, can connect to the recorder. For more information, see "Accessing a Dial-Up Recorder" on page 15.

You can configure the recorder to periodically dial a Remote Access Service (RAS) server at intervals you specify to communicate health and status information to the Administrator Console.

If your computer has access to both a network and a dial-up connection, you can configure the Administrator Console to attempt to connect to the recorder over the network first.

If the connection is unsuccessful, the Administrator Console then attempts to connect to the recorder using the dial-up connection.

For information about the two options outlined above, see the *Setting Up Units for Dial-up Connection Technical Instructions* included on your March Networks CD.

To create a dial-up networking entry for modem connection

When you are working with a dial-up recorder in a non-managed environment, you must first create a dial-up networking entry for modem connection. Using Microsoft Windows Dial-Up Networking, create an entry using the following settings:

- **TCP/IP Settings**. Use the default values. Ensure the **Use default gateway on remote network** check box is not selected. If the check box is selected, Microsoft Windows attempts to use the dial-up interface for your regular network communication.
- **User name and password**. The user name is **DVRDialup** and the password is **MarchDVR**.
- **Testing the dial-up connection**. To test the dial-up connection, ping the recorder by typing ping **192.168.200.1** at the command line prompt. This is the factory default IP address for the recorder over a dial-up connection. If you receive a reply, you are successfully connected to the recorder. If you fail to connect, ensure the recorder is connected to a modem.
- **Enable hardware flow control.** After you create the dial-up networking entry, ensure the hardware flow control option is enabled for the modem. For more information, see the documentation accompanying Microsoft Windows.

You can specify that you want to save the password. If you do not save the password, the March Networks applications cannot connect to the recorder directly.

If you change the dial-up networking password for a recorder, you must also change the saved password in its Phonebook Entry, or override the password for the recorder.

Ensure you create a phonebook entry on every computer that will be used to connect to the dial-up recorder, or change the dial-up recorder's dialing information. Use the same name for every phonebook entry you create. For example, if you name the first phonebook entry recorders, you must name all other phonebook entries recorders on the other computers.

Accessing a Dial-Up Recorder

To access a dial-up recorder using the Administrator Console, you must first establish a dial-up connection between your computer and the dial-up recorder. After the connection is established, you can add the dial-up recorder to the Administrator Console.

NOTE: This section outlines how to configure a dial-up recorder in an organization that does not use an ESM. If your recorder is managed by an ESM, the steps for accessing a dial-up recorder are slightly different. For more information, see the *Setting Up Units for Dial-up Connection Technical Instructions* included on your March Networks CD.

If you have not yet configured the dial-up recorder, you must first configure the dial-up settings. For more information, see "Configuring a Dial-Up Recorder" on page 13.

To access a dial-up recorder

1. Ensure the dial-up networking entry has been created using Microsoft Windows. If it has not yet been created, see "To create a dial-up networking entry for modem connection" on page 14.
2. Using Microsoft Windows Dial-Up Networking, dial the recorder. For more information, see the documentation accompanying Microsoft Windows.
3. After your computer connects to the dial-up recorder, click the **Add Device** button in the Administrator Console.

   The **Add Device** dialog box appears.
4. Type **192.168.200.1**. This is the factory default IP address for dial-up recorders.

NOTE: If you want to add a dial-up recorder that is configured to communicate with an ESM, the steps for adding the dial-up recorder are slightly different. For more information, see the *Setting Up Units for Dial-up Connection Technical Instructions* included on your March Networks CD.

Accessing an Intermittently-Connected Recorder

You can access a recorder that is configured with an intermittent connection in a managed environment. Configuring a recorder with an intermittent connection allows you to conserve network bandwidth usage because it contacts the ESM only at specified intervals, and stays connected to the Administrator Console for 15 minute increments.

An intermittent connection ensures that recorders can be monitored for health and accessed for video download or configuration changes without requiring a constant network connection.

The connection between the recorder and the ESM is terminated if there is no data exchanged for two minutes.

For information about configuring a recorder for intermittent connection, see the *Installing a Recorder and Testing Peripheral Connections Quick Steps* publication included on your March Networks CD.

To access an intermittently-connected recorder

Click the recorder in the **Device Selector** panel.

The recorder connects to the Administrator Console. It is automatically disconnected after 15 minutes.

If you delete an intermittently-connected recorder from the recorder list and then add it again, the recorder will establish a permanent connection.

Connecting to an ESM

If your organization uses an ESM to centrally monitor and maintain recorders on the network, you can specify your user name and password to connect to the ESM.

If your organization does not use an ESM, you can proceed to the next section in this publication.

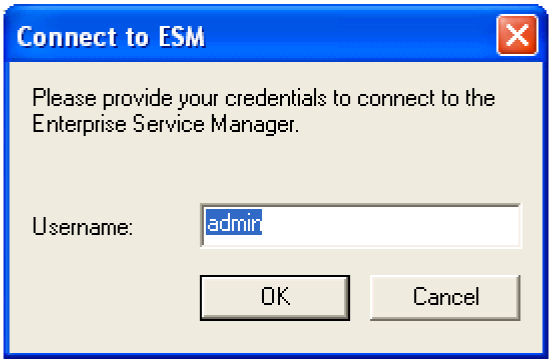
When you connect to the ESM, additional features are available that let you centrally monitor and maintain March Networks recorders on your network, such as simultaneous recorder updates and user account management.

To connect to an ESM

1. On the **File** menu, click **Connect to ESM**.

   The **Connect to ESM** option is not available on the **File** menu if the Administrator Console is not configured to connect to an ESM. For information about configuring the Administrator Console to connect to an ESM, see “To modify the ESM connection information” on page 17.

   The **Connect to ESM** dialog box appears.



Connect to ESM

Please provide your credentials to connect to the Enterprise Service Manager.

Username: admin

2. Type your user name and password.

   Depending on how you configured the Administrator Console, you may first be prompted to choose an ESM before you type your user name and password.

3. Click **OK**.

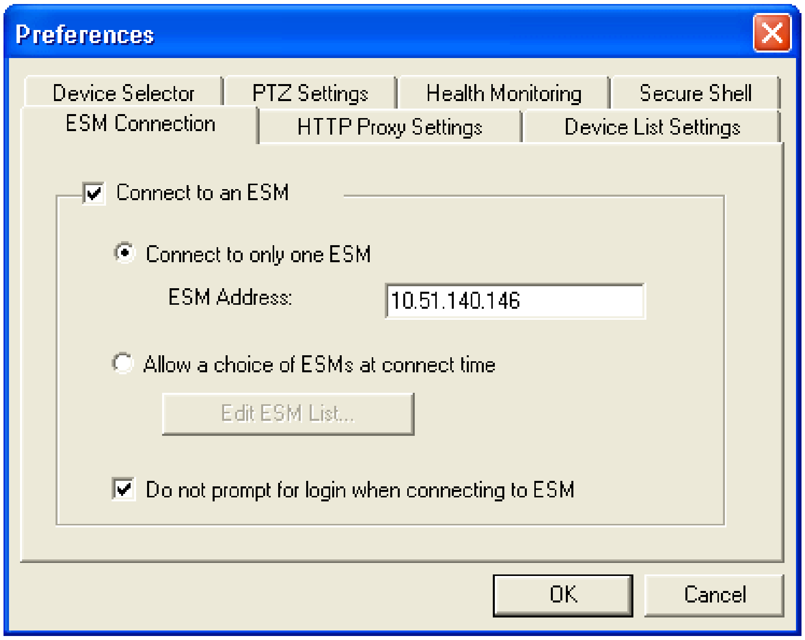
NOTE: To disconnect from the ESM, click **Disconnect from ESM** on the **File** menu.

To modify the ESM connection information

1. On the **File** menu, click **Preferences**.

   The **Preferences** dialog box appears.

2. Click the **ESM Connection** tab.



☑ Connect to an ESM

● Connect to only one ESM

ESM Address: 10.51.140.146

○ Allow a choice of ESMs at connect time

☑ Do not prompt for login when connecting to ESM

3. Specify the ESM connection information.

4. Click the ESM connection option that meets your needs:

   - **Connect to only one ESM**. You will always connect to a single ESM when you start the application.
   - **Allow a choice of ESMs at connect time**. You can choose from a list of ESMs each time you start the application. Click **Edit ESM List** and add the ESMs that you want to appear in the list when you start the Administrator Console.

5. You can configure the Administrator Console to automatically use your Microsoft Windows user credentials to log on to the ESM. This is the SSPI (Security Support Provider Interface) authentication method and it removes the need to type your user name and password each time you start the Administrator Console application. To do this, select the **Do not prompt for login when connecting to ESM** check box.

   For this option to work, the following conditions must be met:

   - You must have an ESM user account with the same user name as your Microsoft Windows user account (see “To create a user account” on page 190).
   - You must select the **SSPI** authentication method when you create the ESM user account (see “To create a user account” on page 190).
   - The ESM server (or servers if clustered) must be in the same domain as the client computer where your Administrator Console is installed.

   For information about creating user accounts, see “Creating User Profiles and Accounts” on page 188.

6. Click **OK**.

   The next time you start the Administrator Console, your changes take effect.

Chapter 4

Device Installation Tasks

The Device Installation task type allows you to view general information about the recorders and test the peripherals, such as cameras and alarms, connected to a recorder installed at your site.

The following topics are covered in this chapter:

- "Viewing Recorder Details"
- "Viewing and Configuring Network Settings"
- "Applying Licenses"
- "Services"
- "Reviewing Storage Information"
- "Testing Analog Cameras"
- "Testing IP Cameras"
- "Testing Audio"
- "Testing Alarms"
- "Testing Dataports"
- "Testing Switches"

Viewing Recorder Details

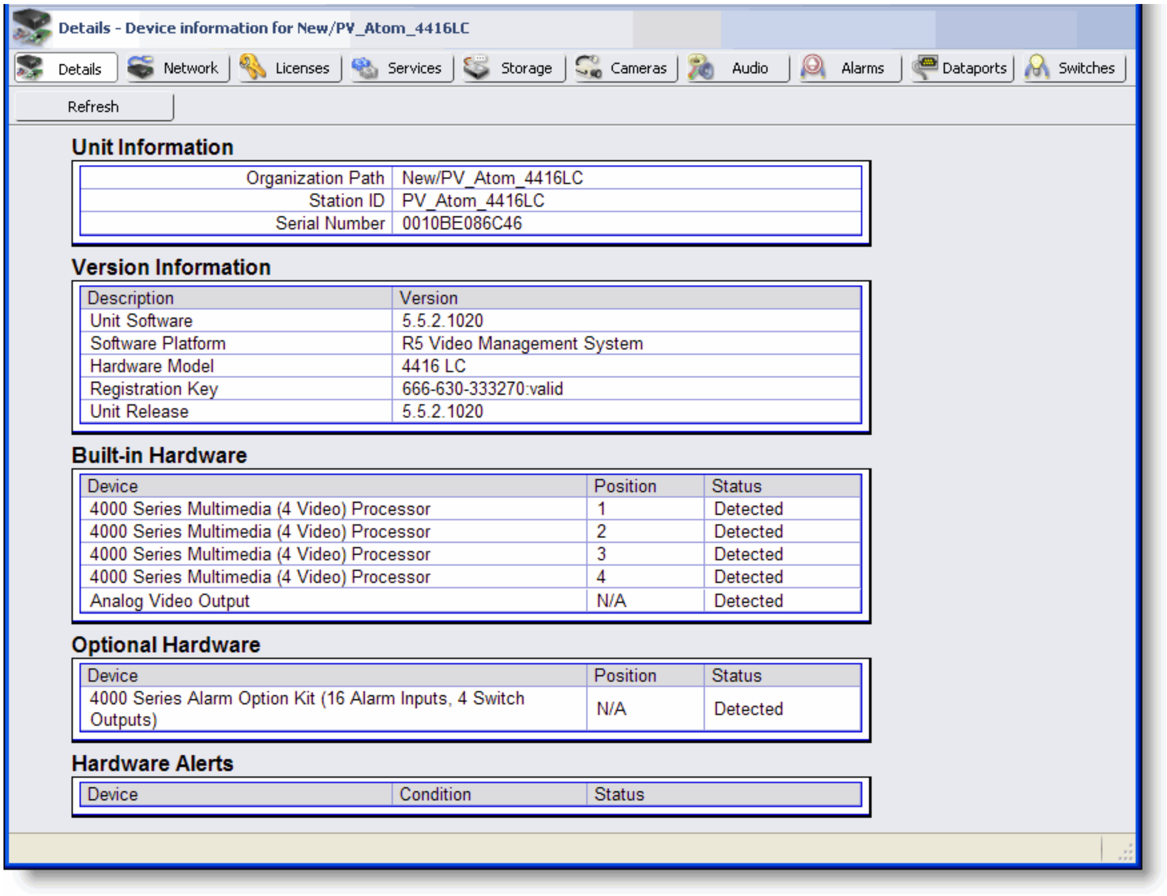
You can view a summary of the recorder's details, including its unit information, version information, built-in hardware details, and optional hardware.

To view recorder details

1. Ensure that the **Device Installation** task type is selected.
2. Click a recorder in the **Device Selector** panel.
3. Click **Details**.

   The details of the recorder are displayed for you to review.

NOTE: You can click Refresh to update the information that appears on the Details page.



Unit Information

Organization Path	New/PV_Atom_4416LC
Station ID	PV_Atom_4416LC
Serial Number	0010BE086C46

Version Information

Description	Version
Unit Software	5.5.2.1020
Software Platform	R5 Video Management System
Hardware Model	4416 LC
Registration Key	666-630-333270:valid
Unit Release	5.5.2.1020

Built-in Hardware

Device	Position	Status
4000 Series Multimedia (4 Video) Processor	1	Detected
4000 Series Multimedia (4 Video) Processor	2	Detected
4000 Series Multimedia (4 Video) Processor	3	Detected
4000 Series Multimedia (4 Video) Processor	4	Detected
Analog Video Output	N/A	Detected

Optional Hardware

Device	Position	Status
4000 Series Alarm Option Kit (16 Alarm Inputs, 4 Switch Outputs)	N/A	Detected

Hardware Alerts

Device	Condition	Status

Viewing and Configuring Network Settings

By default, recorders are pre-configured to automatically obtain an IP address from your network's DHCP server. If required, you can adjust the network settings.

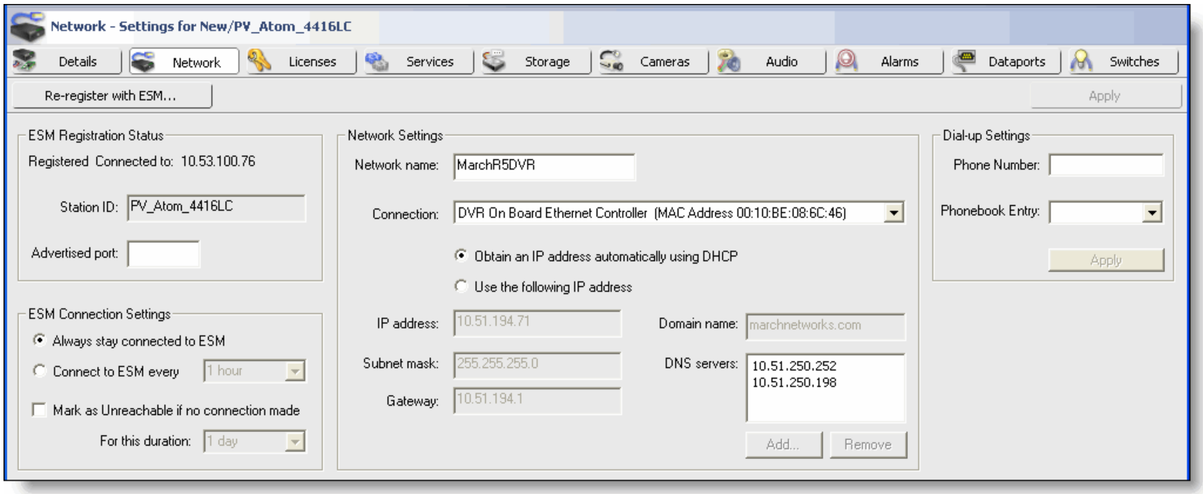
After you configure the recorder's network settings, the March Networks applications, such as the Investigator, can connect to the recorder over the network.

NOTE: If the recorder is installed in a location that does not have network access, you can connect a USB modem to the recorder and then access it over a dial-up (telephone) connection. For more information, see “Configuring a Dial-Up Recorder” on page 13 or the *Setting Up Units for Dial-up Connection Technical Instructions* included on your March Networks CD.

To specify the recorder's network settings

1. Ensure that the **Device Installation** task type is selected.
2. Click a recorder in the **Device Selector** panel.
3. Click **Network**.

   The network settings for the recorder are displayed in the center section.



Network - Settings for New/PV_Atom_4416LC

ESM Registration Status

Registered Connected to: 10.53.100.76

Station ID: PV_Atom_4416LC

Advertised port:

ESM Connection Settings

● Always stay connected to ESM

○ Connect to ESM every 1 hour

□ Mark as Unreachable if no connection made

For this duration: 1 day

Network Settings

Network name: MarchR5DVR

Connection: DVR On Board Ethernet Controller (MAC Address 00:10:BE:08:6C:46)

● Obtain an IP address automatically using DHCP

○ Use the following IP address

IP address: 10.51.194.71

Subnet mask: 255.255.255.0

Gateway: 10.51.194.1

Domain name: marchnetworks.com

DNS servers: 10.51.250.252
10.51.250.198

Dial-up Settings

Phone Number:

Phonebook Entry:

4. The ESM Registration Status section shows information about the ESM the recorder is registered to. If the recorder is not connected to an ESM, the section displays “Not registered with Enterprise Service Manager”.

NOTE: To register or unregister the recorder with an ESM, see “Registering and Unregistering Recorders With an ESM” on page 195.

5. The ESM Connection Settings section is only displayed when the recorder is connected to an ESM. You can configure whether you want the recorder always connected to the ESM, or whether you want it to connect at configurable time periods (every 1 hour, 6 hours, or 12 hours). You can also choose to mark the

recorder's ESM Status as Unreachable if it does not connect to the ESM within a configurable time period (12 hours, 1 day, 2 days).

6. The Network Settings section displays information about the recorder's network settings.
   a) In the Network name field, specify a name to identify the recorder. This name appears in software applications such as the Investigator.
   b) In the Connection list, select the network connection. The default network connection is **DVR On Board Ethernet Controller**.
   Depending on the recorder model and the installed options, additional network connection options may appear. These options correspond to other peripherals that the unit communicates with, such as IP cameras.
   c) Choose one of the following IP address options:
      - Obtain an IP address automatically using DHCP — Select this option to allow the recorder to obtain an IP address, subnet mask, and gateway from the network.
      - Use the following address — Select this option to specify a unique IP address, and specify the subnet mask, gateway, and domain name.
   d) Use the Add and Remove buttons to configure the DNS addresses.
7. You only need the Dial-Up Settings section if you want to add a dial-up recorder that is configured to communicate with an ESM. For more information, see the *Setting Up Units for Dial-up Connection Technical Instructions* included on your March Networks CD.
8. Click Apply to save your settings.

Applying Licenses

If your organization has purchased a license for your recorder, you can apply it to the unit. Licenses are used for a variety of functions in the March Networks software.

For more information, see "Applying Licenses to Recorders" on page 33.

Services

The Device Installation Services page is only necessary when configuring March Networks VMS 1.0. For more information contact your March Networks representative.

Reviewing Storage Information

You can view a summary of the recorder's hard drive storage information, as outlined in the following table.

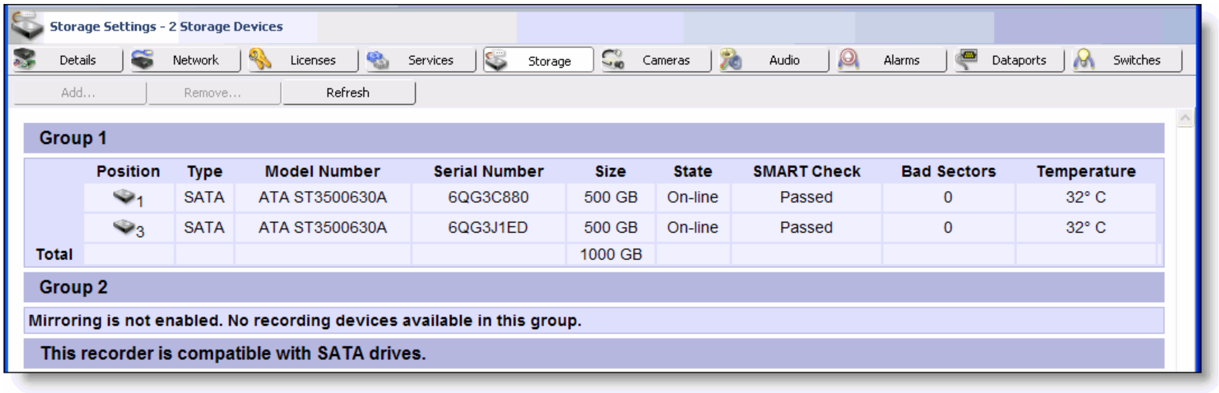
Column	Description
Group 1 or Group 2	To ensure you have a backup copy of media captured by the recorder, you can set up disk mirror recording. When mirroring is set up, the recorder records data to several hard drives simultaneously (if the recorder has more than one hard drive, such as a 4000 C Series NVR, or if you are using external storage). You can assign hard drives to a disk mirror recording group: ●Group 1 — Stores incoming data. ●Group 2 — Stores an additional copy of data from Group 1 hard drives. By default, all hard drives are set to Group 1. If you remove all Group 1 hard drives from the recorder, the Group 2 hard drives store incoming data and a backup copy is not created. Group 1 and Group 2 hard drives can be of varying sizes.
Position	Position of the hard drive in the recorder (position number 1 to 4). **Note:** If you are using external storage with a SCSI connection, this column shows the SCSI ID number (0 - 6) instead.
Type	Type of hard drive (for example, SATA or External).
Serial Number	Serial Number of the hard drive.
Size	Size of the storage in GB. If part of the storage in a hard drive is unusable (for example, if a hard drive partition is offline), the total amount of storage appears in addition to the amount of usable storage. For example, 500 GB (400 GB Usable).
State	State of the hard drive: Online or Offline.
SMART Check	SMART (Self-Monitoring, Analysis, and Reporting Technology) Check status: Passed or Failed.
Bad Sectors	Number of bad sectors: 0 if there are no bad sectors.
Temperature	Temperature of the hard drive.

NOTE: Disk mirror recording is configured using the recorder's built-in provisioning interface. For more information, see the *Provisioning Interface Technical Instructions* included on your March Networks CD.

To review recorder storage

1. Ensure that the **Device Installation** task type is selected.
2. Click a recorder in the **Device Selector** panel.

3. Click **Storage**.



Group 1

	Position	Type	Model Number	Serial Number	Size	State	SMART Check	Bad Sectors	Temperature
	1	SATA	ATA ST3500630A	6QG3C880	500 GB	On-line	Passed	0	32° C
	3	SATA	ATA ST3500630A	6QG3J1ED	500 GB	On-line	Passed	0	32° C
Total					1000 GB				

Group 2

Mirroring is not enabled. No recording devices available in this group.

This recorder is compatible with SATA drives.

4. Review the storage systems connected to the unit and confirm that they are reporting positive status information.

NOTE: You can click Refresh to update the information that appears on the Storage page.

Testing Analog Cameras

You can connect analog cameras to a recorder and view live video to ensure that the field of view captures the scene properly. If adjustments are required, you can adjust the camera's position and view the effect of your change.

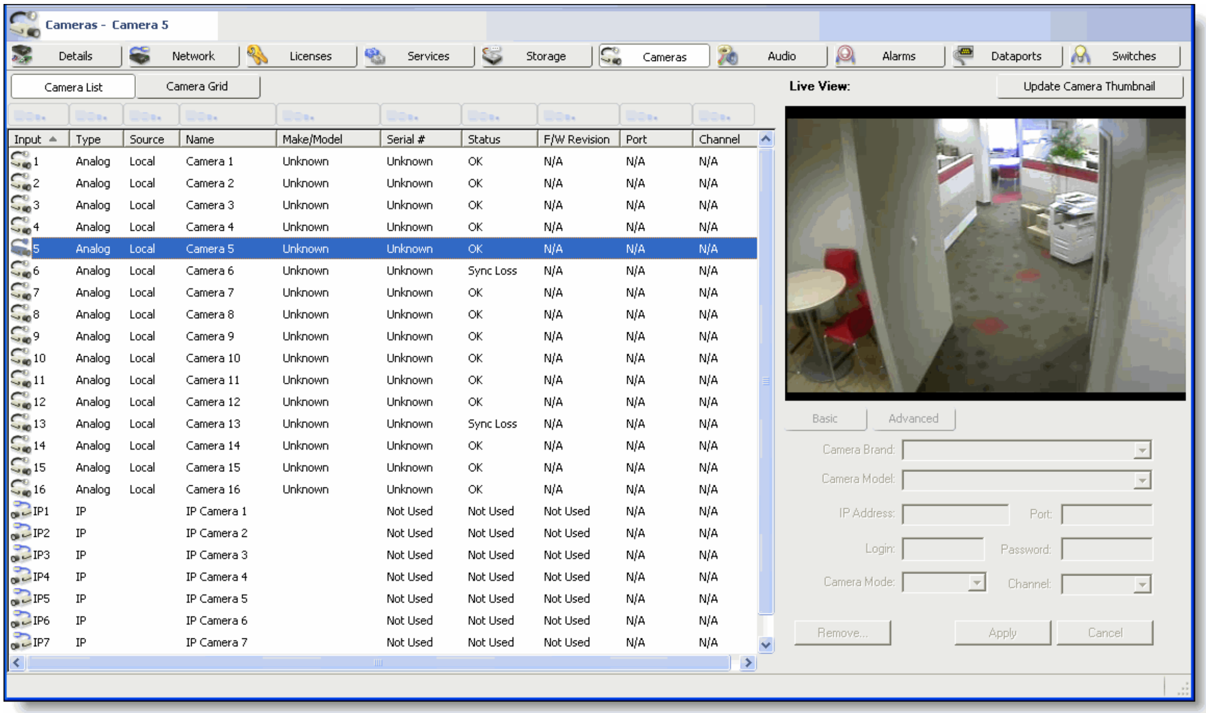
After you adjust the camera and verify that the camera is capturing the scene properly, you can update the camera's preview, which is referred to as a thumbnail. The thumbnail is a reference image that Investigator users will see when reviewing the camera listing, and helps users identify the camera they want to view.

NOTE: For more information about cameras, see "Configuring Cameras" on page 49.

To test an analog camera

1. Ensure that the **Device Installation** task type is selected.
2. In the **Device Selector** panel, click the recorder that the analog camera is connected to.

3. Click **Cameras**.



Input	Type	Source	Name	Make/Model	Serial #	Status	F/W Revision	Port	Channel
1	Analog	Local	Camera 1	Unknown	Unknown	OK	N/A	N/A	N/A
2	Analog	Local	Camera 2	Unknown	Unknown	OK	N/A	N/A	N/A
3	Analog	Local	Camera 3	Unknown	Unknown	OK	N/A	N/A	N/A
4	Analog	Local	Camera 4	Unknown	Unknown	OK	N/A	N/A	N/A
5	Analog	Local	Camera 5	Unknown	Unknown	OK	N/A	N/A	N/A
6	Analog	Local	Camera 6	Unknown	Unknown	Sync Loss	N/A	N/A	N/A
7	Analog	Local	Camera 7	Unknown	Unknown	OK	N/A	N/A	N/A
8	Analog	Local	Camera 8	Unknown	Unknown	OK	N/A	N/A	N/A
9	Analog	Local	Camera 9	Unknown	Unknown	OK	N/A	N/A	N/A
10	Analog	Local	Camera 10	Unknown	Unknown	OK	N/A	N/A	N/A
11	Analog	Local	Camera 11	Unknown	Unknown	OK	N/A	N/A	N/A
12	Analog	Local	Camera 12	Unknown	Unknown	OK	N/A	N/A	N/A
13	Analog	Local	Camera 13	Unknown	Unknown	Sync Loss	N/A	N/A	N/A
14	Analog	Local	Camera 14	Unknown	Unknown	OK	N/A	N/A	N/A
15	Analog	Local	Camera 15	Unknown	Unknown	OK	N/A	N/A	N/A
16	Analog	Local	Camera 16	Unknown	Unknown	OK	N/A	N/A	N/A
IP1	IP		IP Camera 1		Not Used	Not Used	Not Used	N/A	N/A
IP2	IP		IP Camera 2		Not Used	Not Used	Not Used	N/A	N/A
IP3	IP		IP Camera 3		Not Used	Not Used	Not Used	N/A	N/A
IP4	IP		IP Camera 4		Not Used	Not Used	Not Used	N/A	N/A
IP5	IP		IP Camera 5		Not Used	Not Used	Not Used	N/A	N/A
IP6	IP		IP Camera 6		Not Used	Not Used	Not Used	N/A	N/A
IP7	IP		IP Camera 7		Not Used	Not Used	Not Used	N/A	N/A

4. Click an analog camera and view the live image that appears to the right of the camera list. If adjustments are required, you can physically move the camera and see the effect of your change.

NOTE: Click Update Camera Thumbnail to capture a preview image that Investigator users will see when reviewing the camera list. The recorder generates a preview image from the live view that appears at the moment that you clicked Update Camera Thumbnail.

Testing IP Cameras

You can assign an IP camera to a recorder. After you add basic information, including the camera’s IP address, you can perform advanced functions, such as viewing troubleshooting information and camera details, viewing and resetting data rates, forcing a re-connection between the recorder and the IP camera, and viewing the IP camera’s Web page.

NOTE: For more information about cameras, see “Configuring Cameras” on page 49.

To assign an IP camera

1 Ensure that the **Device Installation** task type is selected.

2. In the **Device Selector** panel, select the recorder that the IP camera is connected to.

3. Click **Cameras.**
4. Select an unassigned IP camera in the list.
5. From the Camera Brand list, select the camera manufacturer.
6. From the Camera Model list, select the IP camera model.

   If the IP camera is a PTZ camera, ensure you select the appropriate model.
7. In the Address field, type the camera's IP address.

   Note: The camera's IP address is required to assign it to a recorder. To obtain the IP address, see the documentation accompanying the IP camera.
8. In the Port field, type the camera's port.

   Note: The port is the default used for the selected camera brand and model. It automatically updates when a new camera model or brand is specified.

9 Perform any or all of the following tasks:

- If the camera requires authentication, enter a login ID for the camera in the Login field, and enter a password in the Password field.
- If more than one mode is supported on the camera model, select JPEG or MPEG4 in the Camera Mode list.
- If the camera supports multiple video channels, select a channel in the Channel list.

10 Click Apply.

The recorder connects to the IP camera, and a live video stream displays.

To view the IP camera status

1 Ensure the **Device Installation** task type is selected.

2. In the **Device Selector** panel, select the recorder that the IP camera is connected to.

3 Click **Cameras.**

4 Select an IP camera in the list.

5 Click Advanced.

Note that if you have not configured the IP camera's settings, the Advanced button does not appear. You must first configure the IP camera, as outlined in "To assign an IP camera".

6 Under Status, view any troubleshooting information.

To view IP camera capture rates

1 Ensure that the **Device Installation** task type is selected.

2. In the **Device Selector** panel, select the recorder that the IP camera is connected to.

3 Click **Cameras.**

4 Select an IP camera in the list.

5 Click **Advanced**.

Note that if you have not configured the IP camera's settings, the Advanced button does not appear. You must first configure the IP camera, as outlined in To assign an IP camera.

6 Under Datarates, review the rate at which video is captured.

Note: If you have adjusted the IP camera settings and want to see the effects your changes have made, you can click **Reset data rates** to clear the data rates and restart the report.

To access the configuration web page for an IP camera

1 Ensure that the **Device Installation** task type is selected.

2. In the **Device Selector** panel, select the recorder that the IP camera is connected to.

3 Click **Cameras.**

4 Select an assigned IP camera in the list.

5 Click **Advanced**.

Note that if you have not configured the IP camera's settings, the Advanced button does not appear. You must first configure the IP camera, as outlined in To assign an IP camera.

6 Perform any or all of the following tasks:

- Under **Status**, view any troubleshooting information.
- Under **Camera Information**, view details about camera inputs and outputs, and whether it is a PTZ camera.
- To force the recorder to reconnect to the IP camera, click **Reconnect**.
- To view the IP camera’s Web page, click **Web Page**.
- To reset the data rates, click **Reset data rates**.

To remove an IP camera

1 Ensure that the **Device Installation** task type is selected.

2. In the **Device Selector** panel, select the recorder that the IP camera is connected to.

3 Click **Cameras.**

4 Select an assigned IP camera in the list.

5 Click **Remove**.

6 Click **Yes**.

Testing Audio

You can connect audio inputs and outputs to a recorder, and perform tests to confirm that you can hear audio and that others can hear you when you speak into a connected intercom.

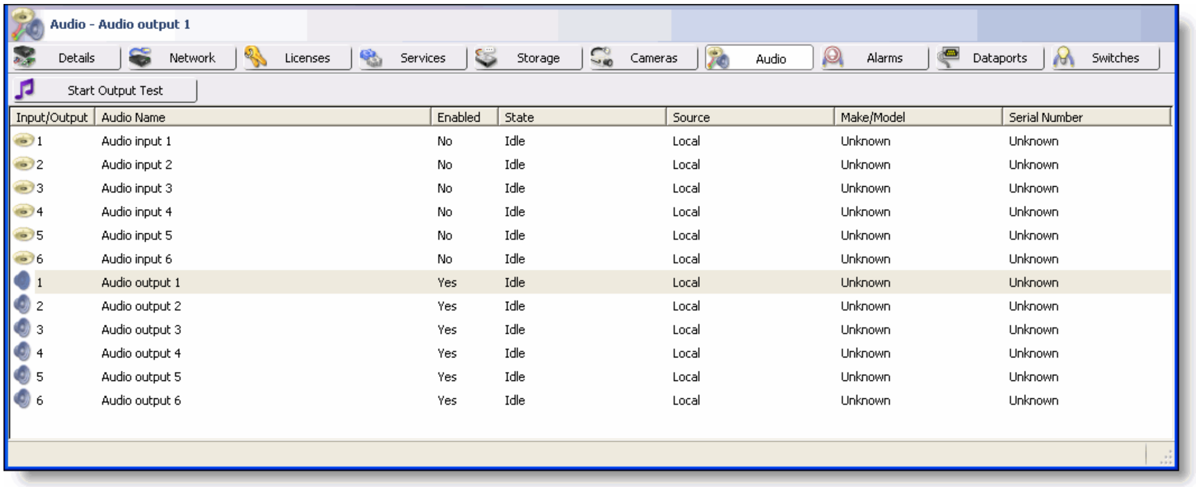
NOTE: For more information about audio, see “Configuring Audio” on page 107.

To test audio

1 Ensure that the **Device Installation** task type is selected.

2. In the **Device Selector** panel, select the recorder that the audio input or output is connected to.

3 Click **Audio.**



Input/Output	Audio Name	Enabled	State	Source	Make/Model	Serial Number
1	Audio input 1	No	Idle	Local	Unknown	Unknown
2	Audio input 2	No	Idle	Local	Unknown	Unknown
3	Audio input 3	No	Idle	Local	Unknown	Unknown
4	Audio input 4	No	Idle	Local	Unknown	Unknown
5	Audio input 5	No	Idle	Local	Unknown	Unknown
6	Audio input 6	No	Idle	Local	Unknown	Unknown
1	Audio output 1	Yes	Idle	Local	Unknown	Unknown
2	Audio output 2	Yes	Idle	Local	Unknown	Unknown
3	Audio output 3	Yes	Idle	Local	Unknown	Unknown
4	Audio output 4	Yes	Idle	Local	Unknown	Unknown
5	Audio output 5	Yes	Idle	Local	Unknown	Unknown
6	Audio output 6	Yes	Idle	Local	Unknown	Unknown

4 Perform one or all of the following tasks:

- Select an audio input, click **Start Input Test**, and use the **Delay** slider to delay audio capture and playback.
  This allows you to start the audio test, move to the microphone to speak into it, and return to your computer to hear the captured audio.
- Select an audio output, click **Start Output Test**, and confirm that the pre-recorded audio recording plays.

NOTE: If you are testing an IP audio input, the input is disabled by default. To test the input, you must first enable it using the Administrator Console.

TIP: Use the volume slider to help with an input test.

Testing Alarms

You can connect alarm inputs and outputs to a recorder, and trigger an alarm to verify that the state change is communicated to the Administrator Console (and the Installer Console).

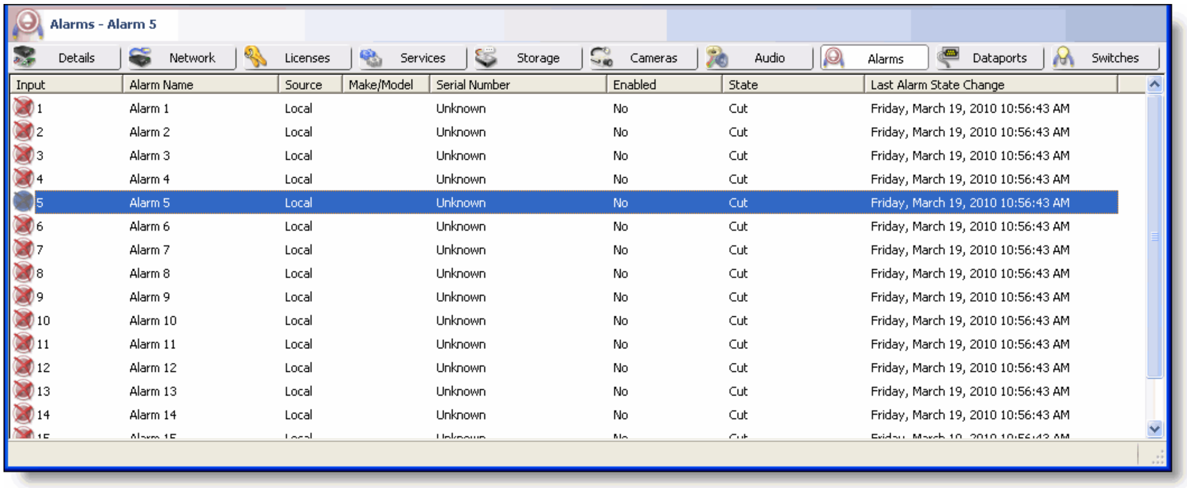
For more information about alarms, see “Configuring Alarms” on page 111.

To test an alarm

1 Ensure that the **Device Installation** task type is selected.

2. In the **Device Selector** panel, select the recorder that the alarm is connected to.

3 Click **Alarms.**



Input	Alarm Name	Source	Make/Model	Serial Number	Enabled	State	Last Alarm State Change
1	Alarm 1	Local		Unknown	No	Cut	Friday, March 19, 2010 10:56:43 AM
2	Alarm 2	Local		Unknown	No	Cut	Friday, March 19, 2010 10:56:43 AM
3	Alarm 3	Local		Unknown	No	Cut	Friday, March 19, 2010 10:56:43 AM
4	Alarm 4	Local		Unknown	No	Cut	Friday, March 19, 2010 10:56:43 AM
5	Alarm 5	Local		Unknown	No	Cut	Friday, March 19, 2010 10:56:43 AM
6	Alarm 6	Local		Unknown	No	Cut	Friday, March 19, 2010 10:56:43 AM
7	Alarm 7	Local		Unknown	No	Cut	Friday, March 19, 2010 10:56:43 AM
8	Alarm 8	Local		Unknown	No	Cut	Friday, March 19, 2010 10:56:43 AM
9	Alarm 9	Local		Unknown	No	Cut	Friday, March 19, 2010 10:56:43 AM
10	Alarm 10	Local		Unknown	No	Cut	Friday, March 19, 2010 10:56:43 AM
11	Alarm 11	Local		Unknown	No	Cut	Friday, March 19, 2010 10:56:43 AM
12	Alarm 12	Local		Unknown	No	Cut	Friday, March 19, 2010 10:56:43 AM
13	Alarm 13	Local		Unknown	No	Cut	Friday, March 19, 2010 10:56:43 AM
14	Alarm 14	Local		Unknown	No	Cut	Friday, March 19, 2010 10:56:43 AM
15	Alarm 15	Local		Unknown	No	Cut	Friday, March 19, 2010 10:56:43 AM

4 Review the alarm information that appears on the Alarms page.

5 Trigger an alarm. The time in the **Last Alarm State Change** column should match the time that you triggered the alarm.

NOTE: If you are testing an IP alarm input, the input is disabled by default. To test the input, you must first enable it using the Administrator Console.

Testing Dataports

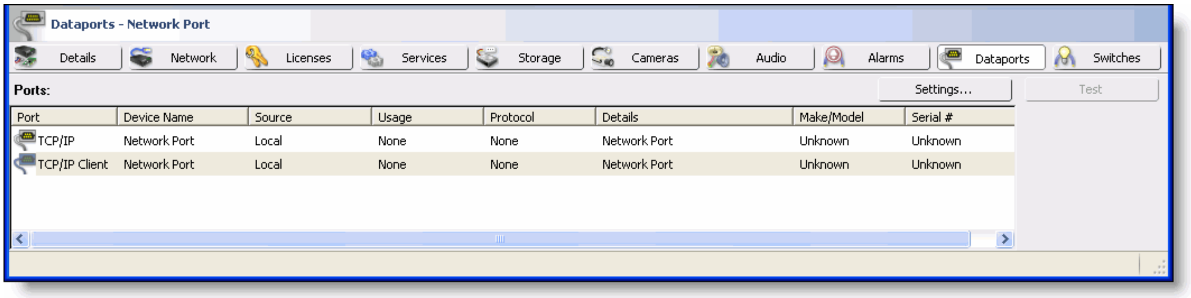
You can connect dataports, such as ATMs, PTZ cameras, and text capture systems to a recorder. For ATMs and other text capture devices, you can send sample text data and confirm that it appears in the Administration Console. You can also configure a PTZ passthrough device so that you can control a PTZ camera with a joystick from your computer.

For more information about dataports, see “Configuring Dataports” on page 117.

To test a dataport

1. Ensure that the **Device Installation** task type is selected.
2. In the **Device Selector** panel, select the recorder that the dataport is connected to.

3. Click **Dataports.**



Port	Device Name	Source	Usage	Protocol	Details	Make/Model	Serial #
TCP/IP	Network Port	Local	None	None	Network Port	Unknown	Unknown
TCP/IP Client	Network Port	Local	None	None	Network Port	Unknown	Unknown

4. Select a dataport, and click **Settings** to configure each port.

   Note that for IP PTZ cameras, the settings are not configurable.

5. Click **OK**.
6. Review the dataport information that appears on the Dataports page.
7. Click **Test**.
   - For text capture systems, text streams in the window to the right of the list.
   - For analog PTZ cameras, click in the video display window to move the camera's field of view. A yellow arrow appears on top of the video display window to indicate the direction that the field of view is moving.

NOTE: If the dataport's general settings have not been specified, the **Test** button is not available.

To configure a PTZ passthrough device

1. Ensure that the **Device Installation** task type is selected.
2. In the **Device Selector** panel, select the recorder that the dataport is connected to.
3. Click **Dataports.**
4. Select the dataport you want to configure for PTZ passthrough and click the **Settings** button.

   The **Dataport Settings** dialog box appears.

5. In the **Device Usage** list, select PTZ.
6. In the Protocol list, click **PTZPassThru**.
7. In the Assigned Cameras box, click **Add**, select the camera you want to use, and click **Test**.
8. In the **COM Port Selection** dialog box, select the COM port you want to use and click OK.
9. Use the joystick to control the direction of the PTZ camera in the display window.

NOTE: You can set a default COM port in the Administrator Console or the Live Monitoring Console using the Preferences dialog box.

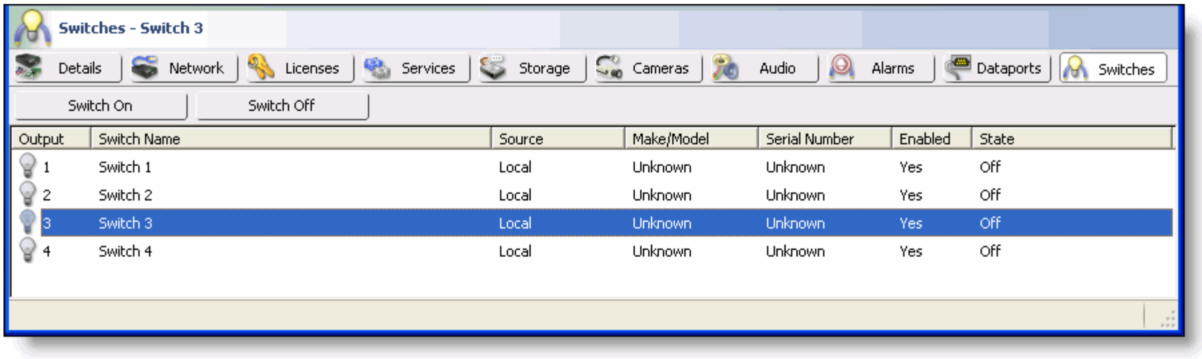
Testing Switches

You can connect switches to a recorder, and use the Installer Console to activate the switch.

For more information about switches, see "Configuring Switches" on page 121.

To test a switch

1. Ensure that the **Device Installation** task type is selected.
2. In the **Device Selector** panel, select the recorder that the switch is connected to.
3. Click **Switches.**



Output	Switch Name	Source	Make/Model	Serial Number	Enabled	State
1	Switch 1	Local	Unknown	Unknown	Yes	Off
2	Switch 2	Local	Unknown	Unknown	Yes	Off
3	Switch 3	Local	Unknown	Unknown	Yes	Off
4	Switch 4	Local	Unknown	Unknown	Yes	Off

4. Review the switch information that appears on the Switches page.
5. Select a switch output, and click **Switch On** or **Switch Off** to test switch operation.

Applying Licenses to Recorders

If your organization has purchased a license for your recorder, you can apply it to the unit. Licenses are used for a variety of functions in the March Networks software, which include:

- Allowing recorders to register with the ESM.
- Enabling features on the recorder, such as camera obstruction detection or people counting.
- Allowing you to upgrade the recorder to the latest software release (for recorders running Release 5.5 and later).

Depending on the type of license you purchased, you will work with licenses in a slightly different manner:

- **Recorder license**: Add the license to a recorder.
- **ESM license**: Obtain a license from the ESM and apply it to the recorder.

For information about purchasing licenses, contact your March Networks Sales representative.

The following topics are covered in this chapter:

Adding Licenses to a Recorder

If you purchased a recorder license, such as a recorder upgrade license, you can add it to the unit.

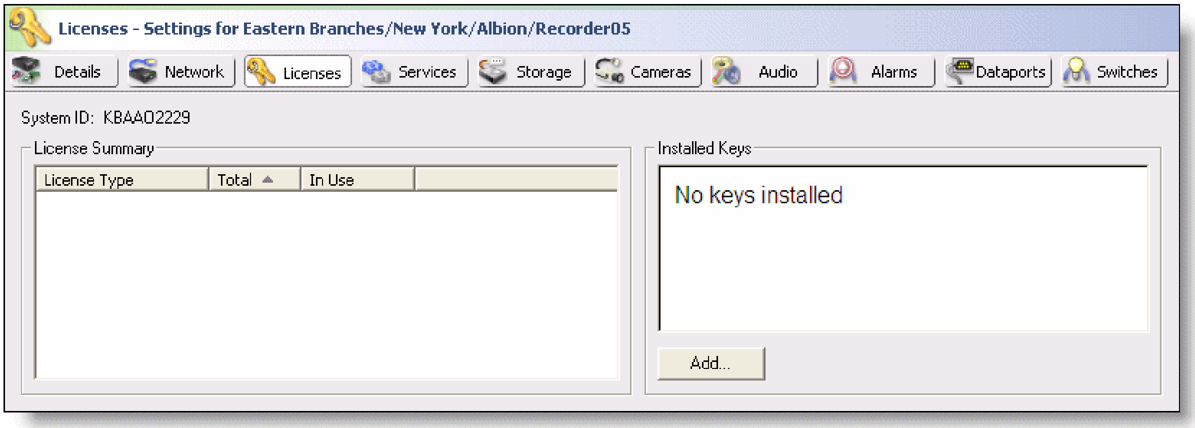
For organizations that use an ESM to centrally manage licenses, you can configure the recorder to obtain its license from the ESM. For more information, see “Obtaining a License from the ESM and Applying it to a Recorder” on page 34.

To add a license to a recorder

1. Ensure the **Device Installation** task type is selected.
2. Click a recorder in the **Device Selector** panel.
3. Click **Licenses**.
4. Under **Installed Keys**, click **Add**.

   The **Add License Key** dialog box appears.
5. In the **License key** box, type the license key that you purchased.

   After the license key is installed and validated, any functionality that was provided as part of the license is available. For example, you can proceed to upgrade the recorder, as outlined in “Upgrading Recorder Software” on page 155.



System ID: KBAA02229

License Type	Total	In Use

No keys installed

Obtaining a License from the ESM and Applying it to a Recorder

When ESM licenses are installed they are stored centrally on the ESM. As you require licenses for your recorders, you can use the Administrator Console to obtain the licenses from the ESM and apply them to your units.

Before you can obtain licenses from the ESM, these licenses must be added to the ESM. For information about adding licenses to an ESM, see “Adding Licenses” on page 187.

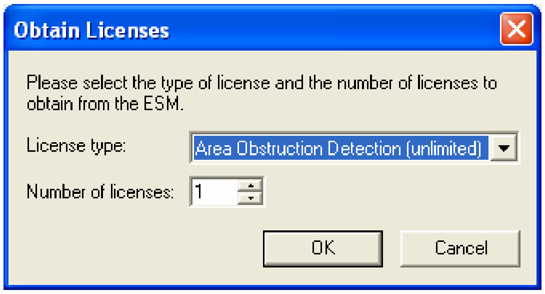
If a recorder no longer requires a license, you can return it to the ESM so it can be applied to other units.

To obtain licenses from the ESM

1. Ensure the **Device Installation** task type is selected.
2. Click a recorder in the **Device Selector** panel.
3. Click **Licenses**.

   The **Licenses** page appears.
4. Under **License Summary**, click **Obtain from ESM**.

   The **Obtain Licenses** dialog box appears.


Obtain Licenses

Please select the type of license and the number of licenses to obtain from the ESM.

License type: Area Obstruction Detection (unlimited)

Number of licenses: 1

5. Click a license type in the **License type** list.
6. In the **Number of licenses** box, type or select the number of licenses you want.

   Depending on the type of license you added, you can do the following after the license is installed and validated:

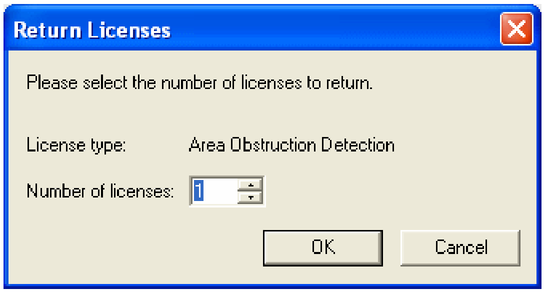
   - If you are adding a license that allows a recorder to register with the ESM, you can now register the unit with the ESM.
   - If you are adding a license to make a feature available, such as camera obstruction detection or people counting, you can now access and configure the feature.
   - If you are adding an upgrade license, you can proceed to upgrade the recorder as outlined in “Upgrading Recorder Software” on page 155.

To return licenses to the ESM

1. Ensure the **Device Installation** task type is selected.
2. Click a recorder in the **Device Selector** panel.
3. Click **Licenses**.

   The **Licenses** page appears.
4. Under **License Summary**, click a license type in the **Number of licenses** list.
5. Click **Return to ESM**.

The **Return Licenses** dialog box appears.



Return Licenses

Please select the number of licenses to return.

License type: Area Obstruction Detection

Number of licenses: 1

6. In the **Number of licenses** box, type or select the number of licenses you want to return to the ESM.
7. Click **OK**.

Chapter 6

Specifying General Options

This chapter describes how to review and configure general recorder information.

The following topics are covered in this chapter:

- "Reviewing and Specifying General Details" on page 38
- "Configuring a Recorder Clock" on page 39
- "Configuring and Reviewing Evidence Retention" on page 40
- "Configuring Network Settings" on page 45
- "Customizing the Network Communication Path" on page 45

Reviewing and Specifying General Details

You can review the recorder's details and specify general information, such as the recorder's serial number and the software release running on the recorder.

All time displays in the Administrator Console use the workstation's local time zone.

To review and specify general recorder details

1. Ensure the **Device Configuration** task type is selected.
2. Click a recorder in the **Device Selector** panel.
3. Click **General**.

   The **General** page appears.
4. Review and configure the details outlined in the following table.

   If you change one or more settings, you can click **Apply Settings** to save the change, or **Cancel Settings** to discard the change.

Setting	Description
Access level	The authorization level a user must have to access the recorder. Users can access recorders with an equivalent or lower access level than what is set in their profile. For example, a user with an access level of five can access recorders set to five or lower. For information about specifying a user's access level, see "Creating User Profiles and Accounts" on page 188. You can choose a number from one to 10 (one is the least-restricted access level and 10 is the most secure). **Tips:** ● You can create a covert, or hidden, recorder by assigning it an access level that is higher than the user access levels. ● If you are not working with an ESM, you do not need to specify an access level. However, if you plan to install an ESM in the future, we recommend you set the access level.
Serial number	The unique serial number or ID provided to the recorder for identification. The serial number also appears on the label on the outside of the recorder.
Software release	The release and version of software running on the recorder. For example, release 5.4 and build 78. **Note:** When you are working with a March Networks Customer Care representative, you may be asked to provide this information.
Station ID	The unique identification that is used to distinguish between recorders on your network. For some models, this number is specified using DIP switches on the recorder. This number can also be specified using the Installer Console or by switching to the **Device Installation** task type.
Camera type	The type, or format, of cameras that are connected to the recorder. The recorder automatically detects the camera type. **Note:** You can connect either NTSC cameras or PAL cameras, but not a combination of the two camera types.

Configuring a Recorder Clock

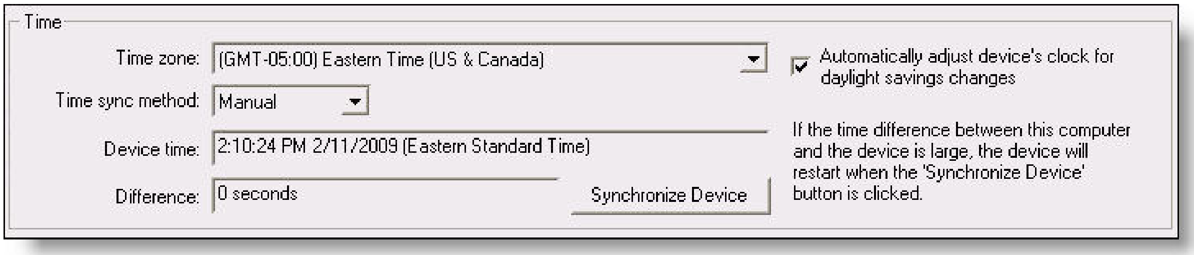
You can configure and review the recorder clock settings, such as the time zone and the method used to ensure the recorder's clock is accurate.

To configure the recorder clock

1. Ensure the **Device Configuration** task type is selected.
2. Click a recorder in the **Device Selector** panel.
3. Click **General**.

   The **General** page appears.
4. Under **Time**, configure the recorder clock settings outlined in the following table.

   If you change one or more settings, you can click **Apply Settings** to save the change, or **Cancel Settings** to discard the change.



Time

Time zone: (GMT-05:00) Eastern Time (US & Canada)

☑ Automatically adjust device's clock for daylight savings changes

Time sync method: Manual

Device time: 2:10:24 PM 2/11/2009 (Eastern Standard Time)

Difference: 0 seconds

If the time difference between this computer and the device is large, the device will restart when the 'Synchronize Device' button is clicked.

Table 1: Recorder Clock Settings

Setting	Description
Time zone	The time zone used by the recorder's built-in clock. Ensure the time zone matches the physical location of the recorder. **Tip:** You can set the clock to automatically update when daylight saving time occurs by selecting the **Automatically adjust device's clock for daylight savings changes** check box.
Time sync method	The method the recorder uses to synchronize its built-in clock to maintain accuracy. You can choose one of the following time synchronization options: • **ESM Server**. Automatically synchronize the recorder clock with an ESM. • **NTP**. Automatically synchronize the recorder clock with a Network Time Protocol (NTP) server. Then, specify the IP address of the NTP server. • **Manual**. Periodically synchronize the recorder clock with your computer using the Administrator Console. When you choose **Manual**, you must click **Synchronize Device** to synchronize the recorder clock with your computer clock. **Warning:** If you select Manual time synchronization, you must regularly monitor the difference between the time reported by the recorder clock and the time reported by your computer clock and click the Synchronize Device button if there is a difference. If these clocks are not synchronized on a regular basis, over time the difference can become significant. Since the video collected by your recorder is time sensitive information, it is highly recommended that you monitor this carefully and on a regular basis.

Table 1: Recorder Clock Settings (Continued)

Setting	Description
Device time	The current time, as reported by the recorder.
Difference	The difference between the current time as reported by the recorder, and the current time as reported by your computer. **Note:** If the time difference is significant, the recorder automatically restarts when you click the Synchronize Device button.

Configuring and Reviewing Evidence Retention

To ensure critical evidence is present when required, recorders are continually capturing and retaining the most recent evidence on their hard drives.

Recorders retain all evidence for a minimum amount of time in the Critical Recording Buffer (CRB).

In addition to always retaining the most recent evidence, you can ensure that the recorder retains schedule or alarm-related evidence longer than most evidence.

If you do not want to continually capture and retain evidence, and instead want to control when evidence is retained, you can disable the CRB. When the CRB is disabled, evidence is only retained when an alarm occurs or a schedule starts. This is useful in situations where legal constraints dictate that video, audio, or text data can only be retained under certain circumstances.

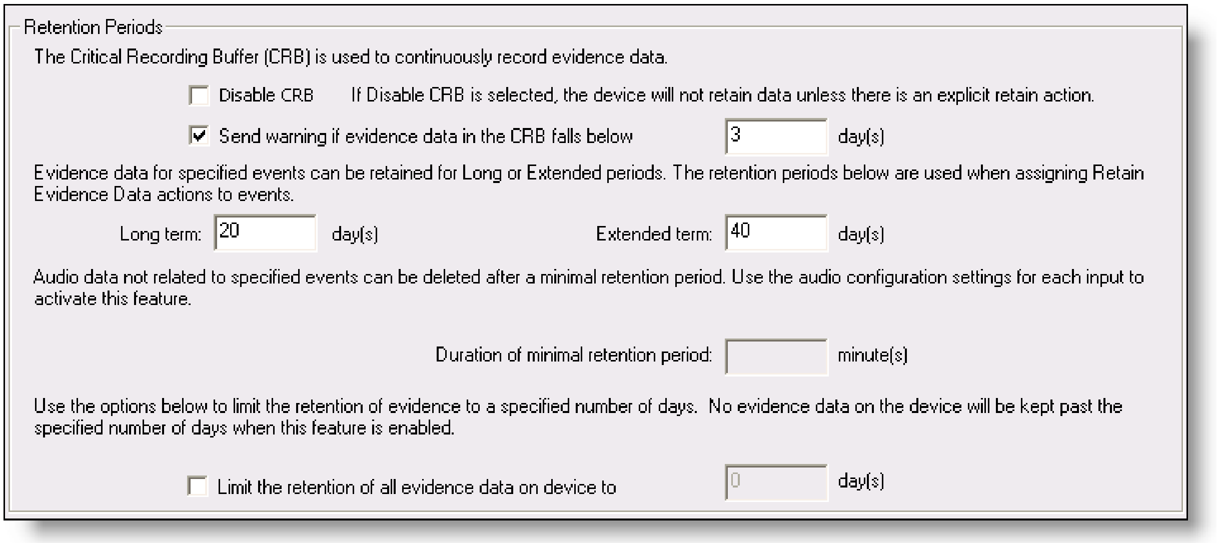
By default, audio is not retained. As part of your audio configuration tasks, you can choose whether you want to retain audio for a specific duration or continuously retain audio. For information about specifying the audio retention period and enabling audio retention, see “Configuring Audio” on page 107.

To configure evidence retention

1. Ensure the **Device Configuration** task type is selected.
2. Click a recorder in the **Device Selector** panel.
3. Click **General**.

   The **General** page appears.
4. Under **Retention Periods**, configure the retention settings outlined in the following table.

If you change one or more settings, click **Apply Settings** to save the change, or **Cancel Settings** to discard the change.



Retention Periods

The Critical Recording Buffer (CRB) is used to continuously record evidence data.

□ Disable CRB   If Disable CRB is selected, the device will not retain data unless there is an explicit retain action.

☑ Send warning if evidence data in the CRB falls below 3 day(s)

Evidence data for specified events can be retained for Long or Extended periods. The retention periods below are used when assigning Retain Evidence Data actions to events.

Long term: 20 day(s)   Extended term: 40 day(s)

Audio data not related to specified events can be deleted after a minimal retention period. Use the audio configuration settings for each input to activate this feature.

Duration of minimal retention period: minute(s)

Use the options below to limit the retention of evidence to a specified number of days. No evidence data on the device will be kept past the specified number of days when this feature is enabled.

□ Limit the retention of all evidence data on device to 0 day(s)

Table 2: Evidence Retention Settings

Setting	Description
Disable CRB	Indicates whether the recorder should continually capture and retain evidence. When the CRB is disabled, the recorder only captures and retains video, audio, and text evidence when triggered by an alarm or a schedule. **Important:** The recorder captures and retains video, audio, and text evidence on the hard drive by default. If you disable the CRB, the recorder will not retain any evidence unless recording is triggered by an alarm or schedule. This also means that evidence captured before the alarm or schedule (also referred to as pre-event evidence) will not be available because the recorder was not continually capturing and retaining evidence. If the CRB is disabled and you want to retain evidence, you must configure the **Retain Evidence Data** action or create a schedule. For more information, see “Configuring Actions” on page 129 or “Creating Schedules” on page 125. **Note:** When evidence retention is enabled or disabled, the change is not tracked in the recorder audit report. The recorder audit report is a tool that shows a history of changes made to the recorder’s configuration. For more information, see “Viewing the Recorder Audit Report” on page 194.

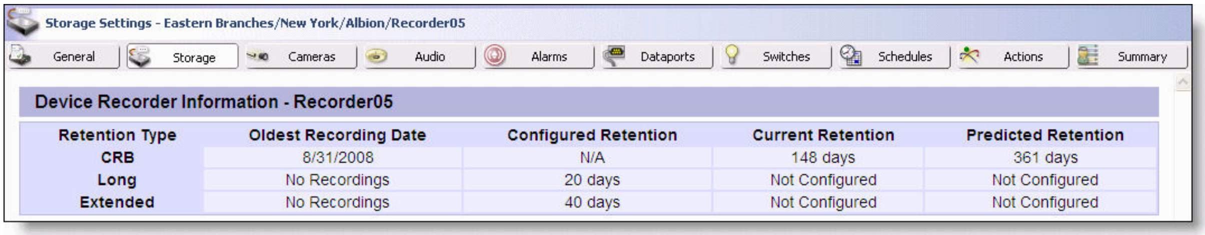
Table 2: Evidence Retention Settings (Continued)

Setting	Description
Send warning if evidence data in the CRB falls below	The CRB ensures that the most recent evidence is always available. The amount of evidence retained in the buffer fluctuates as additional space is required. To ensure that the recorder maintains a minimum amount of data, you can configure it to notify you when the buffer reaches a minimum amount of retention. For example, configure the recorder to notify you when it is retaining less than three days of evidence. To specify the minimum amount of evidence, select the **Send warning if evidence data in the CRB falls below** check box and specify when you want to receive notification that your retention settings are not being met. If you do not want to receive a warning, clear the check box. **Note:** When you receive notification that the recorder is retaining less than the minimum number of days, you may need to increase your storage space (by adding additional hard drives). Or, you may need to change your configuration settings, such as the camera's video quality and compression settings.
Long term and Extended term	The amount of time you want to retain evidence that is flagged for long or extended term retention. As space is required for new evidence, evidence exceeding the configured **Long term** period is deleted first, followed by evidence exceeding the configured **Extended term** period. Finally, evidence is deleted from the CRB, if additional space is still required. You can flag evidence for long term or extended term retention on the **Actions** page. For information about configuring how evidence is flagged for retention, see "Configuring Actions" on page 129.
Duration of minimal retention period	The number of minutes you want to retain audio. After the number of minutes has passed, the recorded audio is deleted. If you want audio to be deleted immediately, type **0** in the **Duration of minimal retention period [] minutes** box. You must also ensure that the **Recording Method** is set to **Minimal retention** for the required audio inputs or outputs, on the **Audio** page. For information about specifying the recording method for audio inputs and outputs, see "Configuring Audio" on page 107. **Note:** This setting is unavailable when the CRB is disabled.
Limit the retention of all evidence data on device to [ ] days	The maximum amount of evidence you want to retain. For example, if you do not want to retain more than 30 days of evidence, type **30** in the **Limit the retention of all evidence data on device to [ ] days** box. If you do not want to limit the retention of evidence data, clear the **Limit the retention of all evidence data on device to [ ] days** check box. **Important:** If evidence is retained that exceeds the specified limit, it is automatically deleted when you change this setting. For example, if you specify that you do not want to retain more than 30 days of evidence, and there are 40 days of evidence retained, the 10 oldest days of evidence are deleted. The retention limit must meet the following criteria: • It must be seven days or more. • It must be greater than the value specified in the **Send warning if evidence data in the CRB falls below** box. • It must be greater than the values specified in the **Long term** and **Extended term** boxes.

To review retention information for a recorder

1. Ensure the **Device Configuration** task type is selected.
2. Click a recorder in the **Device Selector** panel.
3. Click **Storage**.

   The **Storage** page appears.
4. Review the retention information that appears. The following table outlines the information that appears.



Storage Settings - Eastern Branches/New York/Albion/Recorder05

Device Recorder Information - Recorder05

Retention Type	Oldest Recording Date	Configured Retention	Current Retention	Predicted Retention
CRB	8/31/2008	N/A	148 days	361 days
Long	No Recordings	20 days	Not Configured	Not Configured
Extended	No Recordings	40 days	Not Configured	Not Configured

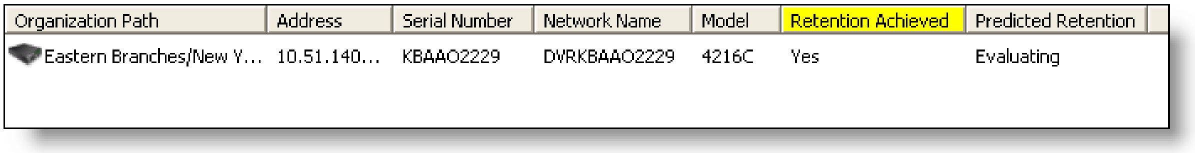
Table 3: Retention Information

Column	Description
Oldest Recording Date	The date of the oldest piece of evidence retained on the hard drive.
Configured Retention	The retention periods that are specified on the recorder's **General** page. **Note:** The **Configured Retention** is always **N/A** for the CRB, as you cannot specify the amount of evidence stored in the CRB. **Note:** The **Configured Retention** is **N/A** when the CRB is disabled.
Current Retention	The number of days the oldest recording has been stored on the recorder. If **Not Configured** appears, retention actions have not been configured. If **Not Applicable** appears, the software version running on the recorder does not support this feature.
Predicted Retention	The predicted number of days that the oldest recording will be stored on the recorder, based on the retention periods specified on the **General** page and the retention achieved over the last week. If **Not Configured** appears, retention actions have not been configured. If **Not Applicable** appears, the software version running on the recorder does not support this feature, or the CRB has been disabled. If **Unknown** appears, a retention action has been configured, but recordings are not available.

NOTE: The **Storage** page provides an overview of the recorder's storage. If you are reviewing this information to confirm that your retention goals are being met, you should keep in mind that if you have recently connected new peripherals, and they have not been retaining evidence for the number of days specified for the retention period, your storage goals for that peripheral are not being met.

To determine if the recorder is meeting its retention goals

1. Ensure the **Device Configuration** task type is selected.
2. In the **Device Selector** panel, view the **Retention Achieved** column.



Organization Path	Address	Serial Number	Network Name	Model	Retention Achieved	Predicted Retention
Eastern Branches/New Y...	10.51.140...	KBAAO2229	DVRKBAAO2229	4216C	Yes	Evaluating

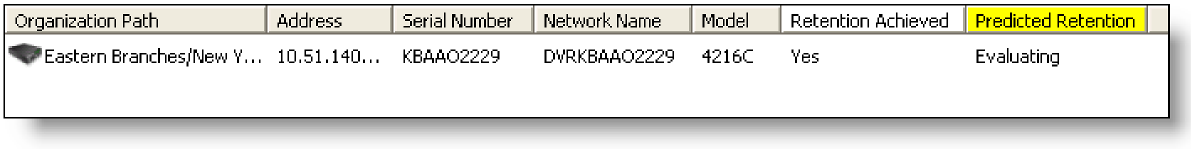
The value in this column tells you whether the recorder is meeting its retention goals:

- **Yes.** Your retention goals are being met.
- **No.** Retention goals are not being met for any of the following reasons:
  - Evidence retained in the CRB is being deleted and the configured CRB time has not been reached.
  - A recorder has been configured with long term retention actions, retained data is being deleted, and the configured long term retention time has not been reached.
  - A recorder has been configured with extended term retention actions, retained evidence is being deleted, and the configured extended term retention time has not been reached.
- **Evaluating.** A recorder has not reached its retention capacity.

NOTE: When the retention goals are not being met, the associated information on the **Storage** page turns red.

To estimate if the recorder will meet its retention goals

1. Ensure the **Device Configuration** task type is selected.
2. In the **Device Selector** panel, view the **Predicted Retention** column:
   - **Achievable.** It is estimated, based on comparisons of existing data rates and retention goals, that retention goals will be met.
   - **Not Achievable.** It is estimated, based on comparisons of existing data rates and retention goals, that retention goals will not be met.
   - **Evaluating.** There is not yet enough information to estimate whether retention goals will be met.



Organization Path	Address	Serial Number	Network Name	Model	Retention Achieved	Predicted Retention
Eastern Branches/New Y...	10.51.140...	KBAAO2229	DVRKBAAO2229	4216C	Yes	Evaluating

Configuring Network Settings

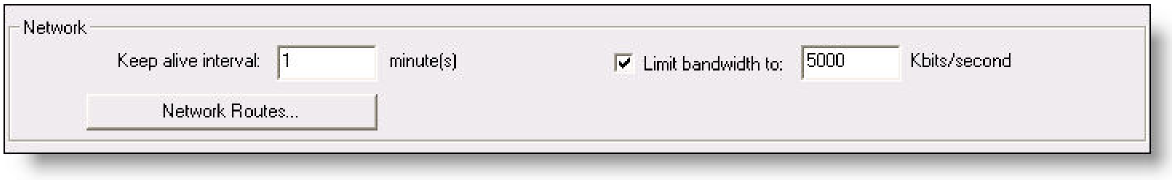
On the General page, you can configure and review the network settings, such as the bandwidth limit and the network routes used for communication.

To configure network settings

1. Ensure the **Device Configuration** task type is selected.
2. Click a recorder in the **Device Selector** panel.
3. Click **General**.

   The **General** page appears.
4. Review the details outlined in the following table.

   If you change one or more settings, you can click **Apply Settings** to save the change, or **Cancel Settings** to discard the change.



Network

Keep alive interval: 1 minute(s)

☑ Limit bandwidth to: 5000 Kbits/second

Table 4: Network Settings

Setting	Description
Keep alive interval	The frequency at which the recorder communicates with the ESM to signal that its connection is still active.
Limit bandwidth to	The bandwidth limit you want to set for network communication. If you do not want to limit the amount of bandwidth the recorder uses, clear the **Limit bandwidth to** check box. **Note:** You can configure the recorder to increase bandwidth usage when an alarm is triggered or a schedule occurs. For more information, see the description of the **Control Bandwidth** action provided in "Configuring Actions" on page 129.
Network routes	The communication path that the software applications, such as the Administrator Console and the Investigator, use to communicate with the recorder. For information about network routes, see "Customizing the Network Communication Path" on page 45.

Customizing the Network Communication Path

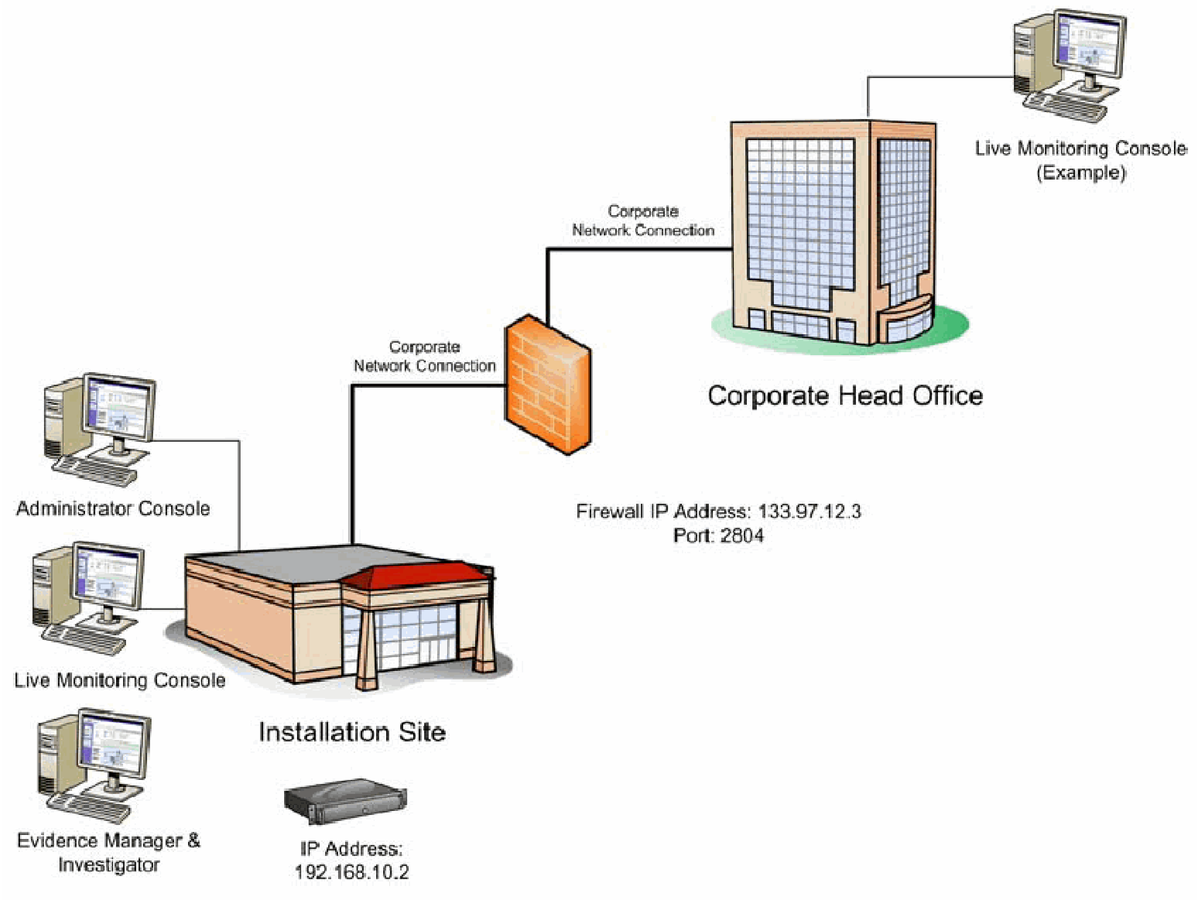
In some network scenarios, you may need to customize the network communication path before you can access the recorder from an external network. For example, your recorder is located behind a network address translation (NAT) system, such as a firewall, and cannot communicate directly with an external network.

To customize the network communication path, you can add a new network route to enable the software applications, such as the Administrator Console and the Investigator, to communicate through the NAT system to reach the recorder.

Adding a new network route is an advanced feature. If you are unsure about adding new network routes, contact your IT department for assistance.

Scenario	You have a central branch where your recorders are located. The recorders are on an internal network. The network is protected by a firewall that ensures network security.
Problem	Employees at the head office, which are on a separate network, cannot access the recorder to perform searches using the Investigator. They cannot access the recorder because they are on a different network and they do not know the recorder's IP address.
Resolution	To ensure employees can communicate with the recorder from outside of the branch's firewall, you can configure the recorder's network routes to enable communication. In this particular scenario, you can add a new network route called **Firewall Access**. When you add the new network route, you will use 133.97.12.3 as the IP address of the new route and 2804 as the port. The following figure illustrates this scenario.

Figure 1: Network Communication Path Customization Scenario



To add a network route

1. Ensure the **Device Configuration** task type is selected.
2. Click a recorder in the **Device Selector** panel.
3. Click **General**.

   The **General** page appears.
4. Under **Network**, click **Network Routes**.

   The **Network Route Manager** dialog box appears.
5. Click **Add**.

   The **Add Network Route** dialog box appears.
6. Specify the network route name, IP address, and port.
7. Click **OK** to close the **Add Network Route** dialog box.

8. Click **OK** to close the **Network Route Manager** dialog box.

9. Click **Apply Settings**.

NOTE: When the software applications, such as the Administrator Console or the Investigator, connect to the recorder, they connect using the order shown in the **Network Route Manager** dialog box, from top to bottom. You can adjust the order by clicking the network interface and then using the **Move Up** and **Move Down** buttons.

Chapter 7

Configuring Cameras

The recorder captures, records, and streams video from connected cameras.

By default, a recorder is pre-configured with camera settings appropriate for most environments. You can adjust these settings to suit your requirements.

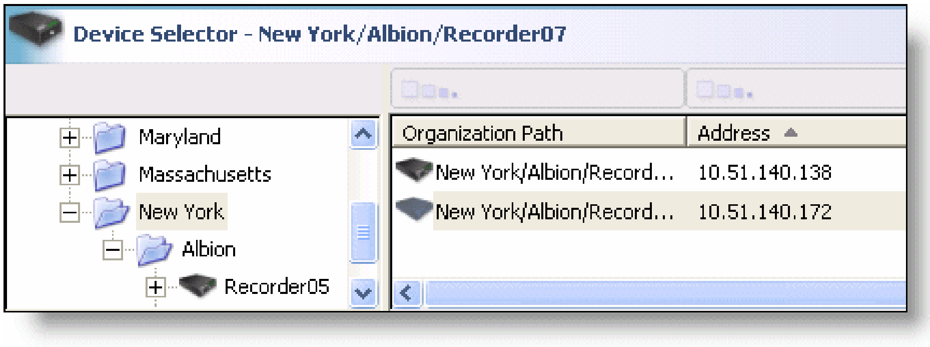
The following topics are covered in this chapter:

Configuring the Camera’s Operation Settings

On the Cameras page, you can enable cameras and configure general settings, such as the camera name, video image size, and video quality.

To configure the camera’s operation settings

1. Ensure the **Device Configuration** task type is selected.
2. Click a recorder in the **Device Selector** panel.



Device Selector - New York/Albion/Recorder07

Organization Path	Address
New York/Albion/Record...	10.51.140.138
New York/Albion/Record...	10.51.140.172

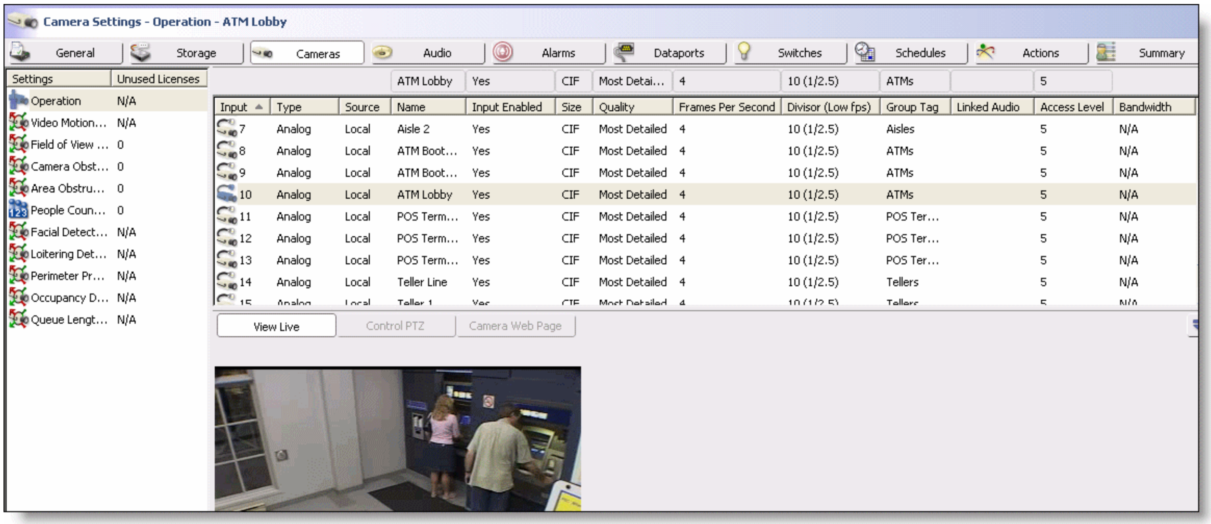
3. Click **Cameras**.

   The **Cameras** page appears.
4. In the **Settings** column on the left, click **Operation**.
5. Click a camera.

   You can configure multiple cameras simultaneously by pressing the **CTRL** or **SHIFT** key and then clicking additional cameras.
6. Review the details outlined in the following table.

   If you change one or more settings, you can click **Apply Settings** to save the change, or **Cancel Settings** to discard the change.

As you configure cameras, you can view live video in the video display window by clicking **View Live**.



Camera Settings - Operation - ATM Lobby

Settings	Unused Licenses
Operation	N/A
Video Motion…	N/A
Field of View …	0
Camera Obst…	0
Area Obstru…	0
People Coun…	0
Facial Detect…	N/A
Loitering Det…	N/A
Perimeter Pr…	N/A
Occupancy D…	N/A
Queue Lengt…	N/A

Input	Type	Source	Name	Input Enabled	Size	Quality	Frames Per Second	Divisor (Low fps)	Group Tag	Linked Audio	Access Level	Bandwidth
			ATM Lobby	Yes	CIF	Most Detai…	4	10 (1/2.5)	ATMs		5	
7	Analog	Local	Aisle 2	Yes	CIF	Most Detailed	4	10 (1/2.5)	Aisles		5	N/A
8	Analog	Local	ATM Boot…	Yes	CIF	Most Detailed	4	10 (1/2.5)	ATMs		5	N/A
9	Analog	Local	ATM Boot…	Yes	CIF	Most Detailed	4	10 (1/2.5)	ATMs		5	N/A
10	Analog	Local	ATM Lobby	Yes	CIF	Most Detailed	4	10 (1/2.5)	ATMs		5	N/A
11	Analog	Local	POS Term…	Yes	CIF	Most Detailed	4	10 (1/2.5)	POS Ter…		5	N/A
12	Analog	Local	POS Term…	Yes	CIF	Most Detailed	4	10 (1/2.5)	POS Ter…		5	N/A
13	Analog	Local	POS Term…	Yes	CIF	Most Detailed	4	10 (1/2.5)	POS Ter…		5	N/A
14	Analog	Local	Teller Line	Yes	CIF	Most Detailed	4	10 (1/2.5)	Tellers		5	N/A
15	Analog	Local	Teller 1	Yes	CIF	Most Detailed	4	10 (1/2.5)	Tellers		5	N/A

Table 5: Camera Operation Settings

Setting	Description
Type	The camera type, such as IP, PTZ, or analog.
Source	The recorder to which the camera is connected, or the IP address of the camera.
Name	The name that identifies the camera. The name appears when Evidence Manager, Evidence Reviewer, and Live Monitoring Console users review clips. The name also appears when Investigator users access the camera, save video clips, or save images.
Input Enabled	When the camera is enabled, you can configure its settings and access live video; video is not captured, recorded, or streamed when the camera is disabled.
Size	The video image size, such as 4CIF or CIF for analog cameras, or 640 x 480 for IP cameras. **Important:** Larger image sizes (for example, 4CIF) require considerably more storage space and can impact how quickly video streams over a network connection, as well as how much network bandwidth the recorder uses. **Note:** If the camera has been set as a people counting camera, you cannot edit the image size.
Quality	The video image quality, such as most compressed, more compressed, medium, more detailed, or most detailed. **Important:** More detailed video requires considerably more storage space than compressed video. The option you choose also impacts how quickly video streams over a network connection and how much network bandwidth the recorder uses.
Frames Per Second	The high frame rate the recorder uses to capture video. **Note:** You can specify that you want the recorder to use this high frame rate when retaining evidence data. For more information, see "Configuring Actions" on page 129. **Note:** If the camera has been set as a people counting camera, you cannot edit the frame rate.

Table 5: Camera Operation Settings (Continued)

Setting	Description
Divisor (Low fps)	For analog cameras, specify the low frame rate the recorder uses to retain video. **Note:** The **Divisor (Low fps)** column shows two numbers: ●The first number, the divisor, is used to calculate the low frame rate, which is used to retain video flagged for long or extended retention. ●The second number, in brackets, is the low frame rate, which the software obtains by dividing the high frame rate by the divisor. For example, 1/5 means one frame is captured every five seconds. ●For an example scenario, see page 53. **Note:** If the camera has been set as a people counting camera, you cannot edit the low frame rate.
Group Tag	The name you can provide to one or more cameras, which helps investigators quickly find evidence for a specific scenario. For example, if investigators at your organization typically view video from cameras A, B, and C when investigating activity at the service desk, specify "Service Desk" as the group tag for cameras A, B, and C. When users open the Investigator, the cameras automatically appear in a group labeled "Service Desk," providing them with quick access to cameras A, B, and C. **Tip:** To specify multiple groups, separate group names using a comma (,) or a semicolon (;).
Linked Audio	Associates an audio input, such as a microphone, with the camera. When enabled, audio is automatically associated to the video.
Access Level	The authorization level a user must have to access live or recorded video from the camera using the March Networks software applications, such as the Investigator. Users can access peripherals with an equivalent or lower access level than what is set in their profile. For example, a user with an access level of five can access peripherals set to five or lower. For information about specifying a user's access level, see "Creating User Profiles and Accounts" on page 188. **Tips:** ●If you are not working with an ESM, you do not need to specify an access level. However, if you plan to install an ESM in the future, we recommend you set the access level as each recorder is installed at your site. ●You can create a covert, or hidden, camera by assigning it an access level that is higher than the user access levels.
Bandwidth	For IP cameras, specify the bandwidth the recorder uses to capture video and display live video, as a portion of the total bandwidth limit for the recorder. **Important:** Do not exceed the recorder's total bandwidth limit.

The following example provides a scenario where you might specify the low frame rate used to retain video:

Scenario

The security director of a 24-hour retail store has updated the security system and needs to configure the recorder to retain the best possible video evidence.

Problem

In the past, the security director has experienced problems where customers have falsely claimed to have had an accident, for example, the customer claimed that they fell at the store. However, when investigating the event, the security director would find that video was not retained because the recorder was only configured to record during video motion detection events and the customer was not actually there. The customer then claimed that the system was not working and that the incident did occur.

Resolution

To avoid this problem, the security director wants to continuously record video at one frame per second to ensure that there is always video evidence, but also wants to ensure the video does not take up a lot of storage space. During periods of motion, the recorder is configured to retain video at eight frames per second for the duration of the motion to capture video.

To specify these settings, the following settings could be configured:

- **Frames per Second.** 8
- **Divisor (Low fps).** 8 (to achieve a low frame rate of 1 frame per second)

Two **Retention** actions would also be configured on the **Actions** page:

- A **Retain Evidence Data** action, configured to retain evidence at a low frame rate during business hours. And, a **Retain Evidence Data** action, configured to retain evidence at a high frame rate when motion occurs.
- For information about creating actions, see “Configuring Actions” on page 129.

Configuring and Adjusting PTZ Cameras

There are two ways you can control PTZ cameras using the Administrator Console:

- Using the Administrator Console’s built-in software controls, as outlined in “Configuring and Adjusting PTZ Cameras using Software Controls” on page 54.
- Using a joystick connected to both your computer and the PTZ camera, as outlined in “Configuring and Adjusting PTZ Cameras Remotely Using a Joystick” on page 56.

Configuring and Adjusting PTZ Cameras using Software Controls

You can use the Administrator Console's built-in tools to adjust a PTZ camera's field of view and to set up preset camera views. Preset camera views let users quickly move the camera's field of view to a particular location.

A camera must be configured as a PTZ camera in the Installer Console or through the **Device Installation** task type before you can control it. For information about configuring a PTZ camera, see the *Installing a Recorder and Testing Device Connections Quick Steps* publication.

If you are working with an IP PTZ camera, see "Adding, Removing, and Configuring IP Cameras or Encoders" on page 60.

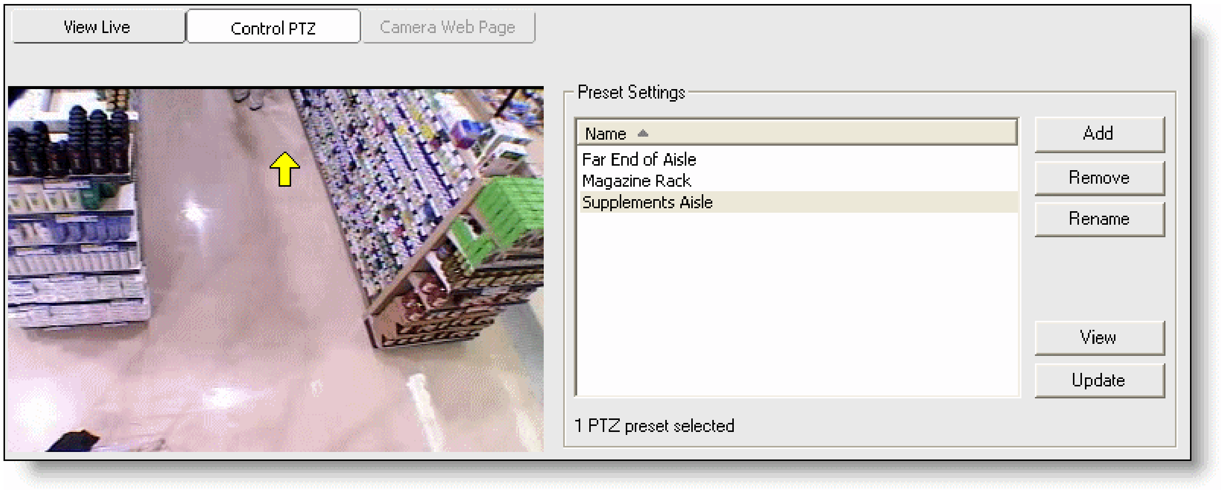
To adjust a PTZ camera

1. Ensure the **Device Configuration** task type is selected.
2. Click a recorder in the **Device Selector** panel.
3. Click **Cameras**.

   The **Cameras** page appears.
4. In the **Settings** column on the left, click **Operation**.
5. Click an enabled camera.
6. Click **Control PTZ.**

   The **COM Port Selection** dialog box appears.
7. Click the COM port you want the camera to use and then click **OK**.
8. Do one of the following:
   - To move the PTZ camera's field of view to a pre-defined spot, click a preset view under **Preset Settings** and then click **View**.
   - To manually move the PTZ camera's field of view, click in the video display window.

A yellow arrow appears on top of the video display window to indicate the direction in which the field of view is moving.



Far End of Aisle
Magazine Rack
Supplements Aisle

1 PTZ preset selected

9. Click **Apply Settings**.

To create a preset view

1. Ensure the **Device Configuration** task type is selected.
2. Click a recorder in the **Device Selector** panel.
3. Click **Cameras**.

   The **Cameras** page appears.
4. In the **Settings** column on the left, click **Operation**.
5. Click an enabled camera.
6. Click **Control PTZ**.

   The **COM Port Selection** dialog box appears.
7. Click the COM port you want the camera to use and then click **OK**.
8. Click in the video display window to move the PTZ camera to a point of interest.

   A yellow arrow appears on top of the video display window to indicate the direction in which the field of view is moving.
9. When you find the view you want to save as a preset, click **Add** under **Preset Settings**.

TIP: You can configure the recorder to move the PTZ camera to a preset view when a particular activity occurs or during a scheduled time period. For example, configure the recorder to move the PTZ camera's field of view to a hallway when a door (with an installed door contact alarm input) is opened. For more information, see "Configuring Actions" on page 129.

To update a preset view

1. Ensure the **Device Configuration** task type is selected.
2. Click a recorder in the **Device Selector** panel.
3. Click **Cameras**.

   The **Cameras** page appears.
4. In the **Settings** column on the left, click **Operation**.
5. Click an enabled camera.
6. Under **Preset Settings**, click a preset view, click **View**, adjust the PTZ camera's field of view in the video display window, and then click **Update**.

NOTE: To remove a preset view, click the view and then click **Remove**.

Configuring and Adjusting PTZ Cameras Remotely Using a Joystick

In Release 5.5 and later, you can use the PTZ passthrough feature to control PTZ cameras using a joystick connected to both your computer and the PTZ camera. This feature provides you with more complete and accurate control over the camera's PTZ functions.

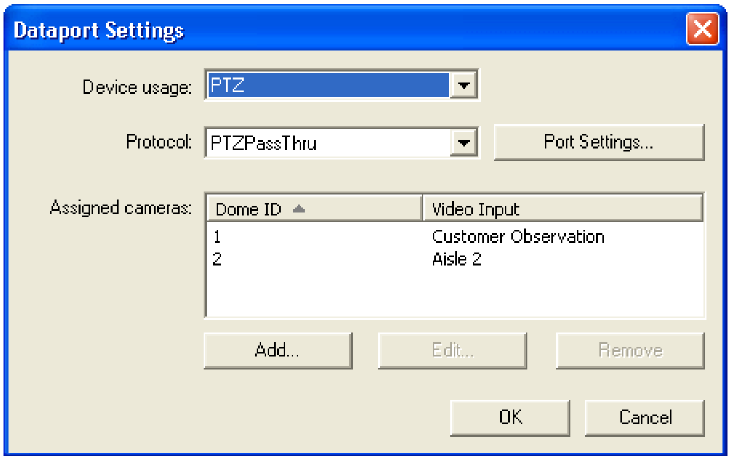
To configure a PTZ passthrough camera

1. Ensure the **Device Installation** task type is selected.
2. Click a recorder in the **Device Selector** panel.
3. Click **Dataports.**

   The **Dataports** page appears.
4. In the **Ports** list, click the dataport to which the camera is connected.
5. Click **Settings**.

   The **Dataport Settings** dialog box appears.
6. In the **Device usage** list, click **PTZ**.

7. In the **Protocol** list, click **PTZPassThru**.



Dataport Settings

Device usage: PTZ

Protocol: PTZPassThru

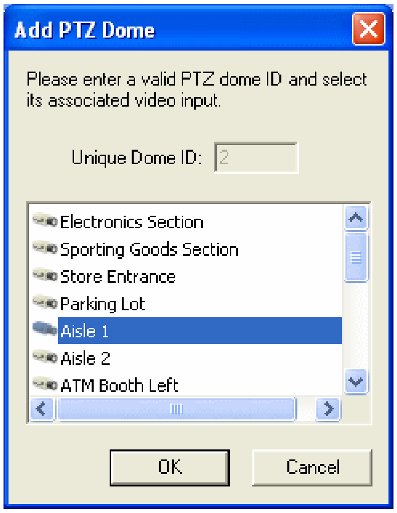
Assigned cameras:

Dome ID	Video Input
1	Customer Observation
2	Aisle 2

8. Click **Add**.

   The **Add PTZ Dome** dialog box appears.

   The **Unique Dome ID** box is unavailable, as a unique identifier is not required for the PTZ passthrough connection.



Add PTZ Dome

Please enter a valid PTZ dome ID and select its associated video input.

Unique Dome ID: 2

- Electronics Section
- Sporting Goods Section
- Store Entrance
- Parking Lot
- Aisle 1
- Aisle 2
- ATM Booth Left

9. Click the camera input you want to associate to the joystick and then click **OK**.

   The camera appears in the **Assigned cameras** list.

10. You can repeat steps 8. and 9. to add multiple camera inputs.

11. Click **Port Settings** to configure the communication settings, if required, and then click **OK**.

    The port settings must match the settings required by the PTZ camera.

12. Click **OK**.

NOTE: You can change a camera in the **Assigned cameras** list by selecting it and then clicking **Edit**. You can then choose a different camera in the **Add PTZ Dome** dialog box.

To remove a camera input from the **Assigned cameras** list, select it and then click **Remove**.

To test a PTZ passthrough camera

When a camera is configured as a PTZ passthrough camera, the Administrator Console's built-in PTZ controls are disabled.

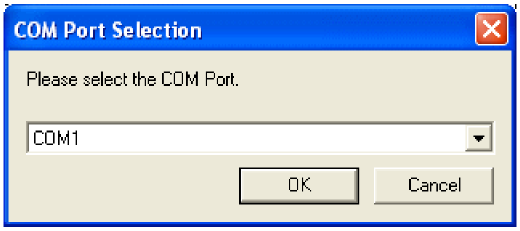
If you select another dataport while you are testing the PTZ passthrough function, the connection will be disabled.

If the network cable becomes disconnected while you are controlling a PTZ camera with a joystick, you must wait for the timeout period to end before you can regain control of the camera.

1. Ensure the **Device Installation** task type is selected.
2. Click a recorder in the **Device Selector** panel.
3. Click **Dataports.**

   The **Dataports** page appears.
4. In the **Ports** list, click the port that is configured for PTZ passthrough and then click **Test**.

   The **COM Port Selection** dialog box appears if you have not set a default COM port. Select the COM port to which the controller is connected and then click **OK**.

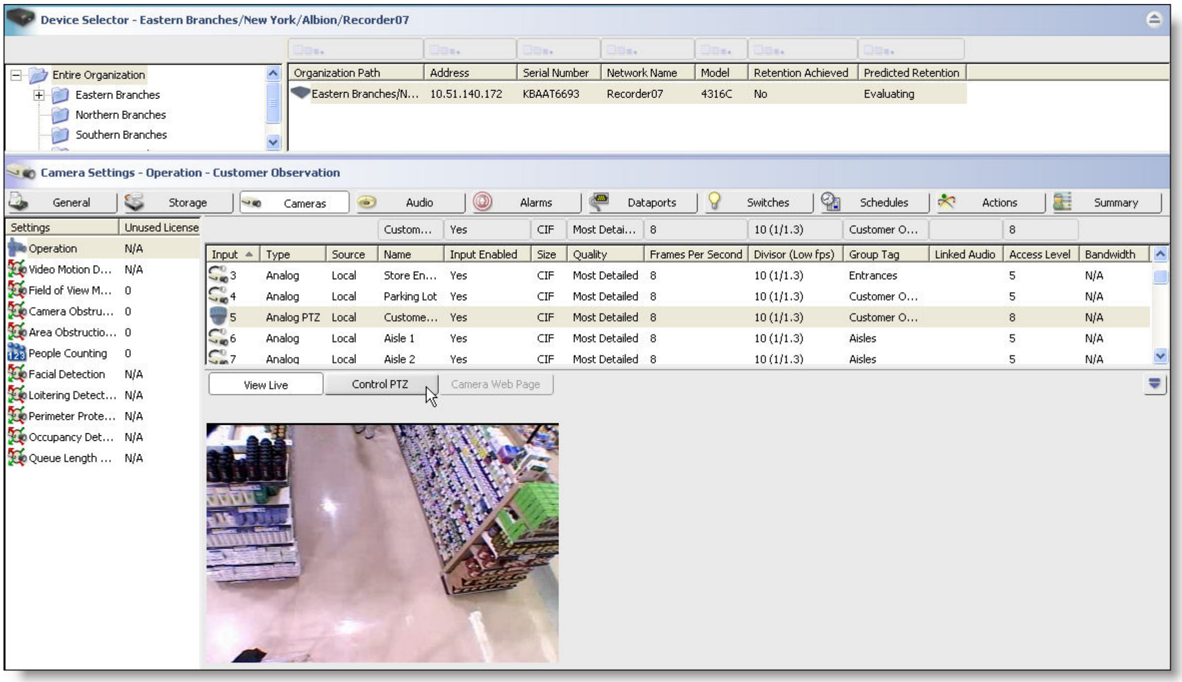


5. Move the joystick to ensure that the camera is responding.

To move a PTZ passthrough camera

1. Ensure the **Device Configuration** task type is selected.
2. Click a recorder in the **Device Selector** panel.
3. Click **Cameras**.

   The **Cameras** page appears.
4. In the **Settings** column on the left, click **Operation**.
5. Click the camera configured as a PTZ passthrough camera.
6. Click **Control PTZ**.



Device Selector - Eastern Branches/New York/Albion/Recorder07

- Entire Organization
  - Eastern Branches
  - Northern Branches
  - Southern Branches

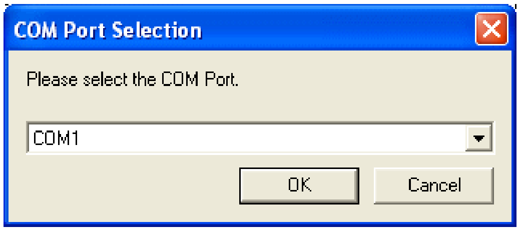
Organization Path	Address	Serial Number	Network Name	Model	Retention Achieved	Predicted Retention
Eastern Branches/N...	10.51.140.172	KBAAT6693	Recorder07	4316C	No	Evaluating

Camera Settings - Operation - Customer Observation

Settings	Unused License
Operation	N/A
Video Motion D...	N/A
Field of View M...	0
Camera Obstru...	0
Area Obstructio...	0
People Counting	0
Facial Detection	N/A
Loitering Detect...	N/A
Perimeter Prote...	N/A
Occupancy Det...	N/A
Queue Length ...	N/A

Input	Type	Source	Name	Input Enabled	Size	Quality	Frames Per Second	Divisor (Low fps)	Group Tag	Linked Audio	Access Level	Bandwidth
			Custom...	Yes	CIF	Most Detai...	8	10 (1/1.3)	Customer O...		8	
3	Analog	Local	Store En...	Yes	CIF	Most Detailed	8	10 (1/1.3)	Entrances		5	N/A
4	Analog	Local	Parking Lot	Yes	CIF	Most Detailed	8	10 (1/1.3)	Customer O...		5	N/A
5	Analog PTZ	Local	Custome...	Yes	CIF	Most Detailed	8	10 (1/1.3)	Customer O...		8	N/A
6	Analog	Local	Aisle 1	Yes	CIF	Most Detailed	8	10 (1/1.3)	Aisles		5	N/A
7	Analog	Local	Aisle 2	Yes	CIF	Most Detailed	8	10 (1/1.3)	Aisles		5	N/A

The **COM Port Selection** dialog box appears if you have not set a default COM port. Select the COM port to which the controller is connected and then click **OK**.



COM Port Selection

Please select the COM Port.

COM1

To avoid setting the COM port every time you configure a camera for PTZ passthrough, you can select a default COM port for passthrough communication. For more information, see “To specify the default COM port for passthrough PTZ communication” on page 120.

7. Move the joystick to control the camera.

Adding, Removing, and Configuring IP Cameras or Encoders

Before the recorder can capture and retain evidence from an IP camera or encoder, you must add the camera to the recorder. After you add the camera, you can perform the following tasks:

- View and reset its recording statistics. View the amount of data transmitted by the IP camera or encoder (also referred to as the data rate). If you have recently repositioned the camera, you can reset the statistics so the data rate accurately reflects the amount of data transferred now that the scene has changed.
- View information about the IP camera or encoder, such as troubleshooting information and details about its inputs and outputs.
- Reconnect to the IP camera or encoder. This is useful if you initially added the IP camera or encoder, however communication could not be established. For example, the IP camera or encoder was starting up.

To add an IP camera or encoder to the recorder and configure its settings

When you modify an IP camera's settings the IP camera may briefly disconnect from the recorder and reconnect, resulting in a brief gap in recorded evidence.

Recorders running Release 5.5.1 (or later) of the recorder software support recording using H.264 compression, but only from March Networks VideoSphere HD cameras. For other March Networks IP cameras or encoders, you must disable H.264 compression and use MPEG4 compression instead. This setting is specified using the IP camera or encoder's Web page.

To remove an IP camera or encoder, select it and then click Remove. Click Yes to confirm the change.

1. Ensure the **Device Installation** task type is selected.
2. Click a recorder in the **Device Selector** panel.
3. Click **Cameras**.

   The **Cameras** page appears.
4. By default, several unassigned IP input slots are available for the connection of IP cameras or encoders. Click an unassigned IP input slot.
5. In the **Camera Brand** list, click the manufacturer.
6. In the **Camera Model** list, click the model.
7. In the **Address** box, type the IP address of the IP camera or encoder.

   To obtain the address, refer to the documentation accompanying the IP camera or encoder.

   The port provided is the default used for the selected brand and model. It automatically updates when you select a new model or brand.

8. Do any of the following:
   - If the IP camera or encoder requires authentication, type a logon ID in the **Login** box and type a password in the **Password** box.
   - If more than one mode is supported on the model, click **JPEG** or **MPEG4** in the **Camera Mode** list.
   - If multiple video channels are supported, click a channel in the **Channel** list.
9. Click **Apply**.

   The recorder connects to the IP camera or encoder and a live video stream appears.

To view information about the IP camera or encoder

You can click **Web Page** to open the IP camera or encoder's Web page. The Web page, which is built into the IP camera or encoder, lets you customize the capture and display settings, in addition to other options.

1. Ensure the **Device Configuration** task type is selected.
2. Click a recorder in the **Device Selector** panel.
3. Click **Cameras**.

   The **Cameras** page appears.
4. Click an IP camera or encoder.
5. Click **Advanced**.
6. Under **Status** and **Camera Information**, view the troubleshooting information that appears and details about the IP camera or encoder's inputs and outputs.

To view and reset the IP camera or encoder's data rates

1. Ensure the **Device Configuration** task type is selected.
2. Click a recorder in the **Device Selector** panel.
3. Click **Cameras**.

   The **Cameras** page appears.
4. Click an IP camera or encoder.
5. Click **Advanced**.
6. Under **Datarates**, view the IP camera or encoder's data rates.
7. To reset the data rates, click **Reset data rates**.

To disconnect and reconnect to the IP camera or encoder

1. Ensure the **Device Configuration** task type is selected.
2. Click a recorder in the **Device Selector** panel.
3. Click **Cameras**.

   The **Cameras** page appears.

4. Click an IP camera or encoder.
5. Click **Advanced**.
6. Click **Reconnect**.

Accessing an IP Camera or Encoder's Web Page

Many IP cameras and encoders have a built-in configuration tool that is accessible from a Web page stored within its software. The configuration tool lets you customize the capture and display settings, in addition to other options.

You can launch the Web-based configuration tool directly from the Administrator Console.

Before you can configure the IP camera or encoder settings, you must first configure the Administrator Console to communicate with the IP camera or encoder. You can specify the required information using the Installer Console or by switching to the Device Installation task type. For more information, see "Adding, Removing, and Configuring IP Cameras or Encoders" on page 60 or the *Installing a Recorder and Testing Peripheral Connections Quick Steps* publication included on your March Networks CD.

To access an IP camera or encoder's Web page

1. Ensure the **Device Configuration** task type is selected.
2. Click a recorder in the **Device Selector** panel.
3. Click **Cameras**.

   The **Cameras** page appears.
4. In the **Settings** column on the left, click **Operation**.
5. Click an IP camera or encoder.
6. Click **Camera Web Page**.

   The Web-based configuration tool appears. If a tool is not available, instructions appear.

Enabling and Configuring Video Motion Detection

Recorders have built-in motion detection abilities that allow them to flag activity as a distinct video motion alarm.

If you are working with an IP camera, be aware that not all IP cameras support video motion detection.

Enabling Video Motion Detection

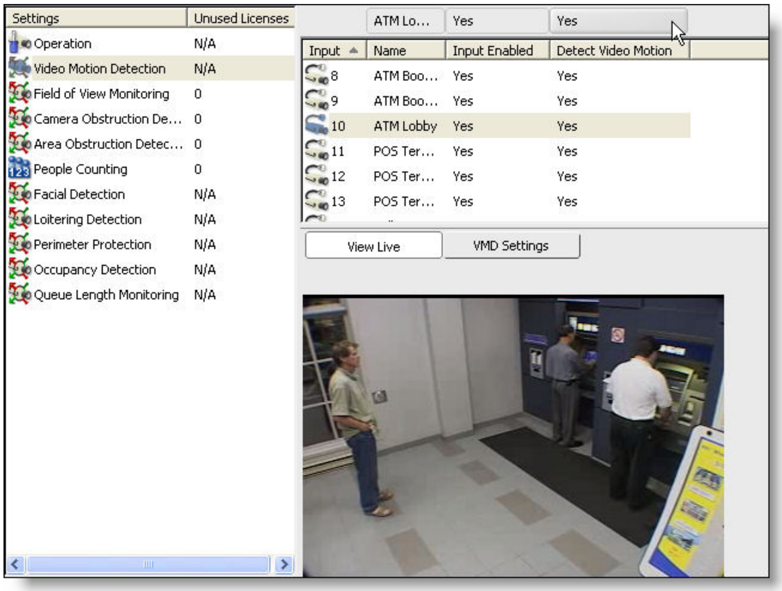
Before you can configure video motion detection, you must enable it.

If the camera has been set as a people counting camera, you cannot configure it to detect motion. For information about people counting cameras, see “Configuring People Counting” on page 83.

To enable video motion detection

1. Ensure the **Device Configuration** task type is selected.
2. Click a recorder in the **Device Selector** panel.
3. Click **Cameras**.

   The **Cameras** page appears.
4. In the **Settings** column on the left, click **Video Motion Detection**.
5. Click an enabled camera.
6. Click the settings bar above the **Detect Video Motion** column and click **Yes**.



Settings	Unused Licenses
Operation	N/A
Video Motion Detection	N/A
Field of View Monitoring	0
Camera Obstruction De...	0
Area Obstruction Detec...	0
People Counting	0
Facial Detection	N/A
Loitering Detection	N/A
Perimeter Protection	N/A
Occupancy Detection	N/A
Queue Length Monitoring	N/A

Input	Name	Input Enabled	Detect Video Motion
	ATM Lo...	Yes	Yes
8	ATM Boo...	Yes	Yes
9	ATM Boo...	Yes	Yes
10	ATM Lobby	Yes	Yes
11	POS Ter...	Yes	Yes
12	POS Ter...	Yes	Yes
13	POS Ter...	Yes	Yes

7. Click **Apply Settings**.

Isolating Areas Monitored for Motion

Recorders can monitor all activity within the camera's field of view, or you can isolate areas that you want to monitor for motion. The following example provides a scenario where you would isolate an area:

Scenario Your camera is monitoring the hallway that leads to the Employees Only office. You want to know when people walk through the hallway, so you have configured the recorder to flag a video motion alarm event when activity occurs in the camera's field of view.

Problem To the left of the hallway, and within the camera's field of view, is the Customer Service department door. This door is frequently opened and closed, which causes the recorder to flag several video motion alarm events.

Resolution To prevent the recorder from flagging activity at the Customer Service department door, use the masking feature to ignore activity at the door and monitor only the hallway entrance for motion.

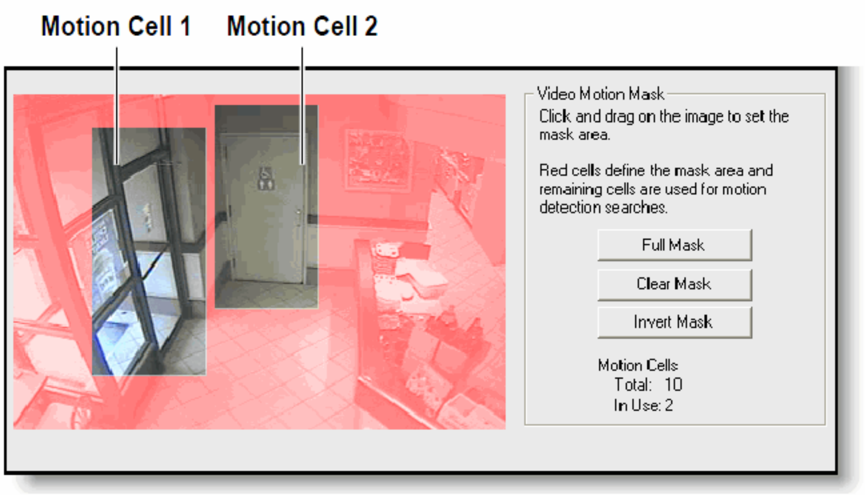
When you specify areas of interest for an IP camera, the areas that you highlight divide the view into motion cells. Depending on the camera make and model, the number of available motion cells varies.

By default, one motion cell is used and the mask is cleared. As you isolate areas of interest, additional motion cells are used. The number of motion cells you can use is limited by the total number available. Ensure you do not exceed the total number available, as indicated under Motion Cells.

If you do exceed the total number available, you can:

- Simplify the mask to reduce the number of motion cells that are In Use (change the masked areas from red to clear).
- Click Clear Mask to start again. Then, click and drag to define fewer masked areas.

The following figure shows an IP camera with two motion cells.



Click and drag on the image to set the mask area.

Red cells define the mask area and remaining cells are used for motion detection searches.

Motion Cells
Total: 10
In Use: 2

To isolate an area monitored for motion

1. Ensure the **Device Configuration** task type is selected.
2. Click a recorder in the **Device Selector** panel.
3. Click **Cameras**.

   The **Cameras** page appears.
4. In the **Settings** column on the left, click **Video Motion Detection**.
5. Click an enabled camera.
6. Click **VMD Settings**.
7. Do any of the following:
   - In the video display window, click and drag on the image to isolate areas that are monitored for motion and areas that are excluded. Areas with no mask (clear cells) are monitored for motion; red cells are not monitored.
   - Click **Full Mask**. With this setting the mask takes up the entire field of view and motion is not detected.
   - Click **Clear Mask**. With this setting, motion in any area of the camera’s field of view is detected.
   - Click **Invert Mask**. Reverses the areas to be monitored for motion. When you click this button, the red areas become clear and the clear areas become red.
8. Click **Apply Settings**.

Specifying Motion Sensitivity

To further customize how the recorder detects motion, you can indicate how much motion must occur before the recorder recognizes it as an alarm. This setting is based on the size of the object in motion and how much room it takes up in the camera’s field of view. The following example provides a scenario where you could customize the motion sensitivity:

Scenario Your camera is monitoring a lobby in an office building. You want to know when people walk into the lobby, so you have configured the recorder to flag a motion alarm event when activity occurs in the camera’s field of view.

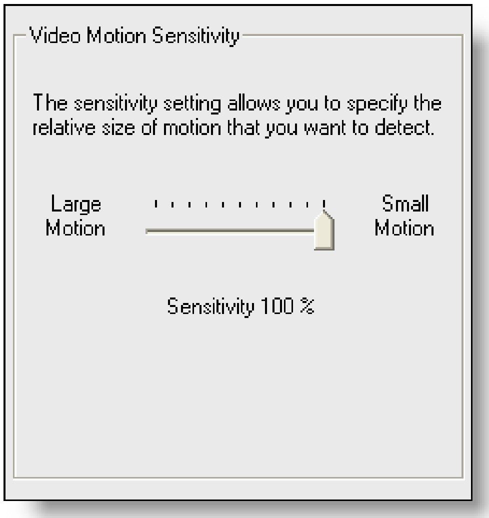
Problem The building has a small hanging sign. When the building’s ventilation system turns on, the sign moves slightly. As the sign moves, the recorder flags the activity as a video motion alarm.

Resolution To prevent the recorder from generating video motion alarms when the sign moves, decrease the motion sensitivity. This allows the recorder to only flag activity when larger amounts of motion are detected, such as a person walking through the lobby.

To specify motion sensitivity

1. Ensure the **Device Configuration** task type is selected.
2. Click a recorder in the **Device Selector** panel.
3. Click **Cameras**.

   The **Cameras** page appears.
4. In the **Settings** column on the left, click **Video Motion Detection**.
5. Click an enabled camera.
6. Click **VMD Settings**.
7. Under **Video Motion Sensitivity**, use the slider to adjust the motion sensitivity between the following settings:
   - **Large Motion.** Flag an alarm when a large amount of activity occurs. This setting is less sensitive to motion.
   - **Small Motion**. Flag an alarm when a small amount of activity occurs. This setting is more sensitive to motion.



Video Motion Sensitivity

The sensitivity setting allows you to specify the relative size of motion that you want to detect.

Sensitivity 100 %

8. Click **Apply Settings**.

Configuring Field of View Monitoring

The field of view monitoring feature lets the recorder monitor connected cameras and alert you when the camera's view changes. This feature is useful when you are monitoring several cameras at different organizations and want to be automatically notified when changes occur.

When the camera's field of view changes, and the change lasts for at least 24 hours, the recorder generates an alert to notify you. For example, the camera's field of view can change when a camera is moved from its original position. It can also change when a camera failure occurs, such as a change in camera focus or decreased signal quality.

Although a change must last for at least 24 hours before an alert is generated, the recorder does not count any periods of time during which there is very low or no interior or exterior light source as part of the 24-hour period. As a result, if there are 12 hours of darkness, an alert can take between 36 to 48 hours to generate.

The following example provides a scenario where you could enable field of view monitoring:

Scenario You are monitoring a network of recorders across a large number of stores. You do not check the cameras every day, as there are thousands of cameras on the network.

Problem You have recently had problems with faulty mounting brackets that cause cameras to shift from their original location. However, you only realized this fact when you tried to locate video related to an investigation and found that the camera was pointing at the floor.

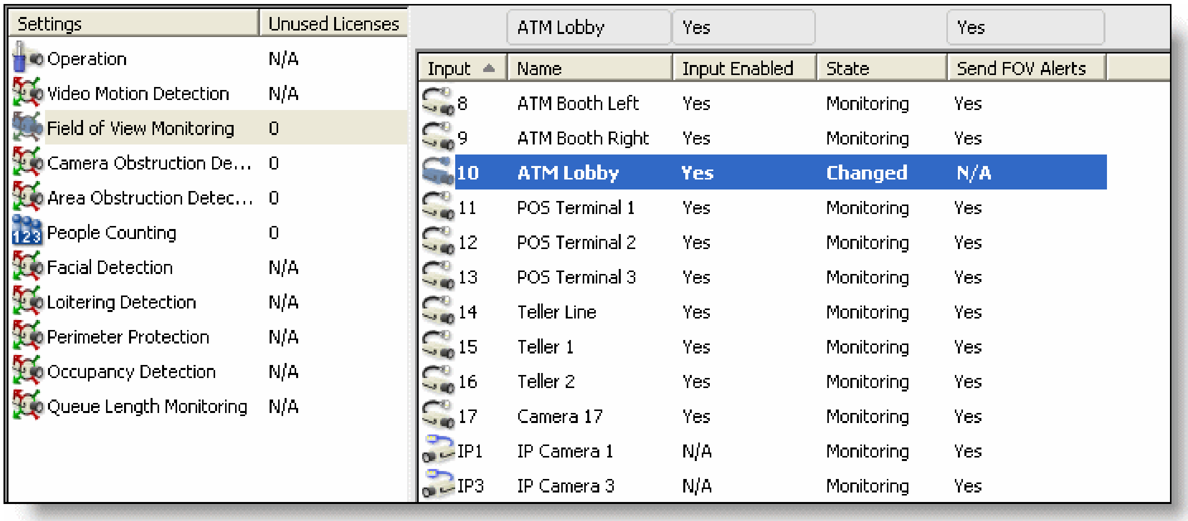
Resolution Enable field of view monitoring to detect when the camera's view changes significantly from its original view.

NOTE: Before you configure this feature, ensure the camera that you are monitoring is set up to maximize the field of view monitoring feature. For more information, see the *Video Analytics Reference Guide*, included on your March Networks CD.

How Does Field of View Monitoring Work?

When you enable a camera, the recorder automatically enters an initial calibration period and starts analyzing the camera’s field of view. During this calibration period, the recorder notes the types of activity and changes that occur each day to gather details on how a typical view would look. After seven days, it uses these details to detect changes to the field of view.

When the calibration period ends, the recorder uses the details it has gathered to detect changes to the camera’s field of view. You can set the recorder to automatically generate an alert so that when a significant change occurs, and lasts for at least 24 hours (excluding times of very low light), you are notified of the change. When an alert occurs, the camera turns bold, and the status is Changed in the State column.



Settings	Unused Licenses
Operation	N/A
Video Motion Detection	N/A
Field of View Monitoring	0
Camera Obstruction De...	0
Area Obstruction Detec...	0
People Counting	0
Facial Detection	N/A
Loitering Detection	N/A
Perimeter Protection	N/A
Occupancy Detection	N/A
Queue Length Monitoring	N/A

	ATM Lobby	Yes		Yes

Input ▲	Name	Input Enabled	State	Send FOV Alerts
8	ATM Booth Left	Yes	Monitoring	Yes
9	ATM Booth Right	Yes	Monitoring	Yes
10	**ATM Lobby**	**Yes**	**Changed**	**N/A**
11	POS Terminal 1	Yes	Monitoring	Yes
12	POS Terminal 2	Yes	Monitoring	Yes
13	POS Terminal 3	Yes	Monitoring	Yes
14	Teller Line	Yes	Monitoring	Yes
15	Teller 1	Yes	Monitoring	Yes
16	Teller 2	Yes	Monitoring	Yes
17	Camera 17	Yes	Monitoring	Yes
IP1	IP Camera 1	N/A	Monitoring	Yes
IP3	IP Camera 3	N/A	Monitoring	Yes

After an alert has occurred, you can respond to the alert and reset the field of view.

Reviewing the Field of View Monitoring Status

When you enable a camera the recorder immediately starts monitoring it for field of view changes. At any time you can view the status.

To review the field of view monitoring status

1. Ensure the **Device Configuration** task type is selected.
2. Click a recorder in the **Device Selector** panel.

   Please note, field of view monitoring is not supported for the 4516 C NVR.
3. Click **Cameras**.

   The **Cameras** page appears.
4. In the **Settings** column on the left, click **Field of View Monitoring**.
5. Click an enabled camera.

   If the camera has been set as a people counting camera, you cannot configure it to detect field of view changes. For information about people counting cameras, see “Configuring People Counting” on page 83.
6. Under **State**, review the field of view status. The following table outlines the statuses that can appear.

Table 6: Field of View Statuses

Status	Description
Calibrating	The recorder is assessing the scene to determine how the field of view would typically look. The calibration period lasts seven days.
Monitoring	The recorder is monitoring the camera’s field of view for changes.
Changed	The camera’s field of view has changed. If field of view alerts are enabled, an alert appears on the **Health Monitoring** page. For more information about enabling field of view alerts, see “Configuring the Recorder to Notify you of Field of View Changes” on page 70. For more information about accessing alerts, see “Monitoring Health” on page 159.
Failed to Calibrate	One of the following situations has occurred: ● There was insufficient light during the seven-day calibration period. There must be at least eight hours of light per day (56 hours over the seven-day period) for the camera to properly assess the scene; otherwise, the calibration period will not be successful. ● Too many structural changes have occurred within the scene for the recorder to properly complete the calibration period. For example, in a parking lot where vehicles are continuously entering and exiting, the recorder will likely be unable to assess the scene. ● The camera is not suitable for the field of view monitoring feature. For example, the camera is a PTZ camera, which moved frequently during the calibration period.
N/A	Field of view monitoring is not supported by the camera or recorder.

Configuring the Recorder to Notify you of Field of View Changes

If you want to receive notification of field of view monitoring changes, you can enable the recorder to send an alert when the a significant change occurs.

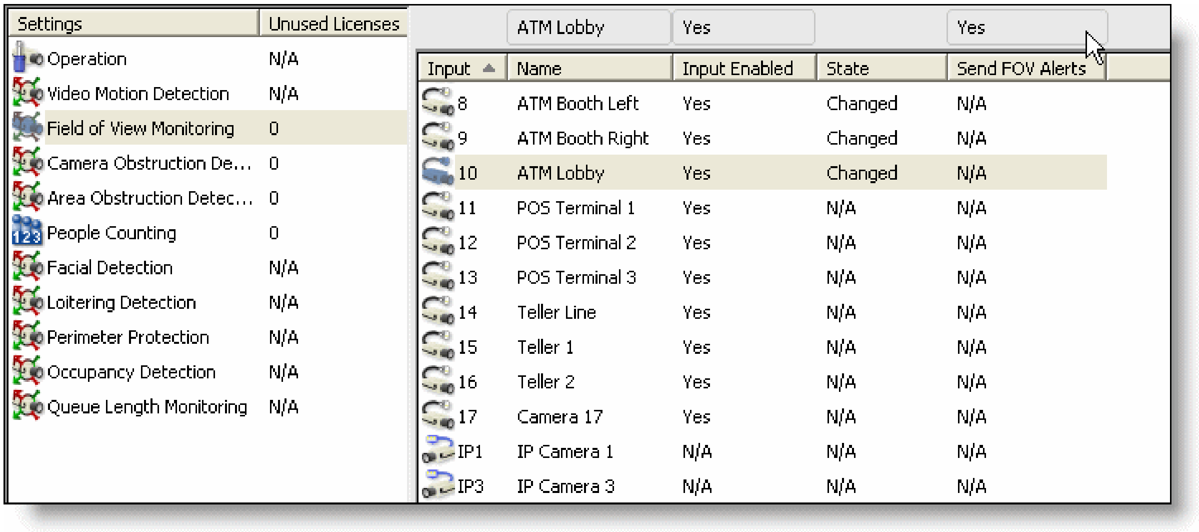
To enable field of view alerts

1. Ensure the **Device Configuration** task type is selected.
2. Click a recorder in the **Device Selector** panel.

   Please note, field of view monitoring is not supported for the 4516 C NVR.
3. Click **Cameras**.

   The **Cameras** page appears.
4. In the **Settings** column on the left, click **Field of View Monitoring**.
5. Click an enabled camera.

   If the camera has been set as a people counting camera, you cannot configure it to detect field of view changes. For information about people counting cameras, see “Configuring People Counting” on page 83.
6. Click the settings bar above the **Send FOV Alerts** column and click **Yes**.
7. Click **Apply Settings**.



Settings	Unused Licenses
Operation	N/A
Video Motion Detection	N/A
Field of View Monitoring	0
Camera Obstruction De...	0
Area Obstruction Detec...	0
People Counting	0
Facial Detection	N/A
Loitering Detection	N/A
Perimeter Protection	N/A
Occupancy Detection	N/A
Queue Length Monitoring	N/A

	ATM Lobby	Yes		Yes
Input	Name	Input Enabled	State	Send FOV Alerts
8	ATM Booth Left	Yes	Changed	N/A
9	ATM Booth Right	Yes	Changed	N/A
10	ATM Lobby	Yes	Changed	N/A
11	POS Terminal 1	Yes	N/A	N/A
12	POS Terminal 2	Yes	N/A	N/A
13	POS Terminal 3	Yes	N/A	N/A
14	Teller Line	Yes	N/A	N/A
15	Teller 1	Yes	N/A	N/A
16	Teller 2	Yes	N/A	N/A
17	Camera 17	Yes	N/A	N/A
IP1	IP Camera 1	N/A	N/A	N/A
IP3	IP Camera 3	N/A	N/A	N/A

Responding to Field of View Change Alerts

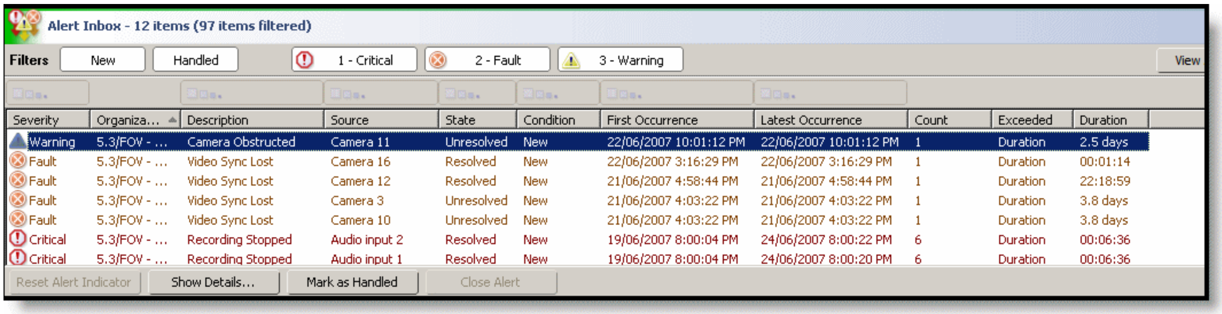
If you have configured the recorder to notify you when the camera's field of view has changed significantly, you will receive an alert. You can respond to the alert to view details, such as the time and time of the change. To help you better understand how to respond, you can review see an image of the camera's intended field of view and an image taken at the time of the alert.

When you handle alerts, it is important to correct the camera before you restart the calibration process.

In the **Field of View Alert** dialog box, you can switch between **Show last matching image** and **Show live video image** as you review and adjust the camera's field of view.

To respond to field of view alerts

1. Ensure the **Health Monitoring** task type is selected.
2. Click a recorder in the **Device Selector** panel.
3. Click a field of view alert in the **Alert Inbox**.
4. Click **Mark as Handled**.



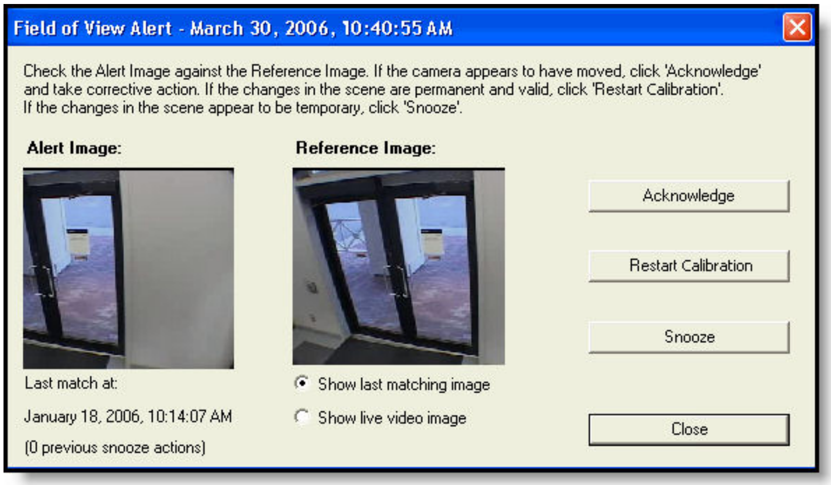
Severity	Organiza...	Description	Source	State	Condition	First Occurrence	Latest Occurrence	Count	Exceeded	Duration
Warning	5.3/FOV - ...	Camera Obstructed	Camera 11	Unresolved	New	22/06/2007 10:01:12 PM	22/06/2007 10:01:12 PM	1	Duration	2.5 days
Fault	5.3/FOV - ...	Video Sync Lost	Camera 16	Resolved	New	22/06/2007 3:16:29 PM	22/06/2007 3:16:29 PM	1	Duration	00:01:14
Fault	5.3/FOV - ...	Video Sync Lost	Camera 12	Resolved	New	21/06/2007 4:58:44 PM	21/06/2007 4:58:44 PM	1	Duration	22:18:59
Fault	5.3/FOV - ...	Video Sync Lost	Camera 3	Unresolved	New	21/06/2007 4:03:22 PM	21/06/2007 4:03:22 PM	1	Duration	3.8 days
Fault	5.3/FOV - ...	Video Sync Lost	Camera 10	Unresolved	New	21/06/2007 4:03:22 PM	21/06/2007 4:03:22 PM	1	Duration	3.8 days
Critical	5.3/FOV - ...	Recording Stopped	Audio input 2	Resolved	New	19/06/2007 8:00:04 PM	24/06/2007 8:00:22 PM	6	Duration	00:06:36
Critical	5.3/FOV - ...	Recording Stopped	Audio input 1	Resolved	New	19/06/2007 8:00:04 PM	24/06/2007 8:00:20 PM	6	Duration	00:06:36

5. Double-click the field of view alert.

   The **Field of View Alert** dialog box appears.

6. Compare the resulting images to determine whether the camera has moved or whether the changes in the scene are permanent:
   - **Alert image**. Shows an image from the time the alert was generated.

- **Reference image**. Shows the last image that matches your intended field of view. The information provided under **Last match at** indicates when the reference image was captured.



Field of View Alert - March 30, 2006, 10:40:55 AM

Check the Alert Image against the Reference Image. If the camera appears to have moved, click 'Acknowledge' and take corrective action. If the changes in the scene are permanent and valid, click 'Restart Calibration'.
If the changes in the scene appear to be temporary, click 'Snooze'.

Last match at:

January 18, 2006, 10:14:07 AM

(0 previous snooze actions)

● Show last matching image

○ Show live video image

7. Correct the issue in one of the ways outlined in the following table, depending on the situation that has occurred.

Table 7: Field of View Changes and Corrective Actions

Situation	Example	Corrective Action
Camera has been moved	The camera view has shifted over time, due to a faulty mounting bracket and no longer captures the intended view.	1 Click **Acknowledge** and then adjust the camera's field of view, as required, to return it to your intended view. The alert automatically changes to the handled state when you click **Acknowledge**. To view the alert, ensure the **Handled** button is pressed in. 2 After the camera has been adjusted, re-open the alert and then click **Restart Calibration**.
Scene has changed permanently	You have replaced the original camera with a new camera.	Click **Restart Calibration**. After the seven-day calibration period ends, the recorder starts monitoring the field of view for changes.
Temporary change of scene	A large crate has been placed in the room and will be moved within 24 hours.	Click **Snooze**. If the scene is still changed, another alert appears in 24 hours.

Configuring Camera Obstruction Detection

A recorder can automatically detect when a camera’s field of view has been obstructed by an object. This feature is useful when you are monitoring several cameras at different organizations and want to be notified of an obstructed camera within five to 30 minutes.

The following example provides a scenario where you could use camera obstruction detection:

Scenario	You are monitoring a small room with two ATMs.
Problem	In the past, you have had problems with individuals covering the camera with a jacket and vandalizing the ATMs during the early morning hours.
Resolution	Enable camera obstruction detection to detect when the camera’s field of view is completely covered by an object. When the camera is obstructed, you receive an alert from the recorder and security staff can investigate.

To configure camera obstruction detection you must first enable the feature. Then, specify how long the obstruction must last before you receive an alert.

Before you configure this feature, ensure the camera that you are monitoring is set up to maximize the camera obstruction detection feature. For more information, see the *Video Analytics Reference Guide*, included on your March Networks CD.

To enable camera obstruction detection

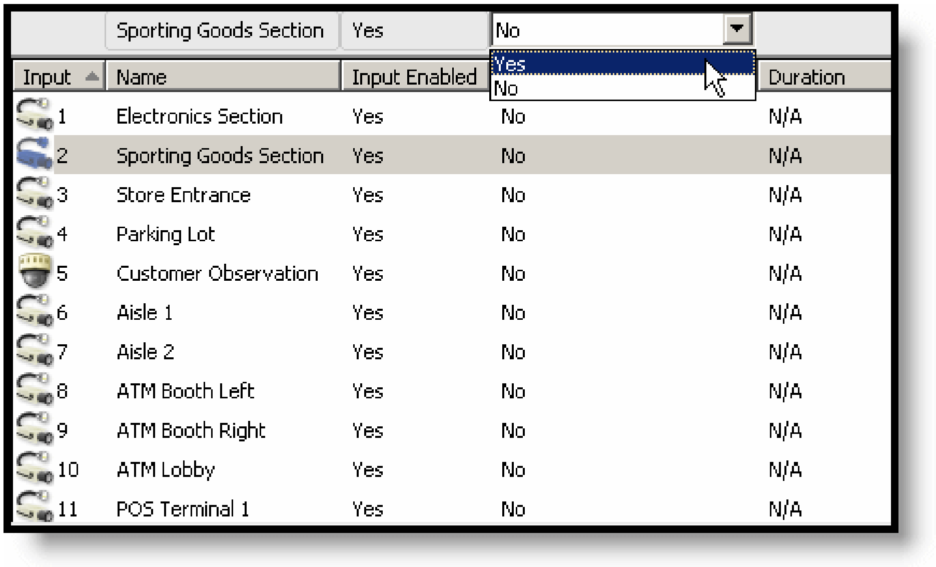
1. Ensure the **Device Configuration** task type is selected.
2. Click a recorder in the **Device Selector** panel.

   Please note, camera obstruction detection is not supported for the 4516 C NVR.
3. Click **Cameras**.

   The **Cameras** page appears.
4. In the **Settings** column on the left, click **Camera Obstruction Detection**.
5. Click an enabled camera.

   If the camera has been set as a people counting camera, you cannot configure it to detect camera obstructions. For information about people counting cameras, see “Configuring People Counting” on page 83.

6. Click the settings bar above the **Detect Camera Obstruction** column and click **Yes**.



	Sporting Goods Section	Yes	No	
			Yes No	
Input ▲	**Name**	**Input Enabled**		**Duration**
1	Electronics Section	Yes	No	N/A
2	Sporting Goods Section	Yes	No	N/A
3	Store Entrance	Yes	No	N/A
4	Parking Lot	Yes	No	N/A
5	Customer Observation	Yes	No	N/A
6	Aisle 1	Yes	No	N/A
7	Aisle 2	Yes	No	N/A
8	ATM Booth Left	Yes	No	N/A
9	ATM Booth Right	Yes	No	N/A
10	ATM Lobby	Yes	No	N/A
11	POS Terminal 1	Yes	No	N/A

7. Click **Apply Settings**.

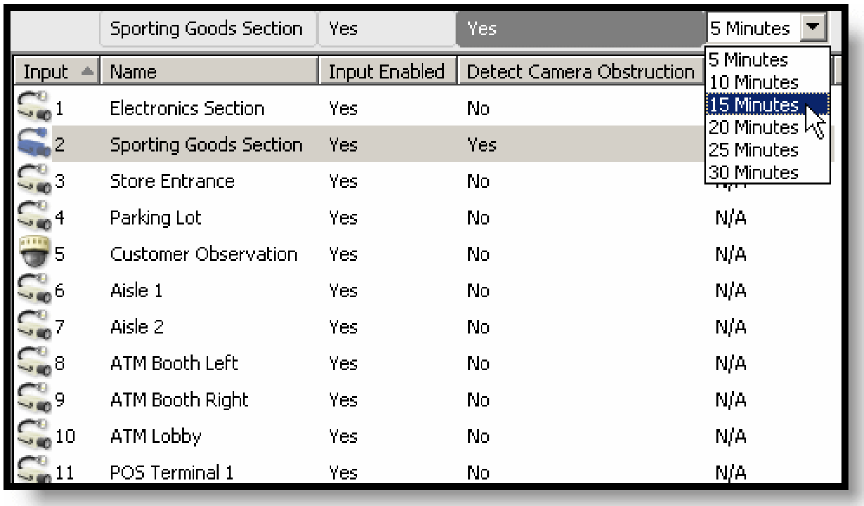
To specify the duration of the obstruction before an alert is generated

1. Ensure the **Device Configuration** task type is selected.
2. Click a recorder in the **Device Selector** panel.

   Please note, camera obstruction detection is not supported for the 4516 C NVR.
3. Click **Cameras**.

   The **Cameras** page appears.
4. In the **Settings** column on the left, click **Camera Obstruction Detection**.
5. Click a camera that has camera obstruction enabled.

6. Click the settings bar above the **Duration** column and click a duration.

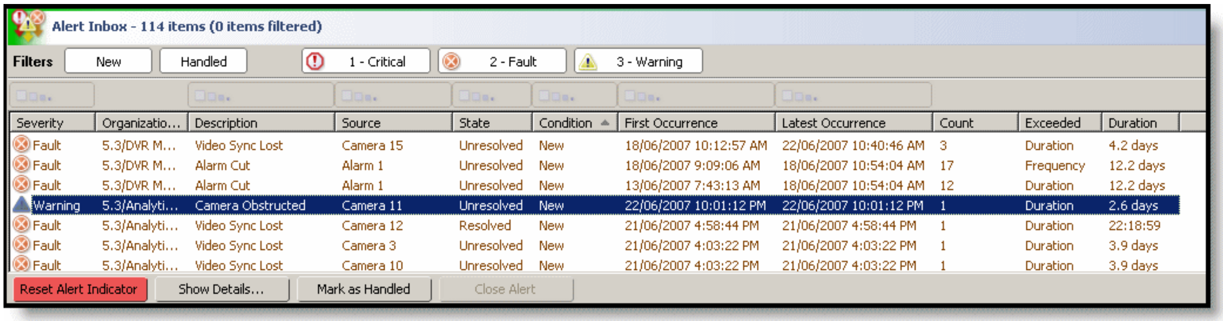


	Sporting Goods Section	Yes	Yes	5 Minutes
Input	**Name**	**Input Enabled**	**Detect Camera Obstruction**	
1	Electronics Section	Yes	No	
2	Sporting Goods Section	Yes	Yes	
3	Store Entrance	Yes	No	N/A
4	Parking Lot	Yes	No	N/A
5	Customer Observation	Yes	No	N/A
6	Aisle 1	Yes	No	N/A
7	Aisle 2	Yes	No	N/A
8	ATM Booth Left	Yes	No	N/A
9	ATM Booth Right	Yes	No	N/A
10	ATM Lobby	Yes	No	N/A
11	POS Terminal 1	Yes	No	N/A

7. Click **Apply Settings**.

To respond to camera obstruction alerts

1. Ensure the **Health Monitoring** task type is selected.
2. Click a recorder in the **Device Selector** panel.
3. Click a camera obstruction alert in the **Alert Inbox**.
4. Click **Mark as Handled**.



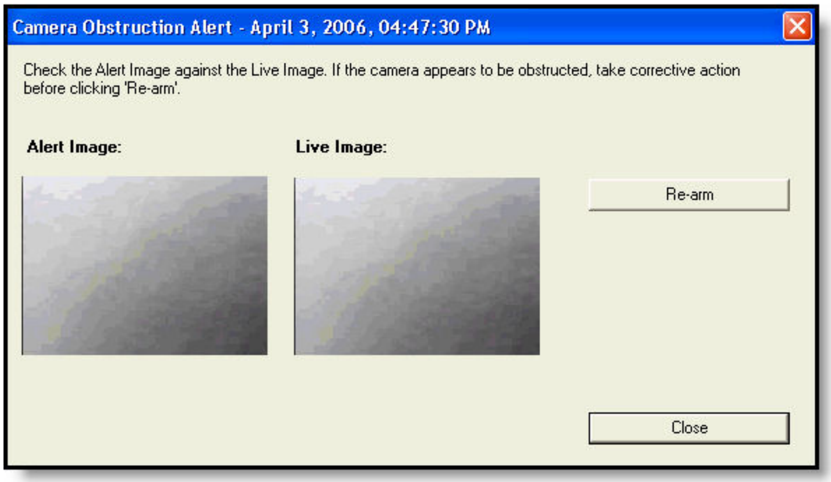
Alert Inbox - 114 items (0 items filtered)

Severity	Organizatio...	Description	Source	State	Condition	First Occurrence	Latest Occurrence	Count	Exceeded	Duration
Fault	5.3/DVR M...	Video Sync Lost	Camera 15	Unresolved	New	18/06/2007 10:12:57 AM	22/06/2007 10:40:46 AM	3	Duration	4.2 days
Fault	5.3/DVR M...	Alarm Cut	Alarm 1	Unresolved	New	18/06/2007 9:09:06 AM	18/06/2007 10:54:04 AM	17	Frequency	12.2 days
Fault	5.3/DVR M...	Alarm Cut	Alarm 1	Unresolved	New	13/06/2007 7:43:13 AM	18/06/2007 10:54:04 AM	12	Duration	12.2 days
Warning	5.3/Analyti...	Camera Obstructed	Camera 11	Unresolved	New	22/06/2007 10:01:12 PM	22/06/2007 10:01:12 PM	1	Duration	2.6 days
Fault	5.3/Analyti...	Video Sync Lost	Camera 12	Resolved	New	21/06/2007 4:58:44 PM	21/06/2007 4:58:44 PM	1	Duration	22:18:59
Fault	5.3/Analyti...	Video Sync Lost	Camera 3	Unresolved	New	21/06/2007 4:03:22 PM	21/06/2007 4:03:22 PM	1	Duration	3.9 days
Fault	5.3/Analyti...	Video Sync Lost	Camera 10	Unresolved	New	21/06/2007 4:03:22 PM	21/06/2007 4:03:22 PM	1	Duration	3.9 days

The **Camera Obstruction Alert** dialog box appears.

5. Compare the following images to determine whether the camera has moved or whether the changes in the scene are permanent:
   - **Alert Image**. Shows an image from the time the alert was generated.
   - **Live Image**. Shows an image from the camera's current field of view.

6. Correct the issue by moving the object or item that is obstructing the view and then clicking **Re-arm**.



Camera Obstruction Alert - April 3, 2006, 04:47:30 PM

Check the Alert Image against the Live Image. If the camera appears to be obstructed, take corrective action before clicking 'Re-arm'.

NOTE: When you handle alerts, it is important to correct the camera before you re-arm the camera obstruction detection feature.

Additional Camera Configuration Options

In addition to the options mentioned in this chapter, you can perform the following activities to further customize how the recorder works with connected cameras:

- **Configure video analytics settings for IP cameras and encoders.** For example, configure the IP camera or encoder to detect alarms when an individual loiters in an area or the number of individuals in an area exceeds a specified limit. For more information, see “Configuring Video Analytic Features” on page 77.
- **Schedule activities.** For example, customize the recorder to retain all activity during the day and retain only video motion activity at night. For more information, see “Creating Schedules” on page 125.
- **Specify how the recorder responds to events.** For example, customize how the recorder responds to an alarm. For more information, see “Configuring Actions” on page 129.

Configuring Video Analytic Features

March Networks recorders, IP cameras, and encoders have built-in video analytic capabilities that allow you to track the movement of people or objects, detect when people move into forbidden zones or loiter in specific areas, and detect the length of queues or waiting areas. You can then configure the Administrator Console to raise alarms when any of these events occurs.

For a list of video analytics supported by each March Networks recorder, IP camera, or encoder, see the video analytics data sheet at www.marchnetworks.com, or contact your March Networks representative.

The following topics are covered in this chapter:

- “Configuring Area Obstruction Detection” on page 78
- “Configuring People Counting” on page 83
- “Setting Up March Networks IP Cameras and Encoders for Analytics” on page 90
- “Setting the Perspective for March Networks IP Cameras or Encoders” on page 92
- “Configuring Loitering Detection” on page 93
- “Configuring Occupancy Detection” on page 95
- “Configuring Perimeter Protection” on page 98
- “Configuring Queue Length Monitoring” on page 101
- “Configuring Facial Detection” on page 104

The following table outlines the video analytics that are available and provides a brief description:

Table 8: Video Analytics

Analytic	Description	Available on
Area obstruction detection	An area within a scene is blocked for longer than a set time.	March Networks recorders
People counting	People enter and exit an area within a camera's field of view.	March Networks recorders
Loitering detection	A person remains in a specified location for longer than a set time.	March Networks IP cameras or encoders
Occupancy detection	The number of people in a scene equals or exceeds a specified amount.	March Networks IP cameras or encoders
Perimeter protection	A person or object crosses a defined line or boundary within a field of view.	March Networks IP cameras or encoders
Queue length monitoring	A line of people within a scene extends further than a set length.	March Networks IP cameras or encoders
Facial detection	A clear facial image is detected within an IP camera's field of view.	March Networks IP cameras or encoders

Configuring Area Obstruction Detection

The area obstruction detection feature allows a recorder to automatically detect when an object obstructs a camera's view and can trigger an alarm to notify you.

The following example provides a scenario where you could enable area obstruction detection:

Scenario	You are monitoring a fire exit that is located beside the shipping and receiving office.
Problem	You have had problems with individuals placing large boxes in front of the emergency exit door.
Resolution	Enable area obstruction detection and specify the area around the emergency exit as the area of interest. Specify the amount of time that objects must obstruct the door before you are notified by an alarm.

To configure area obstruction detection you must first enable the feature. Then, specify how long the obstruction must last before you receive an alert, and specify the area of interest.

To further customize how the recorder detects an obstructed area, you can specify the detection sensitivity, which is the size of the obstruction relative to the area of interest.

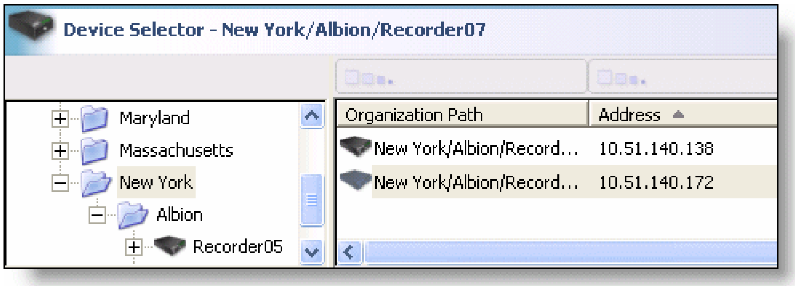
After you configure area obstruction detection, you can test your settings.

NOTE: Before you configure this feature, ensure the camera that you are monitoring is set up to maximize the area obstruction detection feature. For more information, see the *Video Analytics Reference Guide*, included on your March Networks CD.

To enable area obstruction detection

1. Ensure the **Device Configuration** task type is selected.
2. Click a recorder in the **Device Selector** panel.

   Please note, area obstruction detection is not supported for the 4516 C NVR.



Device Selector - New York/Albion/Recorder07

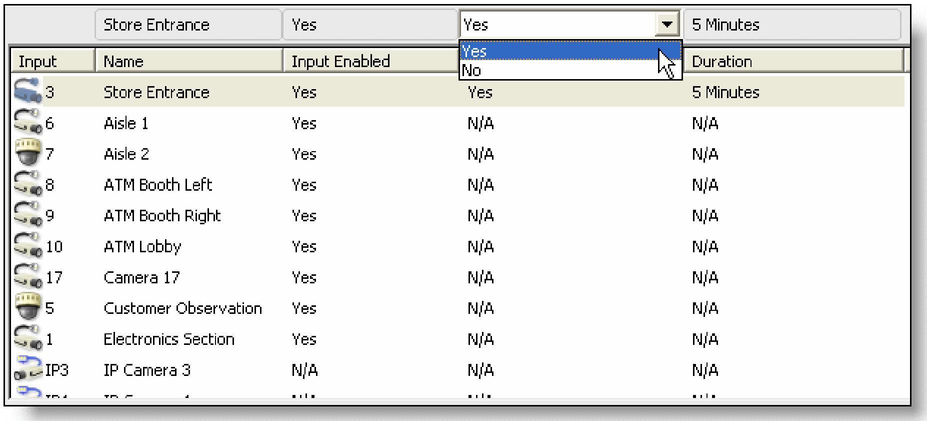
- Maryland
- Massachusetts
- New York
  - Albion
    - Recorder05

Organization Path	Address
New York/Albion/Record...	10.51.140.138
New York/Albion/Record...	10.51.140.172

3. Click **Cameras**.

   The **Cameras** page appears.
4. In the **Settings** column on the left, click **Area Obstruction Detection**.
5. Click an enabled camera.

   If the camera has been set as a people counting camera, you cannot configure it to detect area obstructions. For information about people counting cameras, see "Configuring People Counting" on page 83.
6. Click the settings bar above the **Detect Area Obstruction** column and click **Yes**.
7. Click **Apply Settings**.



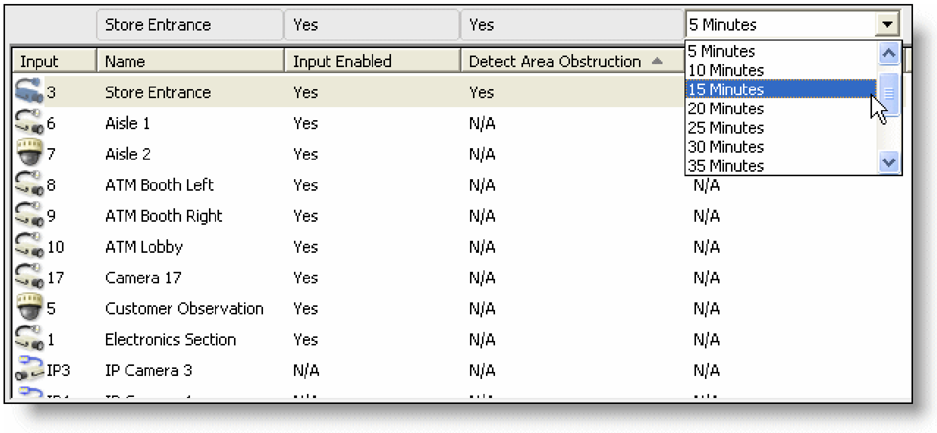
	Store Entrance	Yes	Yes	5 Minutes
Input	Name	Input Enabled		Duration
3	Store Entrance	Yes	Yes	5 Minutes
6	Aisle 1	Yes	N/A	N/A
7	Aisle 2	Yes	N/A	N/A
8	ATM Booth Left	Yes	N/A	N/A
9	ATM Booth Right	Yes	N/A	N/A
10	ATM Lobby	Yes	N/A	N/A
17	Camera 17	Yes	N/A	N/A
5	Customer Observation	Yes	N/A	N/A
1	Electronics Section	Yes	N/A	N/A
IP3	IP Camera 3	N/A	N/A	N/A

To specify the duration of the obstruction before an alarm occurs

1. Ensure the **Device Configuration** task type is selected.
2. Click a recorder in the **Device Selector** panel.
3. Click **Cameras**.

   The **Cameras** page appears.
4. In the **Settings** column on the left, click **Area Obstruction Detection**.
5. Click an enabled camera.

   If the camera has been set as a people counting camera, you cannot configure it to detect camera obstructions. For information about people counting cameras, see “Configuring People Counting” on page 83.
6. Click the settings bar above the **Duration** column and click a duration.



	Store Entrance	Yes	Yes	5 Minutes
Input	Name	Input Enabled	Detect Area Obstruction ▲	
3	Store Entrance	Yes	Yes	
6	Aisle 1	Yes	N/A	
7	Aisle 2	Yes	N/A	
8	ATM Booth Left	Yes	N/A	N/A
9	ATM Booth Right	Yes	N/A	N/A
10	ATM Lobby	Yes	N/A	N/A
17	Camera 17	Yes	N/A	N/A
5	Customer Observation	Yes	N/A	N/A
1	Electronics Section	Yes	N/A	N/A
IP3	IP Camera 3	N/A	N/A	N/A

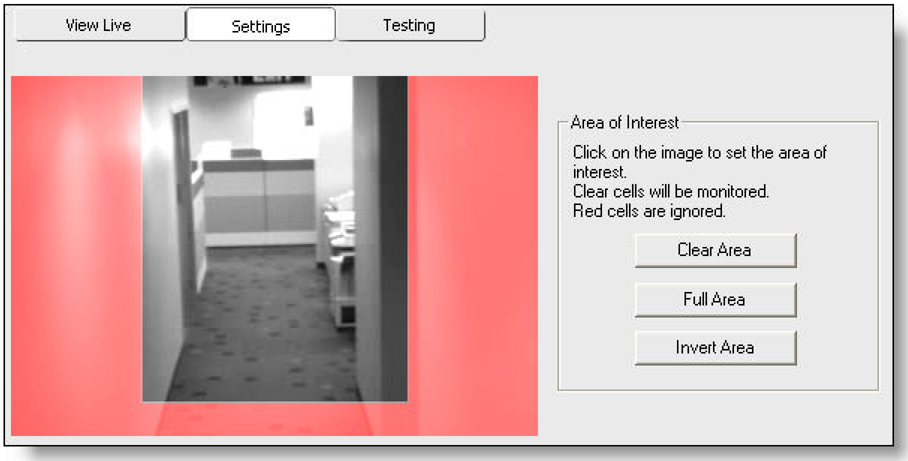
   If you choose a short duration, unwanted alarms may occur. For example, if you set the duration to 1 Minute, a person loitering within the specified area of interest for more than one minute is detected as an area obstruction. We recommend choosing a duration of appropriate length for your application of this feature.
7. Click **Apply Settings**.

To specify an area in which to detect obstructions

1. Ensure the **Device Configuration** task type is selected.
2. Click a recorder in the **Device Selector** panel.
3. Click **Cameras**.

   The **Cameras** page appears.
4. In the **Settings** column on the left, click **Area Obstruction Detection**.
5. Click a camera that has area obstruction detection enabled.
6. Click **Settings**.
7. Do any of the following:
   - In the video display window, click and drag on the image to isolate areas that are monitored for obstructions and areas that are excluded. Areas with no mask (clear cells) are monitored for obstructions; red cells are not monitored.
   - Click **Full Mask**. With this setting the mask takes up the entire field of view and obstructions are not detected.
   - Click **Clear Mask**. With this setting, obstructions in any area of the camera's field of view are detected.
   - Click **Invert Mask**. Reverses the areas to be monitored for obstructions. When you click this button, the red areas become clear and the clear areas become red.

   You can isolate multiple areas of interest/ignored areas within the camera's field of view.



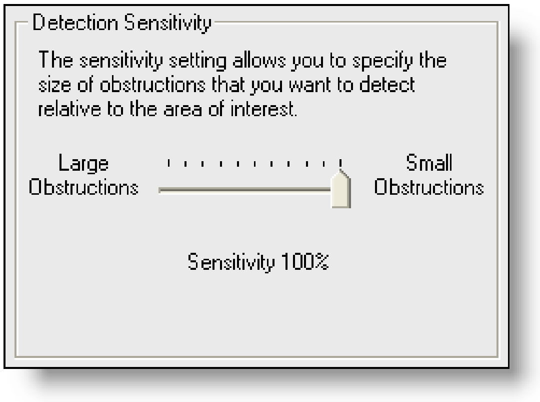
Click on the image to set the area of interest.
Clear cells will be monitored.
Red cells are ignored.

8. Click **Apply Settings**.

To specify object detection sensitivity

1. Ensure the **Device Configuration** task type is selected.
2. Click a recorder in the **Device Selector** panel.
3. Click **Cameras**.

   The **Cameras** page appears.
4. In the **Settings** column on the left, click **Area Obstruction Detection**.
5. Click a camera that has area obstruction detection enabled.
6. Click **Settings**.
7. Under **Detection Sensitivity**, use the slider to adjust the detection sensitivity between the following settings:
   - **Large Obstructions.** Flag an alarm when the full area of interest is obstructed. This setting is less sensitive to obstruction.
   - **Small Obstructions**. Flag an alarm when any part of the area of interest is obstructed. This setting is more sensitive to obstruction.
8. Click **Apply Settings**.



Detection Sensitivity

The sensitivity setting allows you to specify the size of obstructions that you want to detect relative to the area of interest.

Sensitivity 100%

To test the area obstruction detection configuration

1. Ensure the **Device Configuration** task type is selected.
2. Click a recorder in the **Device Selector** panel.
3. Click **Cameras**.

   The **Cameras** page appears.
4. In the **Settings** column on the left, click **Area Obstruction Detection**.
5. Click a camera that has area obstruction detection enabled.
6. Click **Testing**.

   When an object is left in the area of interest, and is large enough to be detected, it is highlighted in the video display.

   If the object is removed before the specified duration is exceeded, the highlight is removed.

Configuring People Counting

Using a camera that is mounted over a doorway, a recorder can count the number of people who enter or exit through the doorway.

How Does People Counting Work?

When you enable people counting, the recorder automatically enters an initial calibration period and starts analyzing the size of people entering or exiting the doorway, enabling it to identify people as they pass the camera.

The amount of time required for the calibration varies, depending on the flow of traffic through the doorway, and ranges from one hour to several hours.

When the calibration period ends, the recorder uses the details it has gathered to count the number of people entering or exiting through the doorway. The ESM receives these counts, after which time the reporting tool can be used to query the database for people counting data.

If you choose to isolate an area of interest, you must do so before calibration. If calibration has already occurred and you want to add or modify a mask, recalibration occurs.

If the recorder is restarted or the camera is disabled and re-enabled after calibration is complete, re-calibration is not required. However, if a recorder is replaced, recalibration occurs.

Enabling People Counting

For the recorder to count people, you must first enable the feature.

Some recorder models require that you only enable certain combinations of video inputs.

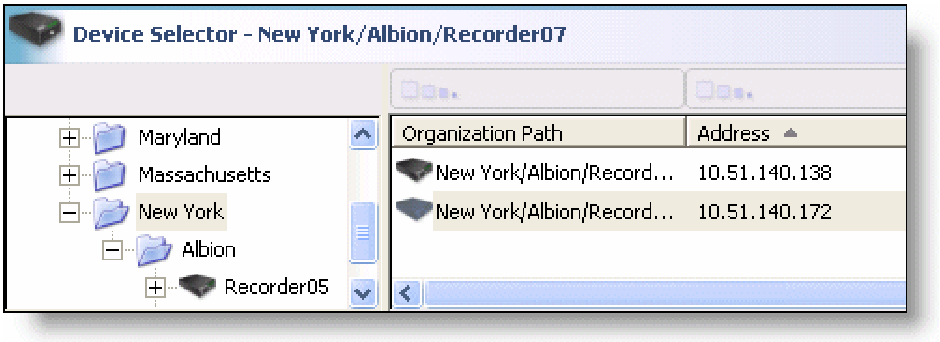
- Second generation 4210 DVR (identified by the vents located at the front left and right of the unit, beside the handles) or 4216 C NVR: If you enable people counting on two or more inputs, you must disable the remaining inputs in the camera group. For example, if inputs 1 and 2 are enabled, you must disable inputs 3 and 4.
- 3108 DVR. Enable and disable inputs in the following manner:
  - If you enable input 1, disable input 2; if you enable input 2, disable input 1
  - If you enable input 3, disable input 4; if you enable input 4, disable input 3
  - If you enable input 5, disable input 6; if you enable input 6, disable input 5
  - If you enable input 7, disable input 8; if you enable input 8, disable input 7

NOTE: If you are enabling the people counting feature on a second generation 4210 DVR (identified by the vents located at the front left and right of the unit, beside the handles) or a 4216 C NVR, and you enable people counting on two or more inputs within a camera group, a message indicates that you must disable the remaining inputs in that group. For example, if you enable people counting on inputs 1 and 2 in the first camera group, you must disable inputs 3 and 4.

To enable people counting

1. Ensure the **Device Configuration** task type is selected.
2. Click a recorder in the **Device Selector** panel.

   Please note, people counting is not supported for the 4516 C NVR.



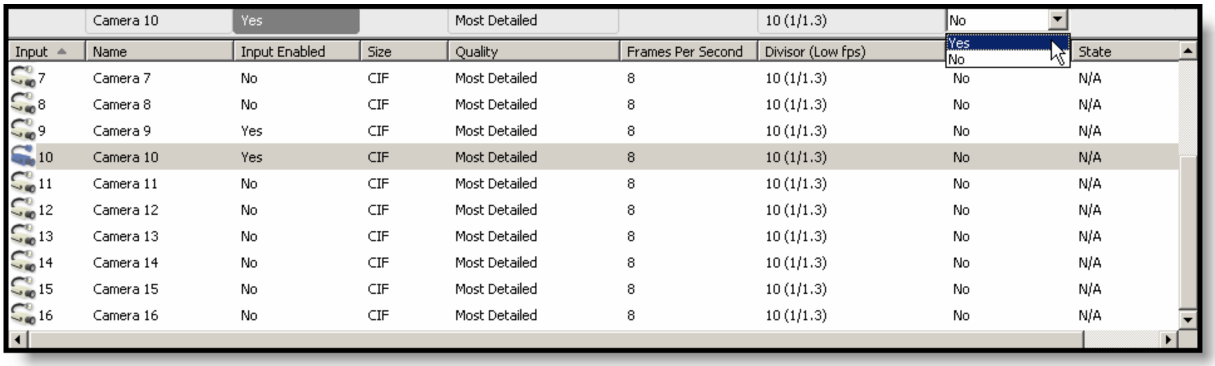
Device Selector - New York/Albion/Recorder07

- Maryland
- Massachusetts
- New York
  - Albion
    - Recorder05

Organization Path	Address
New York/Albion/Record...	10.51.140.138
New York/Albion/Record...	10.51.140.172

3. Click **Cameras**.

   The **Cameras** page appears.
4. In the **Settings** column on the left, click **People Counting**.
5. Click an enabled camera.
6. Click the settings bar above the **Count People** column and click **Yes**.



	Camera 10	Yes		Most Detailed		10 (1/1.3)	No	
Input	Name	Input Enabled	Size	Quality	Frames Per Second	Divisor (Low fps)		State
7	Camera 7	No	CIF	Most Detailed	8	10 (1/1.3)	No	N/A
8	Camera 8	No	CIF	Most Detailed	8	10 (1/1.3)	No	N/A
9	Camera 9	Yes	CIF	Most Detailed	8	10 (1/1.3)	No	N/A
10	Camera 10	Yes	CIF	Most Detailed	8	10 (1/1.3)	No	N/A
11	Camera 11	No	CIF	Most Detailed	8	10 (1/1.3)	No	N/A
12	Camera 12	No	CIF	Most Detailed	8	10 (1/1.3)	No	N/A
13	Camera 13	No	CIF	Most Detailed	8	10 (1/1.3)	No	N/A
14	Camera 14	No	CIF	Most Detailed	8	10 (1/1.3)	No	N/A
15	Camera 15	No	CIF	Most Detailed	8	10 (1/1.3)	No	N/A
16	Camera 16	No	CIF	Most Detailed	8	10 (1/1.3)	No	N/A

7. Click **Apply Settings**.

Configuring People Counting

To configure the people counting feature you must specify the entry and exit direction. Optionally, you can isolate an area of interest within which you want to count people. For example, you can count people in entry and exit areas, but ignore people in loitering areas or cashier stations.

After you configure people counting, you can test your settings.

When people counting is configured, reports are available that provide statistics about the number of people counted. If the recorder is not configured to communicate with an ESM, these reports are not available. For more information, see “Registering and Unregistering Recorders With an ESM” on page 195.

If you configure a camera to count people, you cannot enable any other video analytics on the camera. If other video analytics were enabled on the camera before you enabled people counting, they are disabled, and the video analytics are not automatically re-enabled when you disable people counting.

Before you configure this feature, ensure the camera that you are monitoring is set up to maximize the people counting feature. For more information, see the *Video Analytics Reference Guide*, included on your March Networks CD.

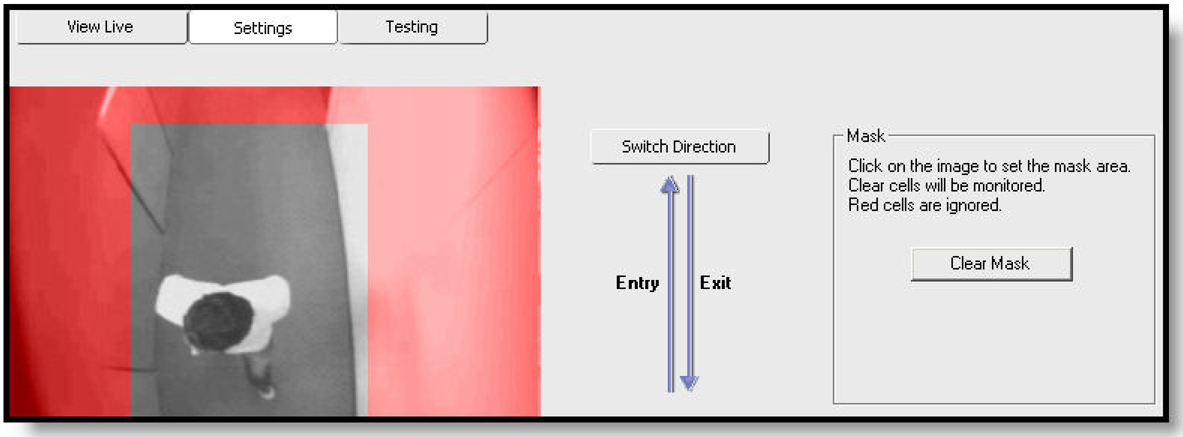
When a camera is set as a people counting camera, the recorder does not retain its video, and users cannot access the camera using the other March Networks software applications, such as the Investigator or Live Monitoring Console.

You can view a live video display to verify the people counting camera setup by clicking **View Live**. While viewing live video for a people counting camera, no other users can access live video from this camera or any other people counting cameras connected to the same recorder.

To specify the entry and exit directions

1. Ensure the **Device Configuration** task type is selected.
2. Click a recorder in the **Device Selector** panel.
3. Click **Cameras**.

   The **Cameras** page appears.
4. In the **Settings** column on the left, click **People Counting**.
5. Click a camera that has people counting enabled.
6. Click **Settings**.
7. Click **Switch Direction** to change the entry and exit directions.



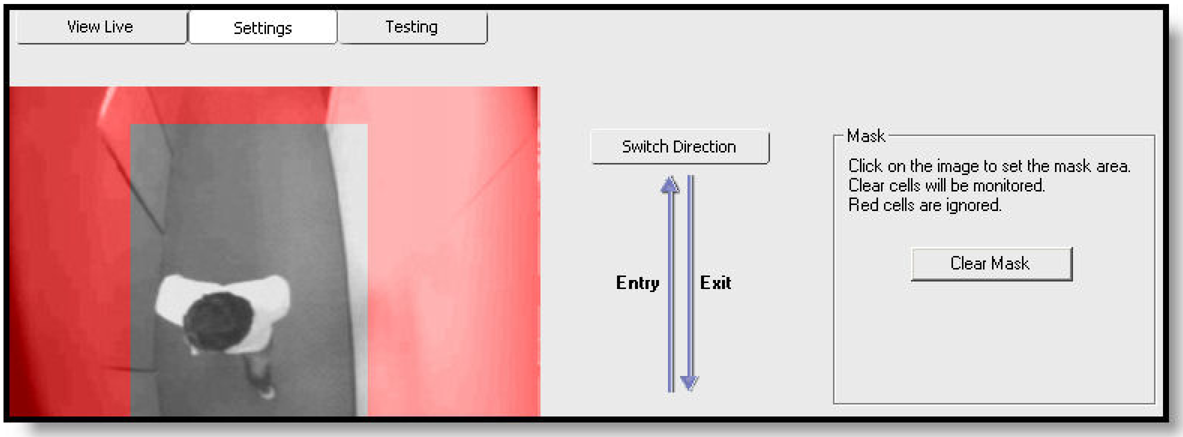
Click on the image to set the mask area.
Clear cells will be monitored.
Red cells are ignored.

8. Click **Apply Settings**.

To specify an area in which people are counted

1. Ensure the **Device Configuration** task type is selected.
2. Click a recorder in the **Device Selector** panel.
3. Click **Cameras**.

   The **Cameras** page appears.
4. In the **Settings** column on the left, click **People Counting**.
5. Click **Settings**.
6. Do any of the following:
   - In the video display window, click and drag on the image to isolate areas in which people are counted and areas that are excluded. Areas with no mask (clear cells) are monitored; red cells are not.
   - Click **Full Mask**. With this setting the mask takes up the entire field of view and people are not counted.
   - Click **Clear Mask**. With this setting, people in any area of the camera's field of view are counted.
   - Click **Invert Mask**. Reverses the areas to be monitored. When you click this button, the red areas become clear and the clear areas become red.



Click on the image to set the mask area.
Clear cells will be monitored.
Red cells are ignored.

7. Click Apply **Settings**.

To test the people counting configuration

1. Ensure the **Device Configuration** task type is selected.
2. Click a recorder in the **Device Selector** panel.
3. Click **Cameras**.

   The **Cameras** page appears.
4. In the **Settings** column on the left, click **People Counting**.
5. Click a camera that has people counting enabled.

6. Click **Testing**.

   A live running count of entries and exits appears. As well, people are highlighted in the video display.

NOTE: You can reset the running counts by clicking **Reset Counts**. Resetting the running counts does not affect the actual counts that are sent to the ESM.

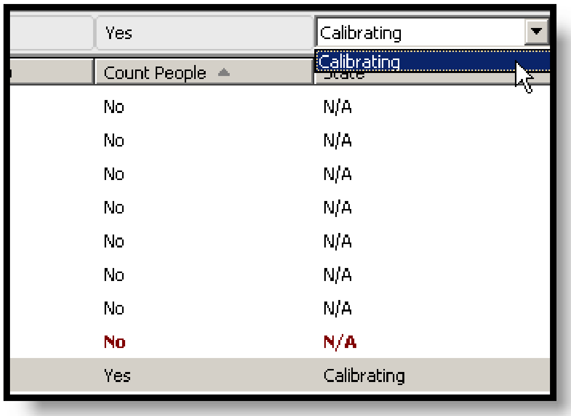
Resetting the People Counting Camera Calibration

If you have adjusted a camera's view, you can reset the camera calibration to obtain an accurate count of people with the adjusted view.

To reset the people counting camera calibration

1. Ensure the **Device Configuration** task type is selected.
2. Click a recorder in the **Device Selector** panel.
3. Click **Cameras**.

   The **Cameras** page appears.
4. In the **Settings** column on the left, click **People Counting**.
5. Click a camera that has people counting enabled.
6. Click the settings bar above the **State** column and click **Calibrating**.



Yes	Calibrating ▼
Count People ▲	**State**
No	N/A
No	N/A
No	N/A
No	N/A
No	N/A
No	N/A
No	N/A
No	N/A
Yes	Calibrating

7. Click **Apply Settings**.

Generating a People Counting Report

The people counting reporting tool is a tool that generates basic reports that show the number of people counted by the recorder over a specified period of time. The tool supports the following browsers:

- Microsoft Internet Explorer® 6 and 7 (latest service pack)
- Latest release of Mozilla® Firefox® (including all service packs)

The reporting interface provides the ability to specify and view reports of the data accumulated through the use of people counting cameras. Data can be gathered from one or multiple cameras configured for people counting. The report data shows counts for entry, exit, and occupancy.

NOTE: An occupancy count is the running difference between the number of people that have entered and exited only during the specified reporting period. The occupancy count does not include entries/exits that occurred outside of the reporting period.

You can generate a people counting report for a specific day, week, or month. The weekly report begins on a Sunday and ends on a Saturday; the monthly report begins on the first day of the month.

To use the people counting reporting tool

If recorder or camera configurations are modified in the Administrator Console while you are working with the people counting reporting tool, you must refresh or restart the Web browser for the changes to take effect.

If you select multiple cameras we recommend that you choose cameras from recorders within the same time zone.

Keep in mind that when multiple cameras are selected, the report shows a total count for all selected cameras.

You cannot specify a daily time range if you are generating a weekly or monthly report. A day within a weekly or monthly report is always 24 hours.

1. Open a Web browser and go to the people counting reporting URL.

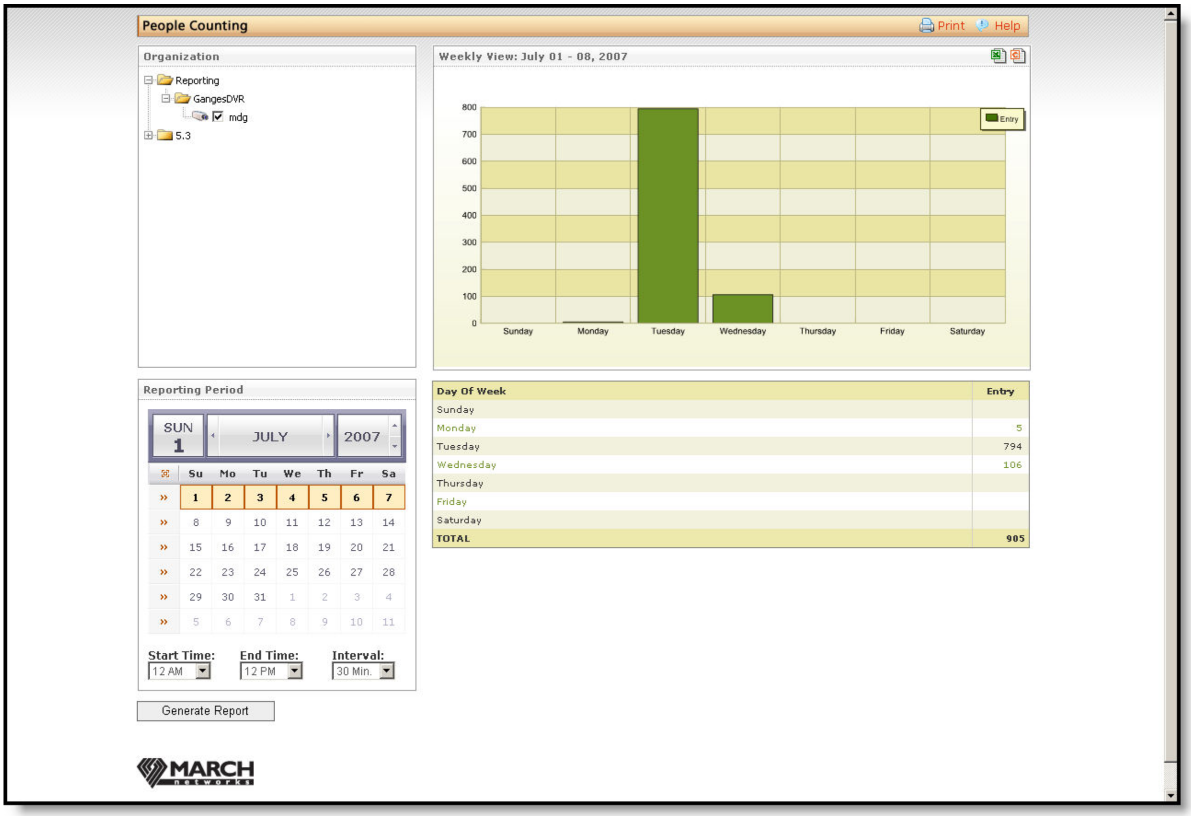
   The people counting reporting URL is configured during installation of the People Counting Reporting Web service. Contact your administrator if you are unsure of the URL.

2. In the **Organization** section of the reporting interface, locate and select the cameras that you want to include in the report.
3. Under **Reporting Period**, select the month and year for the reporting period.
4. Specify the reporting period by doing one of the following:
   - Click the **Month** button, which selects the entire month.
   - Click the **Week** button that corresponds to the week for which you want to specify the reporting period.
   - Click a day in the calendar.

If you click a day in the calendar, click a start time and an end time in the **Start Time** and **End Time** lists.

5. Click **Generate Reports**.

   The report data appears in graphical and tabular format on the right side of the page.



	Su	Mo	Tu	We	Th	Fr	Sa
»	1	2	3	4	5	6	7
»	8	9	10	11	12	13	14
»	15	16	17	18	19	20	21
»	22	23	24	25	26	27	28
»	29	30	31	1	2	3	4
»	5	6	7	8	9	10	11

Start Time: 12 AM
End Time: 12 PM
Interval: 30 Min.

Day Of Week	Entry
Sunday	
Monday	5
Tuesday	794
Wednesday	106
Thursday	
Friday	
Saturday	
TOTAL	905

To filter the report

- With a report open, select the **Entry**, **Exit**, or **Occupancy** check boxes.

  As you select (or clear) each check box, the report is filtered.

To print or export the report

- Click **Print**, **Export to Excel** or **Export to CSV** .

Setting Up March Networks IP Cameras and Encoders for Analytics

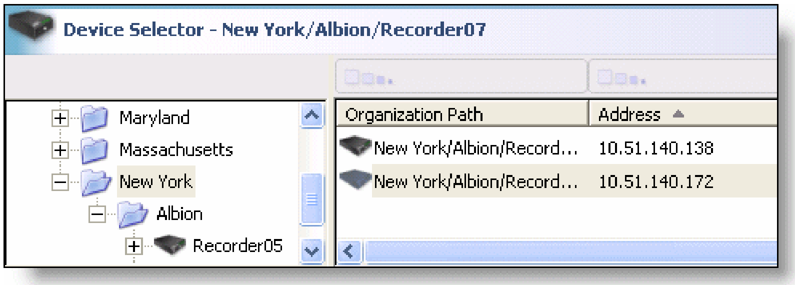
Before you configure the video analytics on March Networks IP cameras or encoders, it is strongly recommended that you perform the setup and perspective tasks, in order for your IP camera or encoder to recognize the major elements in the field of view, and set an accurate perspective.

You can access the IP camera or encoder's Web page to customize the settings for the field of view you are monitoring. The setup is the basic configuration used by all of the video analytics.

You can configure the IP camera or encoder to ignore small objects by setting the Min size parameter in the Setup menu, or you can edit the Luma denoise and Chroma denoise parameters to change the sensitivity levels. For more detailed information about configuring the IP camera or encoder, see the documentation accompanying your IP camera or encoder.

To configure March Networks IP cameras and encoders for video analytics

1. Ensure the **Device Configuration** task type is selected.
2. Click a recorder in the **Device Selector** panel.



Device Selector - New York/Albion/Recorder07

- Maryland
- Massachusetts
- New York
  - Albion
    - Recorder05

Organization Path	Address
New York/Albion/Record...	10.51.140.138
New York/Albion/Record...	10.51.140.172

3. Click **Cameras**.

   The **Cameras** page appears.
4. In the **Settings** column on the left, click **Operation**.
5. Click the IP camera or encoder and then click **Camera Analytics Page**.
6. Type your user name and password to log on to the Web page.
7. On the camera's Web page, click **Senses** (sometimes referred to as **Deepath** on the Web page) and then click **Senses setup**.
8. Configure the IP camera settings outlined in the following table and then click **Save Changes**.

Table 9: March Networks IP Camera and Encoder Settings

Setting	Description
Threshold	Allows the IP camera to distinguish between background color or luminosity and an object of interest that is the same color or luminosity. A positive threshold specifies a fixed difference, and a negative threshold specifies automatic adjustment. Set **-1** for views that do not have strong light variations. Set **-2** (default) for views with strong light variations.
Min. Size	Indicates the smallest size of object that the IP camera should detect. If you have not set the perspective on your IP camera, you can draw the minimum size on the image to represent a portion of the IP camera pixels. After you set the perspective, the IP camera can compensate for objects that are closer to the IP camera and therefore appear larger.
Luma Sensitivity	The minimum amount of brightness for the image.
Chroma Sensitivity	The minimum amount of color depth for the image.
Luma Denoise	The minimum amount of brightness that the IP camera should recognize. The IP camera will “ignore” objects that are below this threshold. This setting helps reduce the effect of signal noise, for example caused by a long coaxial cable. It also defines differences between objects and backgrounds of the same color.
Chroma Denoise	The minimum amount of color fluctuation for the image. The IP camera will ignore color fluctuations or chroma noise below this setting. This setting helps reduce the effect of signal noise, for example caused by a long coaxial cable, and also enhances color contrast.
Scene Cut Percent (%)	The minimum amount of change in the image that must be detected before the IP camera or encoder recalculates the analytics.
Temp. Min. Intensity, Temp. Max. Intensity	These settings are only intended for thermal IP cameras, which are not currently supported. Set to **0**.
Temp. Background	This setting is only intended for thermal IP cameras, which are not currently supported.
Update Frequency (%)	Indicates the number of frames to be used for analysis. A higher value produces a more accurate analysis of the scene. **Note:** Setting an update frequency of 80 percent or higher increases the CPU working load. This setting is useful if your system is heavily loaded and you want to control it.
Backmodel Update	Sets the background image update period in milliseconds. Lower values indicate that the background image will be updated more frequently. **Note:** Frequent updates increase the use of system resources. **Note:** This setting is available only when the threshold is set to **2**.

Setting the Perspective for March Networks IP Cameras or Encoders

Setting the correct perspective on the IP camera or encoder allows it to more easily recognize and process people or objects moving through a field of view. When you configure the perspective, you can use the default size of the average human being or another object, and then specify the sizes of people or objects in other parts of the image for each caliber setting. You must set a minimum of three calibers to configure the perspective. For more information about setting the IP camera perspective, see the documentation accompanying your IP camera or encoder.

To set the perspective for March Networks IP cameras and encoders

1. Ensure the **Device Configuration** task type is selected.
2. Click a recorder in the **Device Selector** panel.
3. Click **Cameras**.

   The **Cameras** page appears.
4. In the **Settings** column on the left, click **Operation**.
5. Click an IP camera or encoder.
6. Click **Camera Analytics Page**.
7. Type your user name and password to log on to the Web page.
8. On the camera's Web page, click **Senses** (sometimes referred to as **Deepath** on the Web page) and then click **Senses setup**.
9. In the list, click **Perspective** and then click **Enabled**.
10. Double-click the **Focal Length** value and type the IP camera's 35 mm equivalent focal length. This measure indicates the angle of view of a particular combination of the lens, the zoom position, and the IP camera sensor.
11. Click a zone and then click **Enabled**.
12. Double-click the **Object Width** value and type a measurement, in centimeters, of the object you want to use as the caliber. The default value is 72 centimeters, which is the width of a typical man.

    The default value should be used unless you are defining the perspective based on objects, such as cars.
13. Double-click the **Object Height** value and type a measurement, in centimeters, of the object you want to use as the caliber. The default value is 180 centimeters, which is the height of a typical man.

    The default value should be used unless you are defining the perspective based on objects, such as cars.
14. Double-click the **Anchor (Horizontal)** value and then click an anchor point. This is the horizontal point of contact between the caliber and the perspective plane. The default value is sufficient for most situations.

15. Double-click the **Anchor (Vertical)** value and then click an anchor point. This is the vertical point of contact between the caliber and the perspective plane. The default value is sufficient for most situations.
16. Double-click the **Caliber 1** value and then click the pencil icon. Draw a box on the video image that corresponds to the size of the person or object in the specific area of the image.

NOTE: Ensure that you place the calibers in different parts of the video image in a triangular pattern. This allows the IP camera to configure the perspective based on the size of the caliber in the background, foreground, and middle of the field of view.

17. Repeat step 16. for at least two more calibers.

NOTE: When you are drawing the calibers in the video image, it is helpful to have a person stand in various parts of the scene so that you can draw more accurate sizes.

18. Click **Save Changes**.

A correct perspective automatically shows the following characteristics:

- White, horizontal lines running the width of the screen. Angled lines indicate that the perspective is inaccurate.
- A blue line appears indicating the horizon of the perspective plane.
- Objects moving horizontally across the screen remain roughly the same size.

Configuring Loitering Detection

March Networks IP cameras and Edge encoders have built-in loitering detection abilities that allow them to detect when an individual remains in an area for longer than the amount of time you specify.

NOTE: For a list of IP cameras and encoders that support this feature, contact your March Networks representative.

When loitering detection is configured and enabled, a loitering alarm is triggered if a person remains in the specified area for longer than the configured time.

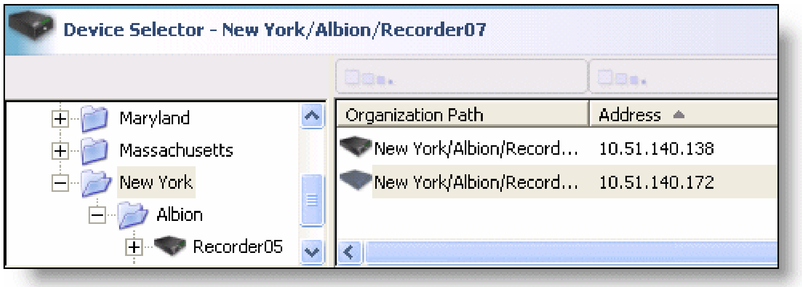
Scenario	You are monitoring an office building lobby.
Problem	In the past, you have had problems with individuals gathering inside the lobby after business hours.
Resolution	On an IP camera that is capturing video from the lobby, enable loitering detection and configure the IP camera to detect when an individual remains in the area for more than five minutes. When an individual loiters in the area for more than five minutes, an alarm is generated and security staff can be notified.

Security staff and investigators can use the Live Monitoring Console to alert them of alarms in real-time, or they can use the Investigator to review alarms that have already occurred.

NOTE: Before you configure this feature, ensure the IP camera or encoder that you are monitoring is set up to maximize the loitering detection feature. For more information, see the Video Analytics Reference Guide, included on your March Networks CD.

To enable and configure loitering detection

1. Ensure the **Device Configuration** task type is selected.
2. Click a recorder in the **Device Selector** panel.



Device Selector - New York/Albion/Recorder07

Organization Path	Address
New York/Albion/Record...	10.51.140.138
New York/Albion/Record...	10.51.140.172

3. Click **Cameras**.

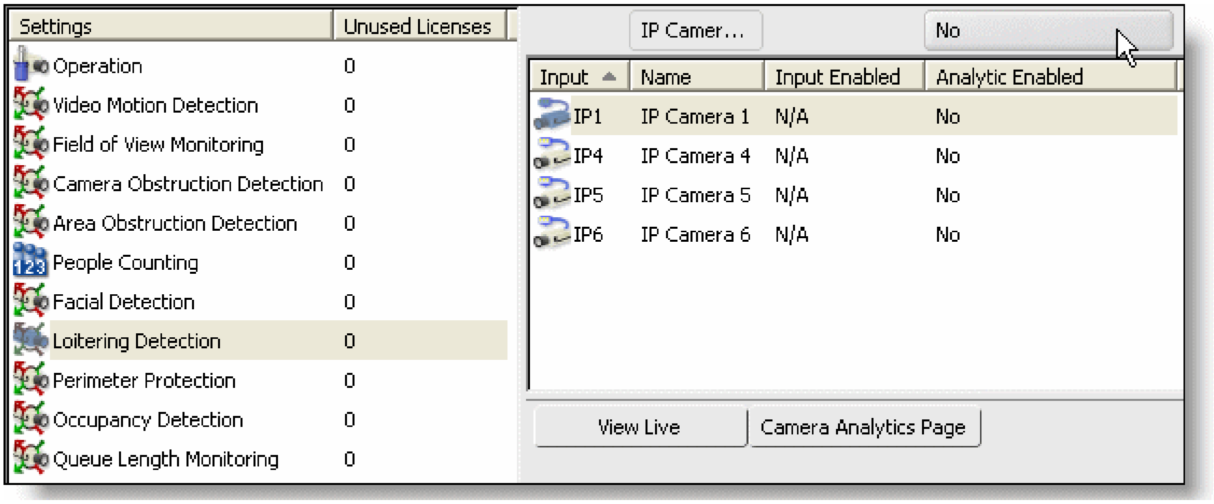
 The **Cameras** page appears.

4. In the **Settings** column on the left, click **Loitering Detection**.
5. Click an IP camera or encoder.

NOTE: Only IP cameras that support this feature appear. For a list of supported IP cameras, contact your March Networks representative.

6. Click the settings bar above the **Analytic Enabled** column and click **Yes**.
7. Click **Apply Settings**.

 Please note that when you enable the analytic, you are enabling the recorder to receive analytic details from the IP camera or encoder. You must also enable and configure the analytic on the IP camera or encoder, as outlined in the remaining steps.



Settings	Unused Licenses
Operation	0
Video Motion Detection	0
Field of View Monitoring	0
Camera Obstruction Detection	0
Area Obstruction Detection	0
People Counting	0
Facial Detection	0
Loitering Detection	0
Perimeter Protection	0
Occupancy Detection	0
Queue Length Monitoring	0

Input	Name	Input Enabled	Analytic Enabled
	IP Camer...		No
IP1	IP Camera 1	N/A	No
IP4	IP Camera 4	N/A	No
IP5	IP Camera 5	N/A	No
IP6	IP Camera 6	N/A	No

8. Click **Camera Analytics Page**.
9. Type your user name and password to log on to the Web page.
10. Using the Web page, perform the following steps to configure the Loitering Alarm settings:
    - If you have not yet done so, install the license on the IP camera or encoder.
    - You may want to clear the setup settings to reset the video analytic features to default settings.

NOTE: If you have already configured other video analytic features, you may decide not to clear the setup settings. If you clear the settings you must reconfigure all of the IP camera or encoder video analytic features.

- Under **Senses setup** (sometimes referred to as **Deepath** on the Web page), enable the **Loitering Alarm** feature. **Senses setup** is only available when an analytic license is installed on the IP camera or encoder.

NOTE: Enabled alarms appear in bold. Selecting an enabled alarm and then clicking **Enabled** will disable the alarm.

- Create and enable an area to monitor, also referred to as a zone. Click **Edit** and then use your mouse in the live image to draw a box around the area you want to monitor.
- Click **Save Changes**.
- Beside **Max Permanence**, double-click the default value and type, in seconds, the amount of time an individual must remain in the area before a loitering alarm is generated.

NOTE: The amount of time you specify applies to a single individual, not a group of individuals.
For example, a person is in an office building lobby for three minutes and is then joined by some friends. After one minute the first person leaves. The friends remain for three minutes and then leave. Because no single person remained in the area for five minutes (which is the configured time period in this example), a loitering alarm was not generated.

- Under **Alarms**, enable the **Loitering Alarm** on the source that is configured for Loitering Alarms and then click **Submit**. Please note, this step is only required when you are working with an Edge 4 Encoder or a CamPX Dome IP camera.

Configuring Occupancy Detection

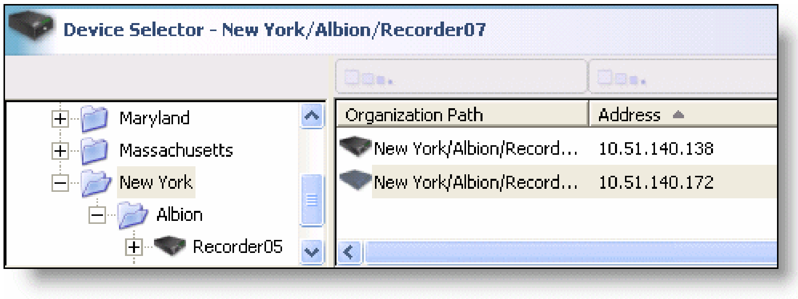
March Networks IP cameras and encoders have built-in occupancy detection abilities that let them detect when the number of people in a scene equals or exceeds a specified amount.

Occupancy detection follows the movement of people or vehicles and stores the information in a real-time database. This information can be used to develop an understanding of activities in the field of view, or to raise an occupancy detection alarm when a person or vehicle moves from one specified zone to another.

Before you configure this feature, ensure the IP camera or encoder that you are monitoring is set up to maximize the occupancy detection feature. For more information, see the *Video Analytics Reference Guide*, included on your March Networks CD.

To enable and configure occupancy detection

1. Ensure the **Device Configuration** task type is selected.
2. Click a recorder in the **Device Selector** panel.



Device Selector - New York/Albion/Recorder07

- Maryland
- Massachusetts
- New York
  - Albion
    - Recorder05

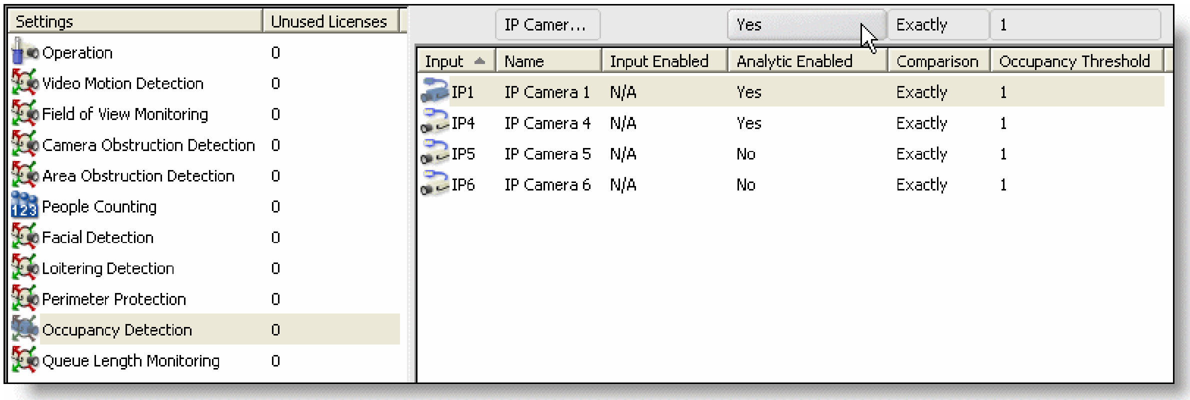
Organization Path	Address
New York/Albion/Record...	10.51.140.138
New York/Albion/Record...	10.51.140.172

3. Click **Cameras**.

   The **Cameras** page appears.
4. In the **Settings** column on the left, click **Occupancy Detection.**
5. Click an IP camera or encoder.

   Only IP cameras and encoders that support this feature appear. For a list of supported IP cameras, contact your March Networks representative.
6. Click the settings bar above the **Analytic Enabled** column and click **Yes**.
7. Click **Apply Settings**.

   Please note that when you enable the analytic, you are enabling the recorder to receive analytic details from the IP camera or encoder. You must also enable and configure the analytic on the IP camera or encoder, as outlined in the remaining steps.



Settings	Unused Licenses
Operation	0
Video Motion Detection	0
Field of View Monitoring	0
Camera Obstruction Detection	0
Area Obstruction Detection	0
People Counting	0
Facial Detection	0
Loitering Detection	0
Perimeter Protection	0
Occupancy Detection	0
Queue Length Monitoring	0

Input	Name	Input Enabled	Analytic Enabled	Comparison	Occupancy Threshold
	IP Camer...		Yes	Exactly	1
IP1	IP Camera 1	N/A	Yes	Exactly	1
IP4	IP Camera 4	N/A	Yes	Exactly	1
IP5	IP Camera 5	N/A	No	Exactly	1
IP6	IP Camera 6	N/A	No	Exactly	1

8. Click the settings bar above the **Comparison** column and click either **Exactly** or **More than**. This setting defines the occupancy threshold.
9. Click the settings bar above the **Occupancy Threshold** column and click a threshold number.
10. Click **Apply Settings**.
11. Click **Camera Analytics Page**.
12. Type your user name and password to log on to the Web page.

    The configuration Web page appears. If the Web page is not available, verify that you have used the correct user name and password, and verify that the IP camera or encoder is online and accessible.
13. Using the Web page, perform the following steps to configure the **Occupancy Detection** settings:
    - If you have not yet done so, install the license on the IP camera or encoder.
    - You can clear the setup settings to reset the video analytic features to default settings.

NOTE: If you have already configured other video analytic features, you may decide not to clear the setup settings. If you clear the settings you must reconfigure all of the IP camera or encoder video analytic features.

- Under **Senses setup** (sometimes referred to as **Deepath** on the Web page), enable the **Tracking Alarm** feature (which is referred to as Occupancy Detection in this publication and the Administrator Console). **Senses setup** is only available when an analytic license is installed on the IP camera or encoder.

NOTE: Enabled alarms appear in bold. Selecting an enabled alarm and then clicking **Enabled** will disable the alarm.

- Double-click the **Min Life (ms)** value and type the minimum time duration, in milliseconds, that an object must be moving before an alarm is triggered.
- Double-click the **Min Distance** value and type the minimum distance that an object must move before an alarm is triggered. This distance is measured in pixels.
- Double-click the **Human/Vehicle** value and select or clear the check box to indicate whether you want the alarm to detect humans and vehicles in the field of view.
- Create and enable an area to monitor, also referred to as a zone. Click **Edit** and then use your mouse in the live image to draw a box around the area you want to monitor.

NOTE: You can create an irregularly shaped zone by drawing different sized rectangles to fill your selected area. Click **Show** to view the zone you created.

- Click **Save Changes**.

- Double-click the **Source** value and then click the zone of origin for people or objects. People or objects that move out of this specified source zone will trigger the occupancy detection alarm.
- Double-click the **Min Time [ms]** value and then click the least amount of time, in milliseconds, that a person or object must be moving while outside of the source zone before an alarm is triggered. Movements that last for less than the specified duration do not trigger an alarm.

  This setting is required only if you are configuring an alarm for people or objects moving between zones.
- Double-click the **Max time [ms]** value and then click the most amount of time that a movement must occur outside of the source zone before an alarm is triggered. Movements that last for longer than the specified duration do not trigger an alarm.

  This setting is required only if you are configuring an alarm for people or objects moving between zones.
- Double-click the **Trigger** value and select the check box to trigger an alarm if the person or object moves between the two zones.
- Double-click the **Alarm on Human** value and select the check box if you want to trigger an occupancy detection alarm for human movement.
- Double-click the **Alarm on Vehicle** value and select the check box if you want to trigger an occupancy detection alarm for the movement of a vehicle.
- Click **Save Changes**.
- Under **Alarms**, enable the **Tracking Alarm** on the source that is configured for occupancy detection alarms and then click **Submit**. Please note, this step is only required when you are working with an Edge 4 Encoder or a CamPX Dome IP camera.

Configuring Perimeter Protection

March Networks IP cameras and encoders have built-in perimeter protection abilities that allow them to detect when an individual or object crosses a certain point in the IP camera’s field of view.

Scenario	You are monitoring an airport security area.
Problem	You want to keep track of individuals exiting the security area through the entry door; you are not interested in individuals exiting the security area through the exit.
Resolution	On an IP camera that is capturing video from the security area, enable perimeter protection. Specify the line that the individual must cross and the direction they must be walking to exit the area. When an individual crosses the line and is walking in the direction you specify, an alarm is generated and security staff can be notified.

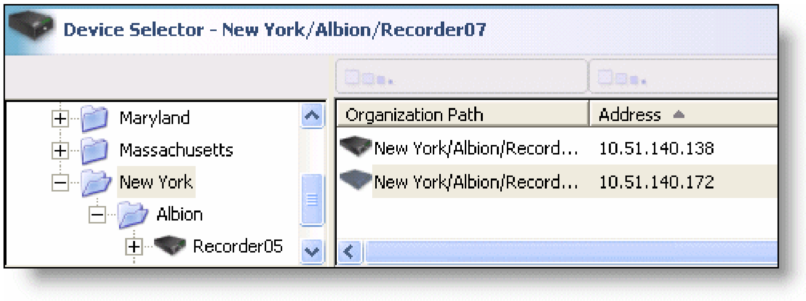
Optionally, you can specify that you only want to detect when an individual crosses the line and is moving in the direction you specify.

After this feature is enabled and configured, security staff and investigators can use the Live Monitoring Console to alert them of alarms in real-time, or they can use the Investigator to review alarms that have already occurred.

Before you configure this feature, ensure the IP camera or encoder that you are monitoring is set up to maximize the perimeter protection feature. For more information, see the *Video Analytics Reference Guide*, included on your March Networks CD.

To enable and configure perimeter protection

1. Ensure the **Device Configuration** task type is selected.
2. Click a recorder in the **Device Selector** panel.



Device Selector - New York/Albion/Recorder07

Maryland
Massachusetts
New York
Albion
Recorder05

Organization Path	Address
New York/Albion/Record...	10.51.140.138
New York/Albion/Record...	10.51.140.172

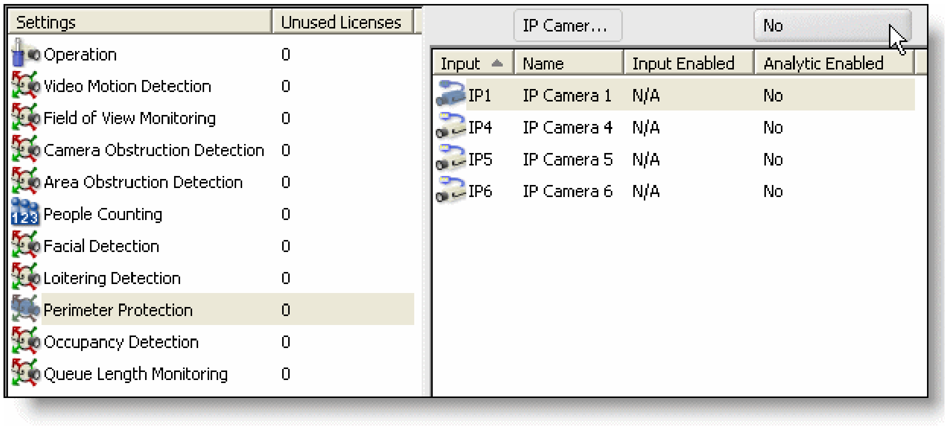
3. Click **Cameras**.

   The **Cameras** page appears.
4. In the **Settings** column on the left, click **Perimeter Protection**.
5. Click an IP camera or encoder.

NOTE: Only IP cameras that support this feature appear. For a list of supported cameras, contact your March Networks representative.

6. Click the settings bar above the **Analytic Enabled** column and click **Yes**.
7. Click **Apply Settings**.

   Please note that when you enable the analytic, you are enabling the recorder to receive analytic details from the IP camera or encoder. You must also enable and configure the analytic on the IP camera or encoder, as outlined in the remaining steps.



Settings	Unused Licenses
Operation	0
Video Motion Detection	0
Field of View Monitoring	0
Camera Obstruction Detection	0
Area Obstruction Detection	0
People Counting	0
Facial Detection	0
Loitering Detection	0
Perimeter Protection	0
Occupancy Detection	0
Queue Length Monitoring	0

IP Camer... No

Input	Name	Input Enabled	Analytic Enabled
IP1	IP Camera 1	N/A	No
IP4	IP Camera 4	N/A	No
IP5	IP Camera 5	N/A	No
IP6	IP Camera 6	N/A	No

8. Click **Camera Analytics Page**.
9. Type your user name and password to log on to the Web page.

   The configuration Web page appears. If the Web page is not available, verify that you have used the correct user name and password, and verify that the IP camera or encoder is online and accessible.
10. Using the Web page, perform the following steps to configure the **Perimeter Protection** settings:
    - If you have not yet done so, install the license on the IP camera or encoder.
    - You may want to clear the setup settings to reset the video analytic features to default settings.

NOTE: If you have already configured other video analytic features, you may decide not to clear the setup settings. If you clear the settings you must reconfigure all of the IP camera or encoder video analytic features.

- Under **Senses setup** (sometimes referred to as **Deepath** on the Web page), enable the **Wire Cross Alarm** feature (which is referred to as Perimeter Protection in this publication and the Administrator Console). **Senses setup** is only available when an analytic license is installed on the IP camera or encoder.
  You can create an irregularly shaped zone by repeatedly drawing different sized rectangles to fill your selected area. Click Show to view the zone you created.

NOTE: Enabled alarms appear in bold. Selecting an enabled alarm and then clicking Enabled will disable the alarm.

- Click **Save Changes**.
- Create and enable an area to monitor, also referred to as a zone.
- Beside **Wire**, double-click the entry in the **Value** column. Click the icon that appears beside the entry.

- Using your mouse, draw a box on the live image to indicate the start and end point of the perimeter wire (the start and end points of the box will be start and end points of the perimeter wire).
- You can indicate the direction that the individual must be traveling for a perimeter protection alarm to be generated. Beside **Direction**, double-click the entry in the **Value** column and then choose either **1** or **-1** (leaving the entry at **0** indicates that perimeter protection alarms are always generated, regardless of the direction).
- Click **Save Changes**.
- Under **Alarms**, enable **Perimeter Protection** on the source that is configured for Perimeter Protection and then click **Submit**. Please note, this step is only required when you are working with an Edge 4 Encoder or a CamPX Dome IP camera.

Configuring Queue Length Monitoring

March Networks IP cameras and encoders have built-in queue length monitoring abilities that allow them to detect when the number of people in a waiting area exceeds a specified capacity.

Scenario	You are monitoring an airport check-in area.
Problem	You want to know when the number of travellers waiting to check in for their flights exceeds a certain level so that more kiosks can be opened.
Resolution	On an IP camera that is capturing video from the security area, enable queue length monitoring. Specify the size of the waiting area and the percentage of the area that must be filled with waiting people before an alarm is triggered.

For a list of IP cameras and encoders that support this feature, contact your March Networks representative.

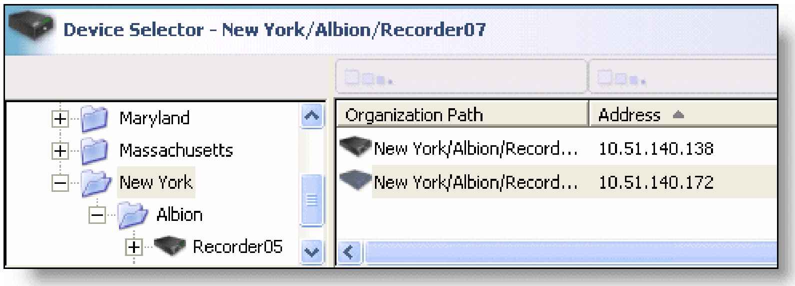
After this feature is enabled and configured, security staff and investigators can use the Live Monitoring Console to alert them to changes in the waiting area capacity, or they can use the Investigator to review alarms that have already occurred.

Before you configure this feature, ensure the IP camera or encoder that you are monitoring is set up to maximize the queue length monitoring feature. For more information, see the *Video Analytics Reference Guide*, included on your March Networks CD.

To enable and configure queue length monitoring

1. Ensure the **Device Configuration** task type is selected.

2. Click a recorder in the **Device Selector** panel.



Device Selector - New York/Albion/Recorder07

- Maryland
- Massachusetts
- New York
  - Albion
    - Recorder05

Organization Path	Address ▲
New York/Albion/Record...	10.51.140.138
New York/Albion/Record...	10.51.140.172

3. Click **Cameras**.

   The **Cameras** page appears.

4. In the **Settings** column on the left, click **Queue Length Monitoring**.

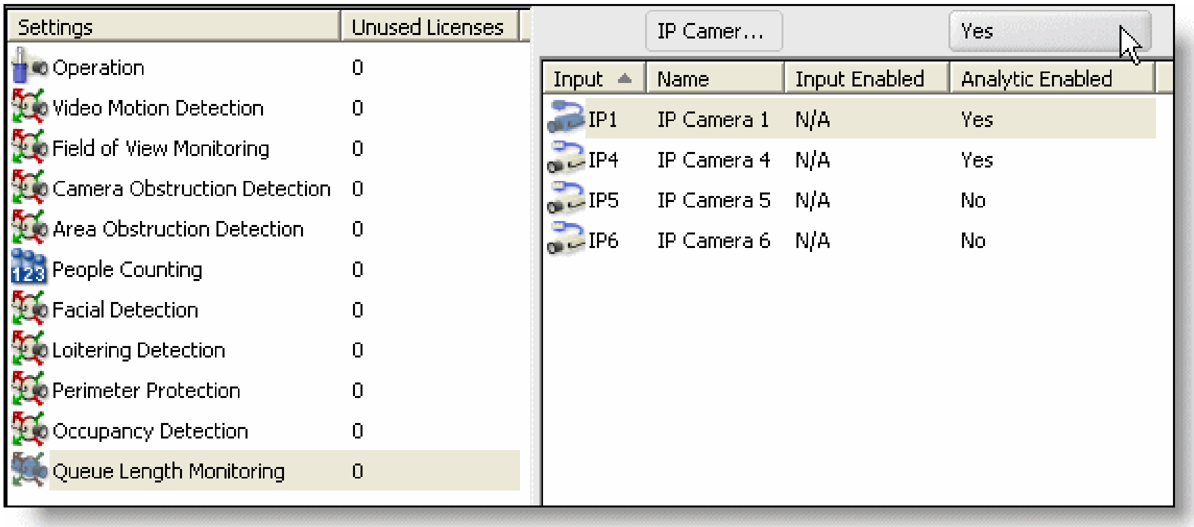
5. Click an IP camera or encoder.

NOTE: Only IP cameras that support this feature appear. For a list of supported IP cameras, contact your March Networks representative.

6. Click the settings bar above the **Analytic Enabled** column and click **Yes**.

7. Click **Apply Settings**.

   Please note that when you enable the analytic, you are enabling the recorder to receive analytic details from the IP camera or encoder. You must also enable and configure the analytic on the IP camera or encoder, as outlined in the remaining steps.



Settings	Unused Licenses
Operation	0
Video Motion Detection	0
Field of View Monitoring	0
Camera Obstruction Detection	0
Area Obstruction Detection	0
People Counting	0
Facial Detection	0
Loitering Detection	0
Perimeter Protection	0
Occupancy Detection	0
Queue Length Monitoring	0

Input ▲	Name	Input Enabled	Analytic Enabled
IP1	IP Camera 1	N/A	Yes
IP4	IP Camera 4	N/A	Yes
IP5	IP Camera 5	N/A	No
IP6	IP Camera 6	N/A	No

8. Click **Camera Analytics Page**.

9. Type your user name and password to log on to the Web page.

The configuration Web page appears. If the Web page is not available, verify that you have used the correct user name and password, and verify that the IP camera or encoder is online and accessible.

10. Using the Web page, perform the following steps to configure the **Queue Length Monitoring** settings:
    - If you have not yet done so, install the license on the IP camera or encoder.
    - You may want to clear the setup settings to reset the video analytic features to default settings.

NOTE: If you have already configured other video analytic features, you may decide not to clear the setup settings. If you clear the settings you must reconfigure all of the IP camera or encoder video analytic features.

- Under **Senses setup** (sometimes referred to as **Deepath** on the Web page), enable the **Queue Alarm** feature (which is referred to as Queue Length Monitoring in this publication and the Administrator Console). **Senses setup** is only available when an analytic license is installed on the IP camera or encoder.

NOTE: Enabled alarms appear in bold. Selecting an enabled alarm and then clicking **Enabled** will disable the alarm.

- Create and enable an area to monitor, also referred to as a zone. Click **Edit** and then use your mouse in the live image to draw a box around the area you want to monitor. You can create an irregularly shaped zone by repeatedly drawing different sized rectangles to fill your selected area. Click **Show** to view the zone you created.
- Click **Save Changes**.
- Double-click the **Trigger Threshold** value and type the minimum amount of time, in seconds, that you want the queue to exist before the alarm is triggered.
- Double-click the **Area Threshold [%]** value and type the percentage of the area that must be occupied before the queue alarm is triggered.
- Click **Save Changes**.
- Under **Alarms**, enable **Queue Length Monitoring** on the source that is configured for Queue Length Monitoring and then click **Submit**. Please note, this step is only required when you are working with an Edge 4 Encoder or a CamPX Dome IP camera.

Configuring Facial Detection

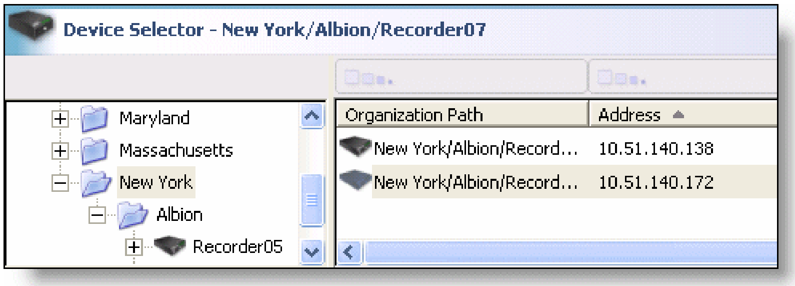
March Networks IP cameras and encoders have built-in facial detection abilities that allow them to detect faces. The IP camera is configured to generate an alarm when a clear image of a face is captured. The facial image generates a face alarm which then triggers the door to unlock.

Scenario	You are monitoring a bank vault.
Problem	You want to ensure that people entering the vault clearly show their faces to the camera.
Resolution	On an IP camera that is capturing video at the bank entrance, enable facial detection and configure the IP camera to only generate an alarm when a clear face is detected and the person's credentials are verified.

Before you configure this feature, ensure the IP camera or encoder that you are monitoring is set up to maximize the facial detection feature. For more information, see the *Video Analytics Reference Guide*, included on your March Networks CD.

To enable and configure facial detection

1. Ensure the **Device Configuration** task type is selected.
2. Click a recorder in the **Device Selector** panel.



Device Selector - New York/Albion/Recorder07

Organization Path	Address
New York/Albion/Record...	10.51.140.138
New York/Albion/Record...	10.51.140.172

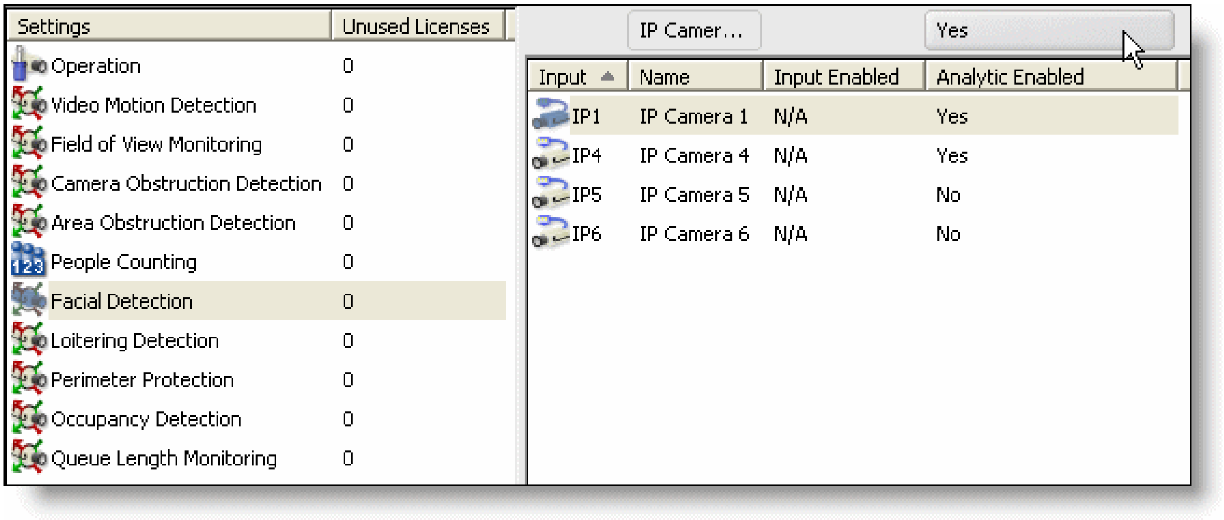
3. Click **Cameras**.

   The **Cameras** page appears.
4. In the **Settings** column on the left, click **Facial Detection**.
5. Click an IP camera or encoder.

NOTE: Only IP cameras that support this feature appear. For a list of supported IP cameras, contact your March Networks representative.

6. Click the settings bar above the **Analytic Enabled** column and click **Yes**.
7. Click **Apply Settings**.

   Please note that when you enable the analytic, you are enabling the recorder to receive analytic details from the IP camera or encoder. You must also enable and configure the analytic on the IP camera or encoder, as outlined in the remaining steps.



Settings	Unused Licenses
Operation	0
Video Motion Detection	0
Field of View Monitoring	0
Camera Obstruction Detection	0
Area Obstruction Detection	0
People Counting	0
Facial Detection	0
Loitering Detection	0
Perimeter Protection	0
Occupancy Detection	0
Queue Length Monitoring	0

Input	Name	Input Enabled	Analytic Enabled
IP1	IP Camera 1	N/A	Yes
IP4	IP Camera 4	N/A	Yes
IP5	IP Camera 5	N/A	No
IP6	IP Camera 6	N/A	No

8. Click **Camera Analytics Page.**
9. Type your user name and password to log on to the Web page.

   The configuration Web page appears. If the Web page is not available, verify that you have used the correct user name and password, and verify that the IP camera or encoder is online and accessible.
10. Using the Web page, perform the following steps to configure the **Facial Detection** settings:
    - If you have not yet done so, install the license on the IP camera or encoder.
    - You may want to clear the setup settings to reset the video analytic features to default settings.

NOTE: If you have already configured other video analytic features, you may decide not to clear the setup settings. If you clear the settings you must reconfigure all of the IP camera or encoder video analytic features.

- Under **Senses setup** (sometimes referred to as **Deepath** on the Web page), enable the **Face Alarm** feature (which is also referred to as **Facial Detection** in this publication and the Administrator Console. **Senses setup** is only available when an analytic license is installed on the IP camera or encoder.

NOTE: Enabled alarms appear in bold. Selecting an enabled alarm and then clicking **Enabled** will disable the alarm.

- Double-click the **Frames Per Second (FPS)** value and type the capture rate.
- Double-click the value for **Min Size** and then click the pencil icon.
- On the live image, use your mouse to draw the minimum size of a detectable face, from eyebrows to chin. Faces smaller than this size will be ignored.
- Double click the value for **Max Size** and then click the pencil icon.

- Click and drag in the video image to draw the maximum size of a detectable face, from eyebrows to chin. Faces larger than this size will be ignored.
- Double-click the **Confidence** [%] value and set a margin of error for detectable faces.
- Double-click the **Trigger Threshold** [**ms**] value and set a minimum trigger threshold time.
- Click **Save Changes**.
- Under **Alarms**, enable **Facial Detection** on the source that is configured for Facial Detection and then click **Submit**. Please note, this step is only required when you are working with an Edge 4 Encoder or a CamPX Dome IP camera.

Configuring Audio

Recorders can retain and stream audio captured by connected audio inputs and outputs, such as microphones and intercoms.

By default, the recorder is preconfigured with settings that are appropriate for most environments. You can adjust these settings to meet your audio capture, recording, and streaming requirements.

You can test audio configurations using the Installer Console or by switching to the Device Installation task type. For information about testing audio inputs or outputs, see the *Installing a Recorder and Testing Peripheral Connections Quick Steps* publication included on your March Networks CD.

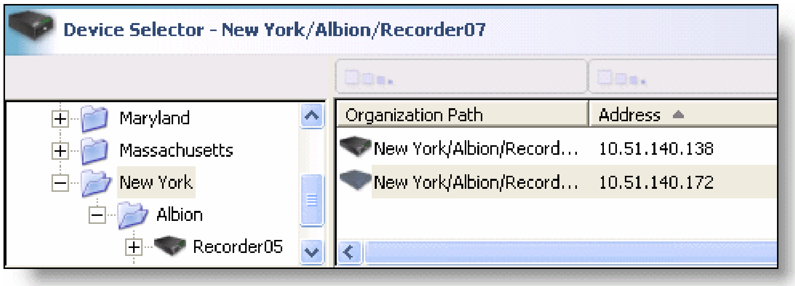
The following topics are covered in this chapter:

Customizing Audio Settings

The following procedure describes how to customize the audio settings of your recorder.

To customize audio settings

1. Ensure the **Device Configuration** task type is selected.
2. Click a recorder in the **Device Selector** panel.



Device Selector - New York/Albion/Recorder07

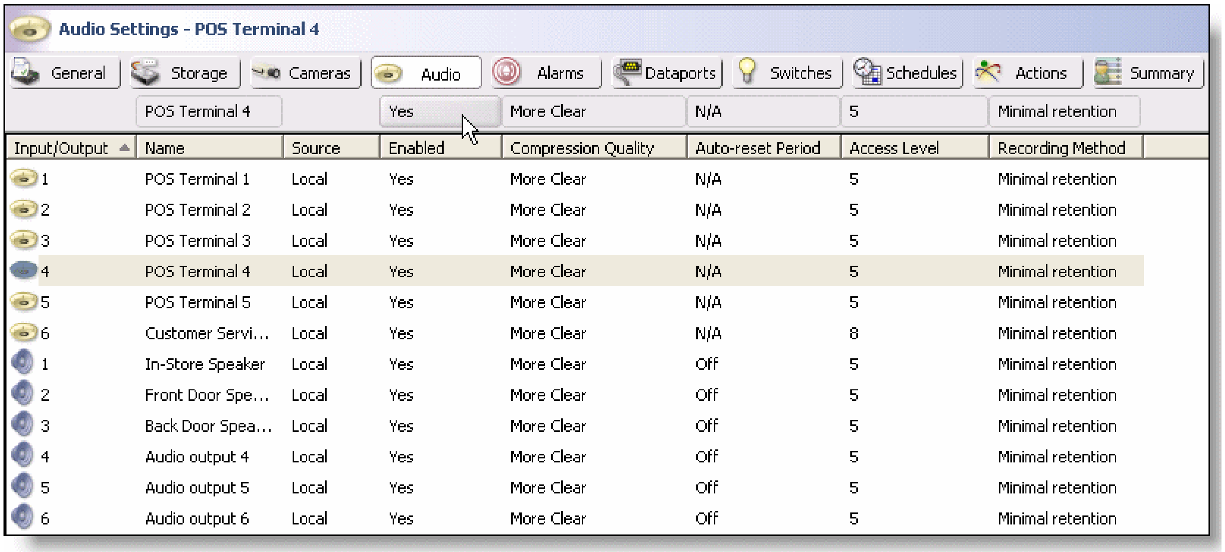
- Maryland
- Massachusetts
- New York
  - Albion
    - Recorder05

Organization Path	Address
New York/Albion/Record...	10.51.140.138
New York/Albion/Record...	10.51.140.172

3. Click **Audio**.

   The **Audio** page appears.
4. Click an audio input or output and customize the settings outlined in the following section ("Recorder Audio Settings").

   If you change one or more settings, you can click **Apply Settings** to save the change, or **Cancel Settings** to discard the change.



Audio Settings - POS Terminal 4

Input/Output	Name	Source	Enabled	Compression Quality	Auto-reset Period	Access Level	Recording Method
	POS Terminal 4		Yes	More Clear	N/A	5	Minimal retention
1	POS Terminal 1	Local	Yes	More Clear	N/A	5	Minimal retention
2	POS Terminal 2	Local	Yes	More Clear	N/A	5	Minimal retention
3	POS Terminal 3	Local	Yes	More Clear	N/A	5	Minimal retention
4	POS Terminal 4	Local	Yes	More Clear	N/A	5	Minimal retention
5	POS Terminal 5	Local	Yes	More Clear	N/A	5	Minimal retention
6	Customer Servi...	Local	Yes	More Clear	N/A	8	Minimal retention
1	In-Store Speaker	Local	Yes	More Clear	Off	5	Minimal retention
2	Front Door Spe...	Local	Yes	More Clear	Off	5	Minimal retention
3	Back Door Spea...	Local	Yes	More Clear	Off	5	Minimal retention
4	Audio output 4	Local	Yes	More Clear	Off	5	Minimal retention
5	Audio output 5	Local	Yes	More Clear	Off	5	Minimal retention
6	Audio output 6	Local	Yes	More Clear	Off	5	Minimal retention

Recorder Audio Settings

The following table describes the audio settings for the recorder.

Audio Setting	Description
Name	The name that identifies the audio input or output. This name helps you identify the peripheral.
Enabled	Specifies whether the peripheral is enabled. When it is enabled, you can configure its settings and access live audio; audio is not captured, recorded, or streamed when the peripheral is disabled.
Compression Quality	The audio quality, such as **Most Clear**, **More Clear**, **More Compressed**, or **Most Compressed**. **Important:** Clearer audio requires more storage space than more compressed audio. The option you choose also impacts how much network bandwidth the recorder uses when streaming audio. **Notes:** • If you are configuring an IP audio input, the available **Compression Quality** options may vary depending on the IP camera model. For information about audio compression, see the documentation accompanying the IP camera. • When the recorder is streaming live audio and video over a low bandwidth network connection, audio may be delivered before video.
Auto-reset Period	The duration after which you want control of an audio output, such as an intercom, to timeout. For example, if you specify five minutes, and an individual has been using the Talk feature in the Investigator for more than five minutes, the peripheral automatically turns off.
Access Level	The authorization level a user must have to access the audio device using the March Networks software applications, such as the Investigator. Users can access peripherals with an equivalent or lower access level than what is set in their profile. For example, a user with an access level of five can access peripherals set to five or lower. For information about specifying a user's access level, see "Creating User Profiles and Accounts" on page 188. **Note:** If you are not working with an ESM, you do not need to specify an access level. However, if you plan to install an ESM in the future, we recommend you set the access level as each recorder is installed at your site. **Tip:** You can create a covert, or hidden, microphone by assigning it an access level that is higher than the user access levels.
Recording Method	The audio retention method. Choose one of the following options: • **Minimal retention.** Audio is retained for the number of minutes specified on the **General** page. After the number of minutes has passed, the recorded audio is deleted. For more information, see "Configuring and Reviewing Evidence Retention" on page 40. • **Full CRB retention.** Audio is always being retained. **Note:** When the CRB is disabled, **Minimal retention** appears. When a retention action is configured, the recording method changes to either **Long Term** or **Extended Term**. For information about configuring actions, see "Configuring Actions" on page 129.

Chapter 10

Configuring Alarms

The recorder communicates with connected alarms, such as door contacts, to detect when the alarm is activated.

In order for the Administrator Console to properly detect the three alarm states (closed, open, and cut), you must install a 200 ohm end of line (EOL) resistor at the alarm (in parallel with the alarm).

In addition to detecting alarms that are physically connected to the unit, you can configure the recorder to receive alarms from third-party applications over the network instead of routing the alarms through a physical connection. These alarms are referred to as virtual network alarm inputs.

The following topics are covered in this chapter:

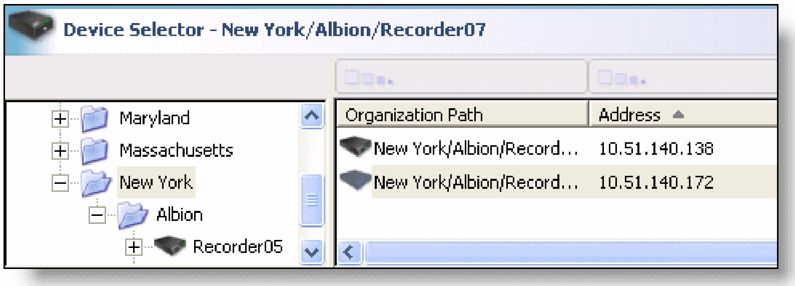
- “Enabling and Configuring Alarms” on page 112
- “Adding Virtual Network Alarm Inputs” on page 114
- “Additional Alarm Configuration Options” on page 115

Enabling and Configuring Alarms

Configure the alarm by enabling it, providing it with a custom name, and specifying other alarm settings.

To customize alarm settings

1. Ensure the **Device Configuration** task type is selected.
2. Click a recorder in the **Device Selector** panel.



Device Selector - New York/Albion/Recorder07

- Maryland
- Massachusetts
- New York
  - Albion
    - Recorder05

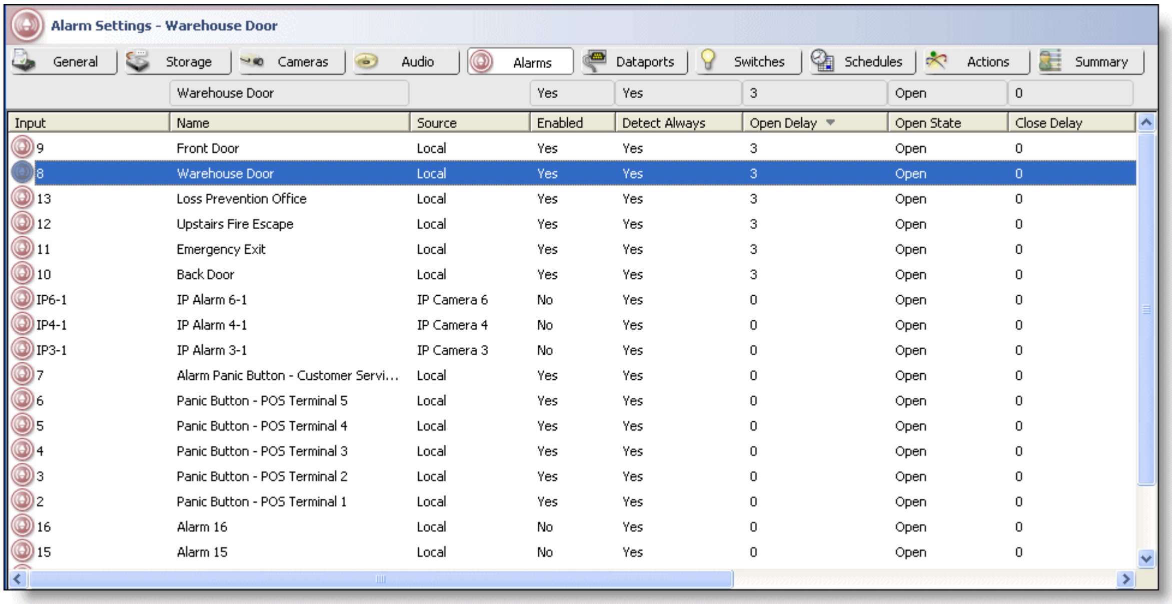
Organization Path	Address
New York/Albion/Record...	10.51.140.138
New York/Albion/Record...	10.51.140.172

3. Click **Alarms**.

   The **Alarm** page appears.

4. Click an alarm and customize the settings outlined in the following table.

   If you change one or more settings, you can click **Apply Settings** to save the change, or **Cancel Settings** to discard the change.



Alarm Settings - Warehouse Door

	Warehouse Door		Yes	Yes	3	Open	0

Input	Name	Source	Enabled	Detect Always	Open Delay	Open State	Close Delay
9	Front Door	Local	Yes	Yes	3	Open	0
8	Warehouse Door	Local	Yes	Yes	3	Open	0
13	Loss Prevention Office	Local	Yes	Yes	3	Open	0
12	Upstairs Fire Escape	Local	Yes	Yes	3	Open	0
11	Emergency Exit	Local	Yes	Yes	3	Open	0
10	Back Door	Local	Yes	Yes	3	Open	0
IP6-1	IP Alarm 6-1	IP Camera 6	No	Yes	0	Open	0
IP4-1	IP Alarm 4-1	IP Camera 4	No	Yes	0	Open	0
IP3-1	IP Alarm 3-1	IP Camera 3	No	Yes	0	Open	0
7	Alarm Panic Button - Customer Servi...	Local	Yes	Yes	0	Open	0
6	Panic Button - POS Terminal 5	Local	Yes	Yes	0	Open	0
5	Panic Button - POS Terminal 4	Local	Yes	Yes	0	Open	0
4	Panic Button - POS Terminal 3	Local	Yes	Yes	0	Open	0
3	Panic Button - POS Terminal 2	Local	Yes	Yes	0	Open	0
2	Panic Button - POS Terminal 1	Local	Yes	Yes	0	Open	0
16	Alarm 16	Local	No	Yes	0	Open	0
15	Alarm 15	Local	No	Yes	0	Open	0

Alarm Setting	Description
Name	The name that identifies the alarm. This name helps administrators identify the alarm.
Enabled	Indicates that the alarm is enabled and the recorder can detect alarms. **Note:** If you disable an alarm and remove the Alarm Option Kit from the recorder, you must reboot the recorder and then handle the Missing Hardware alert that appears. After you complete this step, the alarm is removed from the Administrator Console. For more information, see “Rebooting a Recorder” on page 179 or “Monitoring Health” on page 159.
Detect Always	Enables the recorder to continuously monitor the alarm and detect when it is triggered.
Open Delay	The amount of time the alarm remains in the open state before it is flagged as an alarm event. For example, if you are monitoring a door, you can set the recorder to notify you of an alarm event when the door is open for 60 seconds or more.
Open State	The descriptive name of the open state. This name appears in the Investigator searches to help users identify the alarm state.
Close Delay	The amount of time the alarm must be in the closed state before it is flagged as an event.
Closed State	The descriptive name of the closed state. This name appears in the Investigator searches to help users identify the alarm state.
Primary Camera	The name of the camera that is linked to the alarm. When a camera is linked, investigators can automatically review video associated to alarm events.
Group Tag	The name for one or more alarms, which helps investigators quickly find evidence for a specific scenario. For example, if investigators at your organization typically monitor alarms A, B, and C when investigating activity at the front, back, and side entrances of your building, specify “Doors” as the group tag for alarms A, B, and C. When users open the Investigator, the alarms automatically appear in a group labeled “Doors,” providing them with quick access to alarms A, B, and C. **Tip:** To specify multiple groups, separate group names using a comma (,) or a semicolon (;).
Access Level	The authorization level a user must have to access the alarm using the March Networks software applications, such as the Investigator. Users can access peripherals with an equivalent or lower access level than what is set in their profile. For example, a user with an access level of five can access peripherals set to five or lower. For information about specifying a user’s access level, see “Creating User Profiles and Accounts” on page 188. **Note:** If you are not working with an ESM, you do not need to specify an access level. However, if you plan to install an ESM in the future, we recommend you set the access level as each recorder is installed at your site. **Tip:** You can create a covert, or hidden, alarm by assigning it an access level that is higher than the user access levels.

You can test alarm configurations using the Installer Console or by switching to the **Device Installation** task type. For information about testing alarms, see the *Installing a Recorder and Testing Peripheral Connections Quick Steps* publication included on your March Networks CD.

Adding Virtual Network Alarm Inputs

Virtual network alarm inputs allow the recorder to receive alarms from third-party applications over the network instead of routing the alarms through a physical connection. A recorder can support up to 16 network alarm inputs.

Except for their delivery method, virtual network alarm inputs behave in the same manner as conventional physical alarms.

You cannot use the Administrator Console to configure the open-delay or close-delay for a virtual network alarm input. These settings must be configured in the third-party application.

Virtual network alarm inputs are supported on recorders running Release 5.5 (or later) of the recorder software.

To add a network alarm

1. Ensure the **Device Configuration** task type is selected.
2. Click a recorder in the **Device Selector** panel.
3. Click **Alarms**.

   The **Alarms** page appears.
4. Click **Add Network Alarm**.

   The network alarm, with an assigned number, appears in the list of alarms. For example, **Network-Basic-1**, where **1** is the alarm index.
5. Click **Apply Settings**.

NOTE: You can remove a network alarm by selecting it and then clicking **Remove Network Alarm**.

Changing and Querying Virtual Network Alarm States

After you add virtual network alarm inputs, a third-party application may be used to change and query the alarm states.

The interface provided for the third-party application must have the following characteristics:

- The recorder acts as a network server and is listening on TCP port 4098.
- A maximum of two concurrent connections are supported.
- The recorder closes idle connections after five seconds.
- The recorder does not feed back messages to any connections except to reply to query state messages.

To set the state of a virtual network alarm, the message from the third-party application must use the following format:

<virtual alarm index>:*<state>*

Where <*state*> is **0** for open or **1** for closed.

Where <*virtual alarm index*> is the index of the virtual network alarm.

For example, **1:0** sets the Network_Basic_1 alarm to the open state.

To query the current state of a virtual network alarm from a third-party application, use the following the format:

<virtual alarm index>:?

Where <*virtual alarm index*> is the index of the alarm.

For example, **1:?** queries the state of the Network_Basic_1 alarm.

The recorder's reply to the query state inquiry is:

<virtual alarm index>:*<state>*

Where <*state*> is either **0** for open or **1** for closed.

Where <*virtual alarm index*> is the index of the virtual network alarm.

For example, **1:0** indicates that the Network_Basic_1 alarm is in the open state.

The default state of the virtual network alarm is open. The state of a virtual network alarm can only be changed using a third-party application.

When the recorder is rebooted or restarted, all virtual network alarms are reset to the default open state. When you configure virtual network alarms using the third-party application, ensure the alarm trigger state is the "closed" state.

Additional Alarm Configuration Options

In addition to the options mentioned in this chapter, you can specify how the recorder responds to events. For example, customize the recorder to detect alarms after business hours end. For more information, see "Configuring Actions" on page 129.

Chapter 11

Configuring Dataports

The Administrator Console lets you enable and configure dataports, such as PTZ cameras, passthrough PTZ dataports, and text capture units.

The following topics are covered in this chapter:

- “Dataport Types” on page 118
- “Enabling and Configuring Dataports” on page 118
- “Specifying the Default COM Port for Passthrough PTZ Communication” on page 120
- “Additional Dataport Configuration Options” on page 120

Dataport Types

The following table outlines the dataports you can enable and configure:

Table 10: Types of Dataports

Type	Description
PTZ cameras	Cameras with a mechanical housing that you can pan, tilt, zoom, or focus using the Administrator Console's built-in tools. Unlike standard cameras, PTZ cameras have a dataport connection, which communicates field of view adjustments to the camera, in addition to the typical video connection.
Passthrough PTZ	PTZ cameras that you can remotely control using a joystick connected to your computer. When the recorder's dataport is configured for passthrough, data is sent over the network between the recorder and your computer.
Text capture	Peripherals that provide text data, such as retail transaction details, to the recorder. Peripherals such as Automated Teller Machines (ATMs) and Point of Sale (POS) systems often have a text capture component that streams data to the recorder. The Live Monitoring Console's text overlay feature uses a text capture dataport (for more information on text overlay, see the *Live Monitoring Console Getting Started Guide*).

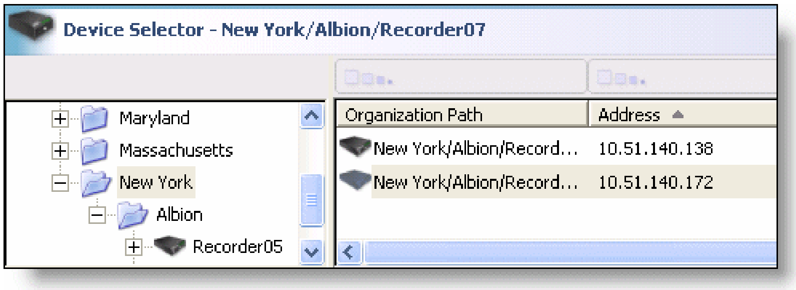
NOTE: Before you start, ensure you have selected the usage type for each dataport. To verify this information, see the *Installing a Recorder and Testing Peripheral Connections Quick Steps* publication included on your March Networks CD.

Enabling and Configuring Dataports

Configure the dataport by enabling it, providing it with a custom name, and specifying other dataport settings.

To customize dataport settings

1. Ensure the **Device Configuration** task type is selected.
2. Click a recorder in the **Device Selector** panel.

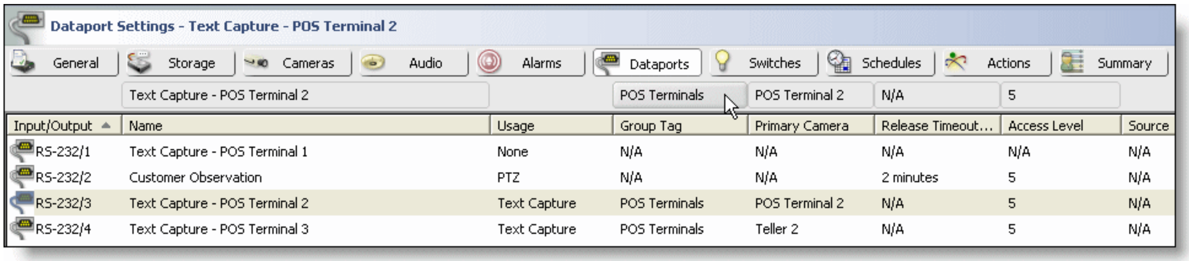


Organization Path	Address
New York/Albion/Record...	10.51.140.138
New York/Albion/Record...	10.51.140.172

3. Click **Dataports**.

   The **Dataports** page appears.
4. Click a dataport and customize the settings outlined in the following table.

If you change one or more settings, you can click **Apply Settings** to save the change, or **Cancel Settings** to discard the change.



Dataport Settings - Text Capture - POS Terminal 2

Input/Output	Name	Usage	Group Tag	Primary Camera	Release Timeout…	Access Level	Source
	Text Capture - POS Terminal 2		POS Terminals	POS Terminal 2	N/A	5	
RS-232/1	Text Capture - POS Terminal 1	None	N/A	N/A	N/A	N/A	N/A
RS-232/2	Customer Observation	PTZ	N/A	N/A	2 minutes	5	N/A
RS-232/3	Text Capture - POS Terminal 2	Text Capture	POS Terminals	POS Terminal 2	N/A	5	N/A
RS-232/4	Text Capture - POS Terminal 3	Text Capture	POS Terminals	Teller 2	N/A	5	N/A

Dataport Setting	Description
Name	The name that identifies the dataport. This name appears in the Investigator to identify the dataport during text searches.
Usage	The type of dataport, such as PTZ or text capture. The usage is specified at the time of installation. You can change the usage by switching to the **Device Installation** task type. For details, see the *Installing a Recorder and Testing Peripheral Connections Quick Steps* publication included on your March Networks CD.
Group Tag	The name of one or more dataports, which helps investigators quickly find evidence for a specific scenario. For example, if investigators at your organization typically monitor text inputs A, B, and C when investigating a row of cash registers, specify “Cash Registers” as the group tag for text inputs A, B, and C. When users open the Investigator, the text inputs automatically appear in a group labeled “Cash Registers,” providing them with quick access to text inputs A, B, and C. **Tip:** To specify multiple groups, separate group names using a comma (,) or a semicolon (;).
Primary Camera	The name of the camera that is linked to the text capture input. When a camera is linked, investigators can automatically review video associated to captured text. **Warning:** If you are setting up dataports for the Live Monitoring Console’s text overlay feature, do not link the same camera to multiple text overlay dataports. A camera can only display the text overlay from one dataport at a time.
Release Timeout Period	The duration after which you want control of a PTZ camera to timeout. For example, if you specify five minutes, and the PTZ camera has been idle for more than five minutes after a user took control of the camera, the user automatically loses control of the camera.
Access Level	The authorization level a user must have to access live or recorded text data or control PTZ cameras using the March Networks software applications, such as the Investigator. Users can access peripherals with an equivalent or lower access level than what is set in their profile. For example, a user with an access level of five can access peripherals set to five or lower. For information about specifying a user’s access level, see “Creating User Profiles and Accounts” on page 188. **Note:** If you are not working with an ESM, you do not need to specify an access level. However, if you plan to install an ESM in the future, we recommend you set the access level as each recorder is installed at your site. **Tip:** Create a covert, or hidden, dataport by assigning it an access level that is higher than the user access levels.

NOTE: You can test dataport configurations using the Installer Console or by switching to the **Device Installation** task type. For more information, see the *Installing a Recorder and Testing Peripheral Connections* PDF (included on your March Networks CD).

Specifying the Default COM Port for Passthrough PTZ Communication

In order to control a passthrough dataport device with a joystick, you must connect the external device controller to your computer's COM port and then specify the COM port used for communication.

To specify the default COM port for passthrough PTZ communication

1. On the **File** menu, click **Preferences**.

   The **Preferences** dialog box appears.
2. Click the **PTZ Settings** tab.
3. Select the **Always use the following COM port with a PTZ joystick** check box and click an available COM port in the **COM Port** list.
4. Click **OK**.

Additional Dataport Configuration Options

In addition to the options mentioned in this chapter, you can perform the following activities to further customize how the recorder works with connected dataports:

- **Customize PTZ cameras.** For example, move a PTZ camera's field of view and define preset views. For more information, see "Configuring and Adjusting PTZ Cameras" on page 53.

  To control a PTZ camera from your desktop, see "Configuring and Adjusting PTZ Cameras using Software Controls" on page 54 and "Configuring and Adjusting PTZ Cameras Remotely Using a Joystick" on page 56.
- **Schedule activities.** For example, define time periods during which you want a PTZ camera to show a particular view. For more information, see "Creating Schedules" on page 125.
- **Specify how the recorder responds to events.** For example, customize the recorder to move a PTZ camera to a preset view when a particular activity occurs. For more information, see "Configuring Actions" on page 129.

Chapter 12

Configuring Switches

The recorder can activate a connected switch, such as a light or an electronic lock.

The following topics are covered in this chapter:

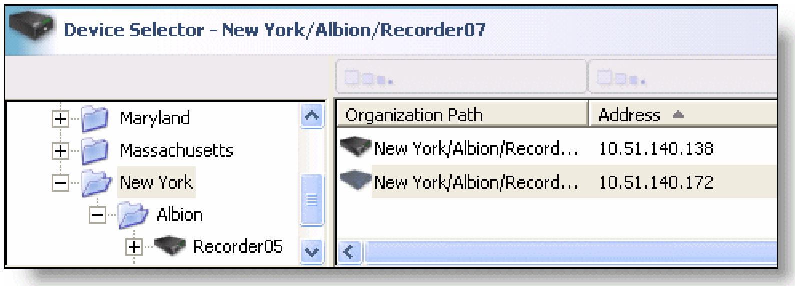
- “Customizing Switch Settings” on page 122
- “Additional Switch Configuration Options” on page 123

Customizing Switch Settings

The following procedure describes how to customize switch settings.

To customize switch settings

1. Ensure the **Device Configuration** task type is selected.
2. Click a recorder in the **Device Selector** panel.

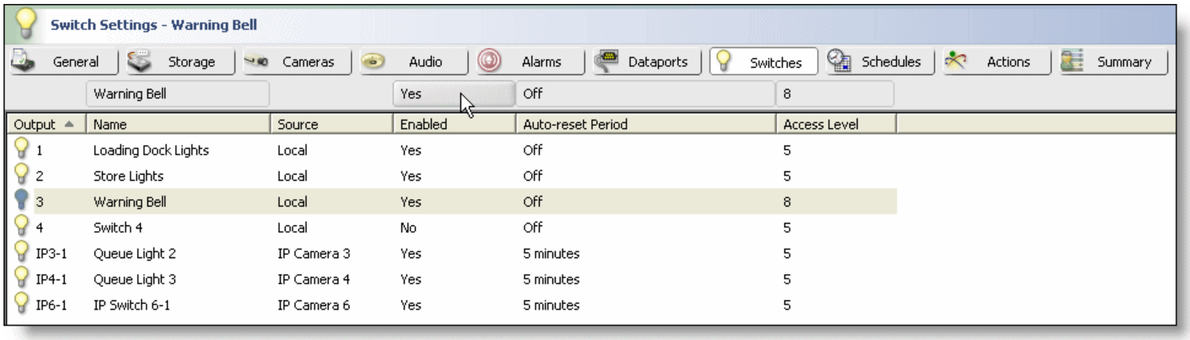


Organization Path	Address
New York/Albion/Record...	10.51.140.138
New York/Albion/Record...	10.51.140.172

3. Click **Switches**.

   The **Switches** page appears.
4. Click a switch and customize the settings outlined in the following table.

   If you change one or more settings, you can click **Apply Settings** to save the change, or **Cancel Settings** to discard the change.



Warning Bell | Yes | Off | 8

Output	Name	Source	Enabled	Auto-reset Period	Access Level
1	Loading Dock Lights	Local	Yes	Off	5
2	Store Lights	Local	Yes	Off	5
3	Warning Bell	Local	Yes	Off	8
4	Switch 4	Local	No	Off	5
IP3-1	Queue Light 2	IP Camera 3	Yes	5 minutes	5
IP4-1	Queue Light 3	IP Camera 4	Yes	5 minutes	5
IP6-1	IP Switch 6-1	IP Camera 6	Yes	5 minutes	5

Switch Setting	Description
Name	The name that identifies the switch.
Enabled	When the switch is enabled, you can configure its settings and turn the switch on or off; the switch cannot be turned on or off when it is disabled.
Auto-reset Period	The amount of time before the switch returns to the off state. For example, if an individual turned on a light and forgot to turn it off, the switch automatically turns off when the auto-reset period is reached.

Access Level	The authorization level a user must have to turn the switch on or off using the March Networks software applications, such as the Investigator. Users can access peripherals with an equivalent or lower access level than what is set in their profile. For example, a user with an access level of five can access peripherals set to five or lower. For information about specifying a user's access level, see "Creating User Profiles and Accounts" on page 188. **Note:** If you are not working with an ESM, you do not need to specify an access level. However, if you plan to install an ESM in the future, we recommend you set the access level as each recorder is installed at your site. **Tip:** You can create a covert, or hidden, switch by assigning it an access level that is higher than the user access levels.

You can test switch configurations using the Installer Console or by switching to the Device Installation task type. For more information about testing switches, see the *Installing a Recorder and Testing Peripheral Connections* PDF included on your March Networks CD.

Additional Switch Configuration Options

You can perform the following activities to further customize how the recorder works with connected switches:

- **Schedule activities.** For example, customize the recorder to switch on a light in the early morning, when you expect the first store employees to arrive. For more information, see "Creating Schedules" on page 125.
- **Specify how the recorder responds to events.** For example, customize the recorder to turn on a switch when a particular activity occurs, such as a video motion event. For more information, see "Configuring Actions" on page 129.

Creating Schedules

You can create a schedule to define a time period during which you want the recorder to perform a particular activity.

The following topics are covered in this chapter:

Scheduling

Scheduled event times are based on the recorder's time zone. If you are working with a recorder in another time zone, you do not need to take time zone changes into account. For example, if you are in New York and the recorder is in Los Angeles, a schedule configured to start at 9:00 A.M., starts at 9:00 A.M., Los Angeles time. For information about time zones, see "Configuring a Recorder Clock" on page 39.

Scenario You are monitoring your retail store for motion during the evenings to detect unauthorized individuals in the store while it is closed.

Problem You are only interested in monitoring motion that occurs after business hours end. You do not want to monitor motion while customers are shopping in the store.

Resolution Select the default Business Hours schedule, which specifies that business hours are from 9:00 A.M. to 5:00 P.M. during weekdays. After you specify the hours, the next step is to configure the recorder to detect motion during the scheduled hours. Details are provided in "Configuring Actions" on page 129.

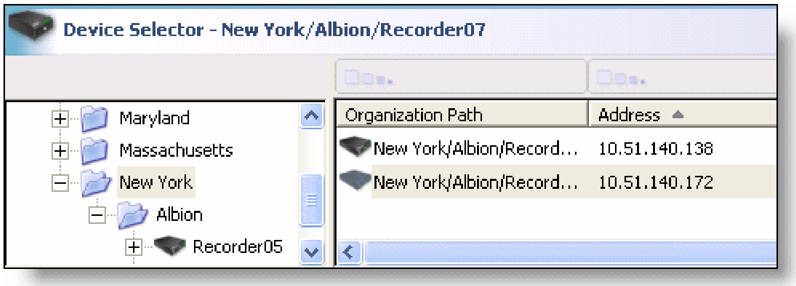
In addition to the options mentioned in this chapter, you can specify how the recorder responds to events. For example, configure the recorder to perform a particular activity, such as detect motion or monitor an alarm input, during the scheduled hours. For more information, see "Configuring Actions" on page 129.

Creating a Schedule

The following procedure describes how to create a schedule.

To create a schedule

1. Ensure the **Device Configuration** task type is selected.
2. Click a recorder in the **Device Selector** panel.



Organization Path	Address
New York/Albion/Record...	10.51.140.138
New York/Albion/Record...	10.51.140.172

3. Click **Schedules**.

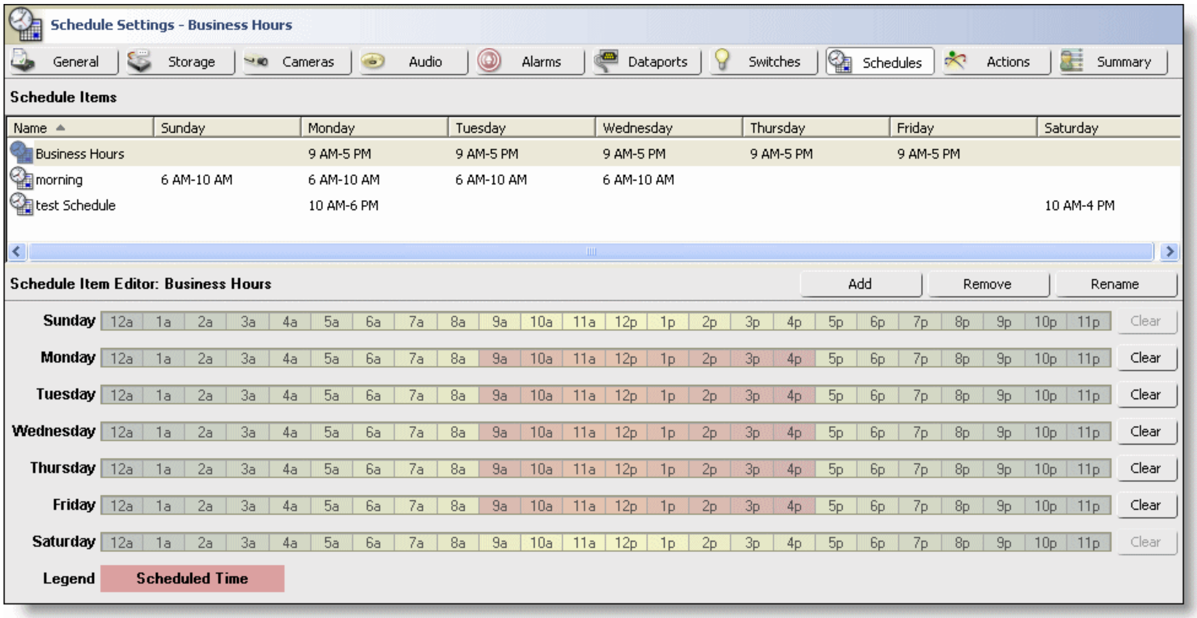
   The **Schedules** page appears.
4. Click **Add**.
5. In the **Name** column, type a descriptive name for the schedule.

6. In the area below the **Schedule Items** list, a table depicting a week appears, with each day divided into hours. Use your pointer to click and drag across the hours you want to include in the schedule.

   Red blocks in the **Schedule Time Editor** represent scheduled time.

   You can set the schedule to start or end on the half hour by stopping the pointer halfway through an hour block.

7. Click **Apply Settings** to save the change, or **Cancel Settings** to discard the change.



Schedule Settings - Business Hours

Schedule Items

Name ▲	Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
Business Hours		9 AM-5 PM	9 AM-5 PM	9 AM-5 PM	9 AM-5 PM	9 AM-5 PM	
morning	6 AM-10 AM	6 AM-10 AM	6 AM-10 AM	6 AM-10 AM			
test Schedule		10 AM-6 PM					10 AM-4 PM

Schedule Item Editor: Business Hours

Sunday	12a	1a	2a	3a	4a	5a	6a	7a	8a	9a	10a	11a	12p	1p	2p	3p	4p	5p	6p	7p	8p	9p	10p	11p	Clear
Monday	12a	1a	2a	3a	4a	5a	6a	7a	8a	9a	10a	11a	12p	1p	2p	3p	4p	5p	6p	7p	8p	9p	10p	11p	Clear
Tuesday	12a	1a	2a	3a	4a	5a	6a	7a	8a	9a	10a	11a	12p	1p	2p	3p	4p	5p	6p	7p	8p	9p	10p	11p	Clear
Wednesday	12a	1a	2a	3a	4a	5a	6a	7a	8a	9a	10a	11a	12p	1p	2p	3p	4p	5p	6p	7p	8p	9p	10p	11p	Clear
Thursday	12a	1a	2a	3a	4a	5a	6a	7a	8a	9a	10a	11a	12p	1p	2p	3p	4p	5p	6p	7p	8p	9p	10p	11p	Clear
Friday	12a	1a	2a	3a	4a	5a	6a	7a	8a	9a	10a	11a	12p	1p	2p	3p	4p	5p	6p	7p	8p	9p	10p	11p	Clear
Saturday	12a	1a	2a	3a	4a	5a	6a	7a	8a	9a	10a	11a	12p	1p	2p	3p	4p	5p	6p	7p	8p	9p	10p	11p	Clear

Legend 🟥 Scheduled Time

Editing a Schedule

The following procedure describes how to edit a schedule.

To edit a schedule

1. Ensure the **Device Configuration** task type is selected.
2. Click a recorder in the **Device Selector** panel.
3. Click **Schedules**.

   The **Schedules** page appears.
4. Click a schedule in the **Schedule Items** list.
5. In the **Schedule Item Editor**, drag to select new schedule hours.
6. Click **Rename** and type a new schedule name.
7. Click **Apply Settings**, or **Cancel Settings** to discard the changes.

NOTE: To remove a schedule, click the schedule in the **Schedule Items** list and then click **Remove**.

Chapter 14

Configuring Actions

This chapter describes how to configure actions. The following topics are covered:

- “Configuring How a Recorder Responds to Events” on page 130
- “Action Configuration Settings” on page 132
- “Retain Evidence Data Action” on page 132
- “Detect Events Action” on page 134
- “Activate Switch Action” on page 135
- “Move PTZ Action” on page 136
- “Output Video Action” on page 137
- “Control Bandwidth Action” on page 138
- “Copy to External Media Action” on page 139

Configuring How a Recorder Responds to Events

You can configure the recorder to perform certain activities when events occur. This lets you maximize your surveillance system to ensure that you are notified of the activities in which you are interested.

Events can include alarms triggered by a peripheral device, such as a door contact alarm, or can include scheduled activities, such as detecting video motion alarms when business hours end.

There are three items you need to think about when specifying how the recorder responds to an event:

- **Trigger**. Something that prompts the recorder to perform an activity. A trigger can be a physical device, such as a door contact alarm. A trigger can also be a scheduled time period.
- **Action**. The activity you want the recorder to perform.
- **Target**. The peripheral that the recorder uses to perform the action.

The following example explains how an action is implemented using an alarm input trigger:

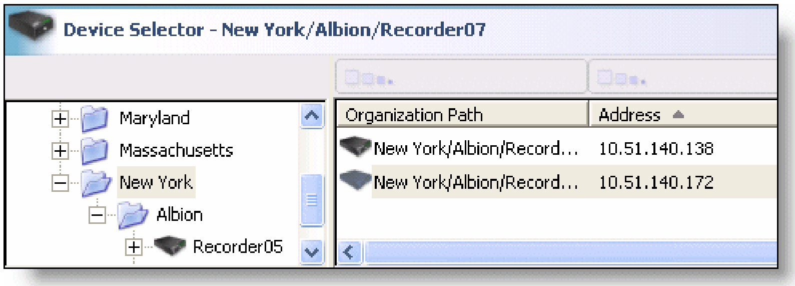
Scenario	You are monitoring an inventory room at your retail store.
Problem	You want to record video when someone enters the room, however, your lighting system is set to turn off after 30 minutes, preventing you from capturing clear video.
Resolution	Assign an **Activate Switch** action to a door contact alarm input installed on the door. Choose the light switch as the target peripheral. When the door opens, the light turns on, allowing the recorder to capture clear video of the activity.

The following example explains how an action is implemented using a scheduled time period trigger:

Scenario	You are monitoring a retail store during the evening to ensure that no one enters the store after it is closed. You are using motion detection to ensure that any activity occurring within the store is detected as an alarm event.
Problem	You have enabled video motion detection 24 hours per day. However, you find that during the day there are numerous video motion events triggered, due to shoppers passing your cameras.
Resolution	To prevent the recorder from detecting motion during the day, configure the recorder to only detect motion outside the times outlined in the **Business Hours** schedule.

To configure how a recorder responds to events

1. Ensure the **Device Configuration** task type is selected.
2. Click a recorder in the **Device Selector** panel.



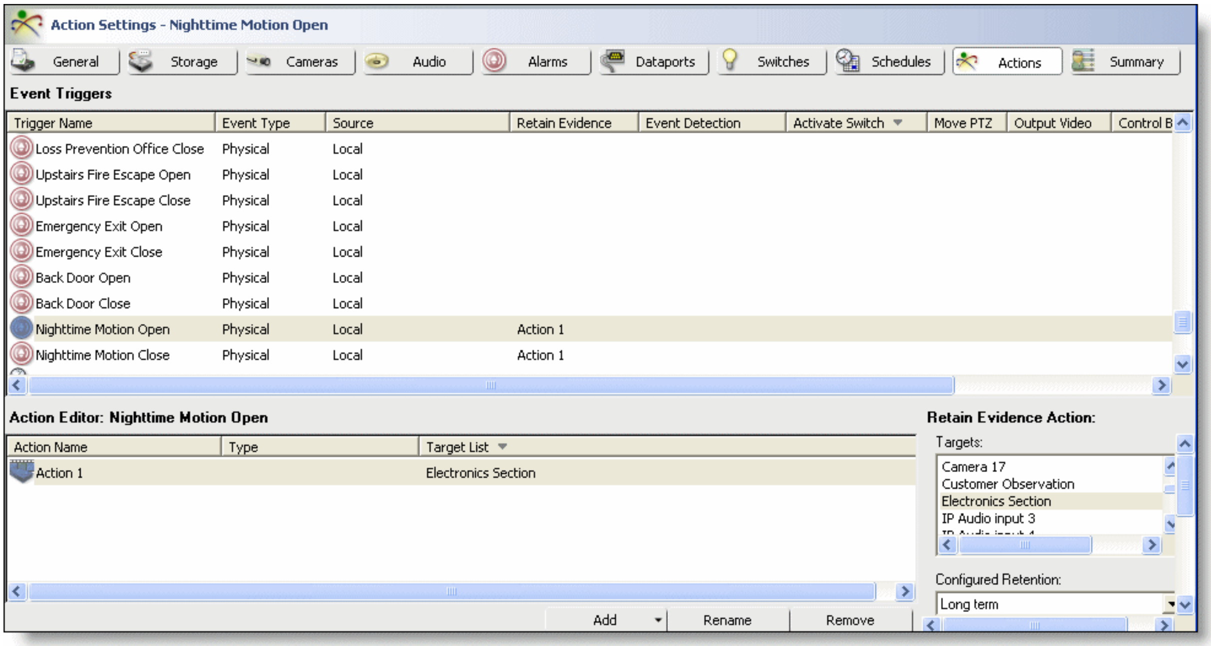
Device Selector - New York/Albion/Recorder07

- Maryland
- Massachusetts
- New York
  - Albion
    - Recorder05

Organization Path	Address
New York/Albion/Record...	10.51.140.138
New York/Albion/Record...	10.51.140.172

3. Click **Actions**.

   The **Actions** page appears.



Action Settings - Nighttime Motion Open

Event Triggers

Trigger Name	Event Type	Source	Retain Evidence	Event Detection	Activate Switch	Move PTZ	Output Video	Control B
Loss Prevention Office Close	Physical	Local						
Upstairs Fire Escape Open	Physical	Local						
Upstairs Fire Escape Close	Physical	Local						
Emergency Exit Open	Physical	Local						
Emergency Exit Close	Physical	Local						
Back Door Open	Physical	Local						
Back Door Close	Physical	Local						
Nighttime Motion Open	Physical	Local	Action 1					
Nighttime Motion Close	Physical	Local	Action 1					

Action Editor: Nighttime Motion Open

Action Name	Type	Target List
Action 1		Electronics Section

Retain Evidence Action:

Targets:

Camera 17
Customer Observation
Electronics Section
IP Audio input 3

Configured Retention:

Long term

4. In the **Event Triggers** list, click a trigger.

   You can use a schedule as a trigger. When the trigger is a schedule, some action settings are unavailable. For information about creating schedules, see “Creating Schedules” on page 125.

IMPORTANT: If the Critical Recording Buffer is disabled and you want to retain evidence, you must select a trigger and configure the **Retain Evidence Data** action. If this action is not configured, the recorder will not retain any evidence. For information about the CRB, see “Configuring and Reviewing Evidence Retention” on page 40.

5. Click **Add** and then click an action.

6. Customize the action settings outlined in the following sections.

   If you change one or more settings, you can click **Apply Settings** to save the change, or **Cancel Settings** to discard the change.

NOTE: The current alarm state is reported to the software applications, such as the Investigator, when the alarm event is triggered. For example, if a recorder is configured to detect an open door outside of business hours (9 A.M. to 5 P.M.), and the door is propped open at 4:55 P.M., the alarm is detected and generated at 5 P.M.

Action Configuration Settings

The following sections describe the configuration settings for the following actions:

- "Retain Evidence Data Action"
- "Detect Events Action"
- "Activate Switch Action"
- "Move PTZ Action"
- "Output Video Action"
- "Control Bandwidth Action"
- "Copy to External Media Action"

Retain Evidence Data Action

This action specifies how long the recorder retains video related to the event. You can also specify how long recording continues when this type of event occurs.

For example, you can configure the recorder to retain video related to a particular alarm longer than other video.

Retain Evidence Data Action:Configuration Settings	Description
Targets	Choose one or more targets from which you want to retain audio, video, or text data.
Retention period	Choose whether you want to retain the audio, video, or text data for the **Long term** or **Extended term** retention period (specified on the **General** page).
Retain high frame rate	Select this check box to enable the recorder to retain the video using the frame rate specified in the **Frames Per Second** column on the **Cameras** page. If you do not select this check box, the recorder retains the video using the frame rate specified in the **Divisor (Low fps)** column on the **Cameras** page.

Retain Evidence Data Action: Configuration Settings	Description
Pre-event duration	Specify the amount of audio, video, or text data that you want to retain, leading up to the event that triggered the alarm. For example, if you are monitoring a loading dock door, you may want to retain five minutes of pre-event video to observe activity that occurred before the door was opened. The pre-event duration setting is unavailable if the CRB is disabled. For information about the CRB, see "Configuring and Reviewing Evidence Retention" on page 40.
Duration after opposite state	Specify the amount of audio, video, or text data that you want to retain after the trigger enters the opposite state, for example, when motion stops or when a door closes. For example, if you are monitoring a door contact at a store entrance, you may want to retain five minutes of post-event video to observe activity that occurred outside the store entrance after the door closed. This setting is unavailable when the event trigger is a schedule.
Failsafe (maximum duration)	Specify how long you want the **Retain Evidence Data** action to be performed. This feature is useful when it is possible that the trigger may not enter the opposite state and you want to avoid recording continuously after a specified duration. For example, if you are monitoring a loading dock door and the door is not closed, the recorder continuously records video. If a failsafe duration is specified, the recorder stops recording when this failsafe duration is reached. This setting is unavailable when the event trigger is a schedule. **Note:** It is important to note that the **Retain Evidence Data** action will not exceed the **Failsafe (maximum duration)** period that you specify, even if the trigger has not entered the opposite state during the failsafe period.

Detect Events Action

This action allows you to configure the recorder to detect alarms when a trigger is activated.

For example, choose this action if you want to configure the recorder to detect alarms after business hours end.

Detect Events Action: Configuration Settings	Description
Targets	Choose the target that you want to detect alarms when the trigger is activated.
Maximum duration	Specify how long you want the **Detect Events** action to be performed. This setting is unavailable when the event trigger is a schedule. If the **Maximum duration** has been reached and the trigger has not yet entered the opposite state, the **Detect Events** action ends.
Stop when entering opposite state	Select this check box to enable the recorder to stop monitoring the alarm input or camera when the trigger enters the opposite state. This setting is unavailable when the event trigger is a schedule. This check box is only available when you are working with alarm inputs or cameras with video motion detection enabled. Selecting this check box lets you maximize how the recorder tracks alarm state changes by telling the recorder to stop detecting alarms as soon as the trigger enters the opposite state, rather than waiting for a defined period of time to pass.

Activate Switch Action

This action allows you to configure the recorder to activate a switch when a trigger is activated.

For example, choose this action if you want to configure the recorder to turn on a light when a camera detects motion.

Activate Switch Action:Configuration Settings	Description
Targets	Choose the switch you want to activate when the trigger is activated.
Asserted state	Choose the state that you want the switch to assume, such as off or on. For example, if you are working with a light, you may want to turn the light on when the camera detects motion.
Maximum duration	Specify how long you want the switch to be activated. This setting is unavailable when the event trigger is a schedule. If the **Maximum duration** has been reached and the trigger has not yet entered the opposite state, the **Activate Switch** action ends.
Stop when entering opposite state	Enable the recorder to deactivate the switch when the trigger enters the opposite state. This setting is unavailable when the event trigger is a schedule. This check box is only available when you are working with alarm inputs or cameras with video motion detection enabled. Selecting this check box lets you maximize how the recorder works with switches by telling the recorder to deactivate the switch as soon as the trigger enters the opposite state, rather than waiting for a defined period of time to pass.

Move PTZ Action

This action allows you to configure the recorder to move a PTZ camera to a particular view when a trigger is activated.

For example, you can configure the recorder to move its field of view to a door when a door (with an installed door contact) opens.

Move PTZ Action: Configuration Settings	Description
Target	Choose the PTZ camera you want to move when the trigger is activated.
PTZ sequences	Create a script that specifies one or more PTZ camera preset views that you want to view. When you choose several preset views, the PTZ camera moves to each view in sequence. For information about setting PTZ camera preset views, see "Configuring and Adjusting PTZ Cameras using Software Controls" on page 54.
Maximum duration	Specify how long you want the action to be performed. This setting is unavailable when the event trigger is a schedule. If the **Maximum duration** has been reached and the trigger has not yet entered the opposite state, the **Move PTZ** action ends.
Stop when entering opposite state	Select this check box to enable the recorder to stop moving the PTZ camera when the trigger enters the opposite state. This setting is unavailable when the event trigger is a schedule. This check box is only available when you are working with alarm inputs or cameras with video motion detection enabled. Selecting this check box lets you maximize how the recorder moves PTZ cameras by telling the recorder to return the PTZ camera to its original setting as soon as the trigger enters the opposite state, rather than waiting for a defined period of time to pass.

Output Video Action

This action allows you to configure the recorder to show one or more camera views in sequence on a monitor when a trigger is activated.

For example, you can configure the recorder to show video from all of the cameras in your organization in sequence on a monitor mounted at the main entrance of your store.

Output Video Action: Configuration Settings	Description
Target	Choose the display (such as a monitor) to which you want to provide video when the trigger is activated.
Output video sequences	Create a script that specifies one or more cameras that you want to show on the display. When you choose several cameras, each camera view is shown in sequence on the display.
Maximum duration	Specify how long you want the action to be performed. This setting is unavailable when the event trigger is a schedule. If the **Maximum duration** has been reached and the trigger has not yet entered the opposite state, the **Output Video** action ends.
Stop when entering opposite state	Enable the recorder to stop providing video to the monitor when the trigger enters the opposite state. This setting is unavailable when the event trigger is a schedule. Selecting this check box lets you maximize how the recorder outputs video to a display by telling the recorder to return to its original camera view as soon as the trigger enters the opposite state, rather than waiting for a defined period of time to pass. The **Stop when entering opposite state** check box is only available when you are working with alarm inputs or cameras with video motion detection enabled.

Control Bandwidth Action

Allows you to increase the amount of network resources available to the recorder when a trigger is activated.

For example, you can configure the recorder to increase the available bandwidth when a silent panic button is pressed.

Control Bandwidth Action:Configuration Settings	Description
Bandwidth limit	Specify the amount of network resources that you want to make available to the recorder when the trigger is activated.
Maximum duration	Specify how long you want the recorder to use the bandwidth limit specified above. If the **Maximum duration** has been reached and the trigger has not yet entered the opposite state, the **Control Bandwidth** action ends. This setting is unavailable when the event trigger is a schedule.
Stop when entering opposite state	Enable the recorder to return to the original bandwidth limit when the trigger enters the opposite state. This setting is unavailable when the event trigger is a schedule. Selecting this check box lets you maximize your network resources by telling the recorder to return to its original bandwidth settings as soon as the trigger enters the opposite state, rather than waiting for a defined period of time to pass.

Copy to External Media Action

Allows you to configure the recorder to capture evidence when a trigger is activated and queue it for further revision in the Investigator or automatically copy it to external media.

For example, you can configure the recorder to capture evidence when an alarm is detected and automatically copy it to a USB drive that is connected to the recorder.

Copy to External Media Action: Configuration Settings	Description
Targets	Choose the input from which you want to capture evidence when the trigger is activated.
Copy When Complete	Select this check box to automatically copy the evidence to external media when the action is complete.
Pre-event duration	For alarm events, specify how much evidence you want to capture before the event occurs.
Duration after opposite state	For alarm events, specify how much evidence you want to capture after the event occurs. This setting is unavailable when the event trigger is a schedule.
Failsafe (maximum duration)	For alarm events, specify the maximum length of time you want to capture evidence. This setting is unavailable when the event trigger is a schedule.

Generating a Configuration Summary

When you generate a summary of a recorder’s configuration settings you can review all of the recorder’s details from one location.

You can view this information, or you can print or save it.

The following topics are covered in this chapter:

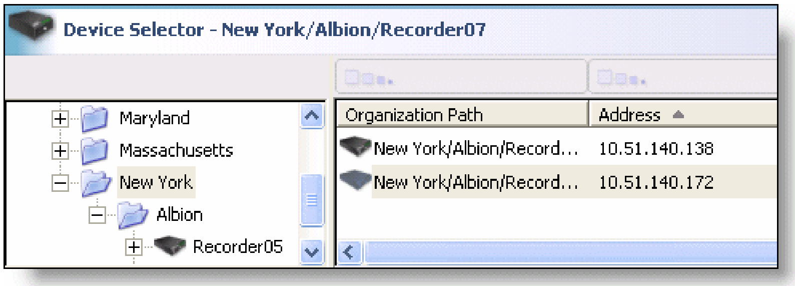
- “Summarizing the Recorder Configuration Settings” on page 142
- “Printing and Saving the Configuration Settings Summary” on page 143

Summarizing the Recorder Configuration Settings

The following procedure describes how to generate a summary of a recorder's configuration settings.

To generate a configuration summary

1. Ensure the **Device Configuration** task type is selected.
2. Click a recorder in the **Device Selector** panel.



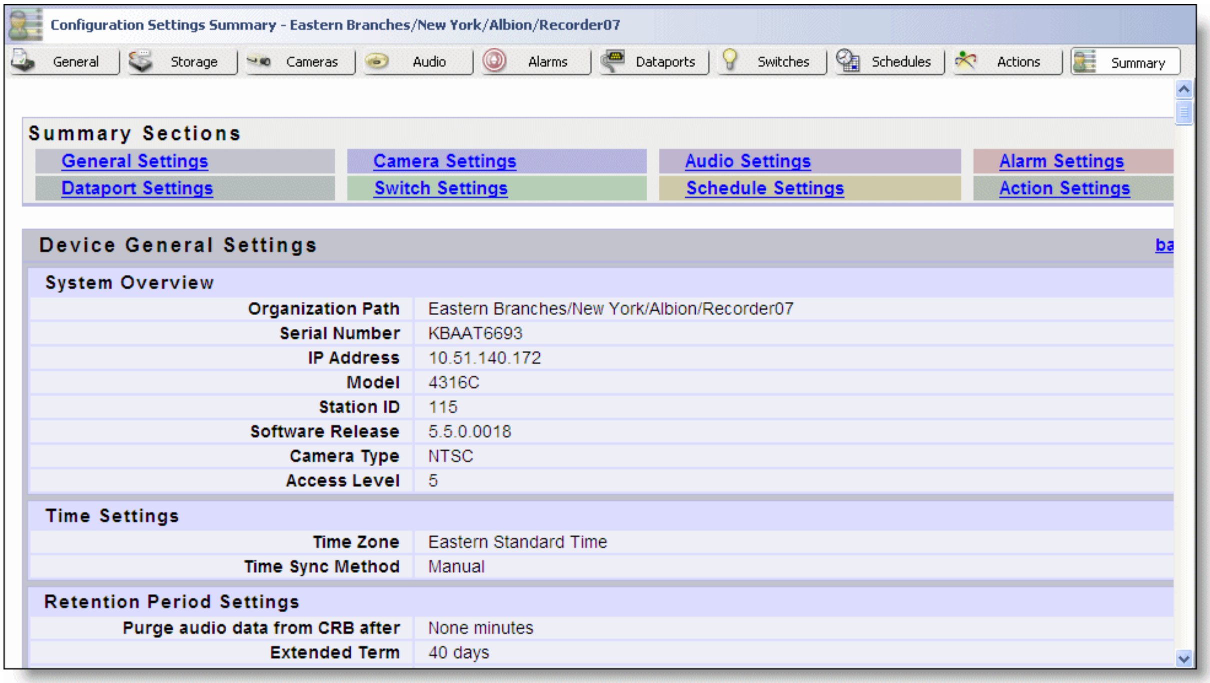
Device Selector - New York/Albion/Recorder07

- Maryland
- Massachusetts
- New York
  - Albion
    - Recorder05

Organization Path	Address
New York/Albion/Record...	10.51.140.138
New York/Albion/Record...	10.51.140.172

3. Click **Summary**.

   The **Summary** page appears.
4. Use the links that appear under **Summary** to navigate through the configuration sections.



Configuration Settings Summary - Eastern Branches/New York/Albion/Recorder07

Summary Sections

General Settings	Camera Settings	Audio Settings	Alarm Settings
Dataport Settings	Switch Settings	Schedule Settings	Action Settings

Device General Settings ba

System Overview

Organization Path	Eastern Branches/New York/Albion/Recorder07
Serial Number	KBAAT6693
IP Address	10.51.140.172
Model	4316C
Station ID	115
Software Release	5.5.0.0018
Camera Type	NTSC
Access Level	5

Time Settings

Time Zone	Eastern Standard Time
Time Sync Method	Manual

Retention Period Settings

Purge audio data from CRB after	None minutes
Extended Term	40 days

Printing and Saving the Configuration Settings Summary

The following procedure describes how to print and save a summary of a recorder’s configuration settings.

To print or save the configuration summary

1. With the configuration summary open, click one of the following:
   - **Print Summary**
   - **Save Summary**

   When you click either of these buttons, the entire summary is printed or saved — not just the section you are reviewing.
2. Specify either the printing options or the location in which you want to save the configuration summary.

Chapter 16

Managing Configuration Templates

This chapter describes how to generate and apply configuration templates to recorders on your network. The following topics are covered:

- “Configuration Template Overview” on page 146
- “Generating Configuration Templates” on page 147
- “Applying Configuration Templates” on page 148

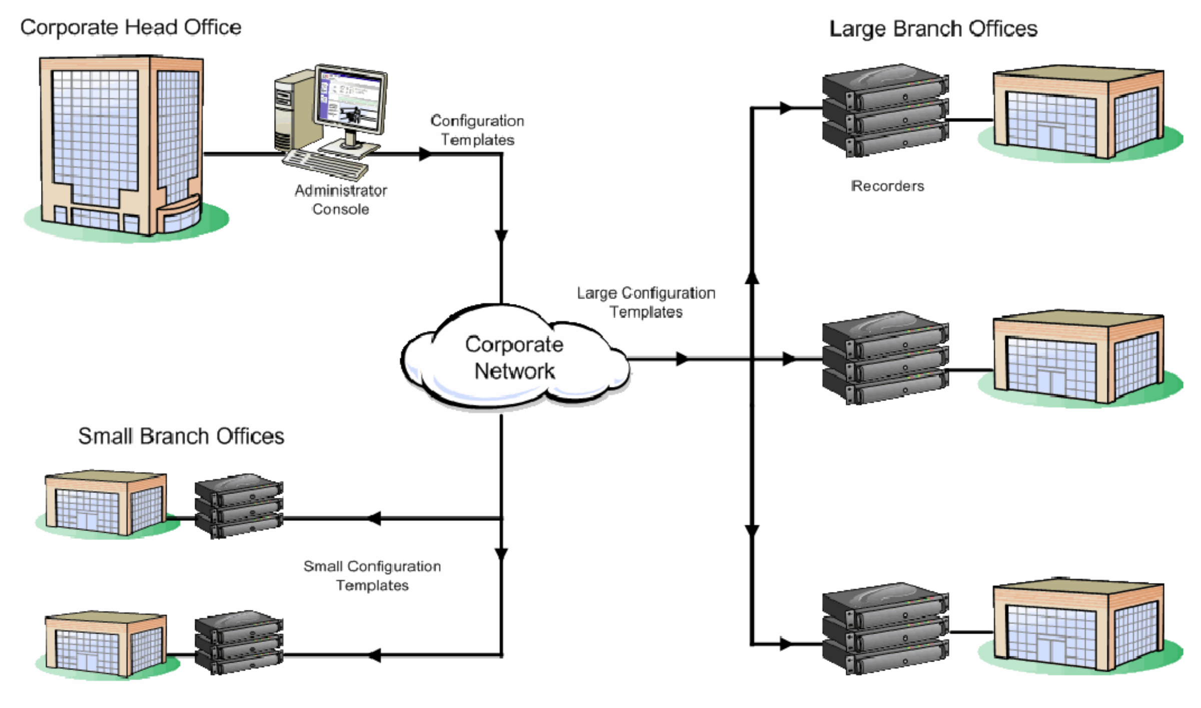
Configuration Template Overview

You can generate and apply configuration templates to recorders on your network. This is useful when:

- You have configured your recorder and want to apply the same settings to other recorders on your network. Or, you would like to share the settings with other administrators.
- You want to create a template of the settings already in use by a recorder on the network, and then apply them to another recorder.
- You want to keep a backup of the recorder's settings on your computer for future use.

When you generate a template, the recorder's configuration information, such as recorder and schedule settings, is exported to a file. Use this file to apply the configuration settings to other recorders.

The following illustration provides an overview of how configuration templates are sent over the network to recorders:



The following example provides a scenario where you could apply a configuration template:

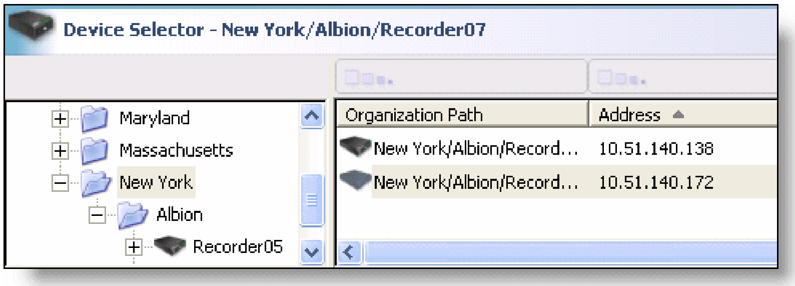
Scenario	You have just received 10 recorders that you are going to install at two bank branches.
Problem	Each recorder will have 16 cameras, six ATM connections, and two alarm inputs, which all share the same configuration settings, with the exception of the input names.
Resolution	Configure one of the recorders with the required settings and peripheral names. Generate a template. Apply the template to the remaining nine recorders. As you load the template onto each recorder, customize the peripheral names and then click Apply Settings.

Generating Configuration Templates

You can generate a configuration template at any time when the Device Configuration task type is selected. These buttons are always available, regardless of the Device Configuration page you are accessing.

To generate a configuration template

1. Ensure the **Device Configuration** task type is selected.
2. Click a recorder in the **Device Selector** panel.

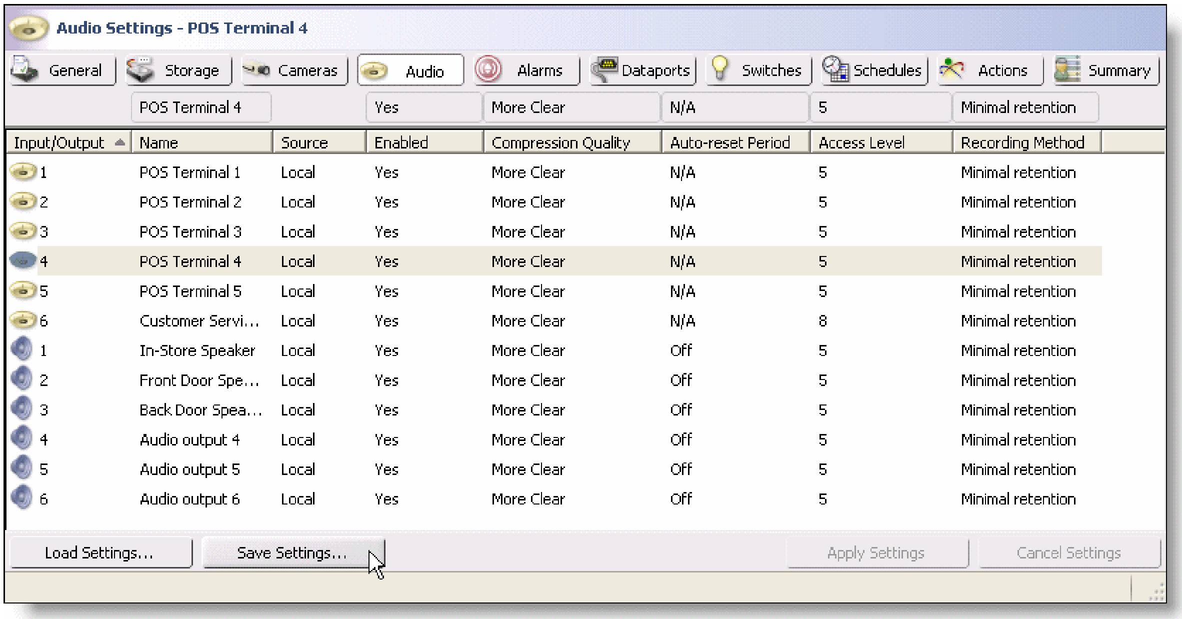

Device Selector - New York/Albion/Recorder07

Organization Path	Address
New York/Albion/Record...	10.51.140.138
New York/Albion/Record...	10.51.140.172

3. Click **Save Settings**.

4. Navigate to the location where you want to save the configuration template.

   The configuration settings (with the exception of the IP address and network name) are saved as a configuration template in .dat format.



	POS Terminal 4		Yes	More Clear	N/A	5	Minimal retention
Input/Output	**Name**	**Source**	**Enabled**	**Compression Quality**	**Auto-reset Period**	**Access Level**	**Recording Method**
1	POS Terminal 1	Local	Yes	More Clear	N/A	5	Minimal retention
2	POS Terminal 2	Local	Yes	More Clear	N/A	5	Minimal retention
3	POS Terminal 3	Local	Yes	More Clear	N/A	5	Minimal retention
4	POS Terminal 4	Local	Yes	More Clear	N/A	5	Minimal retention
5	POS Terminal 5	Local	Yes	More Clear	N/A	5	Minimal retention
6	Customer Servi...	Local	Yes	More Clear	N/A	8	Minimal retention
1	In-Store Speaker	Local	Yes	More Clear	Off	5	Minimal retention
2	Front Door Spe...	Local	Yes	More Clear	Off	5	Minimal retention
3	Back Door Spea...	Local	Yes	More Clear	Off	5	Minimal retention
4	Audio output 4	Local	Yes	More Clear	Off	5	Minimal retention
5	Audio output 5	Local	Yes	More Clear	Off	5	Minimal retention
6	Audio output 6	Local	Yes	More Clear	Off	5	Minimal retention

Applying Configuration Templates

You can apply a configuration template to the recorder to update it with the settings specified in the template.

If the retention limit specified in the configuration template is lower than the current retention limit, the recorder automatically starts deleting evidence that falls outside of the limit when you apply the configuration template. The retention limit is specified on the **General** page in the **Limit retention of all evidence data on device to** [ ] **days** box.

For example, if the retention limit is currently set to 40 days and you change the limit to 30 days by applying the configuration template, the recorder automatically starts deleting the oldest 10 days of evidence when you apply the configuration template. For more information about the retention limit, see “Configuring and Reviewing Evidence Retention” on page 40.

To apply a configuration template

1. Click the recorder to which you want to apply a configuration template in the **Device Selector** panel.
2. Click **Load Settings**.
3. Click **Apply Settings**.

Chapter 17

Organizing Recorders and Exporting the Recorder List

This chapter describes how to organize recorders and export the recorder list. The following topics are covered:

- “Organizing Recorders” on page 150
- “Adding Folders and Customizing the Recorder List” on page 150
- “Exporting the Recorder List” on page 152

Organizing Recorders

To help organize your Recorder Selector panel, you can create folders to sort the recorders into smaller groups. This is useful when you are working with a large number of recorders and want to view each group individually. You can also use the refinement function to filter the recorder list.

You can also export the list of recorders for other system users to access.

If you are connected to an ESM, the buttons in the following table appear. These buttons let you perform activities that are unique to a managed environment.

Button	More Information
View Audit Report	"Viewing the Recorder Audit Report" on page 194
Replace Device	"Replacing Recorders" on page 209
Server Order	"Specifying the Server Connection Order" on page 208
Unregister from ESM	"Registering and Unregistering Recorders With an ESM" on page 195

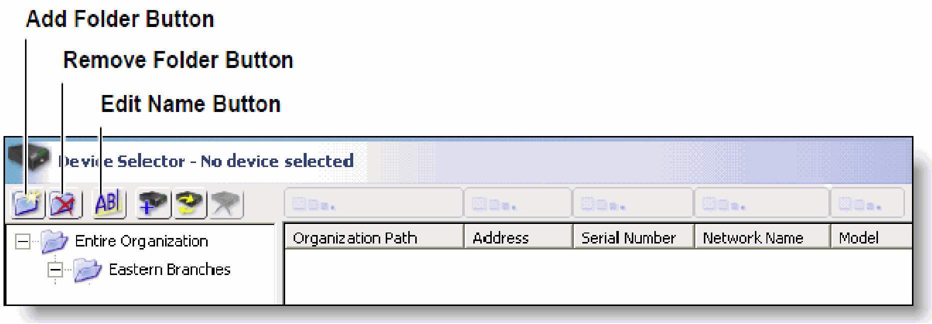
Adding Folders and Customizing the Recorder List

You can create folders within which the recorders are organized.

Empty folders are automatically deleted from the Entire Organization list when you close the Administrator Console. You cannot remove or rename the Entire Organization folder.

To add, remove, or rename a folder

1. Ensure the **Device Management** task type is selected.
2. Perform one of the following tasks:
   - **Add a folder.** Click the **Add Folder** button.
   - **Remove a folder.** Select the folder and then click the **Remove Folder** button. You can only delete empty folders. If a folder contains one or more items, you must first move the recorders to another folder.
   - **Rename a folder.** Select the folder and then click the **Edit Name** button, or double-click it and type the new name.



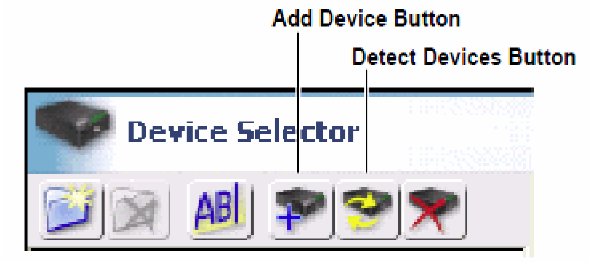
To add a recorder to the Entire Organization list

1. Ensure the **Device Management** task type is selected.
2. Do one of the following tasks:
   - **Manually add a recorder.** Click the **Add Device** button and then type the recorder's IP address or network name.
   - **Detect recorders on your network's subnet.** Click the **Detect Devices** button.

   If this is the first time the recorder is being accessed by the March Networks software, or if it has not yet been organized within a folder, the recorder appears in the **New** folder. If the recorder had been previously deleted and then added again, the recorder is placed in its original folder structure.

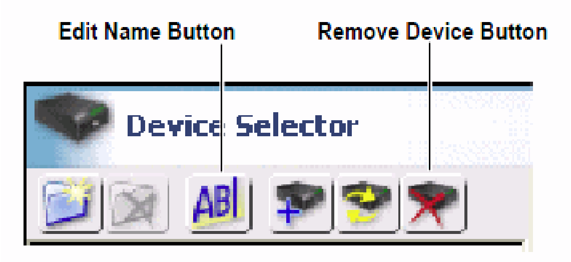
   After you add the recorder, you do not need to add it again. It automatically appears in the **Entire Organization** folder each time you start the application.

   If the Administrator Console is connected to an ESM, the recorders managed by the ESM appear automatically — you do not need to add them. For information about connecting to an ESM, see "Connecting to an ESM" on page 16.



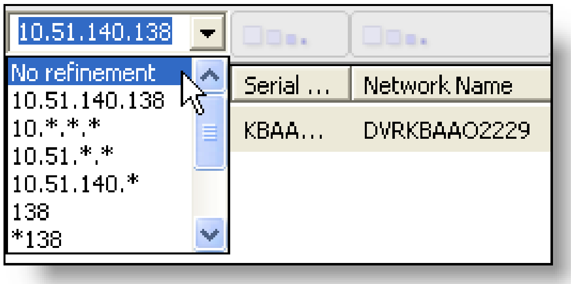
To rename or remove a recorder

1. Ensure the **Device Management** task type is selected.
2. Do one of the following tasks:
   - **Rename a recorder.** Select the recorder and then click the **Edit Name** button.
   - **Remove a recorder.** Click the **Remove Device** button.



To refine the list of recorders

1. In the list of recorders, click a **Refine List** button above the column you want to filter.
2. In the refinement list that appears, type or select a refinement option.



3. To clear the refinement, click the **Refine List** button and then click **No Refinement**.

   To refine the recorder list by address, you must type an asterisk in the refinement option. For example, if you want to filter the list to show only recorders with the number 51 in their IP addresses, you must type *51, *51*, or 51*, depending on where the number appears in the address.

Exporting the Recorder List

When you are working with locally-managed recorders, you can generate a recorder list, which is in DAT (.dat) file format. You can provide this file to other system administrators, installers, or investigators to provide them with access to the recorders in the list.

NOTE: This step is not necessary when you are working with an ESM, as the list of recorders automatically appears when the software applications, such as the Administrator Console and the Investigator, connect to the ESM.

When you provide the list to other users, instruct them to import the list into the application they are using. The import option is available from the application's File menu.

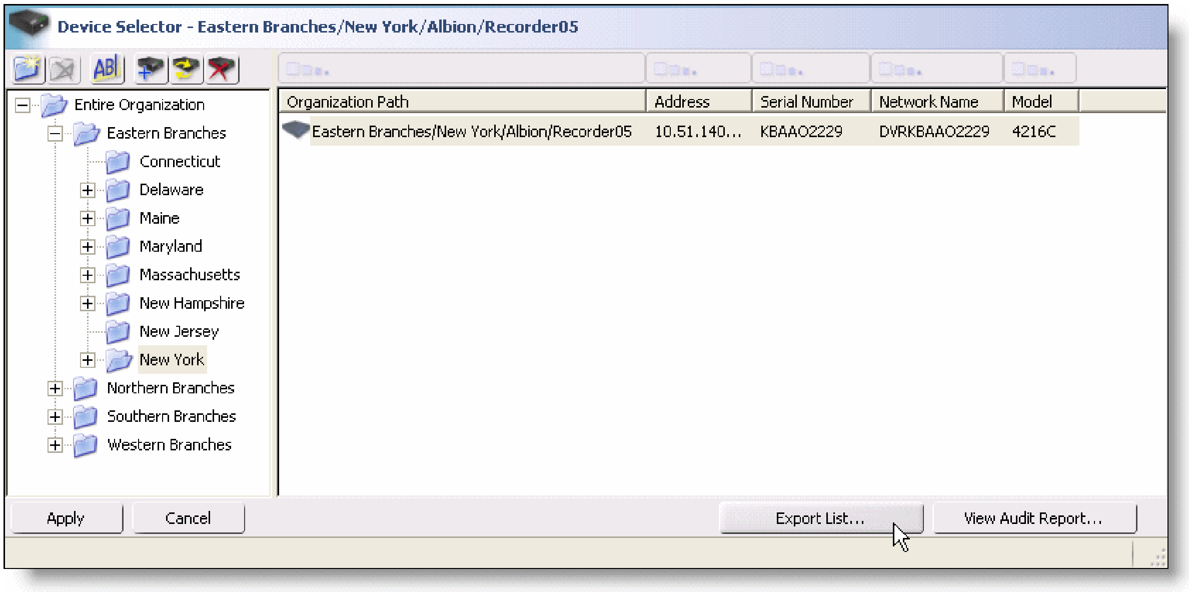
If you are working in a local setting, where your recorders are not managed by an ESM, you must provide the list of recorders to users who will be accessing the recorder using the March Networks software applications, such as the Investigator. If the users do not have this list, they cannot access recorders to perform investigations.

If the list contains dial-up recorders, you must ensure that there is only one dial-up recorder in a folder. If there is more than one dial-up recorder, the March Networks software applications only connect to the first dial-up recorder.

To export the recorder list

1. Ensure the **Device Management** task type is selected.
2. Click **Export List**.

   The **Export Device List** dialog box appears.
3. Navigate to the location where you want to save the list.
4. Type a file name and then click **Save**.



Organization Path	Address	Serial Number	Network Name	Model
Eastern Branches/New York/Albion/Recorder05	10.51.140...	KBAAO2229	DVRKBAAO2229	4216C

Chapter 18

Upgrading Recorder Software

This chapter describes how to upgrade the software running on your recorder. The following topics are covered:

Upgrading Recorder Software

You can upgrade the software running on your recorder to ensure it is running the latest software release.

Use the upgrade file, included on your March Networks CD or provided by a March Networks Customer Care representative, to upgrade the software.

Depending on the release currently running on the unit, you may need to apply several sequential upgrades to bring it to the latest release.

For recorders running Release 5.5 and later, an upgrading license must be installed on each recorder before you can perform a software upgrade. An upgrading license can be used only once, and expires after the software is successfully upgraded. An upgrading license is required for version upgrades only, and not for service packs, patches, or enhancements.

Additional information about the upgrade process, including a list of new features introduced in the release, is available in the upgrade instructions included on your March Networks CD.

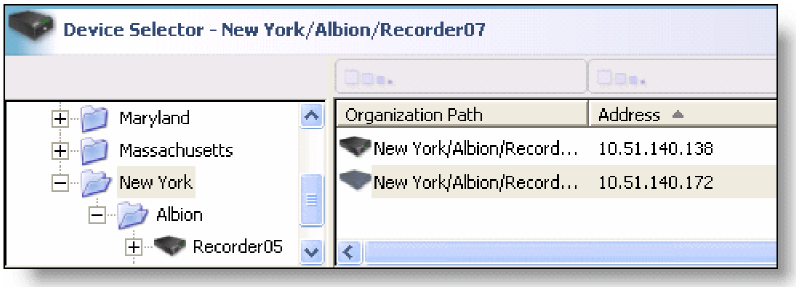
NOTE: The steps outlined in this chapter are typically performed when you are working with locally-managed recorders. If you are working with recorders managed by an ESM, see “Centrally Updating Software” on page 198.

Reviewing a Recorder’s Upgrade Information

The following procedure describes how to review a recorder’s upgrade information.

To review a recorder’s upgrade information

1. Ensure the **Device Update** task type is selected.
2. Click a recorder in the **Device Selector** panel.



Device Selector - New York/Albion/Recorder07

Organization Path	Address
New York/Albion/Record...	10.51.140.138
New York/Albion/Record...	10.51.140.172

3. Review the details outlined in the following table.

Recorder Upgrade Information	Description
Organization Path	Indicates the folders within which the recorder is organized. This path is set up using the **Device Management** task type. For information about organizing recorders, see “Organizing Recorders and Exporting the Recorder List” on page 149.
Address	The IP address of the unit, including the port.
Serial Number	The unique serial number provided to the unit for identification. The serial number also appears on the label on the outside of the recorder.
Network Name	The unit’s network name. The network name is specified using the **Device Configuration** task type on the **General** page. For more information, see “Specifying General Options” on page 37.
Model	The unit model. For example: 4416 represents a 4416 C NVR.
Generation	The generation of the unit model. For example: 1 represents the first generation of the model.
Versions	The version information for the various software components.
Current Release	The version of software currently running on the unit.
Target Release	The version of software you want to run on the unit. This is specified when you apply a software upgrade.
Release Status	Indicates if the unit software is currently at the target release.
Schedule	The name of the unit’s upgrade schedule (if any).
Upgrade Status	The status of the upgrade.

Upgrading a Recorder’s Software

The following procedure describes how to review a recorder’s upgrade information.

To upgrade the software on a recorder

For recorders running Release 5.5 and later, an upgrading license must be installed on each recorder before you perform a software upgrade. An upgrading license can be used only once, and expires after the software is successfully upgraded. An upgrading license is required for version upgrades only, and not for service packs, patches, or enhancements.

1. Ensure the **Device Update** task type is selected.
2. Click a recorder in the **Device Selector** panel.
3. Click **Upgrade Device**.

   The **Upgrade Device** dialog box appears.
4. Click **Browse**.

   The **Select Upgrade File** dialog box appears.
5. Navigate to the location of the upgrade file (.upg) and then click **Open**.

   If a registration key was provided with the file, type the number in the **Registration Key** box within the **Upgrade Device** dialog box.
6. Click **Upgrade**.

   Do not close the Administrator Console during the upgrade. Wait until the upgrade is complete.

   As the upgrade is performed, the status appears in the **Upgrade Status** column.

Chapter 19

Monitoring Health

Recorders report their overall health and operation status. When an issue arises or a system update occurs, the recorder notifies you by sending an alert, which appears in the Administrator Console.

You can configure the Administrator Console to notify you when an alert is received by playing a sound or bringing the Administrator Console application to the front of all other applications on your screen. The recorder's indicators also light up to provide visual notification of the alert at the site.

If your organization uses an ESM to centrally monitor the health of recorders on your network, you can customize alert notification. For more information, see "Customizing Recorder Health Alerts" on page 196.

The following topics are covered in this chapter:

- "Viewing Alert Details and Corrective Actions" on page 160
- "Acknowledging that You Have Reviewed an Alert" on page 161
- "Configuring Notification of Health Alerts" on page 163

Viewing Alert Details and Corrective Actions

The Alert Inbox shows all of the alerts experienced by the recorders you are monitoring, and provides corrective actions you can take.

When field of view monitoring or camera obstruction detection is enabled, warnings are generated to notify you of camera changes or obstructed cameras. For information about responding to field of view alerts and camera obstruction alerts, see "To respond to field of view alerts" on page 71 and "To respond to camera obstruction alerts" on page 75.

To view alert details and corrective actions

1. Ensure the **Health Monitoring** task type is selected.
2. Click an alert in the **Alert Inbox**.
3. Click **Show Details**.
4. Review the alert details and corrective actions. The following table outlines the alert information that appears.

Alert Information	Description
Severity	Indicates whether the alert severity is critical, fault, or a warning.
Organization Path	Indicates the folders within which the recorder is organized. This path is set up using the **Device Management** task type. For information about organizing recorders, see "Organizing Recorders and Exporting the Recorder List" on page 149.
Description	Provides a description of the alert.
Source	Indicates the recorder that triggered the alert.
State	Indicates whether the alert has been resolved. **Note:** Some alerts are automatically resolved when the condition is corrected. For example, alerts about disconnected recorders automatically change to **Resolved** when the connection is restored.
Condition	Indicates whether the alert is new or marked as handled.
First Occurrence	Indicates the time and date of the first occurrence of the issue.
Latest Occurrence	Indicates the most recent time and date of the issue.
Count	Indicates the number of times the issue has occurred.
Exceeded	Indicates which type of threshold has been exceeded.
Duration	Indicates the total amount of time since the first occurrence. **Note:** If the alert has switched between resolved and unresolved several times, the duration represents the total amount of time the alert was in the unresolved state.

To specify the types of alerts that display in the Alert Inbox

1. Ensure the **Health Monitoring** task type is selected.
2. In the **Alert Inbox**, click any of the following buttons:
   - **New** — Displays new, unhandled alerts.
   - **Handled** — Displays handled alerts. Handled alerts represent issues that you are aware of and are in the process of resolving. For example, if you received notification of a hard drive problem, you can mark the alert as handled to indicate that you are in the process of purchasing a new hard drive to be installed in the unit.
   - **1** - **Critical** — Displays critical alerts. Critical alerts occur when the recorder is unable to capture or record audio, video, or text data. For example, you receive a critical alert when the unit cannot record on its hard drives.
   - **2** - **Fault** — Displays faults. Faults occur when a component is unable to function properly, however, the recorder is able to function properly as a whole. For example, you receive a fault when a recorder experiences a loss of video sync, due to a disconnected cable.
   - **3** - **Warning** — Displays warnings. Warnings notify you of system information and minor issues. For example, you receive a warning when the unit's hard drive temperature exceeds system thresholds.

NOTE: If you select multiple buttons, multiple types of alerts display in the Alert Inbox. For example, if you select the **1** - **Critical** button and the **3** - **Warning** button, both critical alerts and warnings display in the **Alert Inbox**.
You can also filter the **Alert Inbox** to view new alerts that you have not reviewed yet, or to view only the alerts that are marked as **Handled**, by clicking the **Refine List** button above the **Condition** column, and then clicking **New** or **Handled**.

Acknowledging that You Have Reviewed an Alert

After you review an alert, you can acknowledge it. When you acknowledge an alert you are indicating that you are aware of the issue and are in the process of resolving it. It remains in the Alert Inbox until the issue is resolved.

To acknowledge that you have reviewed an alert

1. Ensure the **Health Monitoring** task type is selected.
2. Click an alert in the **Alert Inbox**.
3. Click **Mark as Handled**.

   You can also acknowledge that you have reviewed an alert by clicking **Mark as Handled** in the **Show Details** dialog box.

To close an alert and move it to the Alert History

1. Ensure the **Health Monitoring** task type is selected.
2. Click the alert in the **Alert Inbox**.
3. Click **Close Alert**.

   The alert moves to the **Alert History**.

   You can only close an alert when it is marked as Handled and the alert state is Resolved.

   Some alerts are automatically resolved when the issue no longer exists. For example, a video sync lost alert is automatically resolved when the video sync problem is repaired.

NOTE: If you have removed the RS232 and RS485 option cards from the recorder, you will receive a Missing Hardware alert after upgrading the recorder software. Handle and close this alert to remove it from the Administrator Console.

To locate closed alerts in the Alert History

1. Ensure the **Health Monitoring** task type is selected.
2. Click a recorder in the **Device Selector** panel.
3. Under **Alert History**, click a time period in the **Search over the last** list or specify a time period.
4. Click **Begin Search**.

   A list of all closed alerts where the last alert occurrence was within the specified time period appears.

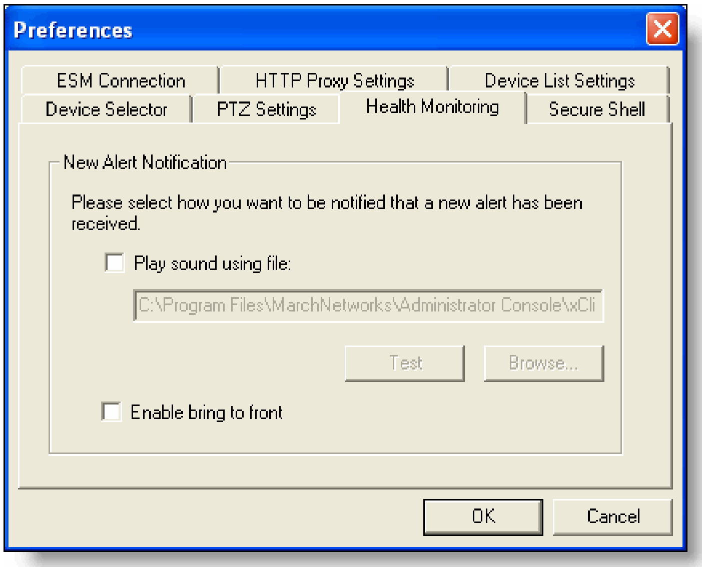
Configuring Notification of Health Alerts

You can configure how you want the Administrator Console to notify you when a new health alert or a change to a current health alert is received.

To configure health alert notification

1. On the **File** menu, click **Preferences**.

   The **Preferences** dialog box appears.
2. Click the **Health Monitoring** tab.



Please select how you want to be notified that a new alert has been received.

☐ Play sound using file:

C:\Program Files\MarchNetworks\Administrator Console\xCli

☐ Enable bring to front

3. If you want the Administrator Console to play a sound file to notify you of a new health alert or a change to a current health alert:
   - Select the **Play sound using file** option.
   - Click **Browse** to select the sound file you want the Administrator Console to play.
   - Click **Test** to listen to the sound file you have selected.
4. If you want to bring the Administrator Console application to the front of all other applications on your screen to notify you of a new health alert or a change to a current health alert, select the **Enable bring to front** option.

   This option will also restore the Administrator Console application from the minimized state in order to bring it to the front of the screen, if necessary.
5. Click **OK**.

Chapter 20

Configuring Alarm Monitoring

If your organization uses the Live Monitoring Console to monitor alarms in real time using the application's Alarm Inbox, you can use the Administrator Console to specify the alarm monitoring settings.

The following topics are covered in this chapter:

- "Choosing the Alarms that are Monitored" on page 166
- "Setting the Alarm Priority" on page 167
- "Associating Cameras with Alarm Sources" on page 168
- "Configuring Alarm Monitoring Settings: ESM Environment" on page 170

Choosing the Alarms that are Monitored

Before alarms can be monitored using the Live Monitoring Console, you must choose one or more alarms and specify the trigger states that you want to monitor.

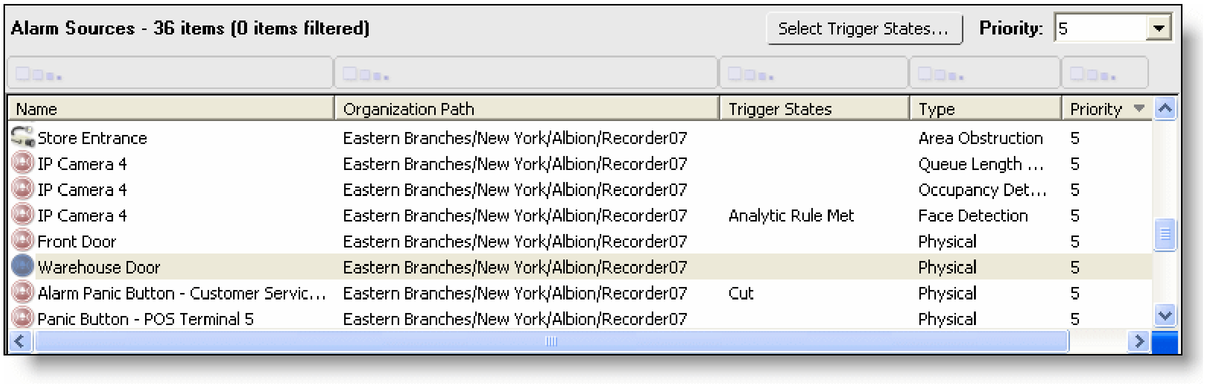
The trigger state is a condition that, when the alarm enters the condition, causes the Live Monitoring Console to automatically present the alarm for investigators to respond to. For example, a door contact alarm typically has an open, closed, and cut state. If you want investigators to be notified when the door is opened, you can choose the open state as the trigger state.

If you do not select at least one trigger state, the alarm source will not be monitored.

If a recorder at a selected site is unavailable, the corresponding alarm sources are unavailable.

To select trigger states that are monitored

1. Ensure the **Alarm Management** task type is selected.
2. In **My Sites**, navigate to and then click a site.
3. In the **Alarm Sources** list, click an alarm source.



Alarm Sources - 36 items (0 items filtered)

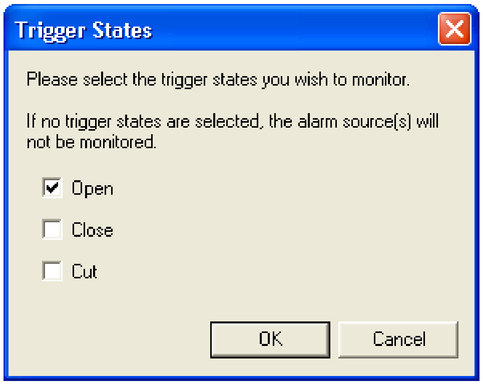
Priority: 5

Name	Organization Path	Trigger States	Type	Priority
Store Entrance	Eastern Branches/New York/Albion/Recorder07		Area Obstruction	5
IP Camera 4	Eastern Branches/New York/Albion/Recorder07		Queue Length ...	5
IP Camera 4	Eastern Branches/New York/Albion/Recorder07		Occupancy Det...	5
IP Camera 4	Eastern Branches/New York/Albion/Recorder07	Analytic Rule Met	Face Detection	5
Front Door	Eastern Branches/New York/Albion/Recorder07		Physical	5
Warehouse Door	Eastern Branches/New York/Albion/Recorder07		Physical	5
Alarm Panic Button - Customer Servic...	Eastern Branches/New York/Albion/Recorder07	Cut	Physical	5
Panic Button - POS Terminal 5	Eastern Branches/New York/Albion/Recorder07		Physical	5

4. Click **Select Trigger States**.

   The **Trigger States** dialog box appears.

5. Select the check boxes that correspond to the trigger states that you want to monitor.



Please select the trigger states you wish to monitor.

If no trigger states are selected, the alarm source(s) will not be monitored.

☑ Open

□ Close

□ Cut

6. Click **OK**.
7. Click **Apply**.

Setting the Alarm Priority

You can assign a priority to an alarm to help investigators determine the order in which to respond to alarms using the Live Monitoring Console. Priorities can be assigned from 1 (highest) to 10 (lowest).

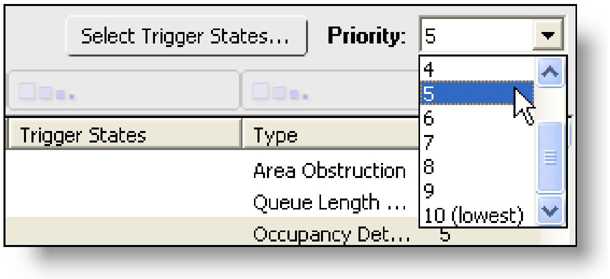
The following example provides a scenario where alarm priorities can be used:

Scenario	Investigators are monitoring several alarm sources at your bank branch, including door contacts, panic buttons, and motion alarms.
Problem	The bank branch is very busy during the morning, with several customers entering the lobby and bank employees entering and exiting the vault.
Resolution	To help investigators monitor alarms, assign different priorities to the various alarms at the bank branch: • **Priority 1.** Panic button alarms • **Priority 2**. Vault alarms generated when the door is opened or closed • **Priority 3**. Motion detection alarms

To set the alarm priority

1. Ensure the **Alarm Management** task type is selected.
2. In **My Sites**, navigate to and then click a site.
3. In the **Alarm Sources** list, click an alarm source.

4. In the **Priority** list, click a priority. You can assign the same priority to multiple alarm sources.



5. Click **Apply**.

Associating Cameras with Alarm Sources

To ensure that video is available when an alarm occurs, you can associate one or more cameras with each alarm source.

After you associate one or more cameras with an alarm source, you can set a primary camera for the alarm. When investigators respond to the alarm in the Live Monitoring Console, video from the primary camera automatically appears. In addition, thumbnail previews from the primary camera appear when the investigator selects a related alarm in the Live Monitoring Console’s **Alarm Inbox**.

If an alarm source is an analytics feature, for example, area obstruction or video motion detection, a camera is associated with the alarm source by default; this association cannot be modified.

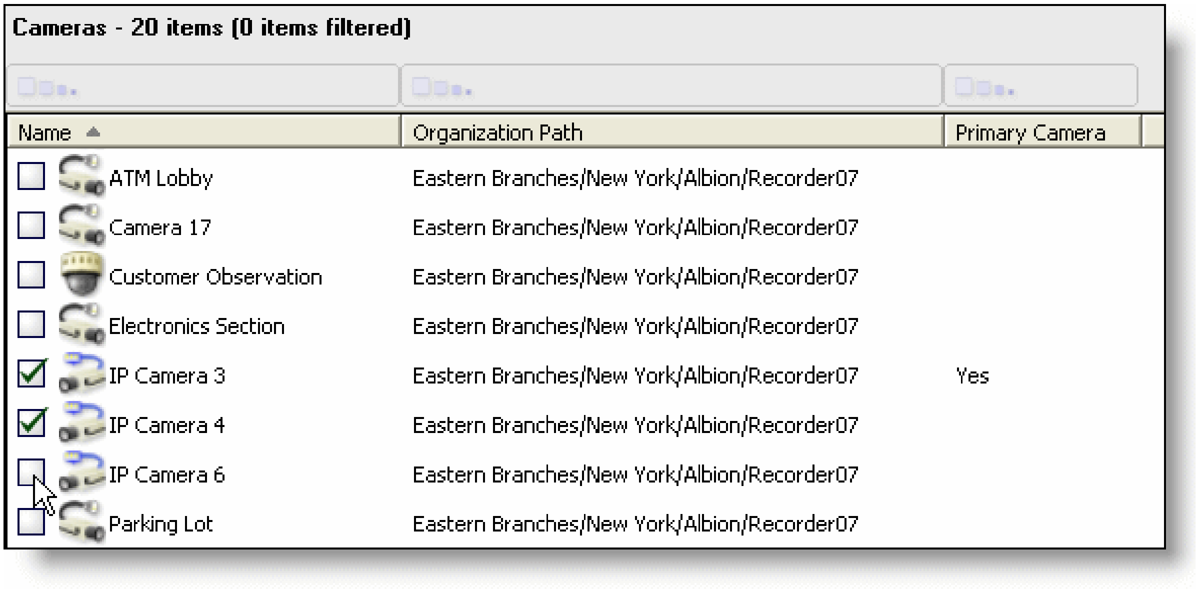
If a recorder at a selected site is unavailable, the corresponding cameras are not available.

It is often useful to associate more than one camera with an alarm to provide additional coverage when an alarm occurs.

To associate a camera with an alarm source

1. Ensure the **Alarm Management** task type is selected.
2. In **My Sites**, navigate to and then click a site.
3. In the **Alarm Sources** list, click an alarm source.

4. In the **Cameras** list, select the check boxes that correspond to the cameras you want to associate with the alarm source.



Cameras - 20 items (0 items filtered)

Name ▲	Organization Path	Primary Camera
□ ATM Lobby	Eastern Branches/New York/Albion/Recorder07	
□ Camera 17	Eastern Branches/New York/Albion/Recorder07	
□ Customer Observation	Eastern Branches/New York/Albion/Recorder07	
□ Electronics Section	Eastern Branches/New York/Albion/Recorder07	
☑ IP Camera 3	Eastern Branches/New York/Albion/Recorder07	Yes
☑ IP Camera 4	Eastern Branches/New York/Albion/Recorder07	
□ IP Camera 6	Eastern Branches/New York/Albion/Recorder07	
□ Parking Lot	Eastern Branches/New York/Albion/Recorder07	

5. Click **Apply**.

   To confirm that you have selected the correct camera, you can view live video or a video image from a selected camera by clicking View Live or View Image.

To set a primary camera

1. Ensure the **Alarm Management** task type is selected.
2. In **My Sites**, navigate to and then click a site.
3. In the **Alarm Sources** list, click an alarm source.
4. In the **Cameras** list, click an associated camera.

   A camera has been associated with an alarm source if the corresponding check box is selected.
5. Click **Set As Primary**.
6. Click **Apply**.

Configuring Alarm Monitoring Settings: ESM Environment

When you are working with a recorder that is centrally monitored and maintained by an ESM, there are additional options that you can configure.

Configuring Alarm Monitoring Settings for Managed Recorders

When you are working in a managed environment, and you have the Alarm Management service installed and activated, you can configure alarm monitoring settings for all sites with recorders managed by the ESM, including:

- Specifying the amount of media to download for an alarm
- Creating filters to limit the alarms that are sent to investigators
- Specifying the number of alarms that an investigator can respond to
- Specify the length of time to keep response logs

For information about activating services, see "Activating ESM Services" on page 184.

To specify the amount of media to download for an alarm

If investigators are currently monitoring alarms using the March Networks alarm monitoring applications, such as the Live Monitoring Console, changes to the pre-alarm and post-alarm durations do not take effect until the application disconnects from the ESM and reconnects.

The download of alarm video is stopped when the post-alarm duration is reached, or when operators click the Finish button in the Live Monitoring Console.

1. Ensure the **Alarm Management** task type is selected.
2. Click **ESM Alarm Management Settings**.

   The **ESM Alarm Management Settings** dialog box appears.
3. Under **Recorded Media Download**, do any of the following:
   - Specify the duration of downloaded video for an alarm by typing or selecting a duration in the **Pre-alarm** and **Post-alarm** boxes.
   - Include linked audio with the downloaded video for an alarm by selecting the **Include Linked Audio** check box.

To create filters to limit the alarms that are sent to investigators

1. Ensure the **Alarm Management** task type is selected.
2. Click **ESM Alarm Management Settings**.

   The **ESM Alarm Management Settings** dialog box appears.
3. Under **Policies**, click one of the following options in the **Alarm Filter** list:
   - **No Filter.** Users receive all monitored alarms in the Alarm Inbox.
   - **One Alarm per Source.** Users only receive one monitored alarm per source. New alarms are not sent to the Alarm Inbox until the existing alarm is finished.
   - **One Alarm per Site.** Users only receive one monitored alarm per site. New alarms are not sent to the Alarm Inbox until the existing alarm is finished.
4. Click **OK**.

To specify the number of alarms that an investigator can respond to

1. Ensure the **Alarm Management** task type is selected.
2. Click **ESM Alarm Management Settings**.

   The **ESM Alarm Management Settings** dialog box appears.
3. Under **Policies**, select the **Restrict users from responding to more than one alarm at a time** check box.
4. Click **OK**.

To specify the length of time to keep response logs

1. Ensure the **Alarm Management** task type is selected.
2. Click **ESM Alarm Management Settings**.

   The **ESM Alarm Management Settings** dialog box appears.
3. Under **Policies**, type or select a duration in the **Keep response log for** box.
4. Click **OK**.

To set up e-mail notification of alarms

To set up e-mail notification, ensure the e-mail server settings for the ESM have been properly configured. For information about configuring e-mail server settings, see “Setting Up E-mail Notification” on page 186.

To specify multiple e-mail addresses, separate each address with a semicolon (;).

1. Ensure the **Alarm Management** task type is selected.
2. Click **ESM Alarm Management Settings**.

   The **ESM Alarm Management Settings** dialog box appears.
3. Select the **Send E-mail Notification of Each Alarm** check box.
4. Type an e-mail address in the **E-mail address** box.

Viewing Alarm Responses in the ESM Response Log

The ESM maintains a history of alarm monitoring activities performed by Live Monitoring Console users and administrators, and also tracks system information. You can view the ESM response log to obtain information about these activities.

To view alarm responses

1. Ensure the **Alarm Management** task type is selected.
2. Click **Search ESM Response Log**.

   The **ESM Response Log** dialog box appears.
3. Click one of the following time ranges in the **Select a time range** list:
   - **On or About**. Searches for entries before and after the date, time, and duration you specify.

     If you click **On or About**, specify a date in the **this date** calendar, type or select a time in the **and this time** box, and type or select a duration in the **and for this duration** box.
   - **Starting at**. Searches for entries starting on the date and at the time and duration you specify.

     If you click **Starting at**, specify a date in the **this date** calendar, type or select a time in the **and this time** box, and type or select a duration in the **and for this duration** box.
   - **On the Day with**. Searches for entries on the date you specify.

     If you click **On the Day with**, specify a date in the **this date** calendar.
   - **In the Last**. Searches for entries within the time period you specify.

     If you click **In the Last**, type or select a duration in the **and for this duration** box.
   - **Older than**. Searches for entries older than the date and time you specify.

     If you click **Older than**, specify a date in the **this date** calendar, and type or select a time in the **and this time** box.
4. Click **Search**.

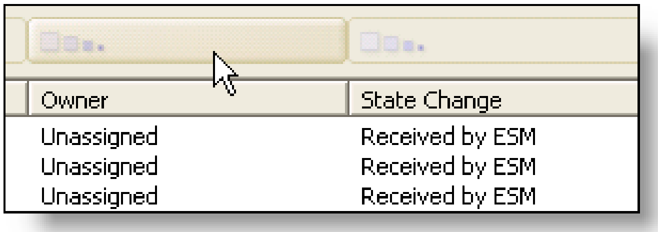
   A list of alarm responses appears.

   A search yields a maximum of 1000 results. If the results exceed this number, the 1000 oldest results are shown.

   For alarms triggered by IP cameras or encoders, two alarm responses will appear: **Triggered by device** (to indicate when the IP camera or encoder triggered the alarm) and **Received by ESM** (to indicate when the ESM received the alarm).

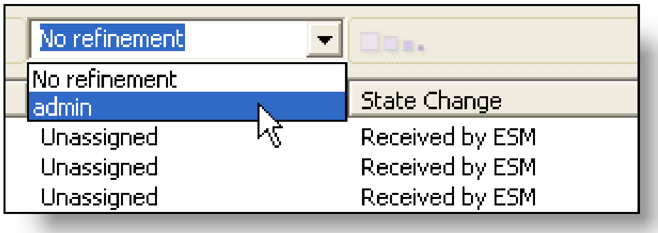
To refine the list of alarm responses

1. In the list of search results within the **ESM Response Log** dialog box, click a result.
2. Click a **Refine List** button above the column you want to refine.



Owner	State Change
Unassigned	Received by ESM
Unassigned	Received by ESM
Unassigned	Received by ESM

3. In the refinement list that appears, type or select a refinement option.



Owner	State Change
Unassigned	Received by ESM
Unassigned	Received by ESM
Unassigned	Received by ESM

NOTE: To clear the refinement, click a refinement list and then click No Refinement. Repeat this task for any other refined columns.

To view alarm response details

1. Ensure the **Alarm Management** task type is selected.
2. In the list of search results within the **ESM Response Log** dialog box, click a result that has an alarm ID and then click **View Response Details**.

To print, copy, or export the search results list

In the **ESM Response Log** dialog box, click **Print**, **Copy**, or **Export**.

To print, copy, or export the entire list, ensure that no items are selected and then click **Print**, **Copy**, or **Export**.

Chapter 21

Troubleshooting the Network Connection and Rebooting Recorders

This chapter describes how to open an external application directly from the Administrator Console to troubleshoot the network connection of a recorder. Using this option automatically exports the information of the selected recorder to the specified software application.

If you encounter problems with a recorder, or if instructed by your March Networks Customer Care representative, you can reboot the unit. When you reboot the unit, it shuts down and then restarts.

The following topics are covered in this chapter:

- "Viewing the Network Communication Path" on page 176
- "Pinging a Recorder" on page 176
- "Configuring a Unit Using the Provisioning Interface" on page 177
- "Rebooting a Recorder" on page 179

Viewing the Network Communication Path

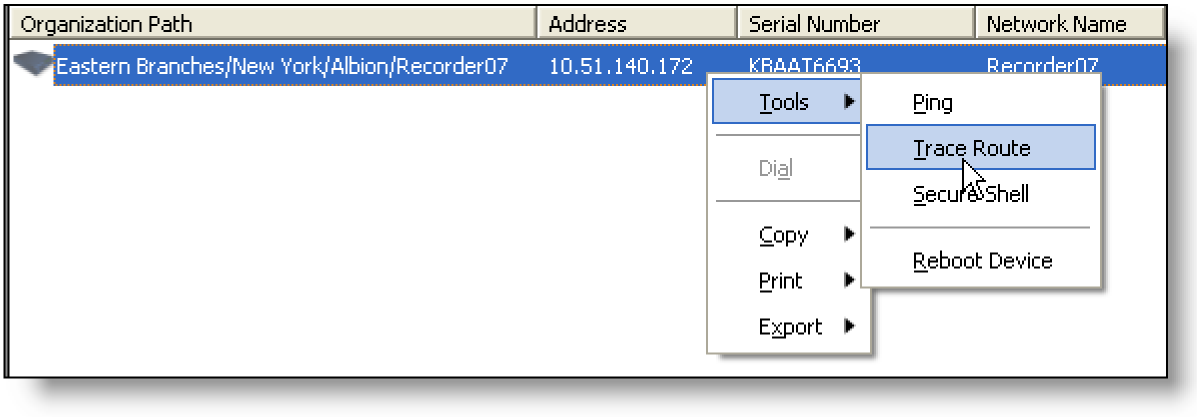
You can open the traceroute utility from the Administrator Console to view the network path through which network communication flows.

For information about using the traceroute utility (tracert), see the documentation accompanying the Microsoft Windows operating system.

To view the network communication path

1. Ensure the **Device Installation**, **Device Configuration**, **Device Management**, **Health Monitoring**, or **Device Update** task type is selected.
2. Click a recorder in the **Device Selector** panel.
3. Right-click the recorder, point to **Tools**, and then click **Trace Route**.

   The **Windows Command Prompt** window opens, and shows information about the network communication path.



Organization Path	Address	Serial Number	Network Name
Eastern Branches/New York/Albion/Recorder07	10.51.140.172	KBAAT6693	Recorder07

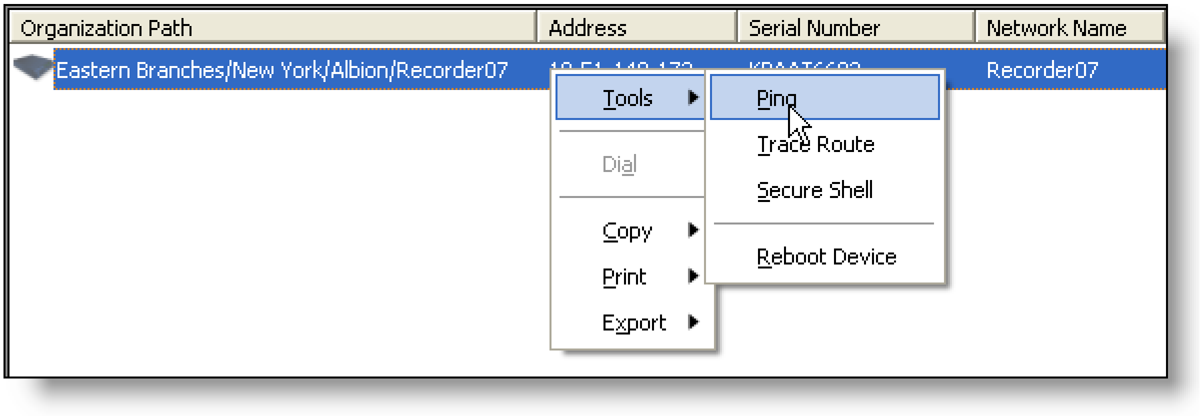
Pinging a Recorder

You can ping a recorder to ensure it is connected to the network and to obtain the network settings using the Microsoft Windows ping utility. For information about working with the ping utility, see the documentation accompanying the Microsoft Windows operating system.

To ping a recorder

1. Ensure the **Device Installation**, **Device Configuration**, **Device Management**, **Health Monitoring**, or **Device Update** task type is selected.
2. Click a recorder in the **Device Selector** panel.
3. Right-click the recorder, point to **Tools**, and then click **Ping**.

The **Windows Command Prompt** window opens, and shows the response to the ping.



Organization Path	Address	Serial Number	Network Name
Eastern Branches/New York/Albion/Recorder07	[illegible]	[illegible]	Recorder07

Configuring a Unit Using the Provisioning Interface

You can log on to the recorder's built-in provisioning interface from the Administrator Console using an SSH client, such as PuTTY. The provisioning interface is a tool that lets you view and configure the recorder's general settings.

Before you try to access a recorder using an SSH client, you must:

- Ensure you have an SSH client installed on your computer. If you do not have an SSH client installed on your computer, contact your IT department.
- Specify the location of the SSH client using the Administrator Console's Preferences dialog box.
- Specify the Application Command Line Arguments. You perform this task when you are working with an SSH client that requires more than just the unit's IP address to establish a connection with the unit. For example, some SSH clients may require you to preface the IP address with an identifier.

For information about using the provisioning interface, see the *Provisioning Interface Technical Instructions* included on your March Networks CD.

To specify the location of the SSH client on your computer

1. On the **File** menu, click **Preferences**.

   The **Preferences** dialog box appears.
2. Click the **Secure Shell** tab.
3. Under **Full Path to Secure Shell Location**, click **Browse**.

   The **Select Secure Shell Application** dialog box appears.
4. Navigate to the location of the SSH client, click the SSH client (.exe), and then click **Open**.
5. Click **OK**.

To specify the application command line arguments

1. On the **File** menu, click **Preferences**.

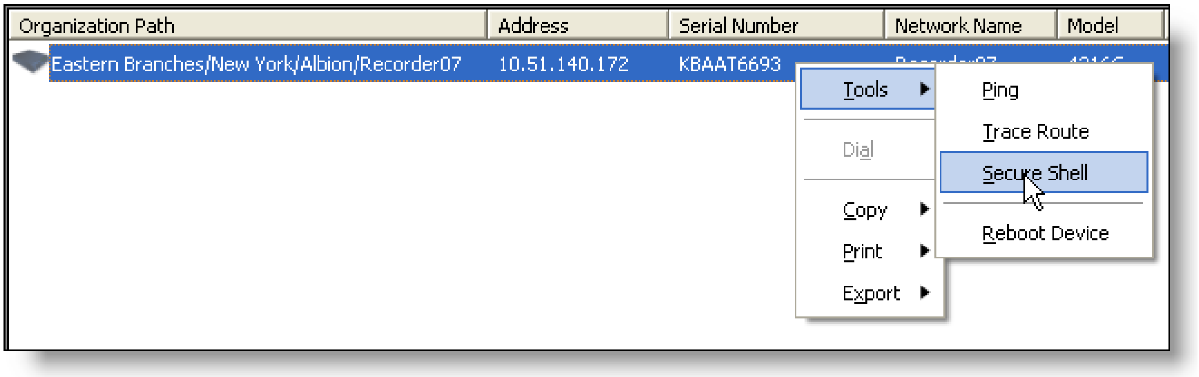
   The **Preferences** dialog box appears.
2. Click the **Secure Shell** tab.
3. Under **Application Command Line Arguments**, type one or more command line arguments. These command line arguments will be sent to the SSH client when it starts.
4. Click **OK**.

NOTE: [IP] appears automatically under **Application Command Line Arguments**. This command line argument allows the Administrator Console to send the recorder's IP address to the SSH client when the SSH client starts. If you are using PuTTY, which is a common secure shell client, leave **[IP]** in the **Application Command Line Arguments** section to allow PuTTY to communicate with the recorder. If you prefer to manually specify the IP address when the SSH client starts, you can delete **[IP]** from the box.

To access a secure shell client

1. Ensure the **Device Installation**, **Device Configuration**, **Device Management**, **Health Monitoring**, or **Device Update** task type is selected.
2. Click a recorder in the **Device Selector** panel.
3. Right-click the recorder, point to **Tools**, and then click **Secure Shell**.

   The SSH client starts.
4. When prompted, specify **radmin** as the user name, and then type the password for the radmin user account. By default, the password is **radmin**. If you are unsure of the password, contact your administrator.



Organization Path	Address	Serial Number	Network Name	Model
Eastern Branches/New York/Albion/Recorder07	10.51.140.172	KBAAT6693		

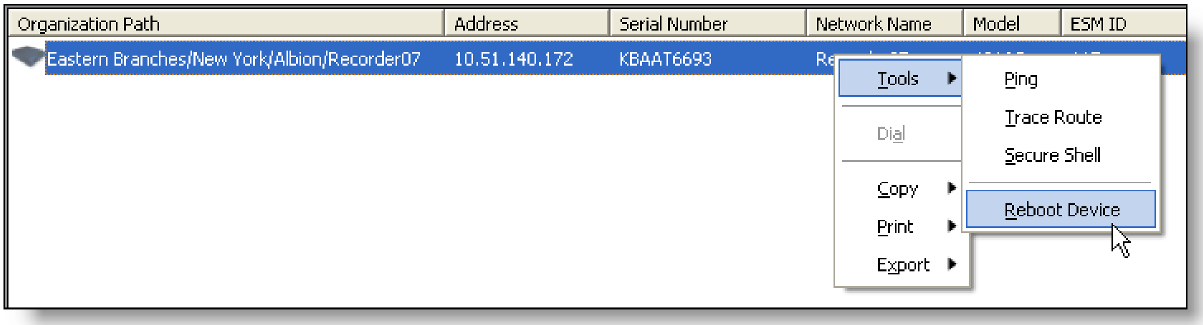
Rebooting a Recorder

If you encounter problems with a recorder, or if instructed by your March Networks Customer Care representative, you can reboot the unit. When you reboot the recorder, it shuts down and then restarts.

To reboot a recorder

1. Ensure the **Device Installation**, **Device Configuration**, **Device Management**, **Health Monitoring**, or **Device Update** task type is selected.
2. Click a recorder in the **Device Selector** panel.
3. Right-click the recorder, point to **Tools**, and then click **Reboot Device**.

   The recorder reboots.



Organization Path	Address	Serial Number	Network Name	Model	ESM ID
Eastern Branches/New York/Albion/Recorder07	10.51.140.172	KBAAT6693	Re		

Chapter 22

Performing Advanced Enterprise Service Manager Tasks

The ESM is a central management tool that maintains communication with recorders on your network to obtain up-to-date health and status information from a single location. The ESM runs on one or more dedicated server computers in a central network location.

The following topics are covered in this chapter:

- "Reviewing General ESM Information" on page 182
- "Adding a Server to Provide Redundant Support" on page 183
- "Activating ESM Services" on page 184
- "Configuring ESMs to Route through Firewalls" on page 185
- "Setting Up E-mail Notification" on page 186
- "Adding Licenses" on page 187
- "Creating User Profiles and Accounts" on page 188
- "Viewing the ESM Audit Report" on page 192
- "Viewing the Recorder Audit Report" on page 194
- "Registering and Unregistering Recorders With an ESM" on page 195
- "Customizing Recorder Health Alerts" on page 196
- "Centrally Updating Software" on page 198

- “Specifying the Server Connection Order” on page 208
- “Replacing Recorders” on page 209

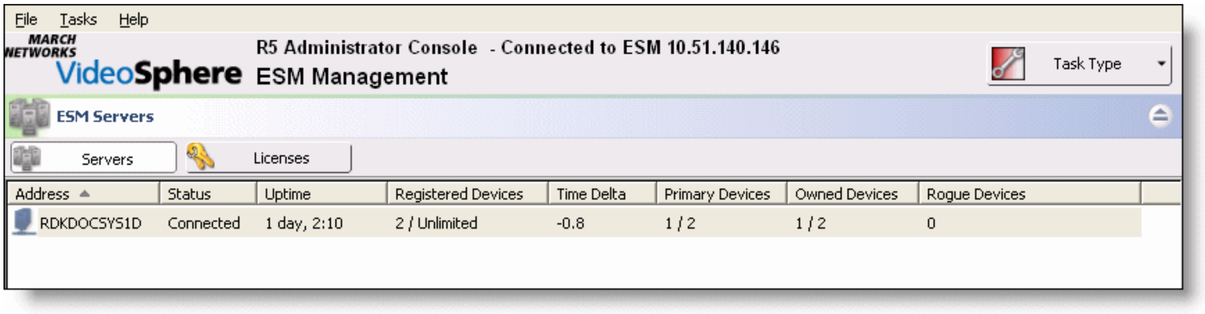
Reviewing General ESM Information

When the ESM Management task type is selected, you can review the general information detailed below for each ESM server.

To review the ESM’s general information

1. Ensure the Administrator Console is connected to the ESM.

   For more information, see “Connecting to an ESM” on page 16.
2. Ensure the **ESM Management** task type is selected.
3. Click an ESM server in the **ESM Servers** list.



R5 Administrator Console - Connected to ESM 10.51.140.146
ESM Management

Address	Status	Uptime	Registered Devices	Time Delta	Primary Devices	Owned Devices	Rogue Devices
RDKDOCSYS1D	Connected	1 day, 2:10	2 / Unlimited	-0.8	1 / 2	1 / 2	0

4. Review the details outlined in the following table.

General ESM Information	Description
Address	The server’s IP address or network name.
Status	The server connection status, such as connected or disconnected.
Uptime	The amount of time the server has been online.
Registered Devices	The number of recorders that are configured to communicate with the server and the total number of allowed connections. *
Time Delta	The time difference between the server’s clock and your computer’s clock, in seconds. When **+** appears, the server’s clock is ahead of your computer’s clock by the number of seconds that appear. When **-** appears, the server’s clock is behind your computer’s clock.
Primary Devices	The number of recorders for which the server is configured as the main server for connection. For information about specifying the primary server, see “Specifying the Server Connection Order” on page 208.
Owned Devices	The number of recorders that are configured to communicate with the server.

General ESM Information	Description
Rogue Devices	The number of recorders that are communicating with the server, but do not have the server specified as their primary server. **Note:** If a rogue recorder appears, we recommend you verify that the network connection between the recorder and the primary server is functioning properly.
*The maximum number of connections is determined by the license installed on the server. For more information, see "Adding Licenses" on page 187.	

Adding a Server to Provide Redundant Support

You can add additional servers to the ESM to provide redundancy for your connected recorders and increase the number of recorders that the ESM can manage.

When additional servers are added, an ESM cluster is formed, which provides redundant support for connected recorders. If a server encounters a problem, for example it loses network connectivity and cannot manage its connected recorders, another server in the list manages those recorders. When the server comes back online, it resumes management of its recorders.

You must add licenses to the primary ESM when you create an ESM cluster. If you are creating a cluster of two ESMs (the primary ESM and one secondary ESM), you must install the R5 ESM Professional license. If you are creating a cluster of three or more ESMs, you must install both the R5 ESM Professional license and the R5 ESM Cluster Service license.

NOTE: When you add a new server, ensure it is configured for NTP clock synchronization. All of the servers within the ESM must be synchronized by the same NTP server to ensure that they are set to the same time.

To add an additional server

1. Install the ESM software on the additional server.

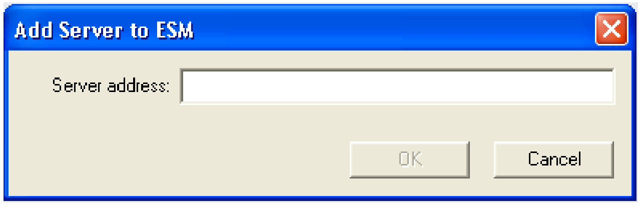
   For more information, see the *ESM Installation Guide* included on your March Networks CD.
2. Ensure the Administrator Console is connected to the primary ESM.

   For more information, see "Connecting to an ESM" on page 16.
3. Ensure the **ESM Management** task type is selected.
4. Click an ESM server in the **ESM Servers** list.
5. Click **Add Server.**

   The **Add Server to ESM** dialog box appears.
6. Type the ESM IP address or network name in the **Server address** box.
7. Click **OK**.

   The ESM server appears in the **ESM Servers** list.

8. Ensure the computers with the installed ESMs can communicate with one another by using the **ping** command.
9. Review the ESM's status to confirm that it is connected; see "To review the ESM's general information" on page 182.



Activating ESM Services

You can install services on the ESM to make additional features available. After services are installed and activated, you can launch the corresponding application to take advantage of the new features. Services are installed on the ESM using the March Networks CD provided at the time of purchase.

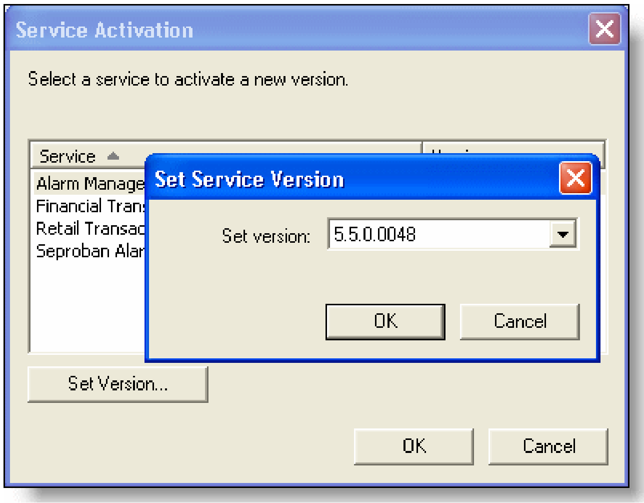
To activate an ESM service

1. Ensure the Administrator Console is connected to the ESM.

   For more information, see "Connecting to an ESM" on page 16.
2. Ensure the **ESM Management** task type is selected.
3. Click an ESM server in the **ESM Servers** list.
4. Click **Services**.

   The **Service Activation** dialog box appears.
5. Click a service and then click **Set Version**.

   The **Set Service Version** dialog box appears.
6. Click the latest software version in the **Set version** list.


Select a service to activate a new version.

Set version: 5.5.0.0048

Configuring ESMs to Route through Firewalls

When you are working with servers that are located behind a firewall or are installed on an internal network, you may have to configure the firewall with IP addresses so the managed recorders or clients are able to contact all of the servers within the ESM.

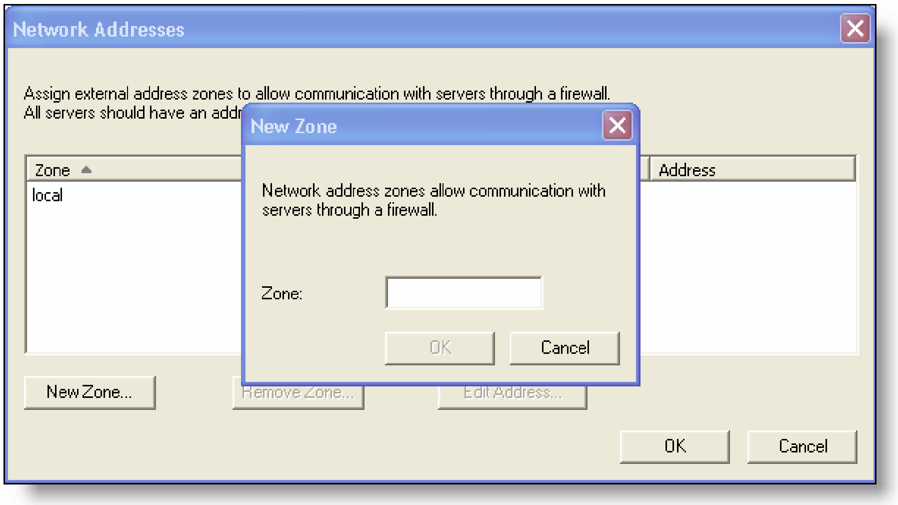
To configure the ESM to route through a firewall

1. Ensure the Administrator Console is connected to the ESM.

   For more information, see “Connecting to an ESM” on page 16.
2. Ensure the **ESM Management** task type is selected.
3. Click an ESM server in the **ESM Servers** list.
4. Click **Addresses**.

   The **Network Addresses** dialog box appears.
5. Click **New Zone**.

   The **New Zone** dialog box appears.
6. Type the IP address and port that are used to access the server through the firewall.


Network Addresses

Assign external address zones to allow communication with servers through a firewall.
All servers should have an addr

New Zone

Network address zones allow communication with servers through a firewall.

Zone:

Zone	Address
local	

TIP: You can also edit a network address by clicking an address zone, clicking a server, clicking **Edit Address**, and, in the **Edit Address** dialog box, modifying the address in the **Address** box.

Setting Up E-mail Notification

The recorder reports its overall health and operation status. When an issue arises or a system update occurs, the recorder notifies you by sending an alert, which appears in the Administrator Console.

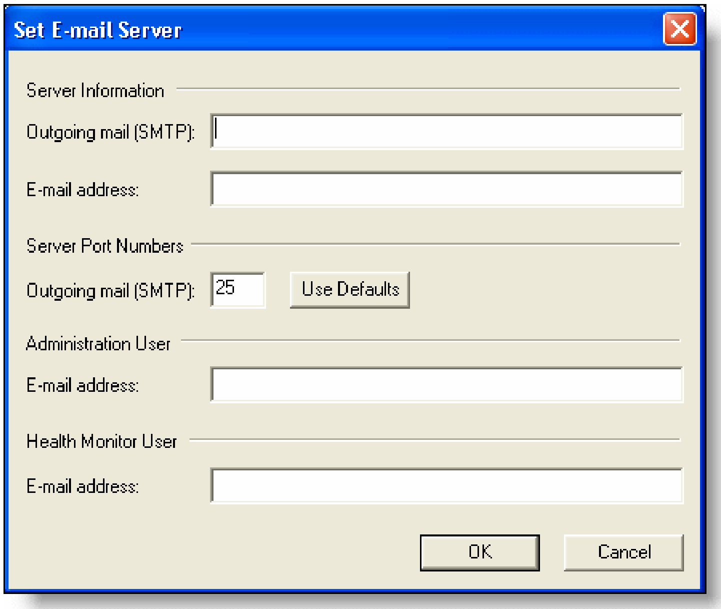
You can configure the ESM to notify the appropriate people in your organization through e-mail when alerts occur. Before the ESM can communicate through e-mail, you must specify the e-mail server used by the ESM.

To set up e-mail notification

1. Ensure the Administrator Console is connected to the ESM.

   For more information, see “Connecting to an ESM” on page 16.
2. Ensure the **ESM Management** task type is selected.
3. Click an ESM server in the **ESM Servers** list.
4. Click **E-mail Server**.

   The **Set E-mail Server** dialog box appears.
5. Specify the e-mail server settings outlined in the following table and click **OK**.



E-mail Server Setting	Description
Server Information	
Outgoing mail (SMTP)	The e-mail server that the ESM uses to send alert notification e-mails. **Note:** This information is provided by your Internet Service Provider (ISP) or can be obtained from your IT department.

E-mail Server Setting	Description
E-mail address	The e-mail address that is used to identify the ESM as the sender of alert notification e-mails.
Server Port Numbers	
Outgoing mail (SMTP)	The Simple Mail Transfer Protocol (SMTP) port of your outgoing e-mail server. **Note:** This information is provided by your ISP or can be obtained from your IT department. **Tip:** You can reset the port number to 25 by clicking **Use Defaults**.
Administration User	
E-mail address	The e-mail address to which you want the ESM to send information about ESM problems. **Tip:** To specify multiple e-mail addresses, separate e-mail addresses using a semicolon (;).
Health Monitor User	
E-mail address	The e-mail address to which you want the ESM to send recorder alerts, such as problems and status change notifications. **Tip:** To specify multiple e-mail addresses, separate e-mail addresses using a semicolon (;).

Adding Licenses

If you have purchased an ESM license, you can add it to the ESM. After you add the license, you can apply it to your recorders to make additional features available.

Licenses are available for purchased features, and allow you to:

- Enable video analytics on recorders.
- Increase the number of simultaneous recorder connections that can be made (the default is five).
- For recorders running Release 5.5 (and later) of the recorder software, upgrade the recorder’s software.

For information about purchasing licenses, contact your March Networks Certified Solutions Provider.

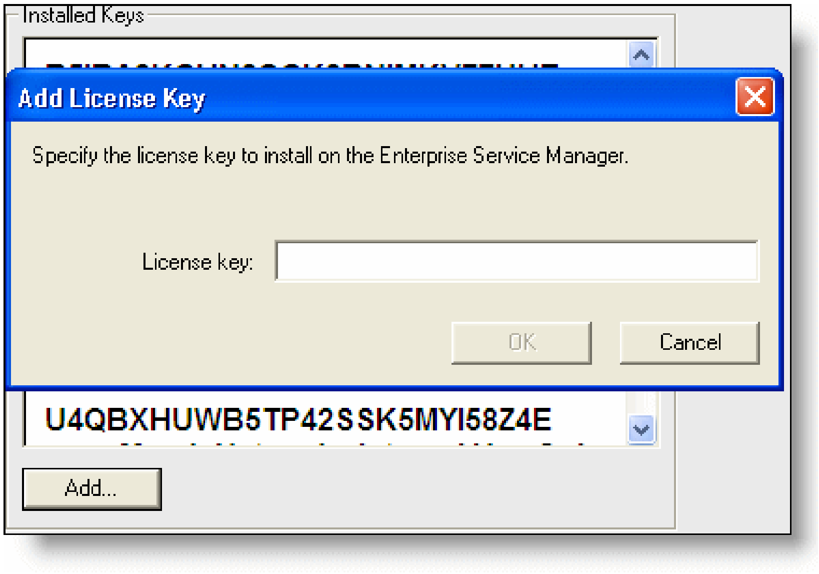
To add a license

1. Ensure the Administrator Console is connected to the ESM.

   For more information, see “Connecting to an ESM” on page 16.
2. Ensure the **ESM Management** task type is selected.
3. Click **Licenses**.
4. Under **Installed Keys**, click **Add**.

   The **Add License Key** dialog box appears.

5. In the **License Key** box, type the license key.



Installed Keys
Add License Key
Specify the license key to install on the Enterprise Service Manager.
License key:
OK
Cancel
U4QBXHUWB5TP42SSK5MYI58Z4E
Add...

Creating User Profiles and Accounts

You can manage the system's users by controlling the application areas they are allowed to use. You can also restrict users by giving them access to particular recorders. To do so, you must create user profiles and accounts.

The following example provides a scenario where you might restrict user access:

Scenario	Your retail store has three main user types: loss prevention officers, store managers, and system administrators. Each type of user has a unique requirement for accessing the recorder. The loss prevention officer wants to locate video evidence; the store manager wants to review video evidence and monitor cameras; the system administrator is interested in installing, configuring, and monitoring the status of the recorder, in addition to setting up user accounts.
Problem	You do not want to provide the loss prevention officer and store manager with unlimited access to the recorder, as this provides them with the ability to change the recorder's configuration settings. However, you do want the system administrator to be able to access all elements of the system.
Resolution	Create three user profiles and specify which applications and tools can be accessed: a Loss Prevention Officer profile, a Store Manager profile, and a System Administrator profile. Customize each profile to specify the applications and tools the users can access.

To create a user profile

When you assign or unassign tasks for a user profile, and a user with that user profile is currently using the affected software application, the changes do not take effect until the user logs off from the ESM and then logs back on.

1. Ensure the Administrator Console is connected to the ESM.

   For more information, see “Connecting to an ESM” on page 16.

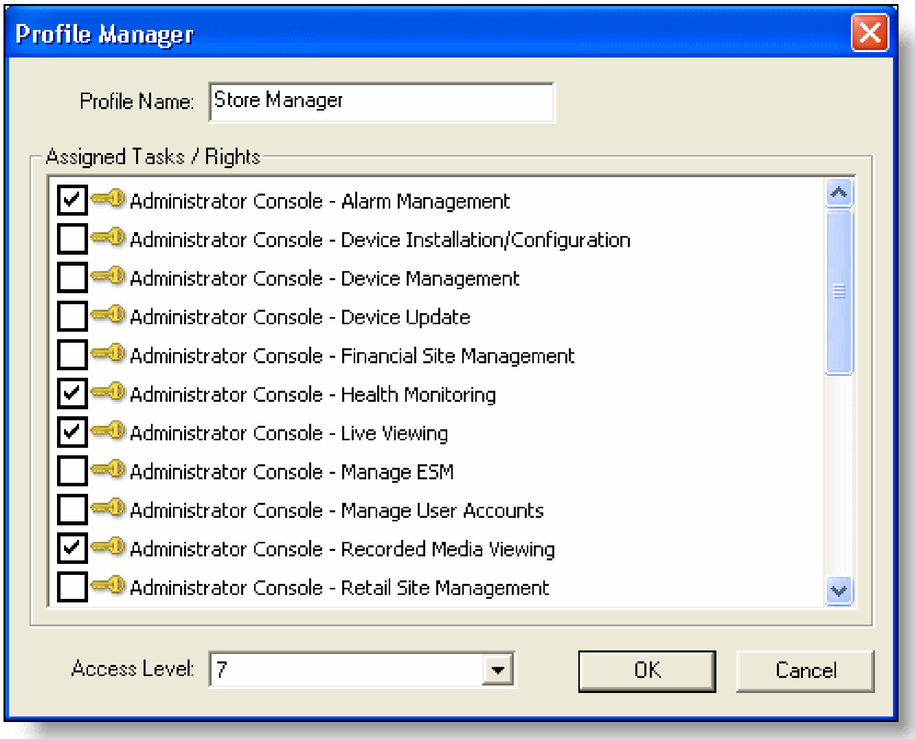
2. Ensure the **User Management** task type is selected.
3. Click **Add Profile.**

   The **Profile Manager** dialog box appears.

4. Type a profile name in the **Profile Name** box.
5. Under **Assigned Tasks/Rights**, select the check boxes that correspond to the tasks and rights you want users to access.
6. In the **Access Level** list, click an authorization level to restrict access to specific recorders and peripherals.

   Users can access recorders or peripherals set to an equivalent or lower number. For example, when you set the access level to five, users can access recorders and peripherals set to five or lower.

7. Click **OK**.



Profile Name: Store Manager

Assigned Tasks / Rights

☑ Administrator Console - Alarm Management
☐ Administrator Console - Device Installation/Configuration
☐ Administrator Console - Device Management
☐ Administrator Console - Device Update
☐ Administrator Console - Financial Site Management
☑ Administrator Console - Health Monitoring
☑ Administrator Console - Live Viewing
☐ Administrator Console - Manage ESM
☐ Administrator Console - Manage User Accounts
☑ Administrator Console - Recorded Media Viewing
☐ Administrator Console - Retail Site Management

Access Level: 7

You can update a user profile by clicking **Modify Profile** and updating the information. Or, you can remove a user profile by clicking the profile, clicking **Remove Profile** and then clicking Yes to confirm the removal.

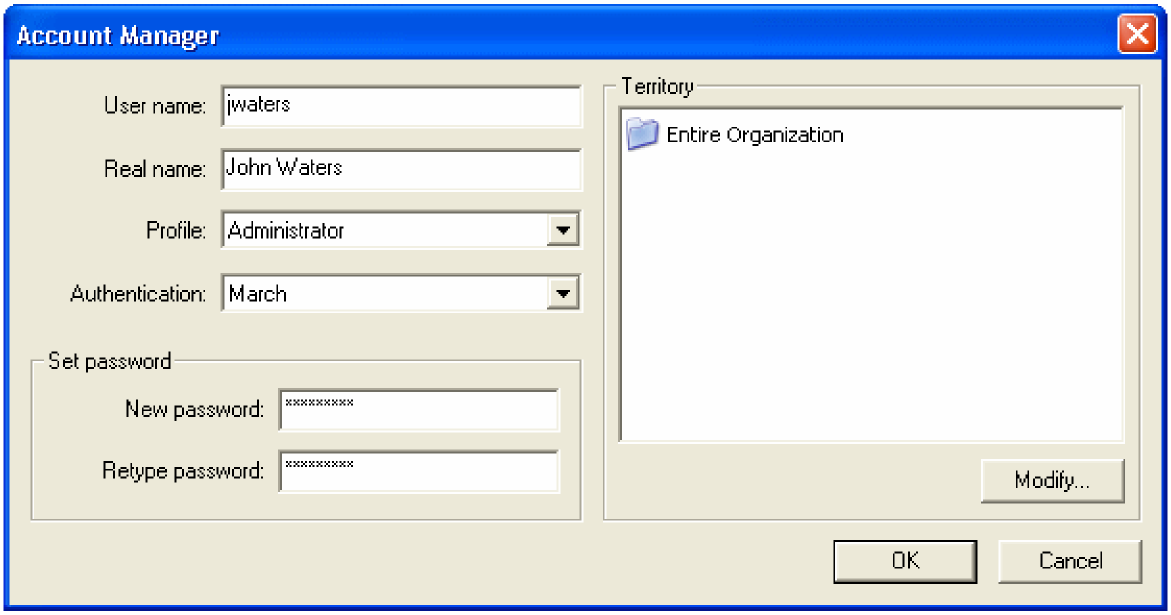
NOTE: If you are creating a user profile for users who will be logging on to the 4000 LC graphical user interface, use the Live Monitoring Console and the Investigator tasks and rights to ensure the users can view live video and search for evidence retained on the 4000 LC hard drive.

To create a user account

1. Ensure the Administrator Console is connected to the ESM.

   For more information, see “Connecting to an ESM” on page 16.
2. Ensure the **User Management** task type is selected.
3. Click **Add Account**.

   The **Account Manager** dialog box appears.



Account Manager

User name: jwaters

Real name: John Waters

Profile: Administrator

Authentication: March

Set password

New password: *********

Retype password: *********

Territory

Entire Organization

4. Type a user name in the **User name** box.

   If you want use the SSPI authentication method (Security Support Provider Interface), you must enter the same user name as your Microsoft Windows user account.

   This authentication method automatically uses the Microsoft Windows user credentials to log on to the ESM, so that the user does not have to enter a user name and password when logging on to the ESM.

   To use this method, the ESM server (or servers if clustered) must be in the same domain as the client computer where your Administrator Console is installed and you must select the **SSPI** authentication method in step 7.

   You must also select the **Do not prompt for login when connecting to ESM** check box in the Preferences dialog box’s **ESM connection** tab (see “To modify the ESM connection information” on page 17)
5. If the user name does not clearly identify the user, you can type the user’s name in the **Real name** box.

6. In the **Profile** list, click a user profile.

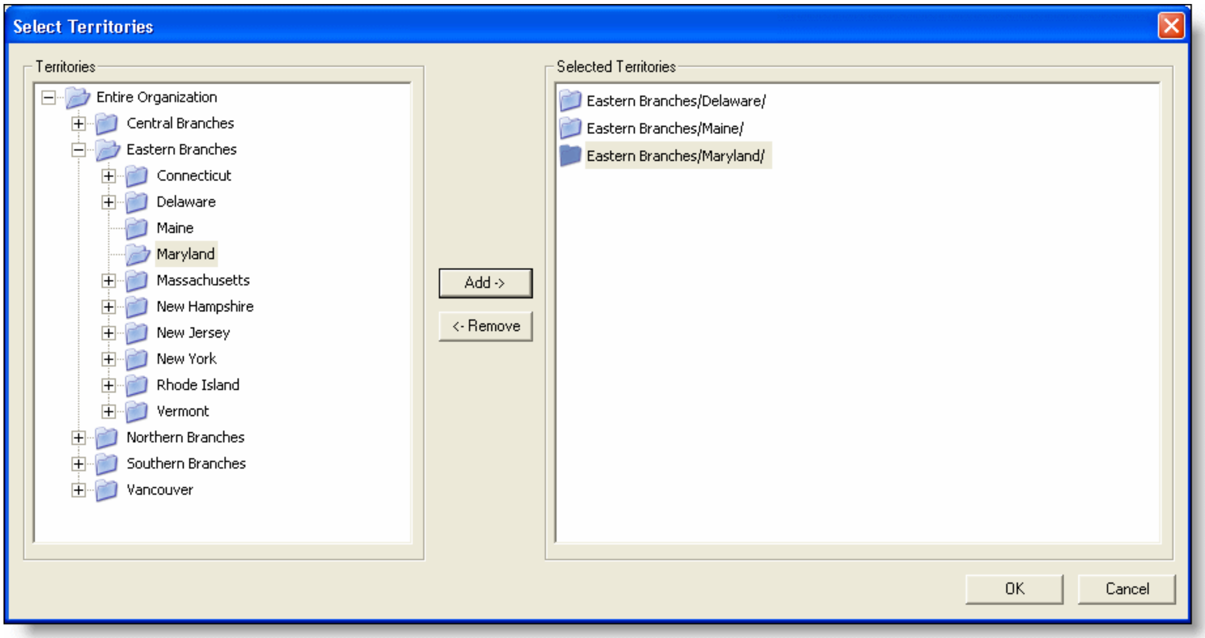
7. In the **Authentication** list, click an authentication method. Select from:

   - **March**
     This authentication method requires the user to enter their user name and password each time they log on to the ESM. To set the password, type and retype the password under **Set password**.
   - **SSPI**
     This authentication method (Security Support Provider Interface) automatically uses the Microsoft Windows user credentials to log on to the ESM so that the user does not have to enter a user name and password when logging on to the ESM. The Set password fields become unavailable when you select this option.
     To use this method, the ESM server (or servers if clustered) must be in the same domain as the client computer where your Administrator Console is installed and you must enter the same user name as your Microsoft Windows user account in step 4.
     You must also select the **Do not prompt for login when connecting to ESM** check box in the Preferences dialog box's **ESM connection** tab (see "To modify the ESM connection information" on page 17).

8. Under **Territory**, you can do the following:

   - Enable the user to access all of the recorders in the organization by leaving the territory set to **Entire Organization**, which is the default setting.
   - Specify the folders and recorders that the user can access by clicking **Modify** and adding folders and recorders to the **Selected Territories** list.

9. Click OK.



You can update user account information by clicking **Modify Account** on the User Management page, or you can remove a user account by clicking **Remove Account** and then clicking **Yes** to confirm the removal.

Viewing the ESM Audit Report

The ESM audit log records changes made to User Accounts and User Profiles in the **User Management** task type.

The following ESM user management audit log entries are recorded:

- **Add User**: When a new user account is created the user name, profile, and the territory are recorded in the Details column of the log entry.
- **Update User**: When a user account is updated, the changes are recorded in the Details column of the log entry. Changes can include a different profile, territory, real name, authentication type, or password.
- **Delete User**: When a user account is deleted the user name is recorded in the User/Profile column of the log entry.
- **Add Profile**: When a new profile is created the profile name, access level, and tasks/rights are recorded in the Details column of the log entry.
- **Update Profile**: When a profile is changed the profile name, new access level, and new tasks/rights are recorded in the Details column of the log entry.
- **Delete Profile**: When a profile is deleted the profile name is recorded in the User/Profile column of the log entry.

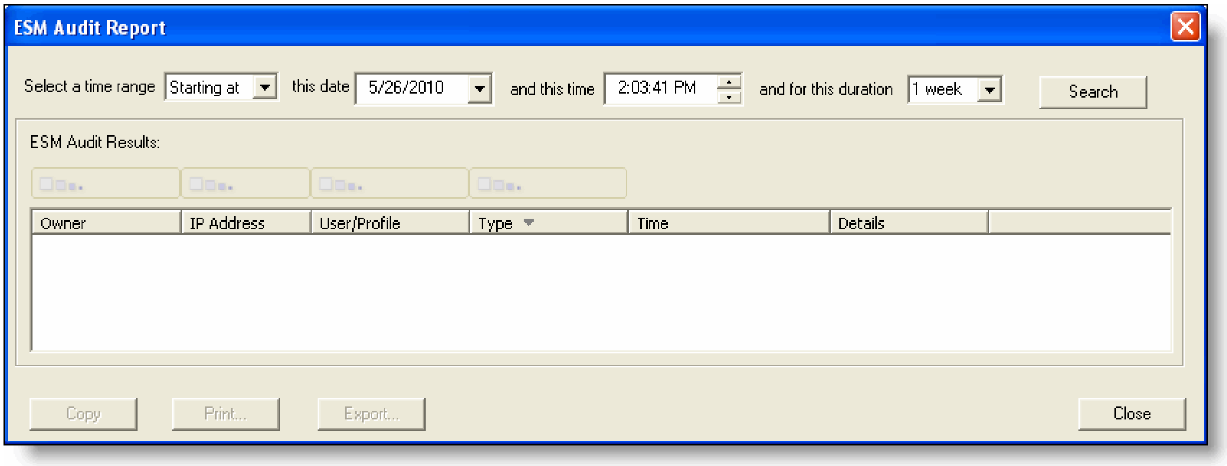
You can also configure the ESM audit to set how long the audit log entries are retained.

To view the ESM audit report

1. Ensure the Administrator Console is connected to the ESM.

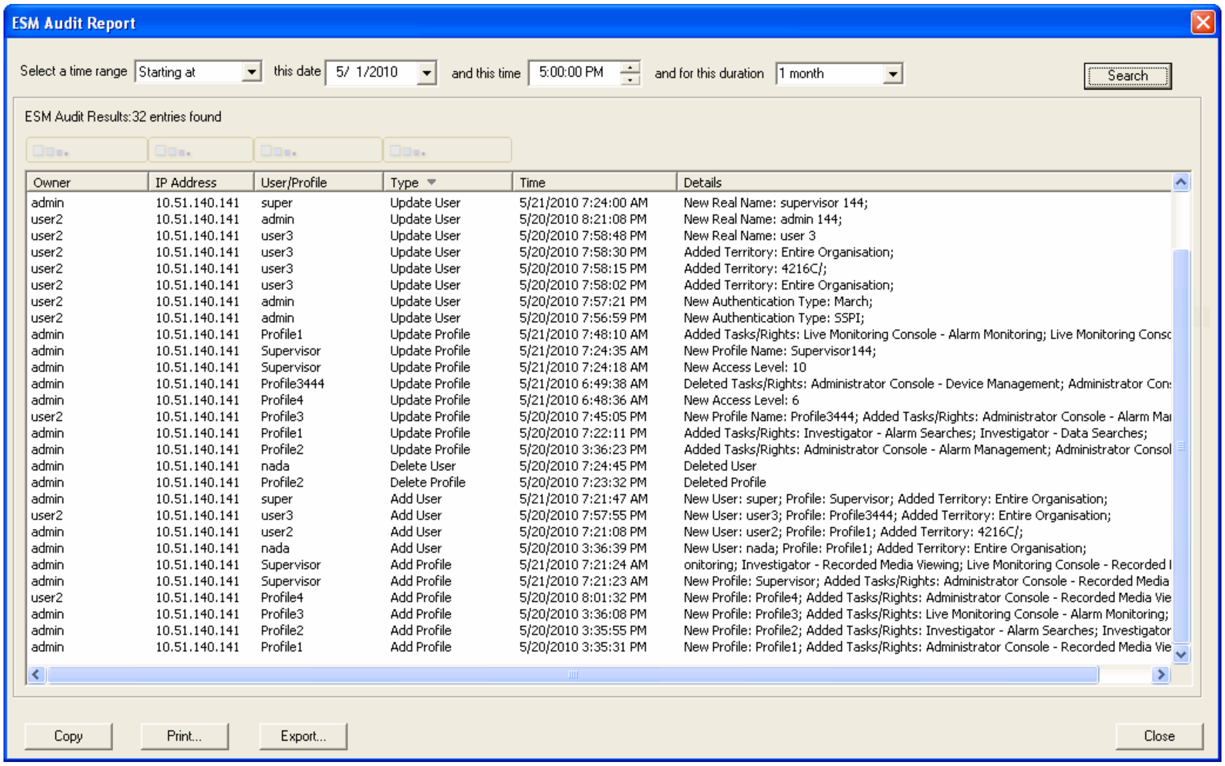
   For more information, see “Connecting to an ESM” on page 16.
2. Ensure the **User Management** task type is selected.
3. Click **ESM Audit**.

   The **ESM Audit Report** window appears.



4. In the **Select a time range** list, select one of the following options:
   - **Starting at** — Searches for audit log entries created starting on the day, time, and duration you specify.
   - **On or About** — Searches for audit log entries created on or about the day, time, and duration you specify.
   - **On the Day with** — Searches for audit log entries created on the day you specify.
   - **In the Last** — Searches for audit log entries created during the duration you specify.
   - **Older than** — Searches for audit log entries created before the day and time you specify.
5. If applicable, in the **this date** list, type or select a date.
6. If applicable, in the **and this time** list, type or select a time.
7. If applicable, in the **and for this duration** list, type or select a duration.
8. Click Search.

   The ESM audit results are displayed.



Select a time range: Starting at
this date: 5/ 1/2010
and this time: 5:00:00 PM
and for this duration: 1 month

ESM Audit Results:32 entries found

Owner	IP Address	User/Profile	Type	Time	Details
admin	10.51.140.141	super	Update User	5/21/2010 7:24:00 AM	New Real Name: supervisor 144;
user2	10.51.140.141	admin	Update User	5/20/2010 8:21:08 PM	New Real Name: admin 144;
user2	10.51.140.141	user3	Update User	5/20/2010 7:58:48 PM	New Real Name: user 3
user2	10.51.140.141	user3	Update User	5/20/2010 7:58:30 PM	Added Territory: Entire Organisation;
user2	10.51.140.141	user3	Update User	5/20/2010 7:58:15 PM	Added Territory: 4216C/;
user2	10.51.140.141	user3	Update User	5/20/2010 7:58:02 PM	Added Territory: Entire Organisation;
user2	10.51.140.141	admin	Update User	5/20/2010 7:57:21 PM	New Authentication Type: March;
user2	10.51.140.141	admin	Update User	5/20/2010 7:56:59 PM	New Authentication Type: SSPI;
admin	10.51.140.141	Profile1	Update Profile	5/21/2010 7:48:10 AM	Added Tasks/Rights: Live Monitoring Console - Alarm Monitoring; Live Monitoring Conso
admin	10.51.140.141	Supervisor	Update Profile	5/21/2010 7:24:35 AM	New Profile Name: Supervisor144;
admin	10.51.140.141	Supervisor	Update Profile	5/21/2010 7:24:18 AM	New Access Level: 10
admin	10.51.140.141	Profile3444	Update Profile	5/21/2010 6:49:38 AM	Deleted Tasks/Rights: Administrator Console - Device Management; Administrator Con
admin	10.51.140.141	Profile4	Update Profile	5/21/2010 6:48:36 AM	New Access Level: 6
user2	10.51.140.141	Profile3	Update Profile	5/20/2010 7:45:05 PM	New Profile Name: Profile3444; Added Tasks/Rights: Administrator Console - Alarm Ma
admin	10.51.140.141	Profile1	Update Profile	5/20/2010 7:22:11 PM	Added Tasks/Rights: Investigator - Alarm Searches; Investigator - Data Searches;
admin	10.51.140.141	Profile2	Update Profile	5/20/2010 3:36:23 PM	Added Tasks/Rights: Administrator Console - Alarm Management; Administrator Consol
admin	10.51.140.141	nada	Delete User	5/20/2010 7:24:45 PM	Deleted User
admin	10.51.140.141	Profile2	Delete Profile	5/20/2010 7:23:32 PM	Deleted Profile
admin	10.51.140.141	super	Add User	5/21/2010 7:21:47 AM	New User: super; Profile: Supervisor; Added Territory: Entire Organisation;
user2	10.51.140.141	user3	Add User	5/20/2010 7:57:55 PM	New User: user3; Profile: Profile3444; Added Territory: Entire Organisation;
admin	10.51.140.141	user2	Add User	5/20/2010 7:21:08 PM	New User: user2; Profile: Profile1; Added Territory: 4216C/;
admin	10.51.140.141	nada	Add User	5/20/2010 3:36:39 PM	New User: nada; Profile: Profile1; Added Territory: Entire Organisation;
admin	10.51.140.141	Supervisor	Add Profile	5/21/2010 7:21:24 AM	onitoring; Investigator - Recorded Media Viewing; Live Monitoring Console - Recorded
admin	10.51.140.141	Supervisor	Add Profile	5/21/2010 7:21:23 AM	New Profile: Supervisor; Added Tasks/Rights: Administrator Console - Recorded Media
user2	10.51.140.141	Profile4	Add Profile	5/20/2010 8:01:32 PM	New Profile: Profile4; Added Tasks/Rights: Administrator Console - Recorded Media Vie
admin	10.51.140.141	Profile3	Add Profile	5/20/2010 3:36:08 PM	New Profile: Profile3; Added Tasks/Rights: Live Monitoring Console - Alarm Monitoring;
admin	10.51.140.141	Profile2	Add Profile	5/20/2010 3:35:55 PM	New Profile: Profile2; Added Tasks/Rights: Investigator - Alarm Searches; Investigator
admin	10.51.140.141	Profile1	Add Profile	5/20/2010 3:35:31 PM	New Profile: Profile1; Added Tasks/Rights: Administrator Console - Recorded Media Vie

To copy, print, or export the ESM audit report

You can copy, print or export all entries in the ESM audit report, or select one or more specific entries in the list.

Click **Copy**, **Print**, or **Export**.

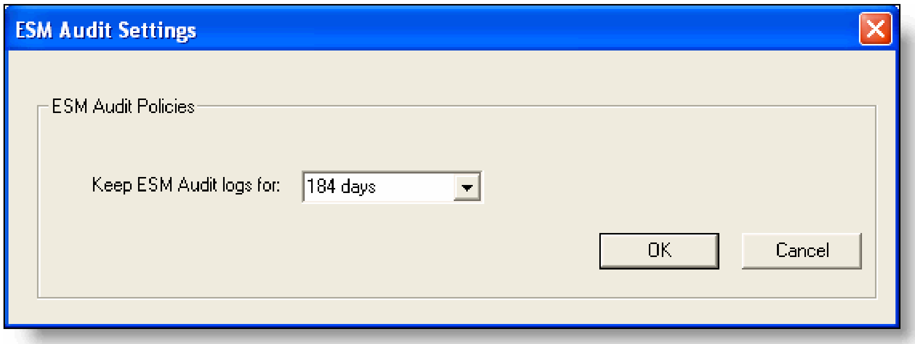
- **Copy** saves the contents of the ESM audit log to the clipboard.
- **Print** opens the **Print** dialog box and allows you to print the contents of the ESM audit log.
- **Export** opens the **Save Audit Report** dialog box and allows you to save the contents of the ESM audit log in CSV format. You can use Microsoft Excel® to open files saved in CSV format.

To configure the ESM audit settings

1. Ensure the Administrator Console is connected to the ESM.

   For more information, see "Connecting to an ESM" on page 16.
2. Ensure the **User Management** task type is selected.
3. Click **ESM Audit Settings**.

   The **ESM Audit Settings** dialog box appears.



ESM Audit Settings

ESM Audit Policies

Keep ESM Audit logs for: 184 days

4. In the **Keep ESM Audit logs for** list, select the amount of time you want the system to keep the logs for. Audit log entries older than the specified duration are deleted.
5. Click OK.

Viewing the Recorder Audit Report

The recorder maintains a history of users that have accessed it. You can review the recorder's audit report to view a summary of interaction between the recorder and the software applications, including the Administrator Console, Installer Console, Investigator, Live Monitoring Console, ESM, and the unit's built-in provisioning interface.

To view the recorder audit report

1. Ensure the Administrator Console is connected to the ESM.

   For more information, see “Connecting to an ESM” on page 16.
2. Ensure the **Device Management** task type is selected.
3. Click a recorder in the **Device Selector** panel.
4. Click **View Audit Report**.
5. Review the list of reported activities that appear in the **Audit Report** dialog box.

To copy, export, or print the recorder audit report

Click **Copy**, **Export**, or **Print**.

- **Copy** saves the contents of the recorder audit log to the clipboard.
- **Export** opens the **Save Audit Report** dialog box and allows you to save the contents of the recorder audit log in CSV format. You can use Microsoft Excel® to open files saved in CSV format.
- **Print** opens the **Print** dialog box and allows you to print the contents of the recorder audit log.

Registering and Unregistering Recorders With an ESM

If your organization uses an ESM to centrally manage recorders on the network, you can register your recorder with the ESM.

After you register the recorder, additional tasks are available in the Administrator Console that let you manage the recorder, such as create user accounts to limit access to the recorder and its peripherals, perform central updates to all recorders on the network, and customize the frequency of health alert notification. For more information, see “Performing Advanced Enterprise Service Manager Tasks” on page 181.

At any point you can unregister the recorder from the ESM.

NOTE: If you are working with a 4000 LC, users can log on to the 4000 LC graphical user interface using the user name and password you specify. Please note, the 4000 LC must be configured to communicate with an ESM before the user name and password can be used to log on to the 4000 LC. For information about configuring a recorder to communicate with an ESM, see the Installing a Recorder and Testing Peripheral Connections Quick Steps publication.

To register a recorder with an ESM

1. Ensure the Administrator Console is connected to the ESM.

   For more information, see “Connecting to an ESM” on page 16.
2. Ensure the **Device Installation** task type is selected.
3. Click a recorder in the **Device Selector** panel.

4. Click **Network**.
5. Click **Register with ESM**.

   If the recorder is already registered with an ESM, the button is labeled **Re-register with ESM**.

   The **Device Registration** dialog box appears.
6. Type the ESM's IP address or hostname in the **Manager address** box.
7. Under **Station ID Assignment**, do one of the following:
   - Select **Use docking station ID.** The station ID that is specified with the recorder's DIP switches appears.
   - Select **Use programmed station ID** and then type a unique station ID. When **Use programmed station ID** is selected, the programmed station ID is used instead of the ID set using the recorder's DIP switches.
8. Click **OK**.

   Observe the registration status under **ESM Registration Status**. It may take a moment for the status to update.

NOTE: You can also use the Installer Console to perform steps 3. to 8..

To unregister a recorder from an ESM

1. Ensure the Administrator Console is connected to the ESM.

   For more information, see "Connecting to an ESM" on page 16.
2. Ensure the **Device Management** task type is selected.
3. Click a recorder in the **Device Selector** panel.
4. Click **Unregister from ESM**.
5. Click **Yes** to confirm the change.

   The recorder is removed from the **Device Selector** panel.

Customizing Recorder Health Alerts

You can customize how recorder health alerts are reported by updating the alert thresholds. Thresholds are the conditions that must be met before the recorder notifies you of the alert.

You can customize configurable alerts that are supported in the ESM version you are running. You can also choose to reapply the ESM default thresholds to customized alerts.

You can view details about an alert by clicking the alert and viewing the description under **Alert Details**.

To view alert thresholds

1. Ensure the Administrator Console is connected to the ESM.

   For more information, see “Connecting to an ESM” on page 16.
2. Ensure the **Health Monitoring** task type is selected.
3. Click **View Alert Thresholds**.

   The **View Alert Thresholds** dialog box appears.
4. View the alert thresholds. The **Threshold** column indicates when the recorder notifies you of the alert.

To customize an alert threshold

1. Ensure the Administrator Console is connected to the ESM.

   For more information, see “Connecting to an ESM” on page 16.
2. Ensure the **Health Monitoring** task type is selected.
3. In the **Alert Inbox**, ensure there are no unresolved alerts for the alert type that you want to customize. If there are unresolved alerts for the alert type, you must acknowledge and close the alerts before you complete the steps below. For more information, see “To acknowledge that you have reviewed an alert” on page 161 and “To close an alert and move it to the Alert History” on page 162.
4. Click **View Alert Thresholds**.

   The **Customize Alert Thresholds** dialog box appears.
5. Click an alert.
6. Click **Customize Thresholds**.

   The **Customize Alert Thresholds** dialog box appears.
7. Click **Use custom threshold**.
8. Click a notification option (options may vary) in the **Report notification** list:
   - **Always Report**. An alert notification is sent as soon as the recorder reports the alert.
   - **Never Report**. An alert notification is never sent.
   - **Use Frequency**. An alert notification is sent when the issue reaches or exceeds a specified frequency in a certain time period.
   - **Use Duration**. An alert notification is sent when the issue lasts for a specified duration range or longer.
   - **Use Duration or Frequency**. An alert notification is sent when an issue reaches or exceeds a specified frequency over a certain time period, or lasts for a specified duration range or longer.
9. In the **Duration limit** box (if available), specify the amount of time during which the alert must occur before an alarm notification is sent. For example, if you specify 30 minutes, when the first alert of that type occurs on a recorder, the recorder monitors the alert for 30 minutes, and then sends an alert notification.

10. In the **Frequency limit** lists (if available), specify the number of times the alert must occur and the time period within which it must occur, before an alert notification is sent. For example, if you specify that the alert must occur 10 times in 30 minutes, when the first alert of that type occurs on a recorder, the recorder monitors the alert. After the alert occurs 10 times within 30 minutes, an alert notification is sent.

    If you specify 1 in the first **Frequency limit** list, the second **Frequency limit** list is unavailable and the alert is always reported.

11. Click **OK** to close the first **Customize Alert Thresholds** dialog box.
12. Click **OK** to close the second **Customize Alert Thresholds** dialog box.

    Depending on when the first occurrence happens, the recorder may monitor the alert for up to an additional 10 minutes.

NOTE: You can revert to the ESM default threshold by clicking Use default threshold.

To reapply ESM default thresholds to customized alerts

1. Ensure the Administrator Console is connected to the ESM.

   For more information, see “Connecting to an ESM” on page 16.

2. Ensure the **Health Monitoring** task type is selected.
3. Click **View Alert Thresholds**.

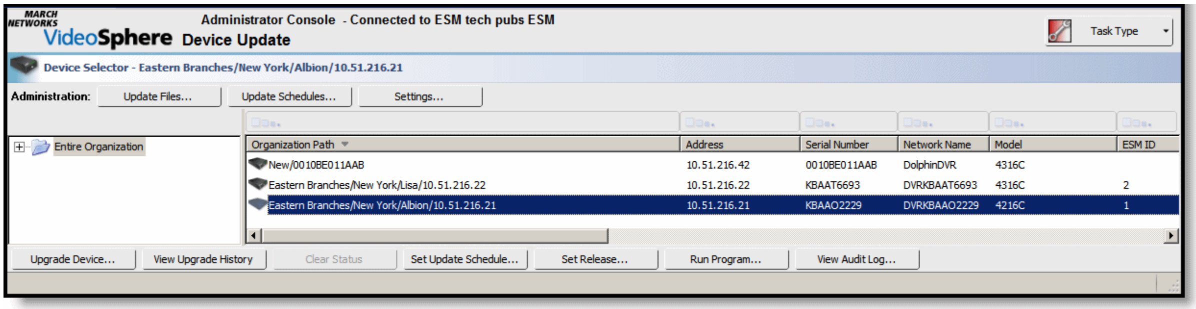
   The **Customize Alert Thresholds** dialog box appears.

4. Click an alert that has been customized.
5. Click **Clear Custom Thresholds**.

TIP: You can also right-click a customized alert, point to **Clear Custom Thresholds**, and then click **All**.

Centrally Updating Software

You can centrally update several managed recorders at a time using a .upd file included on your March Networks CD or provided by your March Networks Customer Care representative. You can specify the software update settings, perform multiple updates through the ESM, and review the update history.



Administrator Console - Connected to ESM tech pubs ESM

Device Update

Device Selector - Eastern Branches/New York/Albion/10.51.216.21

Administration:

Organization Path	Address	Serial Number	Network Name	Model	ESM ID
New/0010BE011AAB	10.51.216.42	0010BE011AAB	DolphinDVR	4316C	
Eastern Branches/New York/Lisa/10.51.216.22	10.51.216.22	KBAAT6693	DVRKBAAT6693	4316C	2
Eastern Branches/New York/Albion/10.51.216.21	10.51.216.21	KBAAO2229	DVRKBAAO2229	4216C	1

Reviewing a Recorder's Update Information

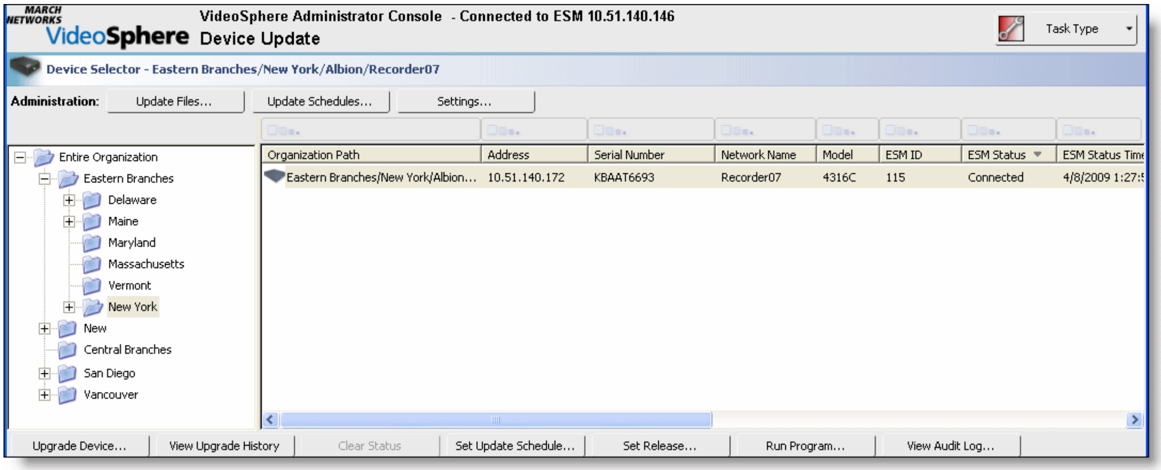
You can review details about the release of software running on the recorder. If an update is scheduled for the recorder, you can view details about when the update will occur.

To review update information for an ESM-managed recorder

1. Ensure the Administrator Console is connected to the ESM.

   For more information, see "Connecting to an ESM" on page 16.

2. Ensure the **Device Update** task type is selected.



VideoSphere Administrator Console - Connected to ESM 10.51.140.146

Device Update

Device Selector - Eastern Branches/New York/Albion/Recorder07

Organization Path	Address	Serial Number	Network Name	Model	ESM ID	ESM Status	ESM Status Time
Eastern Branches/New York/Albion…	10.51.140.172	KBAAT6693	Recorder07	4316C	115	Connected	4/8/2009 1:27:!

3. Review the details outlined in the following table.

Recorder Update Info	Description
Organization Path	Indicates the folders within which the recorder is organized. This path is set up using the **Device Management** task type. For information about organizing recorders, see "Organizing Recorders and Exporting the Recorder List" on page 149.
Address	The IP address of the unit, including the port.
Serial Number	The unique serial number provided to the unit for identification. The serial number also appears on the label on the outside of the recorder.
Network Name	The unit's network name. The network name is specified using the **Device Configuration** task type on the **General** page. For more information, see "Specifying General Options" on page 37.
Model	The unit model, for example 4416 represents a 4416 C NVR.
ESM ID	The station ID of the unit, which uniquely identifies it.
ESM Status	The connection status of the unit.
ESM Status Time	The time of the last status change.

Recorder Update Info	Description
Versions	The version information for the various software components.
Current Release	The version of software currently running on the unit.
Target Release	The version of software you want the ESM to automatically apply to the unit.
Release Status	Indicates if the unit software is currently at the target release.
Schedule	The name of the update schedule (if any).
Upgrade Status	The status of the upgrade.

Specifying Software Settings

You can specify the following general software update settings:

- **Default software release.** Specify the default software release so that any new recorders connected to the network are automatically updated to run this software release.
- **Bandwidth limit.** Specify the maximum amount of network bandwidth to be used during updates. This ensures the network's bandwidth is not monopolized when performing updates.
- **Simultaneous updates.** Specify the maximum number of updates to be performed at one time to limit the amount of network bandwidth used.

The following examples provide scenarios where you might limit bandwidth:

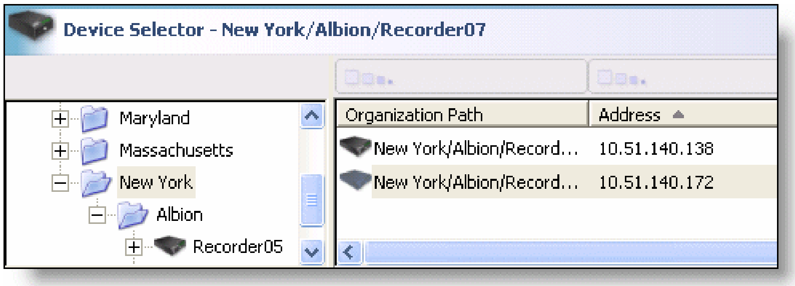
Scenario A	Your ESM is connected to the corporate network over a Wide Area Network (WAN) 128 Kbps DSL connection.
Problem	The amount of bandwidth that can be consumed during updates without impacting other WAN traffic is 64 Kbps.
Resolution	Specify 64 Kbps as the aggregate limit to ensure that regardless of how many units are being updated, the maximum network usage never exceeds 64 Kbps.

Scenario B	Your ESM is connected to the corporate network on a high-speed segment, where bandwidth is not an issue. The units, however, are connected to the corporate network through bandwidth-limited WAN connections.
Problem	Exceeding the bandwidth at each location could cause business to be interrupted at the remote locations.
Resolution	Specify 20 Kbps as the individual limit to ensure that the transmission of an update to any single unit does not exceed 20 Kbps.

To specify the default software release

1. Ensure the Administrator Console is connected to the ESM.

   For more information, see “Connecting to an ESM” on page 16.
2. Ensure the **Device Update** task type is selected.
3. Click a site in the **Device Selector** panel.



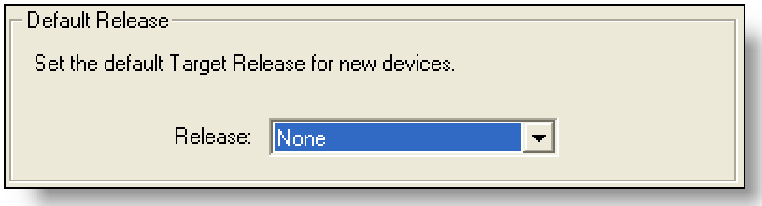
Device Selector - New York/Albion/Recorder07

- Maryland
- Massachusetts
- New York
  - Albion
    - Recorder05

Organization Path	Address
New York/Albion/Record...	10.51.140.138
New York/Albion/Record...	10.51.140.172

4. Click **Settings**.

   The **Device Update Service Settings** dialog box appears.
5. Under **Default Release**, click the default release in the **Release** list.
6. Click **OK**.



Default Release

Set the default Target Release for new devices.

Release: None

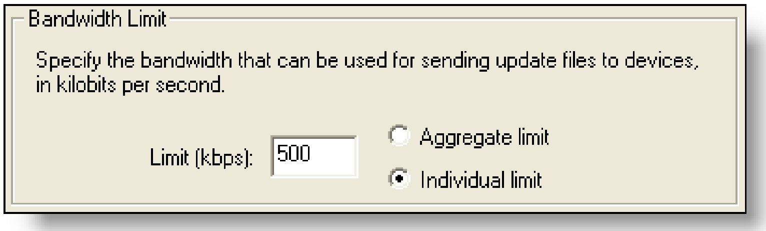
To specify the bandwidth limit

1. Ensure the Administrator Console is connected to the ESM.

   For more information, see “Connecting to an ESM” on page 16.
2. Ensure the **Device Update** task type is selected.
3. Click a site in the **Device Selector** panel.
4. Click **Settings**.

   The **Device Update Service Settings** dialog box appears.
5. Under **Bandwidth Limit**, type a value in the **Limit (kbps)** box.

6. Click one of the following options:
   - **Aggregate limit**. The bandwidth limit you specify is the maximum amount of network bandwidth available at any given time. If you are performing multiple updates, the available bandwidth is divided among the units.
   - **Individual limit**. The amount of network bandwidth you specify is available for each unit being updated. If you are performing multiple updates, each unit can use up to the specified amount.
7. Click **OK**.



Bandwidth Limit

Specify the bandwidth that can be used for sending update files to devices, in kilobits per second.

Limit (kbps): 500

○ Aggregate limit

● Individual limit

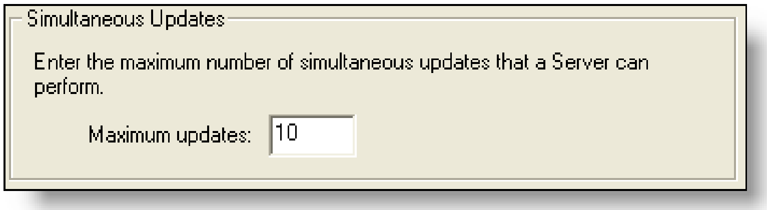
NOTE: If your ESM contains several servers, the bandwidth limit is applied to each server in the cluster. For example, if you have three servers and have set the bandwidth limit to 100 Kbps, each server is limited to 100 Kbps.

To specify the number of simultaneous updates

1. Ensure the Administrator Console is connected to the ESM.

   For more information, see "Connecting to an ESM" on page 16.
2. Ensure the **Device Update** task type is selected.
3. Click a site in the **Device Selector** panel.
4. Click **Settings**.

   The **Device Update Service Settings** dialog box appears.
5. Under **Simultaneous Updates**, type a value in the **Maximum updates** box.
6. Click **OK**.



Simultaneous Updates

Enter the maximum number of simultaneous updates that a Server can perform.

Maximum updates: 10

Performing Multiple Updates through the ESM

When you perform updates through the ESM, you use an update file (.upd) provided by your March Networks Customer Care representative, or included on your March Networks CD, to apply the necessary update, such as a software upgrade, patch, or enhancement.

For recorders running Release 5.5 or later of the recorder software an upgrading license must be installed on the ESM before recorders can be upgraded. An upgrading license is required for version upgrades only, and not for service packs, patches, or enhancements.

To perform multiple updates through the ESM, perform the following tasks:

- Load an update file onto the ESM
- Schedule an update (optional)
- Apply an update

Step 1 - Loading an Update File onto the ESM

Before you can perform an update, you must transfer the update file onto the ESM. After the file is on the ESM, the ESM can update the units you specify.

The files you use to perform multiple updates through the ESM are in .upd format. You can find these files on your March Networks CD.

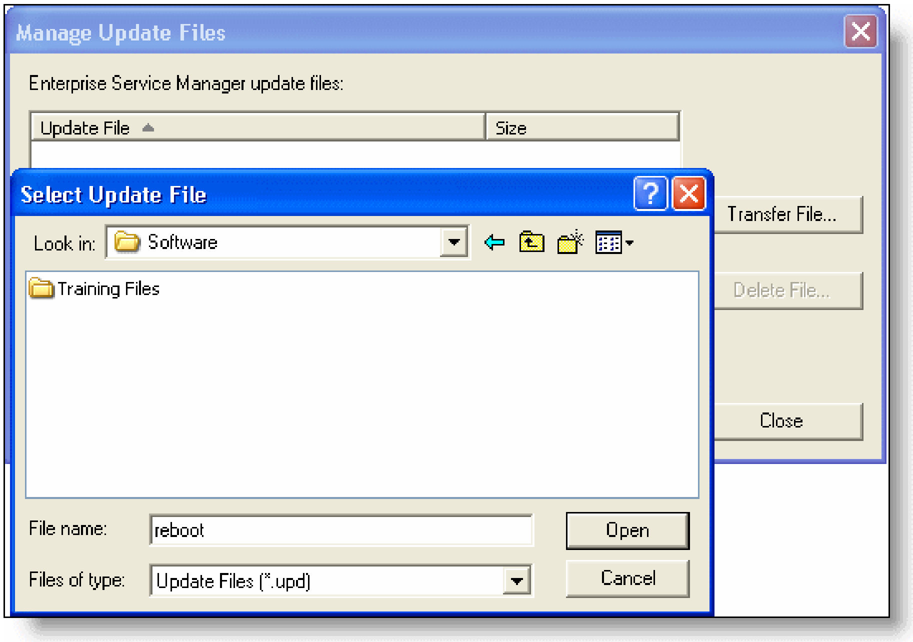
To load an update file onto the ESM

1. Ensure the Administrator Console is connected to the ESM.

   For more information, see “Connecting to an ESM” on page 16.
2. Ensure the **Device Update** task type is selected.
3. Click a site in the **Device Selector** panel.
4. Click **Update Files**.

   The **Manage Update Files** dialog box appears.
5. Click **Transfer File**.
6. Navigate to the update file and select it.

7. Click **Open**.



TIP: You can also delete an update file from the ESM by clicking a file in the **Enterprise Service Manager update files** list and then clicking **Delete File**.

Step 2 - Scheduling an Update (Optional)

If you do not want to apply updates immediately, you can create a schedule to specify the date and time you want updates to occur.

We recommend you schedule the update to occur when you expect little or no activity at the location where the unit is installed, as the unit may restart during the update process.

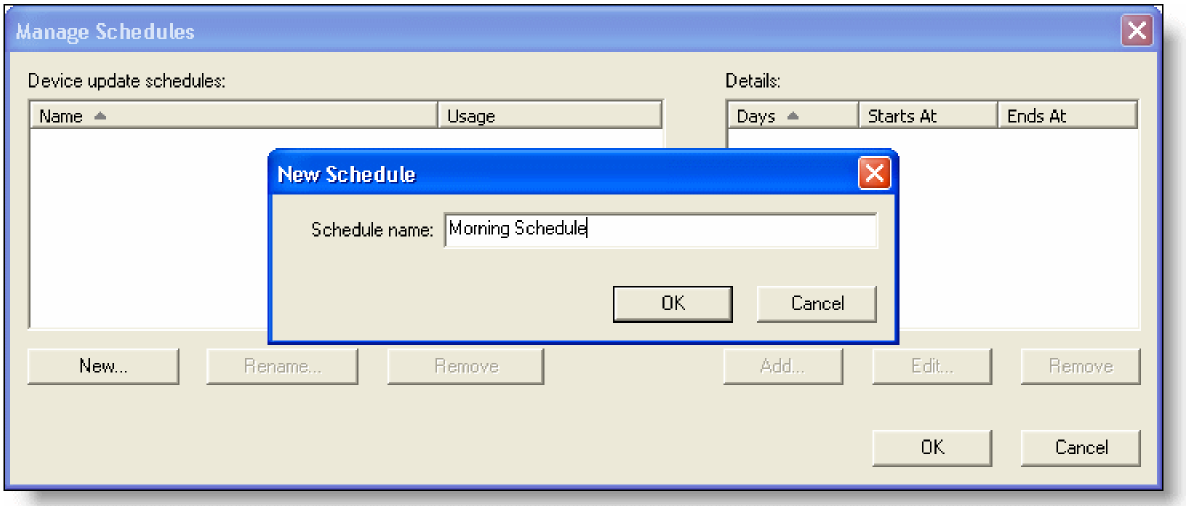
To create a schedule

1. Ensure the Administrator Console is connected to the ESM.

   For more information, see “Connecting to an ESM” on page 16.
2. Ensure the **Device Update** task type is selected.
3. Click a site in the **Device Selector** panel.
4. Click **Update Schedules**.

   The **Manage Schedules** dialog box appears.

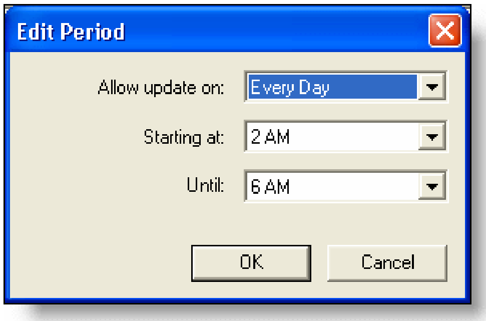
5. Click **New** and type a descriptive name for the schedule.



Schedule name: Morning Schedule

6. Click **OK**.
7. Click **Add**.

   The **Edit Period** dialog box appears.
8. Specify the following information:
   - **Allow update on**. The days you want the schedule to run.
   - **Starting at**. The time you want the update to start on a particular day.
   - **Until**. The time you want the update to end on a particular day.



Allow update on: Every Day

Starting at: 2 AM

Until: 6 AM

9. Click **OK** to close the **Edit Period** dialog box.
10. Click **OK** to close the **Manage Schedules** dialog box.

You can also rename a schedule by clicking the schedule in the Device update schedules list, clicking Rename, and then typing a new name for the schedule.

To remove a schedule, click the schedule in the Device update schedules list and then click Remove.

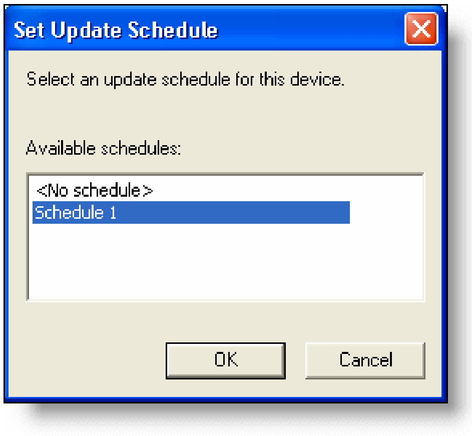
To change a schedule period, click the schedule period in the Periods for schedule list, click Edit, and update any information in the Edit Period dialog box. To remove the schedule period, click the schedule and then click Remove.

To apply a schedule to a unit

1. Ensure the Administrator Console is connected to the ESM.

   For more information, see “Connecting to an ESM” on page 16.
2. Ensure the **Device Update** task type is selected.
3. Click a recorder in the **Device Selector** panel.
4. Click **Set Update Schedule**.

   The **Set Update Schedule** dialog box appears.
5. Click a schedule in the **Available schedules** list.



Set Update Schedule

Select an update schedule for this device.

Available schedules:

<No schedule>
Schedule 1

Step 3 - Applying an Update

Updates can be categorized as software upgrades, software enhancements, or patches. The steps to apply a software upgrade differ slightly from the steps to apply an enhancement or patch.

For recorders running Release 5.5 and later of the recorder software, an upgrading license must be installed on the ESM before software can be upgraded.

To apply an update

1. Ensure the Administrator Console is connected to the ESM.

   For more information, see “Connecting to an ESM” on page 16.
2. Ensure the **Device Update** task type is selected.
3. Click a recorder in the **Device Selector** panel.
4. Click one of the following buttons:
   - **Set Release**. Allows you to perform a software upgrade.
   - **Run Program**. Allows you to apply a software enhancement or patch.

5. Under **Carry out this upgrade**, click one of the following options:
   - **Using update schedules**
   - **Immediately (unscheduled)**

NOTE: If the update does not complete successfully, an error message appears in the Upgrade Status column. You can clear the message by clicking Clear Status.

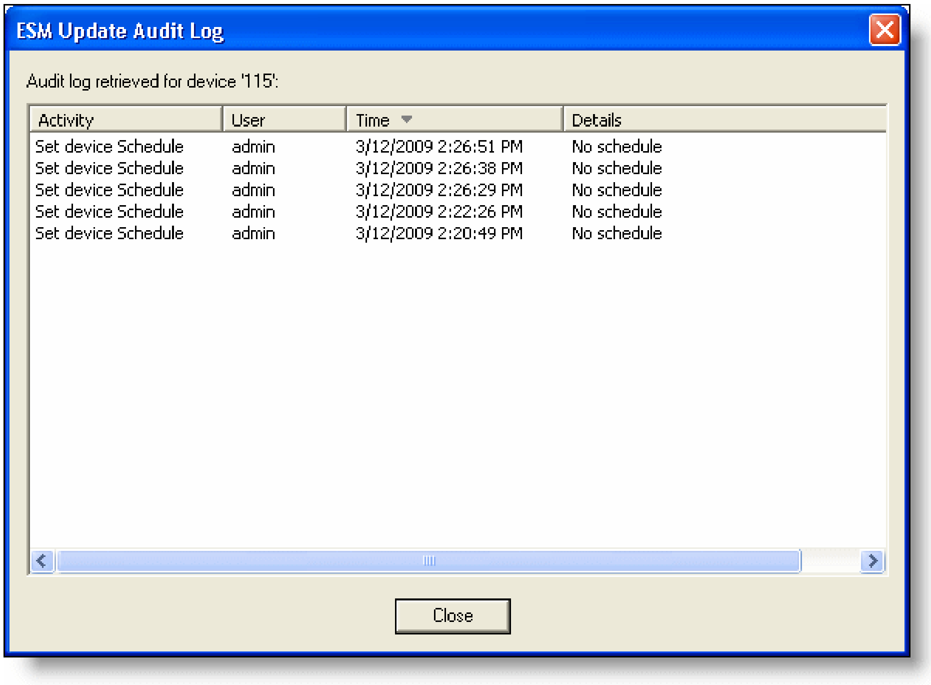
Reviewing Update History

The ESM maintains a history of all updates it performs. You can review the history for each unit to see which updates have been applied, view which user made the change, and determine the time the change occurred.

To review the update history

1. Ensure the Administrator Console is connected to the ESM.

   For more information, see "Connecting to an ESM" on page 16.
2. Ensure the **Device Update** task type is selected.
3. Click a recorder in the **Device Selector** panel.
4. Click **View Audit Log**.



Audit log retrieved for device '115':

Activity	User	Time	Details
Set device Schedule	admin	3/12/2009 2:26:51 PM	No schedule
Set device Schedule	admin	3/12/2009 2:26:38 PM	No schedule
Set device Schedule	admin	3/12/2009 2:26:29 PM	No schedule
Set device Schedule	admin	3/12/2009 2:22:26 PM	No schedule
Set device Schedule	admin	3/12/2009 2:20:49 PM	No schedule

Specifying the Server Connection Order

To ensure redundant support for your recorders, you can configure up to four secondary servers within your ESM. If the primary server encounters a problem, for example it loses network connectivity and cannot manage its connected recorders, the secondary server automatically starts managing the recorders. When the primary server comes back online, it resumes management of the recorders.

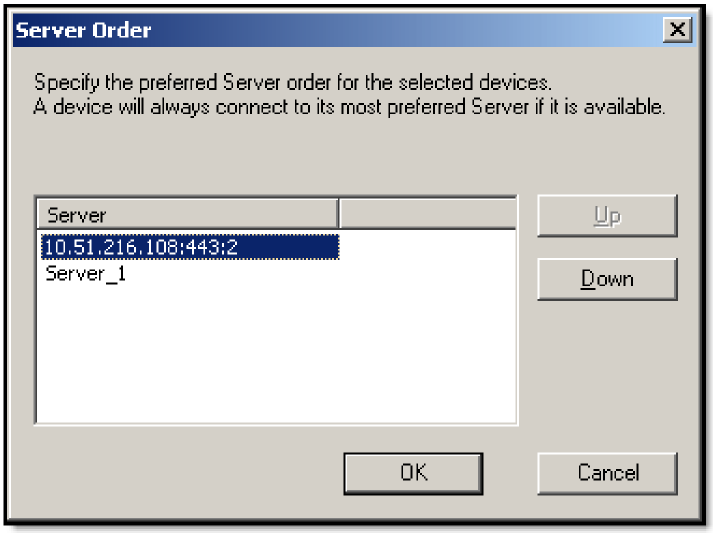
To specify the server connection order

1. Ensure the Administrator Console is connected to the ESM.

   For more information, see “Connecting to an ESM” on page 16.
2. Ensure the **Device Management** task type is selected.
3. Click a recorder in the **Device Selector** panel.
4. Click **Server Order**.

   The **Server Order** dialog box appears.
5. Click a server and then click the **Up** and **Down** buttons to change the server order.

   The server at the top of the list is the primary server for connection.



Specify the preferred Server order for the selected devices.
A device will always connect to its most preferred Server if it is available.

Server	
10.51.216.108:443:2	
Server_1	

Replacing Recorders

The ESM lets you remove a recorder, replace it with another, and then it automatically applies the original settings to the new recorder. This ensures minimal down time when the recorder requires servicing.

WARNING: For this feature to work, you must ensure the replacement recorder has the same station ID as the original. The ESM uses this unique identifier to confirm that the replacement recorder should be updated with the original recorder's settings.

TIP: For some recorder models, the station ID can be specified using the DIP switches on the recorder or docking station. This ID can also be specified using the Installer Console or by switching to the Device Installation task type. As part of the recorder replacement instructions outlined in this chapter, you will specify the new recorder's station ID.

The following example provides a scenario where you might replace a recorder:

Scenario	You are monitoring several bank branches, each with several recorders installed in a rack. The recorders at each bank branch are managed by a central ESM.
Problem	Lightning has struck one of the bank branches and caused a problem with one recorder's internal power supply. To experience minimal down time, a replacement recorder has been shipped to the bank branch.
Resolution	Mark the failed recorder for replacement using the Administrator Console. Remove the failed recorder from the docking station and replace it with the replacement recorder that was shipped to the bank branch. The replacement recorder assumes the original recorder's settings after power is applied and it connects to the ESM.

To mark a recorder for replacement

1. Ensure the Administrator Console is connected to the ESM.

   For more information, see "Connecting to an ESM" on page 16.
2. Ensure the **Device Management** task type is selected.
3. Power down the original, failed recorder.
4. Click the failed recorder in the **Device Selector** panel.
5. Click **Replace Device**.

   Marked for Replacement appears in the **ESM Status** column to indicate the status.
6. Disconnect the original recorder.

   If the recorder is installed in a docking station, undock it.

To install a replacement recorder

1. Ensure the Administrator Console is connected to the ESM.

   For more information, see “Connecting to an ESM” on page 16.

2. Ensure the **Device Management** task type is selected.

   If you have not yet marked the original recorder for replacement, do so now. For more information, see “To mark a recorder for replacement” on page 209.

3. If you want to use a static IP address for the recorder, complete the following tasks (if you want to use DHCP, proceed to step 4.):

   - Connect your computer to the replacement recorder using a cross-over Ethernet cable. Then, power on your computer and the recorder.
   - Start the Administrator Console. With the **Device Installation** task type selected, click the **Detect Devices** button. The replacement recorder automatically appears in the **Device Selector** panel. If the recorder does not appear, it may still be starting up. Wait a minute and then click the **Detect Devices** button again.
   - Click **Network** and then provide the recorder with a static IP address. Please note, the IP address of the replacement recorder does not have to match the IP address of the original recorder.

NOTE: If you have a null modem cable, you can also use the recorder’s built-in provisioning interface to provide the recorder with a static IP address or register it with the ESM. For information about using the provisioning interface, see the *Provisioning Interface Technical Instructions* included on your March Networks CD.

4. Physically connect your computer and the recorder to the network.
5. With the **Device Installation** task type selected in the Administrator Console, click the **Add Device** button.
6. In the **Device Address** box, type the recorder’s hostname or IP address. If the replacement recorder has the same IP address as the original recorder, you may see a note indicating that the recorder cannot be added because it is already in the list. To add the replacement recorder, perform the following task:

   - Click the original recorder in the **Device Selector** panel and then click the **Remove Device** button. Repeat step 6. to add the replacement recorder.

7. Register the recorder with the ESM as outlined in “Registering and Unregistering Recorders With an ESM” on page 195.

WARNING: As part of the ESM registration process, specify a station ID for the recorder. The ID of the replacement recorder must match the original recorder’s ID. Otherwise the replacement recorder will not be updated with the original settings.

8. If the original recorder had one or more installed licenses, add the licenses to the replacement recorder. For information about adding licenses, see “Adding Licenses to a Recorder” on page 34.

9. If the recorder has an IP camera card, configure its network settings. For more information, see the *Installing a Recorder and Testing Peripheral Connections Quick Steps* publication included on your March Networks CD.

Chapter 23

Performing Additional Financial and Retail Site Management Tasks

Financial and retail site administrators must perform tasks in the Administrator Console to allow users to search for ATM, teller, or POS transactions in the Investigator, and view the associated video.

The following topics are covered in this chapter:

Configuring Financial Sites

Individuals at your organization can use the Investigator to search for transactions retained on the ESM, based on date and time, or other search criteria, such as ATM.

You can set up links between your cameras and your teller stations or ATMs, which let the Investigator software automatically link video with the matching transaction. Typically, you set up these links before users are given access to the Investigator, to ensure that both video and transaction receipts are displayed.

After these links are set up, users can search archived transactions and automatically view the video captured during the transaction.

The Financial Site Management task type is only available when:

- You have purchased a Financial Transaction Investigation software license.
- The Financial Transaction Investigation service is activated on the ESM.
- The Administrator Console is connected to the ESM. For information about connecting to an ESM, see "Connecting to an ESM" on page 16.
- Your user profile is configured with access to the Financial Site Management feature.

Users must have the appropriate user rights before they can search for transactions. For information about setting user rights, see "Creating User Profiles and Accounts" on page 188.

Understanding Recorder Organization: Financial Site Management Page

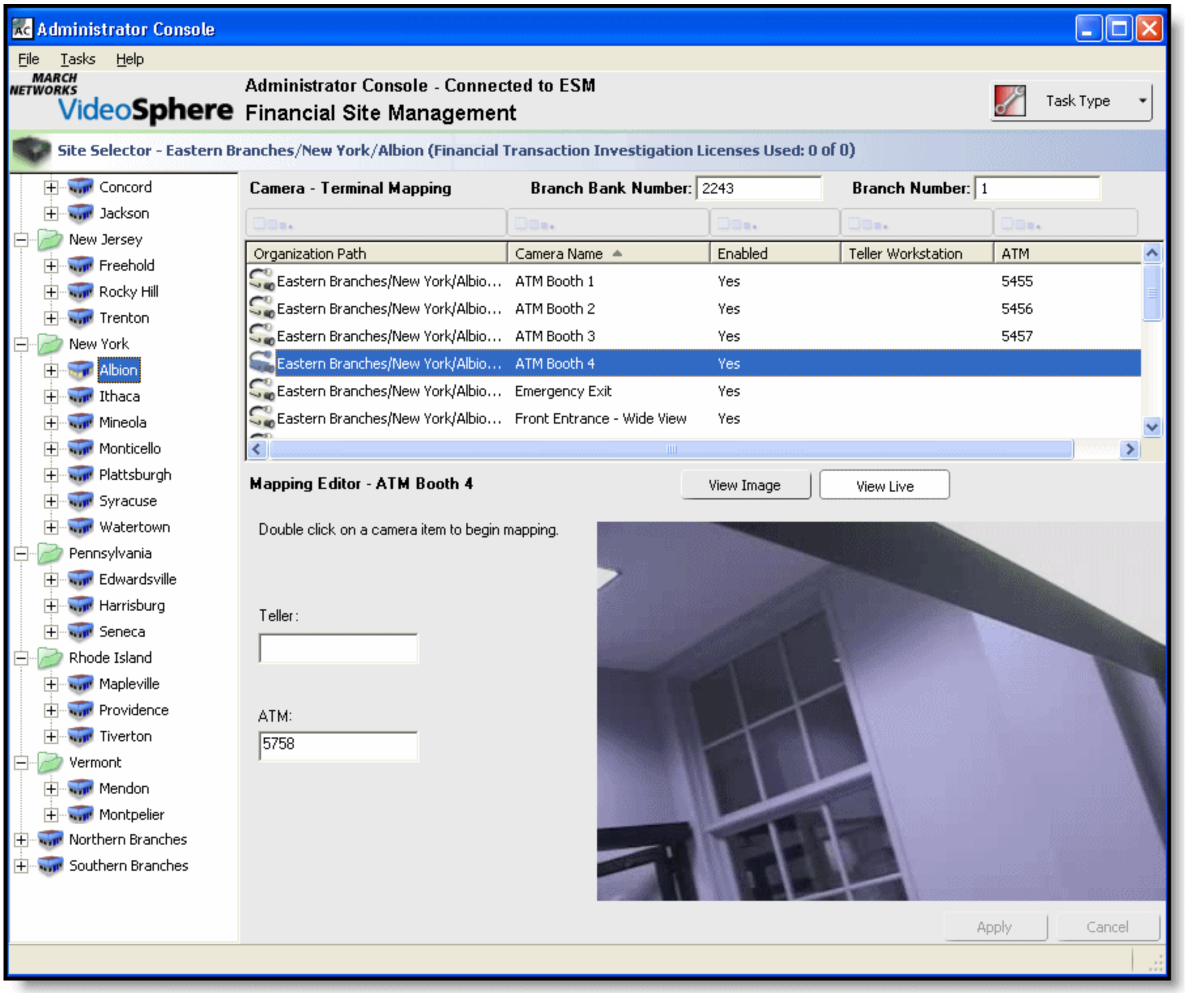
The Site Selector on the Financial Site Management page shows the sites at your organization. Each site can contain one or more recorders.

If you are connected through dial-up, the connection is lost if you switch task types.

The way recorders are grouped within folders on the Device Management page determines how sites are organized in the Site Selector. For information about organizing recorders, see "Organizing Recorders and Exporting the Recorder List" on page 149.

If you have recently reorganized the recorders on the Device Management page, it may take a moment before the changes are reflected in the Site Selector.

The Site Selector does not show individual recorders. To view the individual recorders that are grouped within the site, click the site and then review the Organization Path column in the Camera-Terminal Mapping list.



Administrator Console - Connected to ESM

Financial Site Management

Site Selector - Eastern Branches/New York/Albion (Financial Transaction Investigation Licenses Used: 0 of 0)

Camera - Terminal Mapping

Branch Bank Number: 2243

Branch Number: 1

Organization Path	Camera Name	Enabled	Teller Workstation	ATM
Eastern Branches/New York/Albio...	ATM Booth 1	Yes		5455
Eastern Branches/New York/Albio...	ATM Booth 2	Yes		5456
Eastern Branches/New York/Albio...	ATM Booth 3	Yes		5457
Eastern Branches/New York/Albio...	ATM Booth 4	Yes		
Eastern Branches/New York/Albio...	Emergency Exit	Yes		
Eastern Branches/New York/Albio...	Front Entrance - Wide View	Yes		

Mapping Editor - ATM Booth 4

Double click on a camera item to begin mapping.

Teller:

ATM: 5758

Configuring the ESM to Automatically Link Video to Financial Transactions

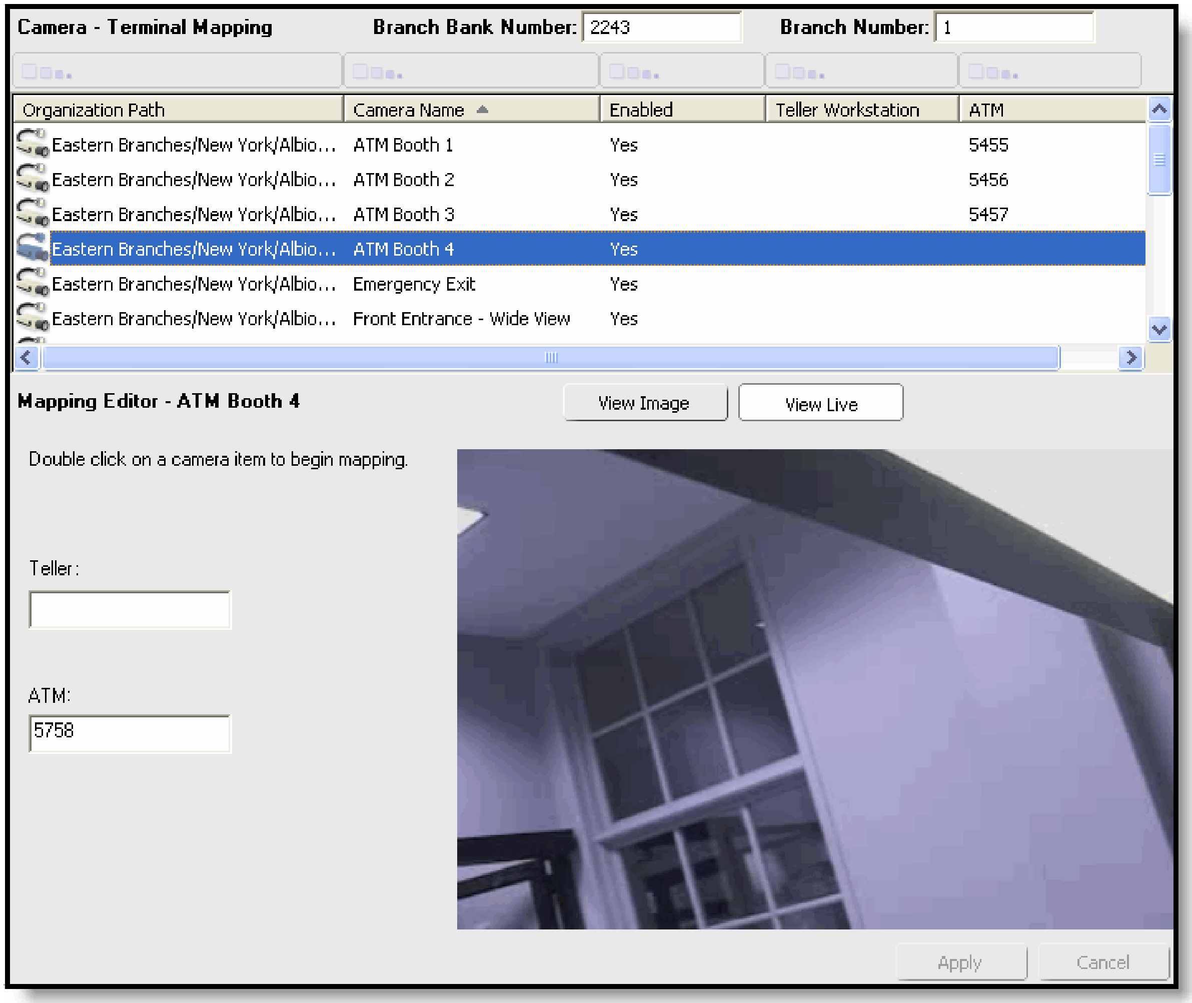
To configure the ESM to automatically link video to transactions, you must map cameras to your ATMs or teller workstations.

To configure the ESM to automatically link video to transactions

1. Ensure the **Financial Site Management** task type is selected.
2. Click a site in the **Site Selector**.
3. If you are linking video to teller transactions, type the branch bank number in the **Branch Bank Number** box, and type the branch number in the **Branch Number** box.

   The branch bank number and the branch number that you specify apply to all recorders at the selected site.
4. In the **Camera - Terminal Mapping** list, double-click an enabled camera.
5. In the **Mapping Editor**, do one of the following:
   - Type the teller ID in the **Teller** box.
   - Type the ATM number in the **ATM** box.
6. Press **ENTER** to accept the value.

7. Click **Apply**.



Camera - Terminal Mapping

Branch Bank Number: 2243

Branch Number: 1

Organization Path	Camera Name	Enabled	Teller Workstation	ATM
Eastern Branches/New York/Albio…	ATM Booth 1	Yes		5455
Eastern Branches/New York/Albio…	ATM Booth 2	Yes		5456
Eastern Branches/New York/Albio…	ATM Booth 3	Yes		5457
Eastern Branches/New York/Albio…	ATM Booth 4	Yes		
Eastern Branches/New York/Albio…	Emergency Exit	Yes		
Eastern Branches/New York/Albio…	Front Entrance - Wide View	Yes		

Mapping Editor - ATM Booth 4

Double click on a camera item to begin mapping.

Teller:

ATM: 5758

Configuring Retail Sites

Individuals at your organization can use the Investigator to search for POS transactions retained on the ESM, based on date and time, or other search criteria, such as void transactions or a price discount amount.

You can set up links between your cameras and your POS terminals, which let the Investigator software automatically link video with the matching transaction. Typically, you set up these links before users are given access to the Investigator, to ensure that both video and transaction receipts are displayed.

After these links are set up, users can search archived transactions and automatically view the video captured during the transaction.

The Retail Site Management task type is only available when:

- You have purchased a Retail Transaction Investigation license.
- The Retail Transaction Investigation service is activated on the ESM.
- The Administrator Console is connected to the ESM. For information about connecting to an ESM, see "Connecting to an ESM" on page 16.
- Your user profile is configured with access to the Retail Site Management feature.
- Users must have the appropriate user rights before they can search for transactions. For information about setting user rights, see "Creating User Profiles and Accounts" on page 188.

Understanding Recorder Organization: Retail Site Management Page

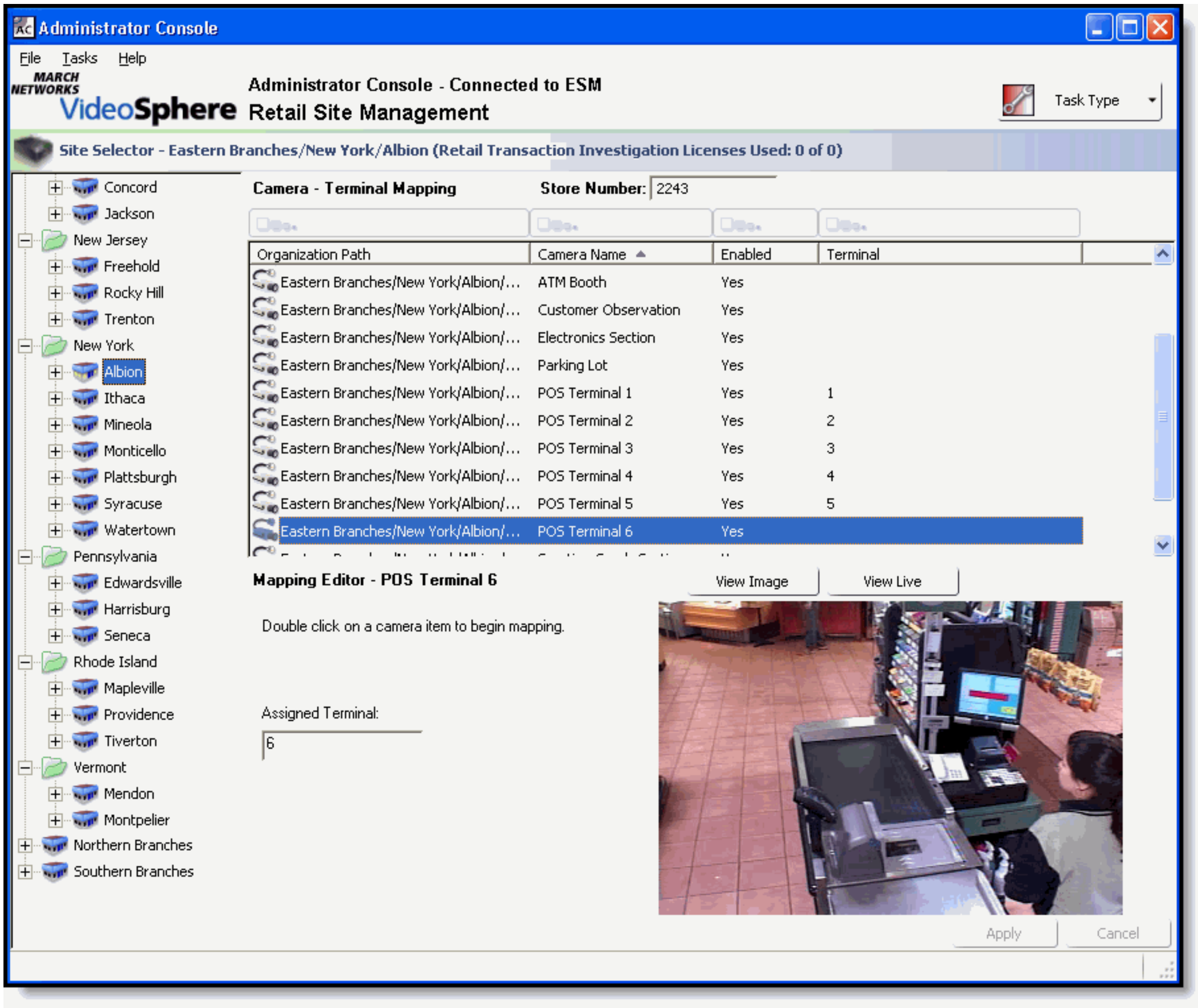
The Site Selector on the Retail Site Management page shows the sites at your organization. Each site can contain one or more recorders.

If you are connected through dial-up, the connection is lost if you switch task types.

The way recorders are grouped within folders on the Device Management page determines how sites are organized in the Site Selector. For information about organizing recorders, see “Organizing Recorders and Exporting the Recorder List” on page 149.

If you have recently reorganized the recorders on the Device Management page, it may take a moment before the changes are reflected in the Site Selector.

The Site Selector does not show individual recorders. To view the individual recorders that are grouped within the site, click the site and then review the Organization Path column in the Camera-Terminal Mapping list.



Administrator Console - Connected to ESM

Retail Site Management

Site Selector - Eastern Branches/New York/Albion (Retail Transaction Investigation Licenses Used: 0 of 0)

- Concord
- Jackson
- New Jersey
  - Freehold
  - Rocky Hill
  - Trenton
- New York
  - Albion
  - Ithaca
  - Mineola
  - Monticello
  - Plattsburgh
  - Syracuse
  - Watertown
- Pennsylvania
  - Edwardsville
  - Harrisburg
  - Seneca
- Rhode Island
  - Mapleville
  - Providence
  - Tiverton
- Vermont
  - Mendon
  - Montpelier
- Northern Branches
- Southern Branches

Camera - Terminal Mapping

Store Number: 2243

Organization Path	Camera Name	Enabled	Terminal
Eastern Branches/New York/Albion/...	ATM Booth	Yes	
Eastern Branches/New York/Albion/...	Customer Observation	Yes	
Eastern Branches/New York/Albion/...	Electronics Section	Yes	
Eastern Branches/New York/Albion/...	Parking Lot	Yes	
Eastern Branches/New York/Albion/...	POS Terminal 1	Yes	1
Eastern Branches/New York/Albion/...	POS Terminal 2	Yes	2
Eastern Branches/New York/Albion/...	POS Terminal 3	Yes	3
Eastern Branches/New York/Albion/...	POS Terminal 4	Yes	4
Eastern Branches/New York/Albion/...	POS Terminal 5	Yes	5
Eastern Branches/New York/Albion/...	POS Terminal 6	Yes	

Mapping Editor - POS Terminal 6

Double click on a camera item to begin mapping.

Assigned Terminal: 6

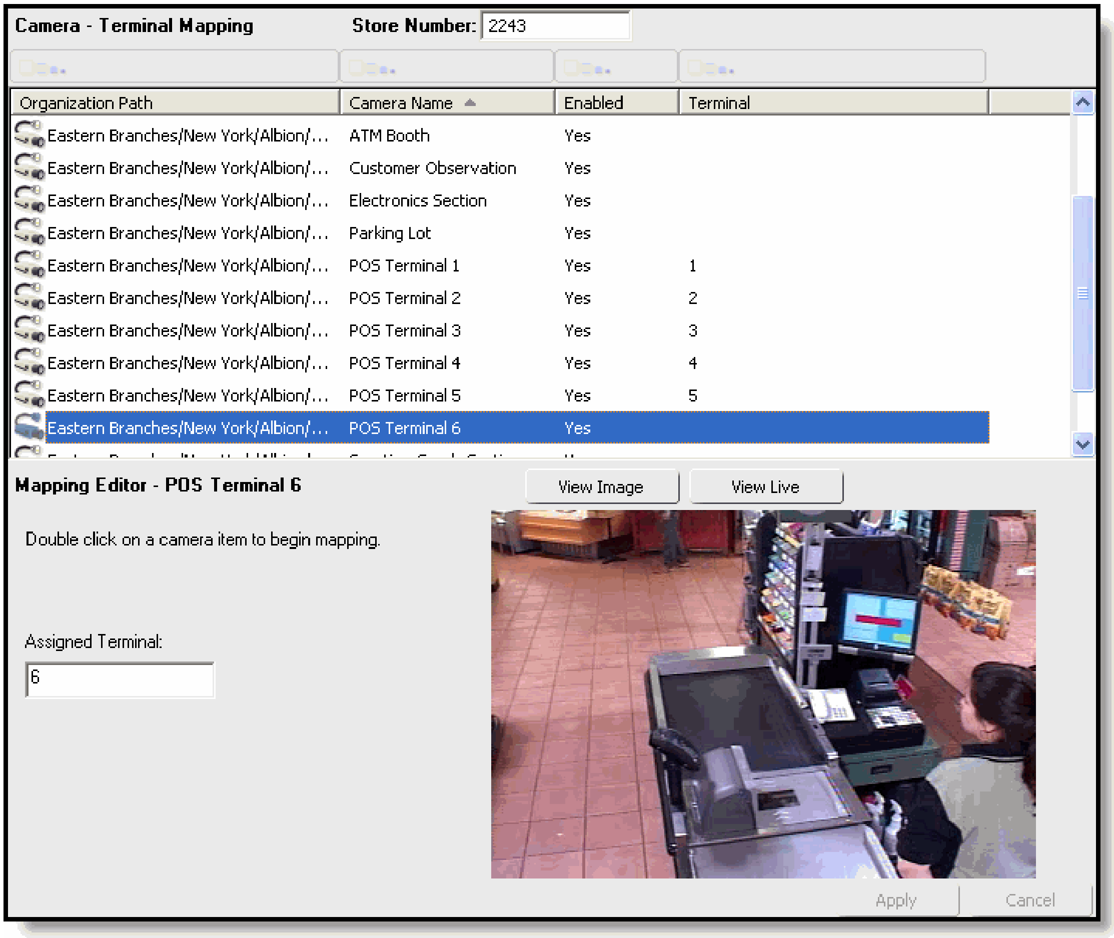
Configuring the ESM to Automatically Link Video to Retail Transactions

To configure the ESM to automatically link video to transactions, you must map cameras to your POS terminals.

To configure the ESM to automatically link video to POS terminals

1. Ensure the **Retail Site Management** task type is selected.
2. Click a site in the **Site Selector**.
3. Type the store number in the **Store Number** box.

   The store number that you specify applies to all recorders at the selected site.
4. In the **Camera - Terminal Mapping** list, double-click an enabled camera.
5. In the **Mapping Editor**, type the POS terminal number in the **Assigned Terminal** box.
6. Press **ENTER** to accept the value.
7. Click **Apply**.



Camera - Terminal Mapping

Store Number: 2243

Organization Path	Camera Name	Enabled	Terminal
Eastern Branches/New York/Albion/...	ATM Booth	Yes	
Eastern Branches/New York/Albion/...	Customer Observation	Yes	
Eastern Branches/New York/Albion/...	Electronics Section	Yes	
Eastern Branches/New York/Albion/...	Parking Lot	Yes	
Eastern Branches/New York/Albion/...	POS Terminal 1	Yes	1
Eastern Branches/New York/Albion/...	POS Terminal 2	Yes	2
Eastern Branches/New York/Albion/...	POS Terminal 3	Yes	3
Eastern Branches/New York/Albion/...	POS Terminal 4	Yes	4
Eastern Branches/New York/Albion/...	POS Terminal 5	Yes	5
Eastern Branches/New York/Albion/...	POS Terminal 6	Yes	

Mapping Editor - POS Terminal 6

Double click on a camera item to begin mapping.

Assigned Terminal: 6

Glossary

Access level The authorization level a user must have to access recorders or peripherals using the March Networks software applications, such as the Investigator. Users can access recorders and peripherals with an equivalent or lower number than what is set in their profile. For example, a user with an access level of five can access recorders and peripherals set to five or lower.

The access level can range from one to 10 (one is the least-restricted access level and 10 is the most secure).

Action The activity you want the recorder to perform when a particular activity occurs. For example, during scheduled hours you want the recorder to retain video from a camera for an extended period of time. In this example, the action refers to the Retention action.

Alarm source A camera or alarm input for which you can set up alarm monitoring.

Analog camera A camera that connects to the recorder’s video inputs using a BNC coaxial cable connection.

DHCP Dynamic Host Configuration Protocol. The protocol by which an IP address is assigned to each node in a network.

Docking station A metal frame that holds a 4000 Series recorder in place. All main peripheral connections, including the required connection to a camera and power source are made to the docking station — not the recorder — allowing peripheral cables to remain in place when the recorder is serviced, or undocked.

ESM Enterprise Service Manager. A server application that lets you monitor and maintain recorders on your network, at one or more sites. The ESM can be made up of one or more servers, which form a cluster.

Event The activation of a trigger. An event can be the activation of a physical peripheral, such as a door contact. Or, an event can refer to activity occurring during a scheduled time period.

Evidence Data captured by a recorder, including video, audio, and text captured from an external peripheral, such as an ATM or POS register.

Evidence Manager A tool that provides senior loss prevention, security, or operations managers with the tools for building and managing investigation cases.

Evidence Reviewer A playback tool that allows third-party investigators or law enforcement authorities to view video captured by the recorder and review cases created with the Evidence Manager.

To ensure that others can review evidence copied to CD, the Evidence Reviewer is automatically included when evidence is burned to CD from the Evidence Manager or Investigator.

Group tag The name provided to one or more peripherals, which helps investigators quickly find evidence for a specific scenario.

For example, if investigators at your organization typically view video from cameras A, B, and C when investigating activity at the service desk, specify “Service Desk” as the group tag for cameras A, B, and C. When users open the Investigator, the cameras automatically appear in a group labeled “Service Desk,” providing them with quick access to cameras A, B, and C.

Installer Console A setup tool that lets installers test the peripherals connected to the recorder.

Investigator A tool that helps security, theft, and fraud investigators locate video evidence linked to an investigation.

The Investigator works alongside the Evidence Manager to allow users to quickly locate video evidence and then organize the evidence for distribution to third-party investigators or law enforcement authorities.

IP camera A camera that connects to the recorder's IP camera card using a CAT5 cable, or streams video to the recorder over a network connection.

Live Monitoring Console A tool that allows security personnel to monitor video and alarms in real time, and respond to alarm events.

Managed environment A site that uses an ESM to centrally monitor and maintain recorders on the network.

Network administrator The person or team responsible for setting up and maintaining the network. Duties of the administrator include installing software, assigning passwords, making backups, and resolving network problems.

Non-managed environment A site that has networked recorders, which are manually monitored and maintained by a system administrator.

NTP server Network Time Protocol server. A server that is used to synchronize computer and server clock times in a network of computers or servers.

Provisioning interface A software application running on the recorder that lets you configure the recorder's general settings. The provisioning interface is accessed using a terminal emulation program, such as HyperTerminal, or a secure shell client, such as PuTTy.

Peripherals Security tools connected to a recorder, such as cameras, audio inputs and outputs, alarm inputs, dataports, and switches.

Recorder A device at your site that captures, retains, and streams audio, video, and text data from connected peripherals.

System administrator An individual within your organization that is responsible for monitoring and maintaining your recorders.

Target The peripheral the recorder uses to perform an action when a trigger is activated. For example, during scheduled hours you want the recorder to retain video from a camera for an extended period of time. In this example, the target is the camera.

Task type An Administrator Console tool that lets you switch between different activities. The user profile assigned to your user account defines the task types you can access.

Each task has its own Administrator Console page where you can review and customize recorder and system settings. To switch between different activities, click the Task Type button at the top right of the Administrator Console.

Trigger Something that prompts the recorder to perform an action. A trigger can be a physical peripheral, such as a door contact. A trigger can also be a scheduled time period. For example, during scheduled hours you want the recorder to retain video from a camera for an extended period of time. In this example, the trigger is the schedule time period.

User profile A set of access rights that can be applied to a user account to restrict access to system tools and recorders.

Index