March Networks

Command Recording Software 2.10

Configuration Guide

North America	+1 800 563 5564
Latin America	+5255 5259 9511
Europe	+39 0362 17935
Asia	+65 6818 0963
Australia and New Zealand	+61 1300 089 419
Middle East and Africa	+971 4 399 5525

www.marchnetworks.com

Notice of Rights

Part Number

38389 Rev1.0 April 2020

Contents

Chapter 1

Welcome to Command Recording Software

March Networks® Command™ Recording Software (CRS) is the key component of the Command Professional and Command Enterprise solutions that supports the recording, storage, retrieval, and management of video evidence. Evidence is streamed to the Command Recording Software by IP cameras, encoders, and NVRs using a network connection. The Command Recording Software also features a client interface, Command Client, that allows security operators to view live video and review and export video evidence archived on the Command Recording Software.

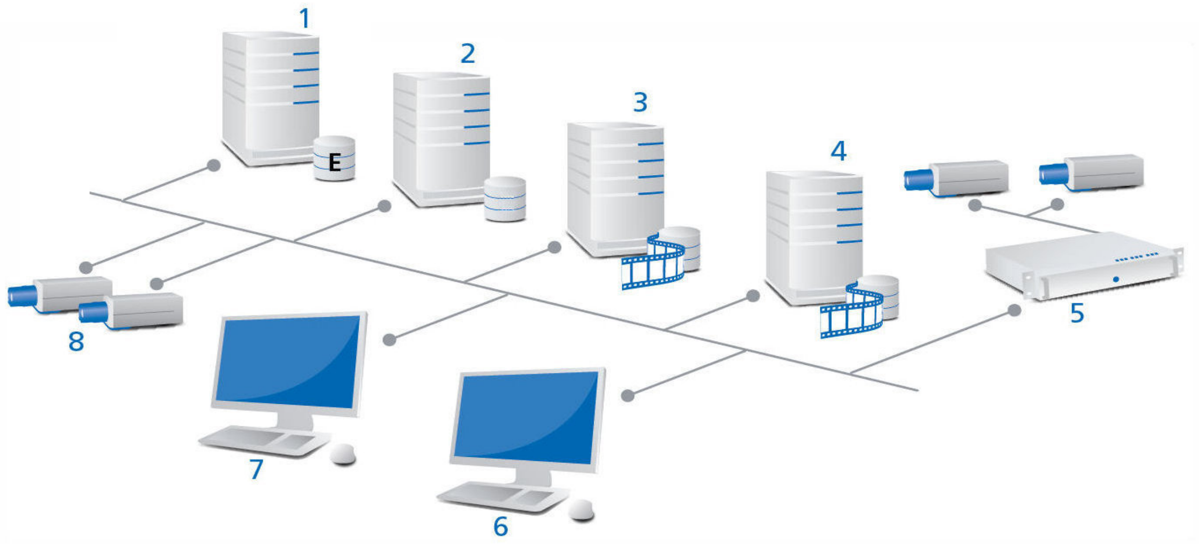
This guide outlines the full installation, configuration and maintenance activities that administrators can perform to locate IP devices on the network, configure evidence storage and recording, and customize recording schedules.

Important Notes:

- Starting from version 2.9, the Command Recording Software has switched from a 32-bit architecture with a 128 camera limit to a 64-bit architecture with a 500 camera limit. The architecture upgrade is entirely managed by the installation wizard.
- For more information about the Command Client installation and usage, see the *Command Client User Guide*, available on the Software DVD, on the Command Recording Software installation package, or from the March Networks Partner Portal and official websites.

Command Enterprise Solution Diagram

The following diagram illustrates the Command Enterprise solution.



1 Enterprise Server Software (with SQL Server)

2 Command Media Archiver

3 Command Recording Software (Primary)

4 Command Recording Software (Backup/Redundant)

5 March Networks Hybrid Network Video Recorder (NVR) with Analog Cameras

- 6700 Series Hybrid NVR
- 8000 Series Hybrid NVR
- 9000 Series NVR
- RideSafe GT, MT, and RT Recorders

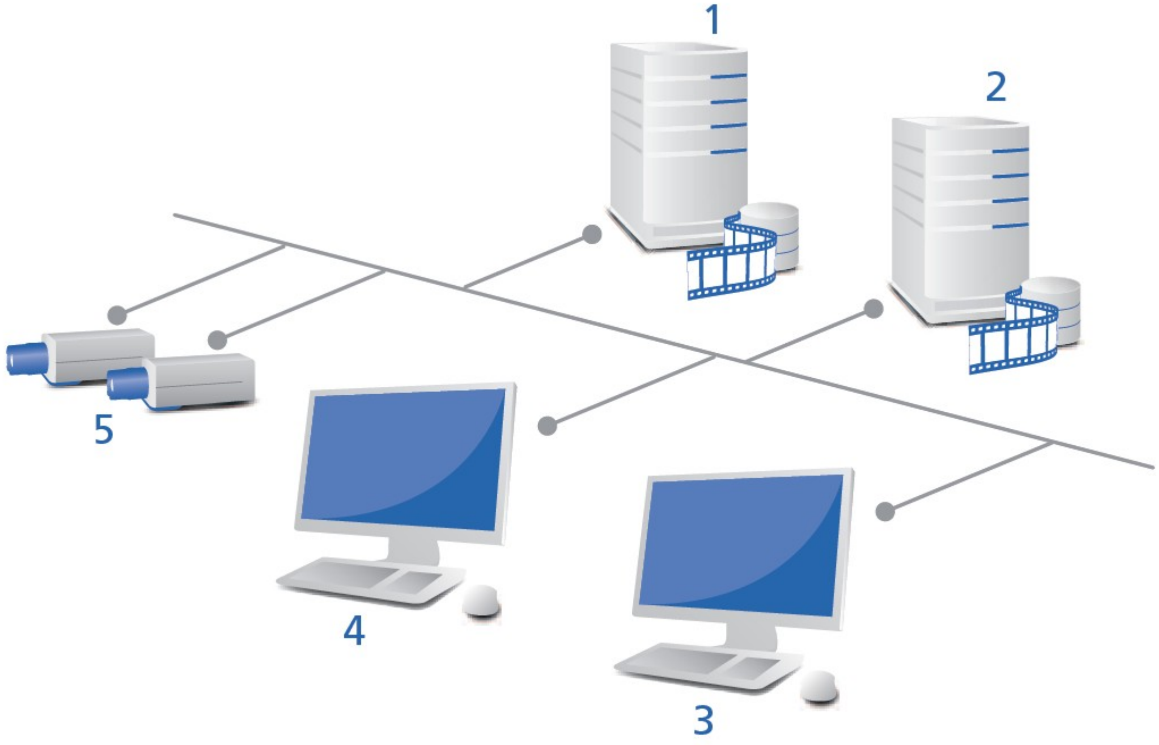
6 Command Config Application for Command Recording Software

7 Command Client Application

8 IP Edge Devices (Encoders and IP Cameras)

Command Professional Solution Diagram

The following illustration identifies the components of a Command Recording Software solution.



1 Command Recording Software

2 Redundant Command Recording Software

3 Command Client Application

4 Command Config Application

5 IP Edge Devices (Encoders and IP Cameras)

Before You Begin

Before you begin, you must properly install the Command Recording Software on a standard server. For more information, see “Installing Command Recording Software” on page 17. Also, ensure you have installed and configured the IP cameras and encoders from which you want to capture video.

Components of the Command Solution

The following table describes the main components of the Command solution.

Component	Description
Command Enterprise Software (CES) 	Command Enterprise Software (CES) is the center of the Command Solution. The CES stores the surveillance system's configuration in a relational database, either on the management server computer itself or on the customer's existing SQL Server on the network. The Enterprise Server also handles global user authentication, user rights, and hosts the web services for Command's web-client. The Enterprise Server software can run on most commercial-off-the-shelf (COTS) servers from top server manufacturers or it can run in a VMware® Virtual Machine. Command Enterprise can support up to 128,000 camera mixed over various recorders, and mix matched with Hybrid NVR's and R5 DVRs. The maximum number of recorders/recording servers in a single system is 10,000.
Command Recording Software (CRS) 	Command Recording Software (CRS) is the primary archive engine for the Command solution. The recording server software is designed to run separately from the Command Enterprise Software. It can be installed directly on any COTS servers or can be purchased from March Networks running on Dell® Platforms. Another option for the recording server software is to run it on a VMware virtual machine (VM). Up to 500 cameras per recording server (v.2.9.0 and higher - 128 cameras for v.2.8.0 and lower). Two types of recording server include: • Primary Recording Server is the primary archiving component of the Command Recording Software architecture • Redundant Recording Server redundant/failover archiving component of the Command Recording Software architecture
Command Lite Software 	Command Lite is a limited, free version of Command Professional. It can be installed either on standard servers or compatible PCs with Windows 7® or higher. Command Lite allows you to: • Add up to six IP cameras • Configure continuous and programmed recording • Retain the video archive for up to 7 days • Configure user accounts and permissions • Configure and manage storage

Component	Description
Command Client Software 	Command Client is the primary client user interface for Command. Command Client is a standalone application that offers an intuitive user interface that allows administrators and users alike to manage their Command video surveillance network. **Note:** Edge devices a still use the browser-based interface (Command Client 1.11) downloaded directly from the device.
Command Config 	Command Config is a client user interface for configuration and management. Command Config is a standalone application that can be downloaded directly from server running Command Recording Software.
March Networks Recorders (NVRs and Hybrid NVRs) 	• 8000 Series Recorders • 9000 Series Full-IP NVRs • 6700 Series Hybrid NVR • RideSafe GT, MT, and RT Recorders Devices that capture, retain, and stream audio, video, and text data from connected peripherals. Analog cameras are connected to hybrid NVRs or encoders using BNC connection.
Searchlight application 	An application running on a Command Enterprise Server that integrates video with point-of-sale (POS - retail version), ATM, and teller workstations (banking version) transaction data to create reports and charts, and identify and investigate suspicious transactions and stop theft.
Command Transportation 	An application running on a Command Enterprise Server that integrates video from mobile recorders with GPS coordinates. The application allows the user to create detailed incident reports and perform searches based on the metadata recorded with the video.

Command Recording Software Overview

Command Recording Software is the key component of the Command Professional and Command Enterprise recording solutions.

The Command Recording Software is managed by two tools:

- Command Config Application
- Command Client Application

Command Config

Command Config is a standalone application downloaded directly from the Command Recording Software that lets you discover devices on the network, and customize the video surveillance system to ensure that the video your organization relies on is always available.

Specifically, Command Config lets you:

- Create user profiles and specify user access levels for all aspects of the video surveillance system.
- Schedule monitoring, access, and recording activities to ensure that users have access during required times.
- Configure storage group and manage storage disks.
- Add cameras and set up Shadow Archive to synchronize recorded video from IP cameras and encoders when the network is unavailable (for example, during scheduled server maintenance, or when network connectivity or power is lost).

Command Client

Command Client is a standalone application that lets you view live video of the cameras added to a Command Recording Software. It also allows you to review and export recorded video evidence. For more information about the Command Client usage, see the *Command Professional and Client User Guide*, available on the Software DVD, from the March Networks Partner Portal and official websites, or as the Online Help for Command Client.

Acronyms and Abbreviations

The following acronyms and abbreviations are used in this guide.

Acronym	Description
AUX	**Auxiliary Channel**. Devices (such as LEDs, sirens, and switches) connected to the auxiliary channels of cameras, recorders and extension boards. Command Config refers to auxiliary channels as *Switches*.
CES	**Command Enterprise Server**. The center of the Command Solution, capable of managing 8000/9000 Series recorders, RideSafe recorders, 6700 Series Hybrid NVRs, and Command Recording Softwares.
CMA	**Command Media Archiver.** The Command Media Archiver component collects and stores data for the Command Enterprise case management functionality, allowing users to share case files. It also stores transaction data for the Searchlight application, and GPS, incident and metadata for the Command Transportation application.
CME	**Command Multimedia Evidence**. A proprietary video format that can be played back only using the Command Player application.
CRS	**Command Recording Software**. The recording component of the Command Professional and the Command Enterprise product offerings.
DVR	**Digital Video Recorder**. Devices that capture, retain, and stream audio, video, and text data from peripherals (such as analog cameras) directly connected to the device.
LDAP	**Lightweight Directory Access Protocol**. A protocol used for network administration and security, in particular for user authentication services.
NAS	**Network Attached Storage**. An external storage connected to the network.
NAT	**Network Address Translation**. A technique that allows remapping a given address space into another address space by modifying the network address information in the IP packet headers while transferring the packet across a traffic routing device.
NVR	**Network Video Recorder**. Devices that capture, retain, and stream audio, video, and text data from connected peripherals on the network.
ONVIF	**Open Network Video Interface Forum**. A standard protocol for the communication of IP devices in a video surveillance infrastructure.
OSD	**On Screen Display**. The native configuration menu of an edge device (in particular for sensors and PTZ controls).
PTZ	**Pan**, **Tilt**, **Zoom**. A PTZ camera is a closed-circuit television camera with remote directional, zoom, and, optionally, focus and iris control.
RAID	**Redundant Array of Independent Disks**. A storage technology that combines multiple storage disks into a logical unit
VMS	**Video Management System**. A recording software running on standard servers. Command Recording Software is March Networks' VMS application.

Other Available Publications

Additional publications about the Command solution are available in PDF format on your March Networks DVD or Command installation package, and are available for download from the March Networks Partner Portal and official websites.

Note: The Command Recording Software Configuration Guides are available in English, Français, Italiano, and Español from the March Networks Partner Portal and official websites.

System Disposal

If elements of your video surveillance system become obsolete, you must take care of the disposal of all types of media used to store data, including magnetic hard drives (HDD), solid state drives (SSD), self-encrypting drives (SED), SD cards, USB keys and other flash based portable media (portable flash) and flash memory on board in an embedded device (embedded flash). For more information about system disposal, download the *Data Protection and Privacy Application Note* from the March Networks Partner Portal.

What's Next

To install and configure a Command Recording Software, you can perform the following functions:

- Install the Command Recording Software. For more information, see “Installing Command Recording Software” on page 17.
- Install the Command Config application and access the Command Recording Software. For more information, see “Getting Started” on page 29.
- Configure the software's main feature using the Configuration Wizard. For more information, see “Using the Configuration Wizard” on page 48.
- Add user accounts, create user profiles, and specify user preferences. For more information, see “Managing User Profiles” on page 60.
- Manage connections to the server. For more information, see “Managing User Sessions and Network Connections” on page 99.
- Add and configure identification certificates for enhanced security. For more information, see “Configuring Identification Certificates” on page 104.
- Configure local and system settings. For more information, see “Configuring System Settings” on page 109.
- Add and manage storage disks. For more information, see “Creating Storage Groups” on page 135.
- Discover, add and configure IP cameras and PTZ cameras. For more information, see “Managing Cameras with Command” on page 144.
- Create and configure recording schedules. For more information, see “Creating Recording Schedules” on page 197.
- Configure physical alarms and create new alarms based on conditions. For more information, see “Creating and Customizing Alarms” on page 213.

- Configure the switches connected to edge devices or to the I/O Extension Board. For more information, see “Managing Switches” on page 229.
- Configure input and output (*talk*) audio channels. For more information, see “Managing Audio Channels” on page 242.
- Create custom conditions for alarms and recording. For more information, see “Creating Custom Conditions” on page 247.
- Configure text insertion filters for alarms and recording. For more information, see “Configuring Text Insertion Filters” on page 256.
- Set redundant machines for backup support. For more information, see “Setting Redundant Machines” on page 260.

Chapter 2

Installing Command Recording Software

This chapter describes how to install and uninstall a Command Recording Software, and start the Command Recording Software service.

Important: This chapter refers to a new installation of the Command Recording Software or an upgrade from a previous version to version 2.10. For more information about Command software updates, see the latest *Release Notes* for the Command solution, available for download from the March Networks Partner Portal and official websites.

This chapter contains the following sections:

- "System Requirements" on page 18
- "Installing Command Recording Software" on page 19
- "Managing the Command Recording Software" on page 24

System Requirements

Before you install the Command Recording Software, ensure your server meets the recommended requirements.

Important Notes:

- To install Command Recording Software on a system that has Internet Information Server (IIS) installed, you must change the HTTP (default: 80) and HTTPS (default: 443) ports by accessing the **Command Management** application. For more information, see “Managing the Command Recording Software” on page 24.
- When used with a 32-bit system, it is not possible to upgrade to version 2.9 or higher (64-bit version).
- It is strongly recommended that you consult your March Networks Sales Engineer for any questions or concerns before deploying the Command Recording Software solution for centralized environment.

	SMALL Less than 32 Cameras	MEDIUM 32 to 64 Cameras
Operating system	Windows Server 2012, 2012 R2, 2016, or 2019 Windows 8, 8.1, or 10 (All systems including the operating system must be 64-bit.)	
Processor (CPU)	Dual Core Intel i5	Quad Core Intel i7
HDD Space	100 GB for CRS installation and usage	
Storage for Video Archive	Storage volumes for video recording must be exclusive to the CRS and managed by the CRS server’s Operating System. Consider RAID volumes for optimal performance and resilience. For external storage, consider DAS (Direct Attached Storage) or Block Level SAN technologies such as iSCSI or virtual disks. We do not recommend SMB/CIFS storage because of inconsistent performance. Use the March Networks System Design Tool (or an appropriate third-party camera calculator) to calculate the required storage size to meet retention needs. It is extremely important that the Video Storage volume and its connection to the CRS can indefinitely sustain recording on all cameras simultaneously (consistent write speed is greater than the total camera aggregated bit rate). Consult your March Networks Sales Engineer for any questions or concerns.	
Network Interface	Gigabit Ethernet	2x Gigabit Ethernet (dedicated NIC for camera network)
Memory	4 GB (minimum)	6 GB

	LARGE 65 to 128 Cameras	EXTRA LARGE 129 to 500 Cameras
Operating system	Windows Server 2008 R2, 2012, 2012 R2, 2016, or 2019 Windows 8, 8.1, or 10 (All systems including the operating system must be 64-bit.)	
Processor (CPU)	Quad Core Intel Xeon	Eight Core Intel Xeon Silver
HDD Space	200 GB for CRS installation and usage	100 GB for CRS installation + 100 GB every 100 cameras (i.e. for 500 cameras: 600 GB)
Storage for Video Archive	Storage volumes for video recording must be exclusive to the CRS and managed by the CRS server's Operating System. Consider RAID volumes for optimal performance and resilience. For external storage, consider DAS (Direct Attached Storage) or Block Level SAN technologies such as iSCSI or virtual disks. We do not recommend SMB/CIFS storage because of inconsistent performance. Use the March Networks System Design Tool (or an appropriate third-party camera calculator) to calculate the required storage size to meet retention needs. It is extremely important that the Video Storage volume and its connection to the CRS can indefinitely sustain recording on all cameras simultaneously (consistent write speed is greater than the total camera aggregated bit rate). Consult your March Networks Sales Engineer for any questions or concerns.	
Network Interface	2 to 4x Gigabit Ethernet (One or more dedicated NICs for camera networks)	4x Gigabit Ethernet (One or more dedicated NICs for camera networks)
Memory	16 GB	32 GB

Installing Command Recording Software

Use your Command Software DVD to install the Command Recording Software on the server.

WARNING: Some antivirus software programs may interfere during the installation of the Command Recording Software. It is strongly recommended that you temporarily disable the antivirus program before you install the Command Recording Software application.

To install Command Recording Software

1. Insert your Command Software DVD into the server's DVD-ROM drive or double-click the **Autorun.exe** file on the installation package.
2. On the main page, click **Software**.
3. On the **Software** page, click **Command Recording Software**.

   The setup wizard appears.
4. Read the software license agreement and select the **I accept the terms in the License Agreement** check box.

   Note: You must accept the software license agreement before you can install Command Recording Software. If you do not accept the agreement, the installation process stops.

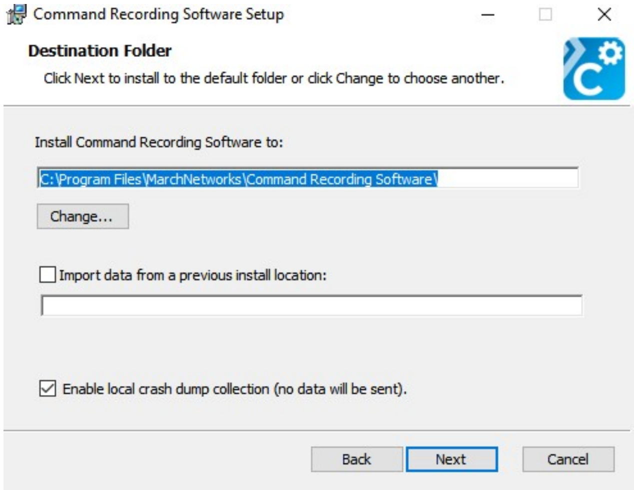
5 Click **Install** to proceed, or click **Close** to close the setup wizard.

The setup process initializes and automatically installs the components required to install the software. The **Command Recording Software Setup** dialog box appears.

6 Click **Next** to proceed to the **Destination Folder** page, or click **Cancel** to close the dialog box.

Note: The Command Recording Software verifies the amount of RAM memory in the system, warning if the amount of RAM is under 4GB.

7 Choose the folder in which you want to install the Command Recording Software. You can enter the folder path, or you can click **Change** to navigate to and select the folder.



Command Recording Software Setup

Destination Folder

Click Next to install to the default folder or click Change to choose another.

Install Command Recording Software to:

C:\Program Files\MarchNetworks\Command Recording Software\

☐ Import data from a previous install location:

☑ Enable local crash dump collection (no data will be sent).

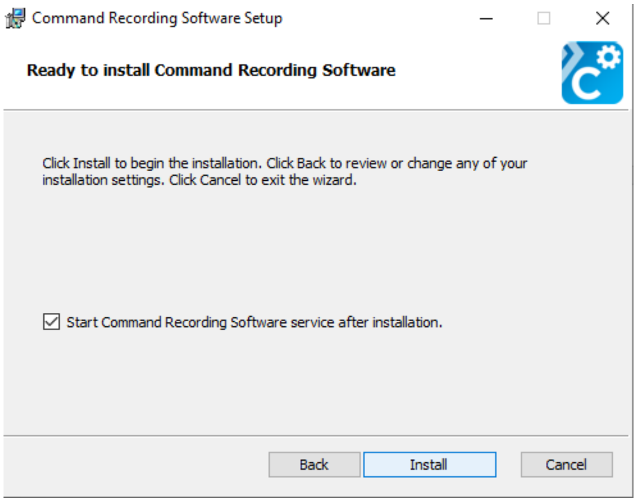
8 Ensure the **Import data from a previous install location** check box is cleared.

9 (Optional) Clear the **Enable Local Crash Dump Collection** check box to negate the OS the permission to collect information about the Command Recording Software system crashes.

10 Click **Next** to proceed, or click **Back** to return to the previous step.

Note: The setup wizard verifies the amount of free disk space, warning if the amount is under 50GB.

11 (Optional) Clear the **Start Command Recording Software after installation** check box to manually start the CRS service from the Command Management interface (see “Managing the Command Recording Software” on page 24).



Ready to install Command Recording Software

Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.

☑ Start Command Recording Software service after installation.

12 Click **Install** to launch the installation process, click **Back** to return to the previous step, or click **Cancel** to cancel the software installation and close the dialog box.

Note: During the installation process, the setup wizard verifies the Windows Firewall status, warning if the firewall is not installed or running.

13 Click **Close** to complete the installation and close the setup wizard. There is no need to reboot the server and, if the **Start Command Recording Software after installation** check box was selected, the CRS automatically starts.

Upgrading Command Recording Software

If you have already installed a previous 32-bit version of Command Recording Software, you can quickly upgrade to the version 2.9 or higher (64-bit version) by downloading the updated installer from the March Networks Partner Portal.

Notes:

- Starting from version 2.9, the Command Recording Software has switched from a 32-bit architecture with a 128 camera limit to a 64-bit architecture with a 500 camera limit. The architecture upgrade is entirely managed by the installation wizard.
- It is not possible to downgrade from version 2.9 to lower versions.
- It is recommended that you back up the configuration of your Command Recording Software before the upgrade. To back up the configuration, access the **System** menu and click **Export**. For more information, see “Exporting and Importing Configuration Settings” on page 111.
- If Command finds a duplicate name for a resource (such as cameras, switches, alarms) on a page during the upgrade, it automatically updates the name of the duplicated resource. To confirm the changes, access the pages with the modified resources and click the 💾 button.

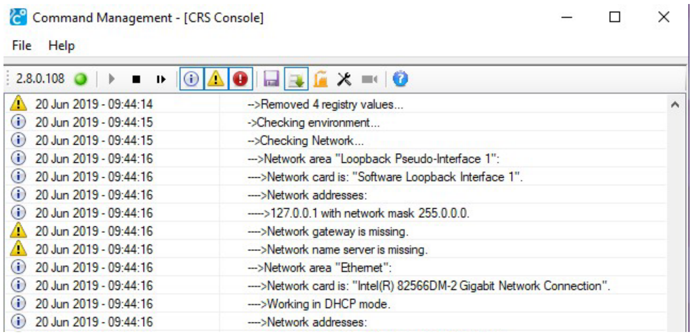
To upgrade Command Recording Software

1 Download the Command Recording Software 2.10 installation package from the March Networks Partner Portal.

Tip: You can download either the full DVD image for Command Recording Software 2.10 (including also SiteManager, documentation and legal notices) or just the software installer.

2 On the server's **Start** menu, point to **March Networks**, and then click **Command Recording Software Management**.

The **Command Management** interface appears.



```
⚠ 20 Jun 2019 - 09:44:14    -->Removed 4 registry values...
ⓘ 20 Jun 2019 - 09:44:15    ->Checking environment...
ⓘ 20 Jun 2019 - 09:44:15    -->Checking Network...
ⓘ 20 Jun 2019 - 09:44:16    --->Network area "Loopback Pseudo-Interface 1":
ⓘ 20 Jun 2019 - 09:44:16    ---->Network card is: "Software Loopback Interface 1".
ⓘ 20 Jun 2019 - 09:44:16    ---->Network addresses:
ⓘ 20 Jun 2019 - 09:44:16    ----->127.0.0.1 with network mask 255.0.0.0.
⚠ 20 Jun 2019 - 09:44:16    ---->Network gateway is missing.
⚠ 20 Jun 2019 - 09:44:16    ---->Network name server is missing.
ⓘ 20 Jun 2019 - 09:44:16    --->Network area "Ethernet":
ⓘ 20 Jun 2019 - 09:44:16    ---->Network card is: "Intel(R) 82566DM-2 Gigabit Network Connection".
ⓘ 20 Jun 2019 - 09:44:16    ---->Working in DHCP mode.
ⓘ 20 Jun 2019 - 09:44:16    ---->Network addresses:
```

3 Click the ■ button to stop the Command Recording Software service.

When the Command Recording Software service is stopped, a new entry is added to the system log.

4 Unzip the Command Recording Software installation package in a directory of your choice.

5 According to the installation package downloaded, double-click the **Autorun.exe** file to launch the installation interface or directly launch the Command Recording Software installer.

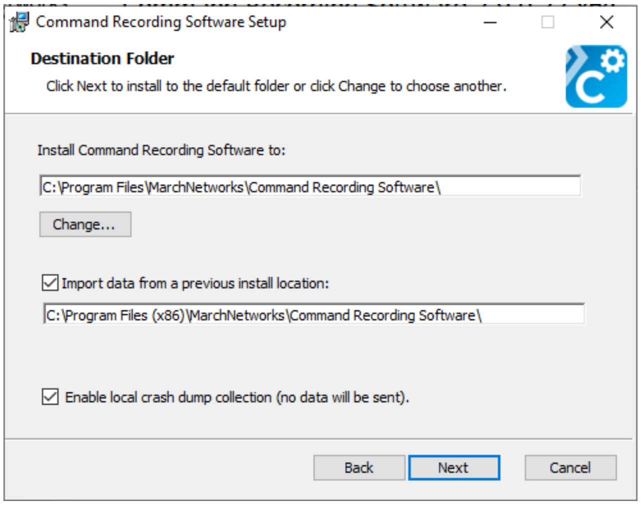
6 Follow the procedure described in "To install Command Recording Software" on page 19.

7 When the **Destination Folder** page appears select the new installation path for the 64-bit version. You can manually enter the folder path, or you can click **Change** to navigate to and select the folder.

8 Select the **Import data from a previous install location** check box and verify that the installation path for the previous CRS installation is correct.

Note: The installation wizard automatically scans the Program Files (x86) folder to search for the *CRSsrv.exe* file.

9 (Optional) Clear the **Enable Local Crash Dump Collection** check box to negate the OS the permission to collect information about the Command Recording Software system crashes.



Command Recording Software Setup

Destination Folder

Click Next to install to the default folder or click Change to choose another.

Install Command Recording Software to:

C:\Program Files\MarchNetworks\Command Recording Software\

☑ Import data from a previous install location:

C:\Program Files (x86)\MarchNetworks\Command Recording Software\

☑ Enable local crash dump collection (no data will be sent).

10 Click **Next** to proceed.

11 Proceed with the installation as described in “To install Command Recording Software” on page 19.

Managing the Command Recording Software

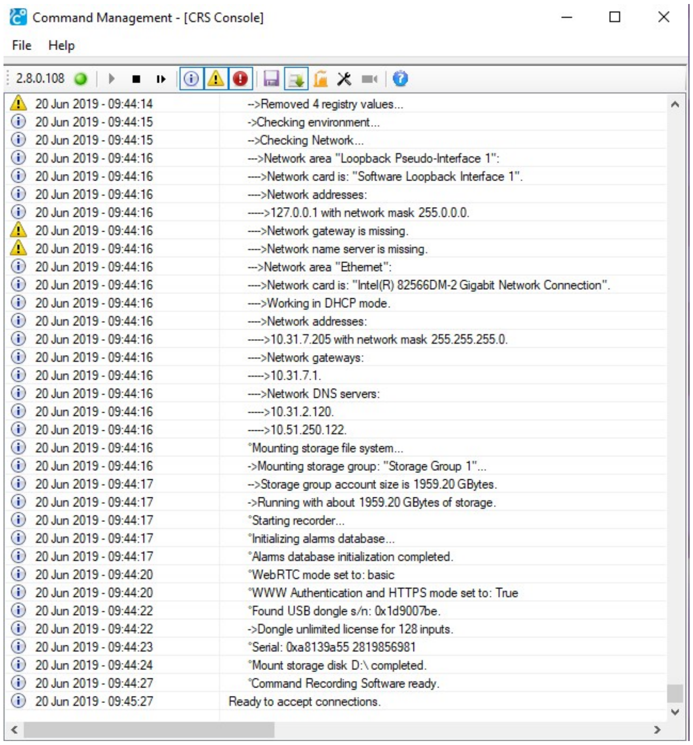
The Command Recording Software Management console is a tool that allows you to view and export the system log, start, stop and restart the Command Recording Software, modify the security settings, and revert all of the configurations to factory defaults without accessing the Command Config interface.

Note: You can access the tool only on the server where the Command Recording Software is installed. The Command Recording Software Management tool requires that Microsoft.NET Framework (version 2.0 or higher) is installed on the server.

To manage the Command Recording Software

1 On the server's **Start** menu, point to **March Networks**, and then click **Command Recording Software Management**.

The **Command Management** console appears.

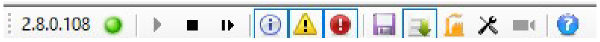


```
⚠ 20 Jun 2019 - 09:44:14     -->Removed 4 registry values...
ⓘ 20 Jun 2019 - 09:44:15     ->Checking environment...
ⓘ 20 Jun 2019 - 09:44:15     -->Checking Network...
ⓘ 20 Jun 2019 - 09:44:16     --->Network area "Loopback Pseudo-Interface 1":
ⓘ 20 Jun 2019 - 09:44:16     ---->Network card is: "Software Loopback Interface 1".
ⓘ 20 Jun 2019 - 09:44:16     ---->Network addresses:
ⓘ 20 Jun 2019 - 09:44:16     ----->127.0.0.1 with network mask 255.0.0.0.
⚠ 20 Jun 2019 - 09:44:16     ---->Network gateway is missing.
⚠ 20 Jun 2019 - 09:44:16     ---->Network name server is missing.
ⓘ 20 Jun 2019 - 09:44:16     --->Network area "Ethernet":
ⓘ 20 Jun 2019 - 09:44:16     ---->Network card is: "Intel(R) 82566DM-2 Gigabit Network Connection".
ⓘ 20 Jun 2019 - 09:44:16     ---->Working in DHCP mode.
ⓘ 20 Jun 2019 - 09:44:16     ---->Network addresses:
ⓘ 20 Jun 2019 - 09:44:16     ----->10.31.7.205 with network mask 255.255.255.0.
ⓘ 20 Jun 2019 - 09:44:16     ---->Network gateways:
ⓘ 20 Jun 2019 - 09:44:16     ----->10.31.7.1.
ⓘ 20 Jun 2019 - 09:44:16     ---->Network DNS servers:
ⓘ 20 Jun 2019 - 09:44:16     ----->10.31.2.120.
ⓘ 20 Jun 2019 - 09:44:16     ----->10.51.250.122.
ⓘ 20 Jun 2019 - 09:44:16     *Mounting storage file system...
ⓘ 20 Jun 2019 - 09:44:16     ->Mounting storage group: "Storage Group 1"...
ⓘ 20 Jun 2019 - 09:44:17     -->Storage group account size is 1959.20 GBytes.
ⓘ 20 Jun 2019 - 09:44:17     ->Running with about 1959.20 GBytes of storage.
ⓘ 20 Jun 2019 - 09:44:17     *Starting recorder...
ⓘ 20 Jun 2019 - 09:44:17     *Initializing alarms database...
ⓘ 20 Jun 2019 - 09:44:17     *Alarms database initialization completed.
ⓘ 20 Jun 2019 - 09:44:20     *WebRTC mode set to: basic
ⓘ 20 Jun 2019 - 09:44:20     *WWW Authentication and HTTPS mode set to: True
ⓘ 20 Jun 2019 - 09:44:22     *Found USB dongle s/n: 0x1d9007be.
ⓘ 20 Jun 2019 - 09:44:22     ->Dongle unlimited license for 128 inputs.
ⓘ 20 Jun 2019 - 09:44:23     *Serial: 0xa8139a55 2819856981
ⓘ 20 Jun 2019 - 09:44:24     *Mount storage disk D:\ completed.
ⓘ 20 Jun 2019 - 09:44:27     *Command Recording Software ready.
ⓘ 20 Jun 2019 - 09:45:27   Ready to accept connections.
```

The console is divided into two main sections:

- The toolbar
- The system log

2 You can use the toolbar located at the top of the console to manage your Command Recording Software.



The following table provides a description of the toolbar buttons.

Playback Control	Action
▶	Starts the Command Recording Software.
■	Stops the Command Recording Software.
❙▶	Restarts the Command Recording Software.
ⓘ	Filters the standard entries in the system log.
⚠	Filters the warnings in the system log.
❗	Filters the error in the system log.
💾	Exports the system log. **Note:** This button opens a saving window.
📥	Enables the autoscroll feature. With the autoscroll enabled, the system log always displays the latest entry.
🏭	Destroys the current Command Recording Software configuration, reverting the configuration to the factory defaults.
🛡	Opens the **Security Settings** dialog box (see "Configuring the Security Settings" on page 26). **Note:** Some of the options in the dialog box can be configured only when the Command Recording Software service is stopped.
📹	Updates the supported cameras list. **Notes:** • The supported cameras list is updated together with the Command Recording Software. This option must be used only in specific cases and under the March Networks Technical Support guidance. • This button is enabled only when the Command Recording Software service is stopped.
❓	Opens the **About** dialog box.

3 Check the Command Recording Software service status by checking the toolbar. If the green light on the right of the software version flashes, the service is up and running. Otherwise, click the ▶ button to start the Command Recording Software service.

Configuring the Security Settings

The Command Recording Software Management console allows you to configure the security settings for the Command Recording Software.

Notes:

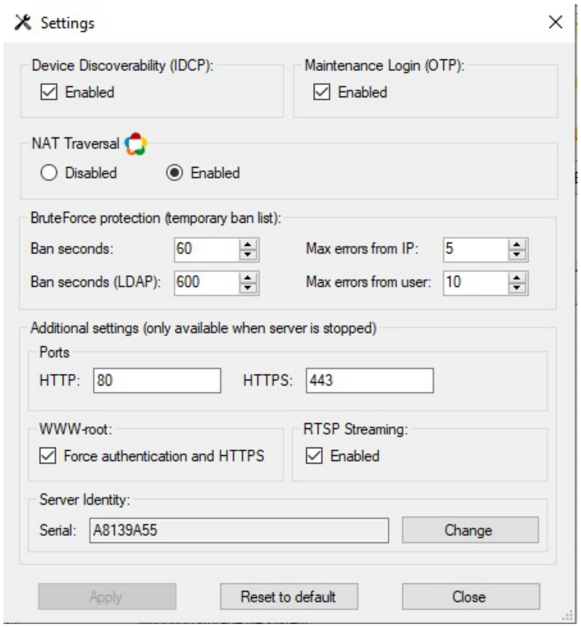
- The **Ports**, **WWW-Root**, **RTSP Streaming**, and **Server Identity** options can be configured only when the Command Recording Software service is stopped.
- The server serial number in the **Server Identity** option should be changed only in specific cases where the Command Recording Software is managed by a CES, and must be approved by March Networks.
- For more information about the NAT Traversal feature, and TURN/STUN servers, download the latest *Command Enterprise User Guide*, available for download from the March Networks corporate website and the Partner Portal.

To configure the security settings

1 Click the ■ button to stop the Command Recording Software service.

2 Click the 🛡 button.

The **Security Settings** dialog box appears.



Settings

Device Discoverability (IDCP):
☑ Enabled

Maintenance Login (OTP):
☑ Enabled

NAT Traversal
○ Disabled ● Enabled

BruteForce protection (temporary ban list):
Ban seconds: 60
Max errors from IP: 5
Ban seconds (LDAP): 600
Max errors from user: 10

Additional settings (only available when server is stopped)
Ports
HTTP: 80
HTTPS: 443

WWW-root:
☑ Force authentication and HTTPS

RTSP Streaming:
☑ Enabled

Server Identity:
Serial: A8139A55

3 In the **Device Discoverability** section, clear the **Enabled** check box to make the Command Recording Software invisible to the Discovery Browser software, Command Enterprise Servers and different Command Recording Softwares.

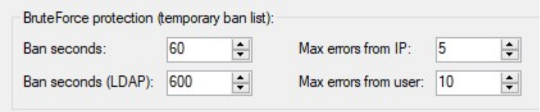
4 In the **Maintenance Login** section, clear the **Enabled** check box to access the Command Recording Software as the administrator using the OTP (One-Time Password) validation protocol (see “Accessing the Command Recording Software Using the OTP Validation Protocol” on page 40).

5 In the **NAT Traversal** section, select your configuration:

- Click **Disabled** to disable the NAT Traversal feature on the Command Recording Software. It is possible to connect to the server only through a direct connection from the client and the communication ports must be opened on the network. This is the default configuration.
- Click **Enabled** to enable the NAT Traversal feature on the Command Recording Software. It is possible to use the Command Enterprise Server as a gateway for the connection to the Command Recording Software.

  Note: When you connect to a Command Recording Software using the NAT Traversal feature it is not possible to open the configuration interface for cameras added to the Command Recording Software.

6 In the **BruteForce protection** section, you can configure when a user is temporary locked after too many failed login attempts. To configure the temporary lock:



BruteForce protection (temporary ban list):

Ban seconds: 60 Max errors from IP: 5

Ban seconds (LDAP): 600 Max errors from user: 10

a Enter or select the duration of the lock for local user profiles in the **Ban seconds** field.

b Enter or select the duration of the lock for LDAP users or groups in the **Ban seconds (LDAP)** field.

c Enter or select the maximum number of failed login attempts from the same IP address in the **Max errors from IP** field.

d Enter or select the maximum number of failed login attempts from the same user profile both local and LDAP) in the **Max errors from user** field.

7 In the **Ports** section, enter new communication ports for the **HTTP** and **HTTPS** protocols, if required.

Note: The default communication ports are 80 for the HTTP protocol, and 443 for the HTTPS protocol. Click **Reset to Default** to revert the communication ports to the default values.

8 In the **www-root access** section, select the **Force authentication and HTTPS** check box to disable any connection to the landing page and to the **Statistics Dashboard** page using the HTTP communication protocol. To access the landing page, you must enter
https://<serverhostname> as the address, and authenticate using a valid **User Name** and **Password**.

9 In the **RTSP streaming** section, clear the **Enabled** check box to disable RTSP streaming from the Command Recording Software to media player applications.

10 Click **Apply** to save and apply the changes.

11 Click **Close** to close the **Security Settings** dialog box.

12 Click the ▶ button to start the Command Recording Software service.

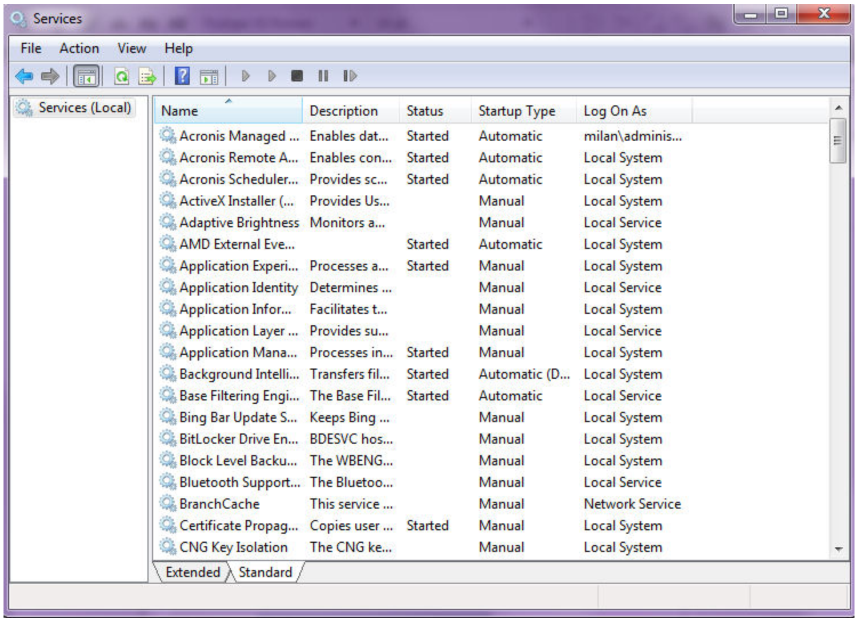
Enabling the SSDP Discovery Service

The SSDP Discovery service is disabled by default on Windows Server 2008 R2 systems. This service is required to add to the network discovery tool the capability to search for several third party cameras on the network using the UPNP protocol.

To enable the SSDP Discovery service

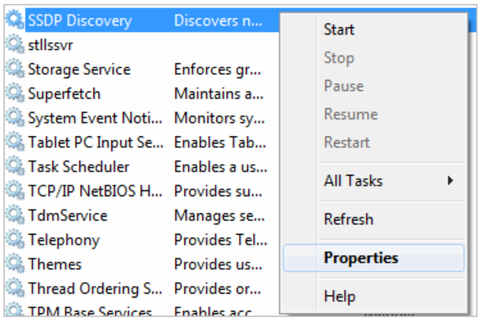
1 On the Windows' **Start** menu, enter **services.msc** in the **Search** field, and then hit **ENTER** key.

The **Services** dialog box appears.



Name	Description	Status	Startup Type	Log On As
Acronis Managed ...	Enables dat...	Started	Automatic	milan\adminis...
Acronis Remote A...	Enables con...	Started	Automatic	Local System
Acronis Scheduler...	Provides sc...	Started	Automatic	Local System
ActiveX Installer (...	Provides Us...		Manual	Local System
Adaptive Brightness	Monitors a...		Manual	Local Service
AMD External Eve...		Started	Automatic	Local System
Application Experi...	Processes a...	Started	Manual	Local System
Application Identity	Determines ...		Manual	Local Service
Application Infor...	Facilitates t...		Manual	Local System
Application Layer ...	Provides su...		Manual	Local Service
Application Mana...	Processes in...	Started	Manual	Local System
Background Intelli...	Transfers fil...	Started	Automatic (D...	Local System
Base Filtering Engi...	The Base Fil...	Started	Automatic	Local Service
Bing Bar Update S...	Keeps Bing ...		Manual	Local System
BitLocker Drive En...	BDESVC hos...		Manual	Local System
Block Level Backu...	The WBENG...		Manual	Local System
Bluetooth Support...	The Bluetoo...		Manual	Local Service
BranchCache	This service ...		Manual	Network Service
Certificate Propag...	Copies user ...	Started	Manual	Local System
CNG Key Isolation	The CNG ke...		Manual	Local System

2 Right-click the **SSDP Discovery** service in the list and select **Properties**.

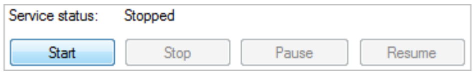


SSDP Discovery	Discovers n...
stllssvr	
Storage Service	Enforces gr...
Superfetch	Maintains a...
System Event Noti...	Monitors sy...
Tablet PC Input Se...	Enables Tab...
Task Scheduler	Enables a us...
TCP/IP NetBIOS H...	Provides su...
TdmService	Manages se...
Telephony	Provides Tel...
Themes	Provides us...
Thread Ordering S...	Provides or...
TPM Base Services	Enables acc...

The service properties dialog box appears.

3 Select **Automatic** from the **Startup type** list.

4 Click **Start** to start the service.


Service status: Stopped

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

Chapter 3

Getting Started

Command Config is the application that allows you to configure a Command Recording Software. You can download the Command Config installer from the Command Recording Software.

This chapter contains the following sections:

- "System Requirements" on page 30
- "Installing Command Config and Connecting to the Server" on page 31
- "Upgrading Command Config" on page 42
- "Configuring the Command Config Settings" on page 43
- "Applying Licenses to a Command Recording Server" on page 44

System Requirements

Ensure the computer from which you will access your Command Recording Software meets the recommended requirements.

The following table outlines the requirements for Command Config.

	COMMAND CLIENT **Minimum Specs**
Operating system (OS)	Windows 8, Windows 8.1, and Windows 10
Processor (CPU)	Intel i3 or equivalent (minimum)
HDD space (clients)	200 MB
Network interface	Gigabit Ethernet
Memory	4 GB (minimum)
Video Card	Intel HD 4000 video card (minimum) or an equivalent video card compatible with Microsoft DirectX 11 and Direct3D

Notes:

- For Windows 8.1 users, it is required to download and install the following updates from the Microsoft website. The updates must also be applied in the following order:
  1- KB2919442
  2- KB2919355
  For more information about the updates, please click the following links:
  https://support.microsoft.com/en-us/kb/2919442
  https://support.microsoft.com/en-us/kb/2919355
- March Networks does not support Command Client in Virtual Desktop Infrastructure (VDI). VDI is not ideal for CCTV clients because its architecture shares a pool of resources between multiple simultaneous clients. This means that client performance is dependent on available hardware resources, backend software and configuration, number of concurrent sessions, number of simultaneous streams viewed, and their profiles.

Installing Command Config and Connecting to the Server

Command Config is the standalone interface that allows you to configure a Command Recording Software.

Notes:

- You must have Administrator level privileges on the computer where you want to install Command Config.
- The following procedure explains how to directly access a Command Recording Software using the HTTP or HTTPS protocol. If you want to connect to the Command Recording Software through a Command Enterprise Server, see “Connecting to the Command Recording Software Through a Command Enterprise Server” on page 36. If you want to connect to the Command Recording Software through a Command Enterprise Server using the NAT Traversal feature, see “Connecting to the Command Recording Software Using the NAT Traversal Feature” on page 38.

To install Command Config and access the Command Recording Software

1 To access the installation package, either:

- In the **Address** bar of a Web browser, enter http://<*serverhostname*>. When the landing page appears, click the **Download Command Config Installation Package** button.

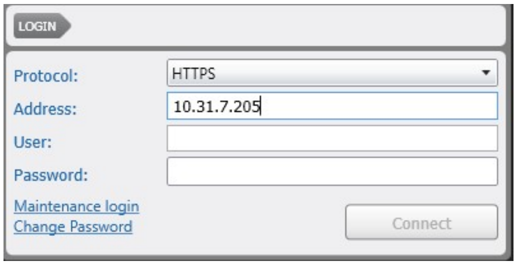
- From the Command software installation DVD or software installation package, double-click the **Autorun.exe** file to open the install interface. Click **Software** to open the Software page. On the **Software** page, click **Command Config** to run the installation file.
- Go to the March Networks Partner Portal website to download the Command Config installation file and run it.

The **End User License Agreement** appears.

2 Click **Accept**.

After a few seconds, the **Command Config** shortcut appears on your computer’s desktop and is inserted into the Windows’ Start menu.

The Command Config application is automatically launched and the **Login** page appears.



Protocol: HTTPS

Address: 10.31.7.205

3 Select the communication **Protocol** from the list.

Options include **HTTP** and **HTTPS**.

4 In the **Address** field, enter the IP address or host name of the Command Recording Software that you want to access followed by ":" and the communication port, if different from the default ones (80 for HTTP and 443 for HTTPS).

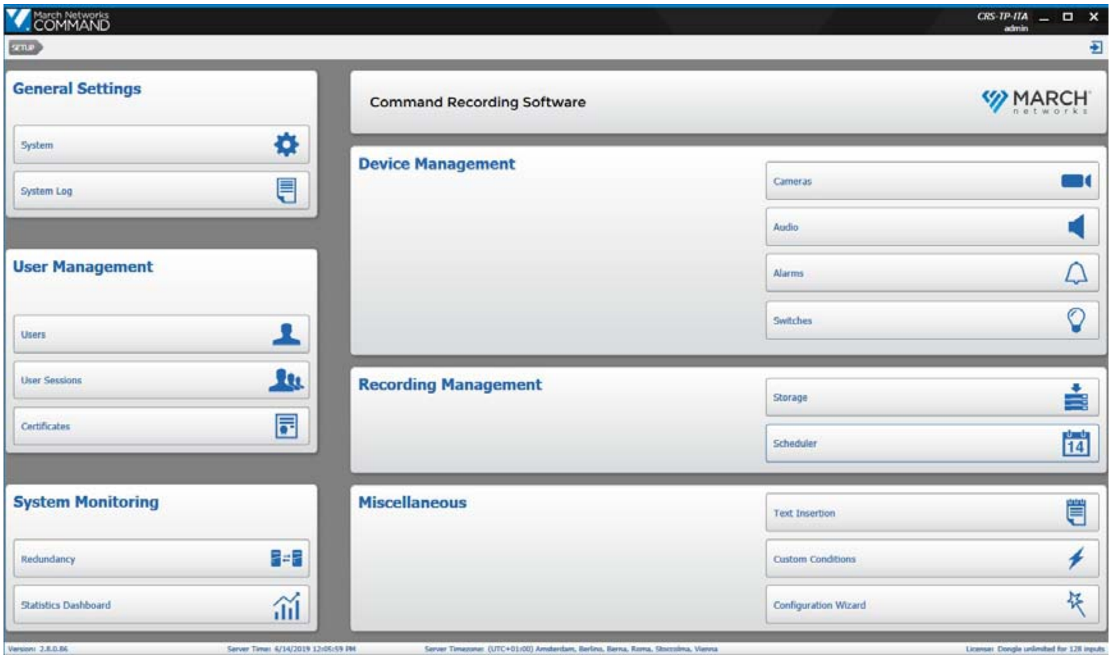
Note: Command Config automatically enters the address of the last Command Recording Software that you accessed.

5 Log on with a valid **User** name (default: admin) and **Password** (default: no password).

Note: It is strongly recommended that you change the credentials for the administrator's account by clicking the **Change Password** link (see "Changing the Password From the Login page" on page 33). Command also allows you to synchronize user accounts with LDAP users. For more information, see "Managing User Profiles" on page 60.

6 Click **Connect**.

The Command Config main page appears.



Version: 2.8.0.86 Server Time: 6/14/2019 12:05:59 PM Server Timezone: (UTC+01:00) Amsterdam, Berlino, Berna, Roma, Stoccolma, Vienna License: Dongle unlimited for 128 inputs

Changing the Password From the Login page

Command Config allows you the change the password for your user profile from the **Login** page. The password change can be manually triggered, or automatically triggered in the following cases:

- The password is expired (see “Configuring Extended Features for a User Profile” on page 74)
- The **Force change password at next login** check box has been selected for the user (see “Configuring Extended Features for a User Profile” on page 74).
- The password does not respect the configured password policy (see “Configuring the Password Policy” on page 123)

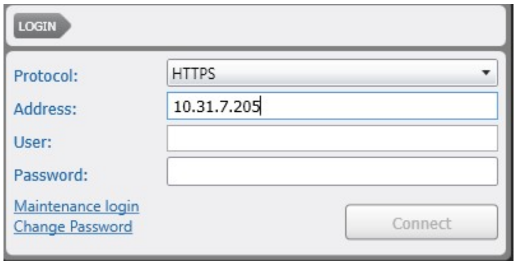
Select your configuration:

- “To change the password from the Login page” on page 33
- “To change the password after the password expired or to respect the policy” on page 35

To change the password from the Login page

1 Launch the Command Config application on a client PC.

The **Login** page appears.



2 Select the communication **Protocol** from the list.

Options include **HTTP** and **HTTPS**.

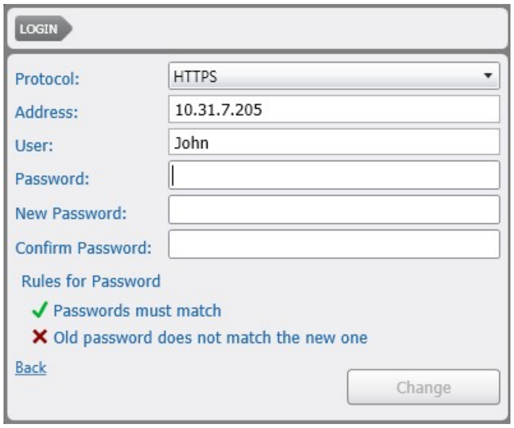
3 In the **Address** field, enter the IP address or host name of the Command Recording Software that you want to access followed by “:” and the communication port, if different from the default ones (80 for HTTP and 443 for HTTPS).

Note: Command Config automatically enters the address of the last Command Recording Software that you accessed.

4 Enter the user profile name in the **Name** field.

5 Click the **Change Password** link.

The **Password Change** dialog box appears.



Protocol: HTTPS
Address: 10.31.7.205
User: John
Password:
New Password:
Confirm Password:

Rules for Password
✓ Passwords must match
✗ Old password does not match the new one

6 Enter the current password in the **Password** field.

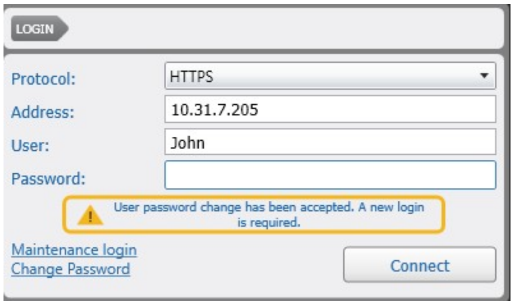
7 Enter the new password in the **New Password** field.

8 Enter the new password a second time in the **Confirm Password** field.

Tip: The dialog box warns if the passwords do not match or if the new password does not respect the password policy configured in the **System** page.

9 Click **Change** to confirm.

The **Login** dialog box appears.



Protocol: HTTPS
Address: 10.31.7.205
User: John
Password:

User password change has been accepted. A new login is required.

10 Enter the new password in the **Password** field.

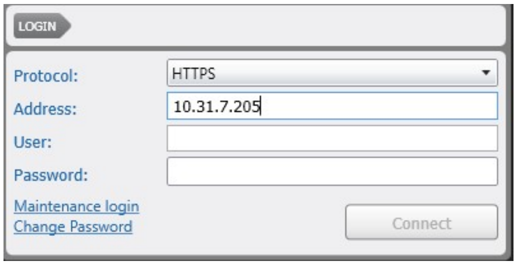
11 Click **Connect**.

The Command Config main page appears.

To change the password after the password expired or to respect the policy

1 Launch the Command Config application on a client PC.

The **Login** page appears.



LOGIN

Protocol: HTTPS

Address: 10.31.7.205

User:

Password:

2 Select the communication **Protocol** from the list.

Options include **HTTP** and **HTTPS**.

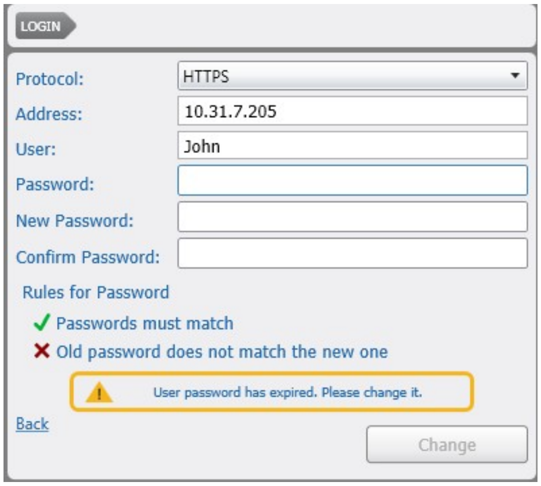
3 In the **Address** field, enter the IP address or host name of the Command Recording Software that you want to access followed by ":" and the communication port, if different from the default ones (80 for HTTP and 443 for HTTPS).

Note: Command Config automatically enters the address of the last Command Recording Software that you accessed.

4 Enter the user profile name and the current password for the user account in the **Name** and **Password** fields.

5 Click **Connect**.

The **Password Change** dialog box automatically appears.



LOGIN

Protocol: HTTPS

Address: 10.31.7.205

User: John

Password:

New Password:

Confirm Password:

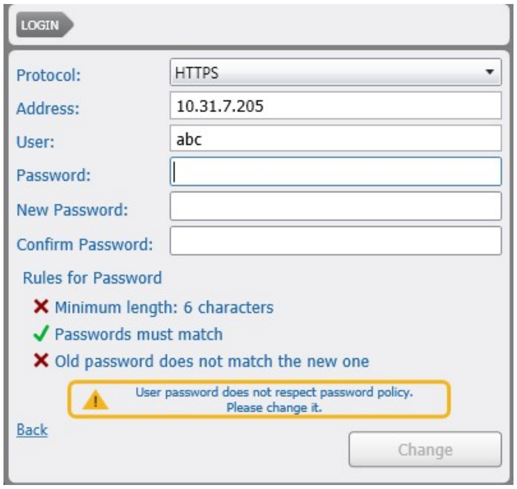
Rules for Password

✓ Passwords must match

✗ Old password does not match the new one

⚠ User password has expired. Please change it.

Password Expired



LOGIN

Protocol: HTTPS

Address: 10.31.7.205

User: abc

Password:

New Password:

Confirm Password:

Rules for Password

✗ Minimum length: 6 characters

✓ Passwords must match

✗ Old password does not match the new one

⚠ User password does not respect password policy. Please change it.

Password Policy Not Respected

6 Enter the old password in the **Password** field.

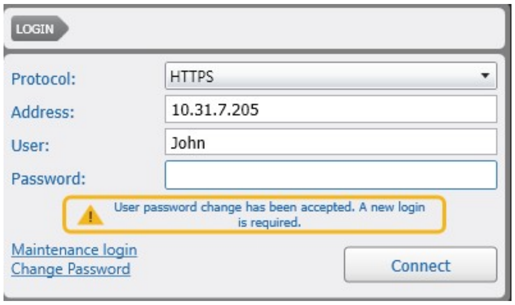
7 Enter the new password in the **New Password** field.

8 Enter the new password a second time in the **Confirm Password** field.

Tip: The dialog box warns if the passwords do not match or if the new password does not respect the password policy configured in the **System** page.

9 Click **Change** to confirm.

The **Login** dialog box appears.



Protocol: HTTPS
Address: 10.31.7.205
User: John
Password:

User password change has been accepted. A new login is required.

10 Enter the new password in the Password field.

11 Click **Connect**.

The Command Config main page appears.

Connecting to the Command Recording Software Through a Command Enterprise Server

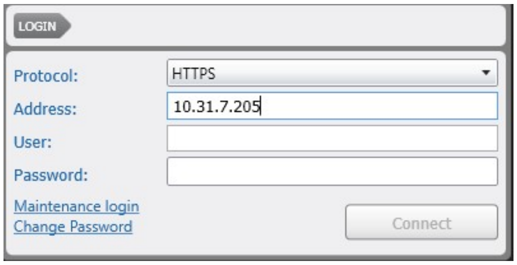
It is possible to connect to the Command Recording Software through the Command Enterprise Server it is registered to.

Note: When Command Config connects to the CES for the first time, a warning dialog box from Windows Firewall may appear. To continue, add Command Config as an exception, and then click **Ok** to close the dialog box.

To connect to the Command Recording Software through a Command Enterprise Server

1 Launch the Command Config application on a client PC.

The **Login** page appears.



Protocol: HTTPS
Address: 10.31.7.205
User:
Password:

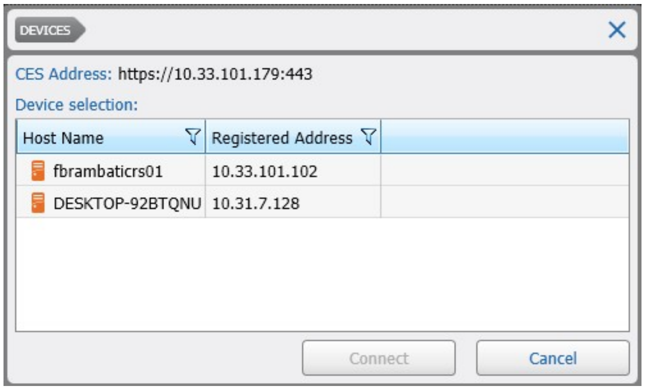
2 Select **HTTPS** from the protocol list.

3 In the **CES Address** field, enter the IP address or host name of the Command Enterprise Server the Command Recording Software is registered to followed by ":" and the communication port, if different from the default one (443).

4 Log on to the CES with a valid **User** name and **Password**. The CES user account must corresponds to an existing Command Recording Software user profile.

5 Click **Connect**.

Command Config connects to the CES and, after a few seconds, the **Devices** dialog box appears.



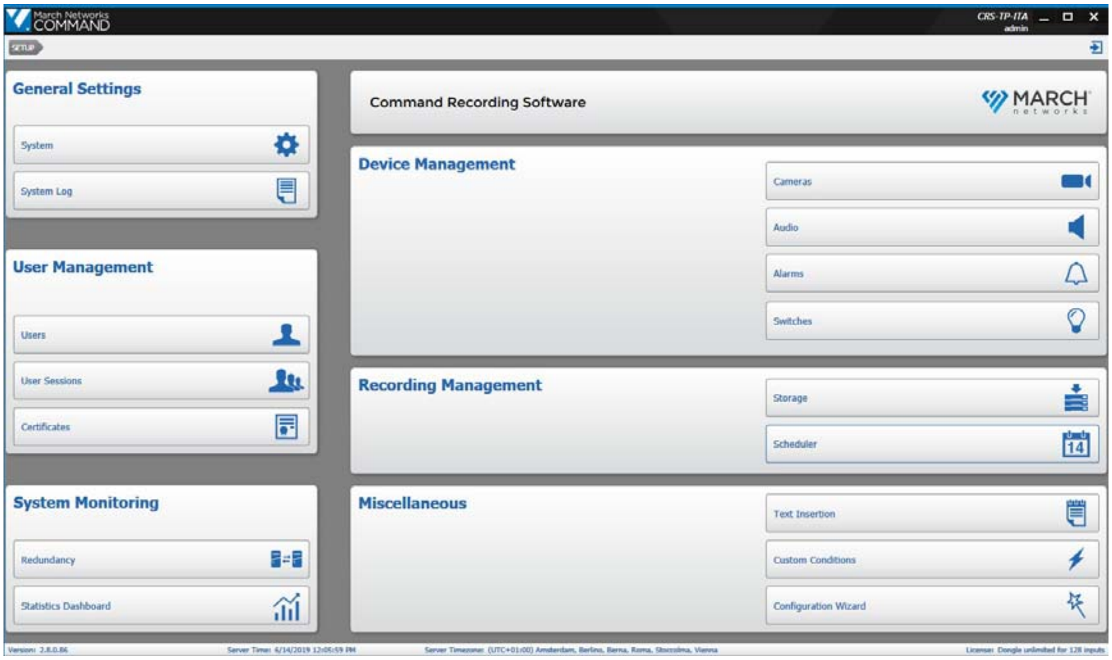
CES Address: https://10.33.101.179:443

Device selection:

Host Name	Registered Address
fbrambaticrs01	10.33.101.102
DESKTOP-92BTQNU	10.31.7.128

6 Select the Command Recording Software you want to connect to in the list, and then click **Connect**.

The Command Config main page appears.



Version: 2.8.0.86 Server Time: 6/14/2019 12:05:59 PM Server Timezone: (UTC+01:00) Amsterdam, Berlino, Berna, Roma, Stoccolma, Vienna License: Dongle unlimited for 128 inputs

Connecting to the Command Recording Software Using the NAT Traversal Feature

The Command solution integrates the NAT Traversal feature, allowing you to use the Command Enterprise Server as a gateway for the connection to the Command Recording Software. This is useful to enhance the security of your network by minimizing the inbound ports that needs to be opened on the routers.

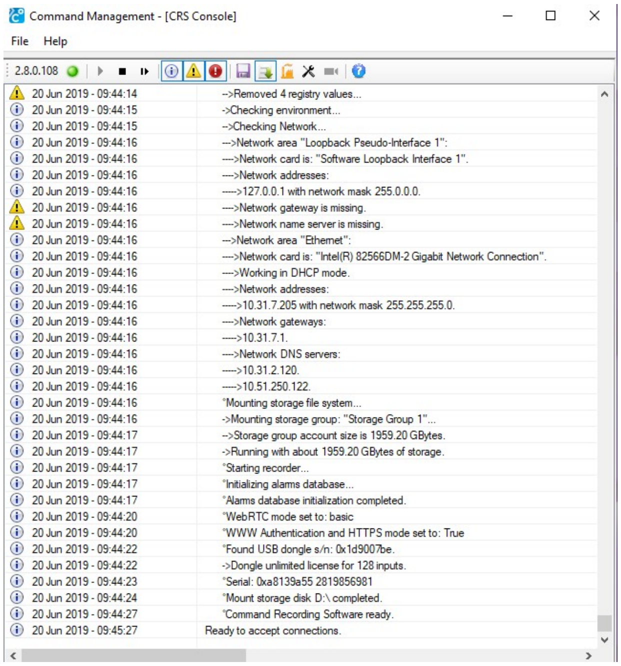
Important Notes:

- Before using the NAT Traversal feature, you must properly configure the NAT Traversal options for your Command Enterprise Server. For more information, see the latest *Command Enterprise and Client User Guide*, available for download from the March Networks corporate website and the Partner Portal.
- You must create a LDAP or a local user account on the CES that corresponds to a Command Recording Software user profile. The user must possess the **NAT Traversal** right on the CES (**Enabled** option on the Command Management Console). For more information, see the latest Command Enterprise and Client User Guide, available for download from the March Networks corporate website and the Partner Portal.
- When Command Config connects to the CES for the first time, a warning dialog box from Windows Firewall may appear. To continue, add Command Config as an exception, and then click **Ok** to close the dialog box.
- When you connect to a Command Recording Software using the NAT Traversal feature it is not possible to open the configuration interface for cameras added to the Command Recording Software.

To connect to the Command Recording Software using the NAT Traversal feature

1 On the server’s **Start** menu, point to **March Networks**, and then click **Command Recording Software Management**.

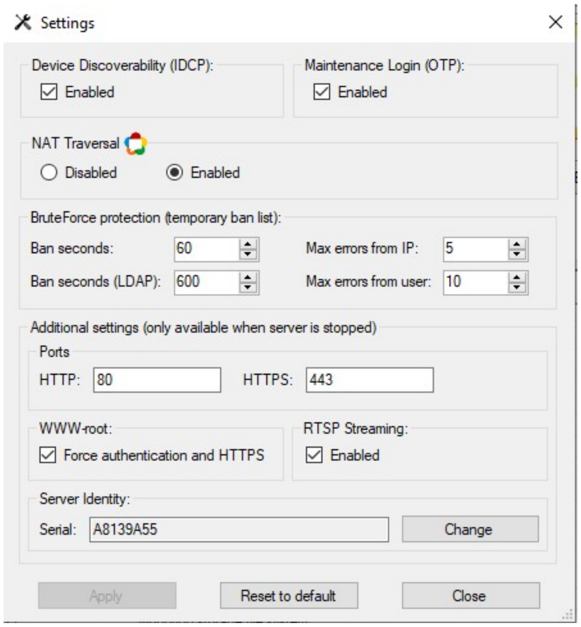
The **Command Management** console appears.



```
⚠ 20 Jun 2019 - 09:44:14    -->Removed 4 registry values...
ⓘ 20 Jun 2019 - 09:44:15    ->Checking environment...
ⓘ 20 Jun 2019 - 09:44:15    -->Checking Network...
ⓘ 20 Jun 2019 - 09:44:16    --->Network area "Loopback Pseudo-Interface 1":
ⓘ 20 Jun 2019 - 09:44:16    ---->Network card is: "Software Loopback Interface 1".
ⓘ 20 Jun 2019 - 09:44:16    ---->Network addresses:
ⓘ 20 Jun 2019 - 09:44:16    ----->127.0.0.1 with network mask 255.0.0.0.
⚠ 20 Jun 2019 - 09:44:16    ---->Network gateway is missing.
⚠ 20 Jun 2019 - 09:44:16    ---->Network name server is missing.
ⓘ 20 Jun 2019 - 09:44:16    --->Network area "Ethernet":
ⓘ 20 Jun 2019 - 09:44:16    ---->Network card is: "Intel(R) 82566DM-2 Gigabit Network Connection".
ⓘ 20 Jun 2019 - 09:44:16    ---->Working in DHCP mode.
ⓘ 20 Jun 2019 - 09:44:16    ---->Network addresses:
ⓘ 20 Jun 2019 - 09:44:16    ----->10.31.7.205 with network mask 255.255.255.0.
ⓘ 20 Jun 2019 - 09:44:16    ---->Network gateways:
ⓘ 20 Jun 2019 - 09:44:16    ----->10.31.7.1.
ⓘ 20 Jun 2019 - 09:44:16    ---->Network DNS servers:
ⓘ 20 Jun 2019 - 09:44:16    ----->10.31.2.120.
ⓘ 20 Jun 2019 - 09:44:16    ----->10.51.250.122.
ⓘ 20 Jun 2019 - 09:44:16    °Mounting storage file system...
ⓘ 20 Jun 2019 - 09:44:16    ->Mounting storage group: "Storage Group 1"...
ⓘ 20 Jun 2019 - 09:44:17    -->Storage group account size is 1959.20 GBytes.
ⓘ 20 Jun 2019 - 09:44:17    ->Running with about 1959.20 GBytes of storage.
ⓘ 20 Jun 2019 - 09:44:17    °Starting recorder...
ⓘ 20 Jun 2019 - 09:44:17    °Initializing alarms database...
ⓘ 20 Jun 2019 - 09:44:17    °Alarms database initialization completed.
ⓘ 20 Jun 2019 - 09:44:20    °WebRTC mode set to: basic
ⓘ 20 Jun 2019 - 09:44:20    °WWW Authentication and HTTPS mode set to: True
ⓘ 20 Jun 2019 - 09:44:22    °Found USB dongle s/n: 0x1d9007be.
ⓘ 20 Jun 2019 - 09:44:22    ->Dongle unlimited license for 128 inputs.
ⓘ 20 Jun 2019 - 09:44:23    °Serial: 0xa8139a55 2819856981
ⓘ 20 Jun 2019 - 09:44:24    °Mount storage disk D:\ completed.
ⓘ 20 Jun 2019 - 09:44:27    °Command Recording Software ready.
ⓘ 20 Jun 2019 - 09:45:27  Ready to accept connections.
```

2 Click the 🛡 button.

The **Security Settings** dialog box appears.



Settings

Device Discoverability (IDCP): ☑ Enabled

Maintenance Login (OTP): ☑ Enabled

NAT Traversal: ○ Disabled ● Enabled

BruteForce protection (temporary ban list):

Ban seconds: 60

Max errors from IP: 5

Ban seconds (LDAP): 600

Max errors from user: 10

Additional settings (only available when server is stopped)

Ports

HTTP: 80

HTTPS: 443

WWW-root: ☑ Force authentication and HTTPS

RTSP Streaming: ☑ Enabled

Server Identity:

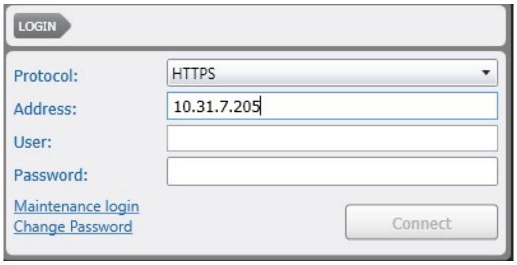
Serial: A8139A55

3 In the **NAT Traversal** section, ensure that the **Enabled** option is selected.

4 Click **Apply** and then click **Close** to close the dialog box.

5 Launch the Command Config application on a client PC.

The **Login** page appears.



LOGIN

Protocol: HTTPS

Address: 10.31.7.205

User:

Password:

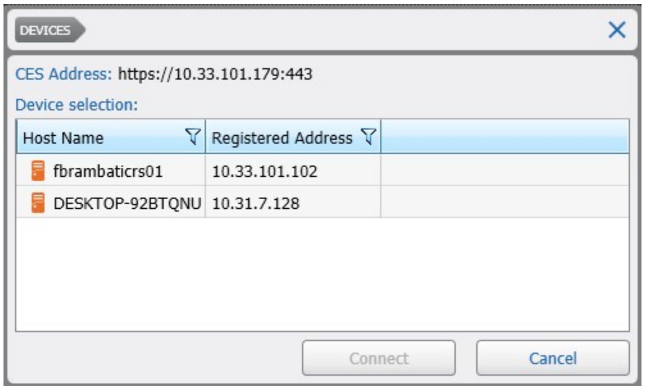
6 Select **HTTPS** from the protocol list.

7 In the **Address** field, enter the IP address or host name of the Command Enterprise Server the Command Recording Software is registered to followed by ":" and the communication port, if different from the default one (443).

8 Log on to the CES with a valid **User** name and **Password**. The CES user account must corresponds to an existing Command Recording Software user profile.

9 Click **Connect**.

Command Config connects to the CES and, after a few seconds, the **Devices** dialog box appears.



CES Address: https://10.33.101.179:443

Device selection:

Host Name	Registered Address
fbrambaticrs01	10.33.101.102
DESKTOP-92BTQNU	10.31.7.128

10 Select the Command Recording Software you want to connect to in the list, and then click **Connect**.

The Command Config main page appears.

Accessing the Command Recording Software Using the OTP Validation Protocol

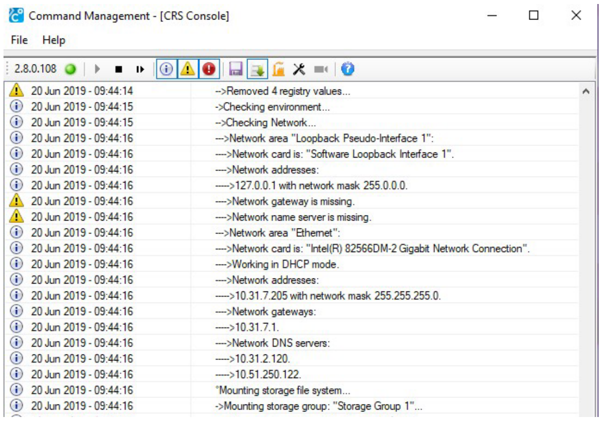
In case of severe and urgent issues (for example: a defective disk can be substituted and mounted only by the system administrator, but he is not available), Command Config allows you to connect to the Command Recording Software as the system administrator using the OTP (One-Time Password) validation protocol, a fast and secure procedure that involves the March Networks Technical Support.

Note: Each access with the OTP validation protocol is audited both by the Command Recording Software and by March Networks Technical Support.

To access the Command Recording Software using the OTP validation protocol

1 On the server's **Start** menu, point to **March Networks**, and then click **Command Recording Software Management**.

The **Command Management** console appears.

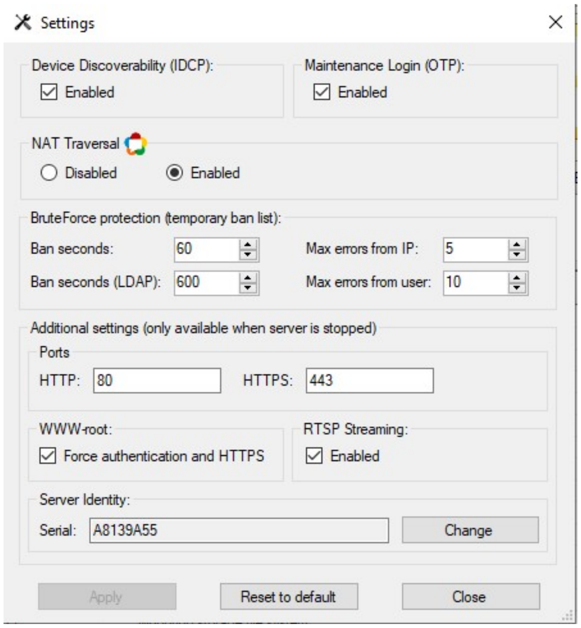


```
20 Jun 2019 - 09:44:14    -->Removed 4 registry values...
20 Jun 2019 - 09:44:15    ->Checking environment...
20 Jun 2019 - 09:44:15    -->Checking Network...
20 Jun 2019 - 09:44:16    --->Network area "Loopback Pseudo-Interface 1":
20 Jun 2019 - 09:44:16    ---->Network card is: "Software Loopback Interface 1".
20 Jun 2019 - 09:44:16    ---->Network addresses:
20 Jun 2019 - 09:44:16    ----->127.0.0.1 with network mask 255.0.0.0.
20 Jun 2019 - 09:44:16    ---->Network gateway is missing.
20 Jun 2019 - 09:44:16    ---->Network name server is missing.
20 Jun 2019 - 09:44:16    --->Network area "Ethernet":
20 Jun 2019 - 09:44:16    ---->Network card is: "Intel(R) 82566DM-2 Gigabit Network Connection".
20 Jun 2019 - 09:44:16    ---->Working in DHCP mode.
20 Jun 2019 - 09:44:16    ---->Network addresses:
20 Jun 2019 - 09:44:16    ----->10.31.7.205 with network mask 255.255.255.0.
20 Jun 2019 - 09:44:16    ---->Network gateways:
20 Jun 2019 - 09:44:16    ----->10.31.7.1.
20 Jun 2019 - 09:44:16    ---->Network DNS servers:
20 Jun 2019 - 09:44:16    ----->10.31.2.120.
20 Jun 2019 - 09:44:16    ----->10.51.250.122.
20 Jun 2019 - 09:44:16    *Mounting storage file system...
20 Jun 2019 - 09:44:16    ->Mounting storage group: "Storage Group 1"...
```

2 Click the ■ button to stop the Command Recording Software service.

3 Click the 🛡 button.

The **Security Settings** dialog box appears.



Settings

Device Discoverability (IDCP):
☑ Enabled

Maintenance Login (OTP):
☑ Enabled

NAT Traversal
○ Disabled ● Enabled

BruteForce protection (temporary ban list):
Ban seconds: 60
Max errors from IP: 5
Ban seconds (LDAP): 600
Max errors from user: 10

Additional settings (only available when server is stopped)
Ports
HTTP: 80
HTTPS: 443

WWW-root:
☑ Force authentication and HTTPS

RTSP Streaming:
☑ Enabled

Server Identity:
Serial: A8139A55

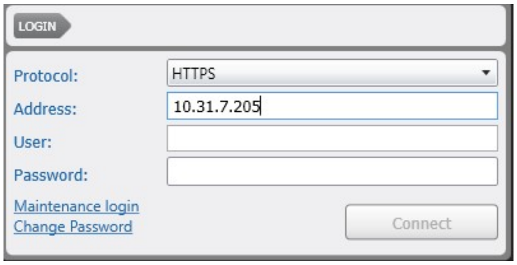
4 In the **Maintenance Login** section, ensure that the **Enabled** check box is selected.

5 Click **Apply** and then click **Close** to close the dialog box.

6 Click the ▶ button to start the Command Recording Software service.

7 Launch the Command Config application on a client PC.

The **Login** page appears.



LOGIN

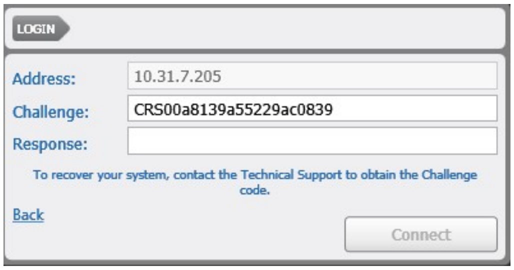
Protocol: HTTPS
Address: 10.31.7.205
User:
Password:

8 Select **HTTPS** from the **Protocol** list.

9 In the **Address** box, enter the IP address or host name of the Command Recording Software.

10 Click the **Maintenance Login** link.

A dialog box appears.



Address: 10.31.7.205

Challenge: CRS00a8139a55229ac0839

Response:

To recover your system, contact the Technical Support to obtain the Challenge code.

11 Copy the code in the **Challenge** field.

12 Contact the March Networks Technical Support and then send an e-mail with the **Challenge** code. The March Networks Technical Support will provide you with an authorization code.

13 Paste the authorization code in the **Response** field.

14 Click **Connect** to access the Command Recording Software as system administrator.

Note: You can log on to the Command Recording Software using the **Response** code only one time.

Upgrading Command Config

After a upgrading the Command Recording Software to a higher version, you can also automatically upgrade Command Config by simply connecting to the Command Recording Software.

To upgrade Command Config

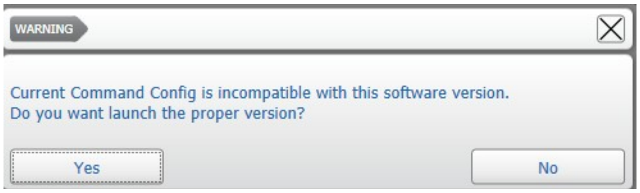
1 After you upgrade the Command Recording Software (see “Upgrading Command Recording Software” on page 21), launch the Command Config application.

2 Select the communication **Protocol** from the list.

3 In the **Address** box, enter the IP address or host name of the Command Recording Software.

4 Log on with a valid **User** name and **Password**.

A warning dialog box appears.



Current Command Config is incompatible with this software version.
Do you want launch the proper version?

5 Click **Yes** to upgrade Command Config to the required version.

The **End User License Agreement** appears.

6 Click **Accept**.

7 After a few seconds the upgraded Command Config application is automatically launched and the **Login** page appears.

Configuring the Command Config Settings

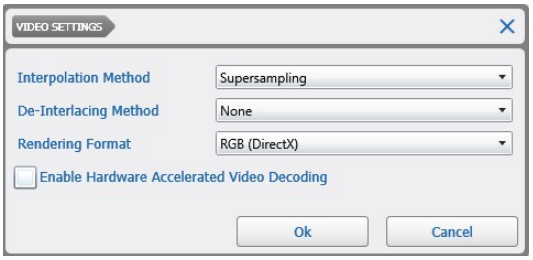
All users can modify the settings for the Command Config application.

To change the Command Config settings

1 Click the button at the upper-left of Command to display the main menu.

2 From the main menu, select **Settings**.

The **Video Settings** dialog box appears.



VIDEO SETTINGS

Interpolation Method: Supersampling

De-Interlacing Method: None

Rendering Format: RGB (DirectX)

□ Enable Hardware Accelerated Video Decoding

3 Select an interpolation algorithm method for the video channels from the **Interpolation Method** list,.

4 Select a de-interlacing algorithm method for the video channels from the **De-Interlacing Method** list.

5 Select a format from the **Rendering Format** list

The default is **RGB (DirectX)**. If you are working on a system (such as a virtual desktop environment) that does not support Direct3D (part of DirectX), you cannot view video using the default setting of RGB (DirectX).
In this case, select the **Bitmap (Software)** option, and video displays normally.

6 Select the **Enable Hardware Accelerated Video Decoding** check box if you want to enable the graphics processing unit (GPU) to decode video, which frees the central processing unit (CPU) and saves power.

7 Click **Ok** to save the changes and close the dialog box.

Applying Licenses to a Command Recording Server

After you perform a fresh installation of the Command Recording Server software on the server, the software has no license and it is automatically configured to Command Lite mode, with limited functionalities (6 cameras, 7 days of video retention, no alarms, switches, custom conditions, identification certificates, and redundancy). You must apply a valid license to unlock all of the CRS functionalities.

Important Notes:

- The ESM licensing method is no longer supported and the ESM page is no longer available on Command.
- The USB dongle licensing method is supported but no longer used on new installations.

You can apply a license to your server by doing any of the following:

- By applying Command Professional software licenses. For more information, see “Adding and Applying Software Licenses” on page 44.
- By applying Command Professional licenses using the USB dongle. For more information, see “Applying Additional Licenses Using USB Dongles” on page 46.
- By applying camera licenses from a March Networks Command Enterprise server. For more information, see “Applying Licenses With Command Enterprise” on page 47.

Adding and Applying Software Licenses

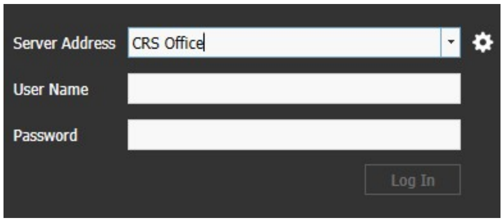
Command Recording Software supports software licenses. Before you can add a license, you need to purchase the number of required licenses. To apply a software license, you must access the Command Client interface, retrieve the CRS ID number, and then send an email to March Networks’ Customer Operations.

Important Note: To apply licenses, you must install the Command Client application on a client PC. For more information about the Command Client installation and usage, see the *Command Client User Guide*, available on the Software CD, on the CRS installation package, or on the March Networks Partner Portal.

To add and apply a software license

1 Launch the Command Client application.

The **Client Login** page appears.



Server Address: CRS Office

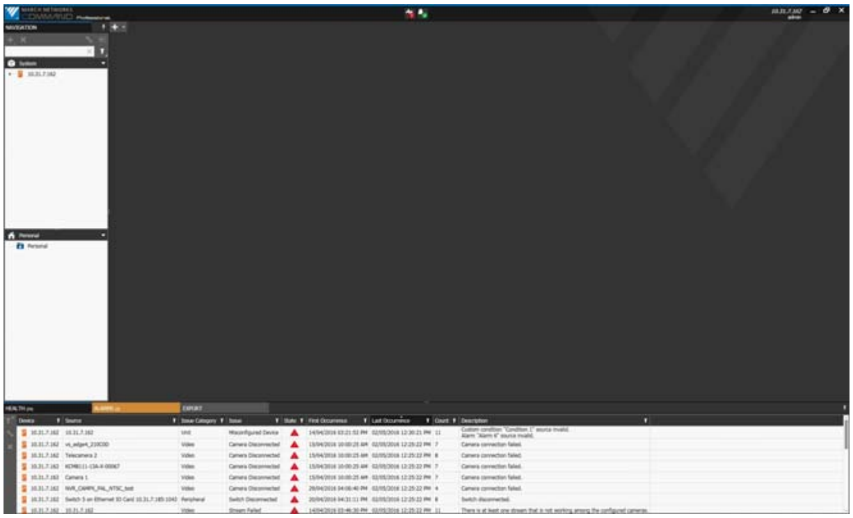
2 In the **Server Address** field enter the host name or IP address of your Command Lite followed by “:” and the communication port, if different from the default one (443 for HTTPS and 80 for HTTP).

Note: Command Client automatically connects to the server using the HTTPS communication protocol. If you want to connect to the server using the HTTP protocol, enter “http://” followed by the IP address, “:”, and the communication port, if different from the default one (80):

For example: *http://192.128.154.13:82*

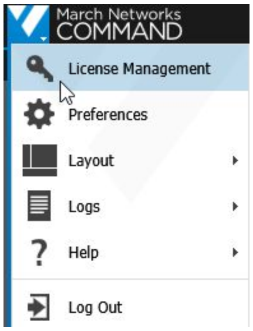
3 Enter a valid **User Name** (default: admin) and **Password** (default: no password) and then click **Log In**.

The Command Client interface appears.

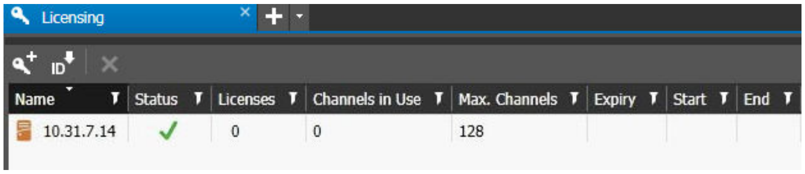


4 Click the button at the upper-left of Command to display the main menu.

5 From the main menu, select **License Management**.



The **Licensing** tab opens.



Name	Status	Licenses	Channels in Use	Max. Channels	Expiry	Start	End
10.31.7.14	✓	0	0	128			

6 On the **Licensing** toolbar, click the ID button.

You are prompted to save a text file (*id.txt*) to a local folder on your computer.

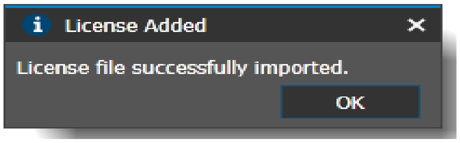
7 Contact March Networks Customer Operations to complete the transaction to purchase the required number of channel and recorder licenses.

Note: March Networks will send you an e-mail, with simple instructions that detail how to generate your license key file (license.xml file).

8 To import/enable the new licenses, click the button on the **Licensing** toolbar.

9 Locate and select the license.xml file and click **Open**.

The **License Added** dialog box appears indicating the licenses have been applied to the Command Recording Server and the licensing status bar refreshes with the license details.



License Added

License file successfully imported.

Note: If the license failed to import, an error message will appear indicating the reason for the failure.

Applying Additional Licenses Using USB Dongles

The USB dongle is a USB key that contains the channel licenses.

Important: The USB dongle must stay permanently plugged into the system to allow you to configure Command. If the dongle is removed from the server, all cameras and recording schedules are disabled without discarding the current configuration. When the dongle is plugged into the server again, the cameras and recording schedules will be fully restored.

To apply the license using the USB dongle

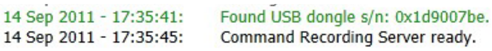
1 Plug the USB dongle into the server. The dongle includes one channel license and must be upgraded with the purchased licenses.

2 Connect to the Command Recording Software using the Command Config application. For more information, see “Installing Command Config and Connecting to the Server” on page 31.

3 On the Command Config main page, under **General Settings**, click **System Log**.

The **System Log Configuration** page appears.

4 Search for a *Found USB dongle* entry. If unavailable, verify that the USB dongle is plugged into the Command Recording Software server and then reboot the server.



```
14 Sep 2011 - 17:35:41:     Found USB dongle s/n: 0x1d9007be.
14 Sep 2011 - 17:35:45:     Command Recording Server ready.
```

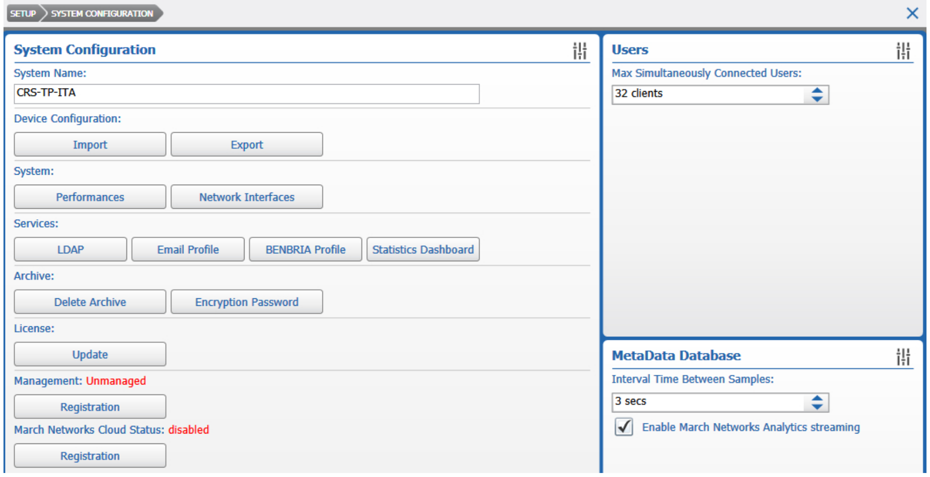
5 Make a note of the serial number. Send it in an email to March Networks Customer Operations at:

- Americas: *Salesrsmsupport@MarchNetworks.com* or 1-800-563-5564
- All other regions: *SalesSupport-EMEA@MarchNetworks.com*

6 Customer Operations generates a license and sends it as a UPT2 file.

7 On the Command Config main page, under **General Settings**, click **System**.

The **System Configuration** page appears.



System Configuration

System Name: CRS-TP-ITA

Device Configuration:

System:

Services:

Archive:

License:

Management: Unmanaged

March Networks Cloud Status: disabled

Users

Max Simultaneously Connected Users: 32 clients

MetaData Database

Interval Time Between Samples: 3 secs

☑ Enable March Networks Analytics streaming

8 In the **License** section, click **Update**.

The **Open** dialog box appears.

9 Navigate to the folder where the UPT2 license file you want to apply is located, and click **Open**.

The USB dongle license is automatically updated.

Note: You can check the number of licensed inputs on the bottom-right corner of Command Config.

Applying Licenses With Command Enterprise

If your Command Recording Software is part of a Command Enterprise system, you can add camera licenses to Command Enterprise and then download them individually to your Command Recording Software. For more information, see the *Command Enterprise User Guide*, available on the March Networks Partner Portal.

Chapter 4

Using the Configuration Wizard

The **Configuration Wizard** is an intuitive tool that allows you to quickly configure the basic functionalities (IP cameras, storage, recording and local user profiles) of your Command Recording Software in six steps. Specifically, it allows you to:

1. Specify the system name and change the administrator password
2. Add IP video channels to the Command Recording Software
3. Enable/disable the added IP cameras and specify video settings
4. Add storage disks and configure archive settings
5. Configure recording settings for the Command Recording Software (continuous and programmed recording)
6. Create and customize local user profiles

Notes:

- The **Configuration Wizard** destroys any previous Command Recording Software configuration.
- Only the *admin* account can access the **Configuration Wizard.**
- The wizard is a tool designed to simplify and speed up the configuration process for the basic functionalities of the Command Recording Software: most of the advanced configurations (such as specific permissions for user profiles, on-event recording, alarms and text insertion management) must be performed by accessing the specific configuration pages on Command Config.

This chapter contains the following sections:

- "Step 1: Configuring the System Settings" on page 49
- "Step 2: Adding IP Cameras" on page 50
- "Step 3: Selecting Video Settings" on page 54
- "Step 4: Adding Storage Disks" on page 56
- "Step 5: Configure Recording Settings" on page 57
- "Step 6: Creating and Customizing Local User Profiles" on page 58

Launching the Configuration Wizard

Only the *admin* account is allowed to access and use the **Configuration Wizard**.

To launch the Configuration Wizard

1 Log on to Command Config using the *admin* account credentials.

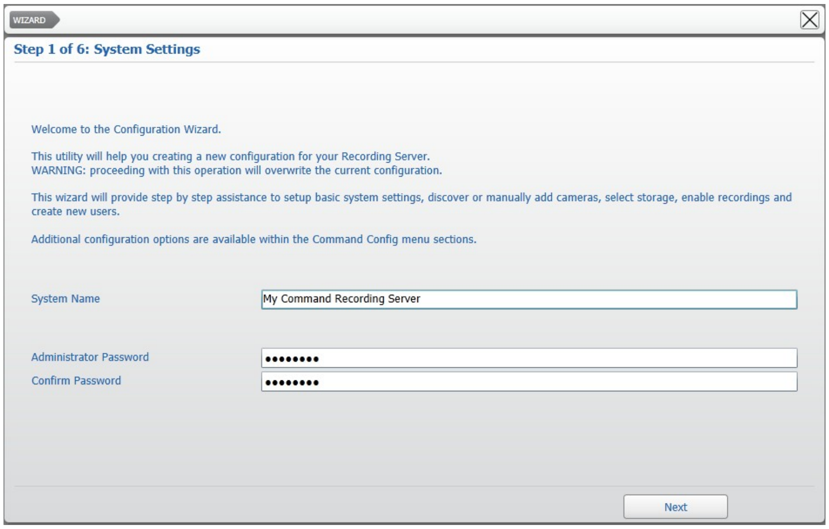
The Command Config main page appears.

2 Under **Miscellaneous**, click **Configuration Wizard**.

The **Configuration Wizard** appears.

Step 1: Configuring the System Settings

The **System Settings** page allows you to specify the system name and change the administrator password.



Step 1 of 6: System Settings

Welcome to the Configuration Wizard.

This utility will help you creating a new configuration for your Recording Server.
WARNING: proceeding with this operation will overwrite the current configuration.

This wizard will provide step by step assistance to setup basic system settings, discover or manually add cameras, select storage, enable recordings and create new users.

Additional configuration options are available within the Command Config menu sections.

System Name: My Command Recording Server

Administrator Password: ••••••••

Confirm Password: ••••••••

To configure the system settings

1 In the **System Name** box, enter a name for the Command Recording Software.

Note: March Networks applications identify the Command Recording Software by this name.

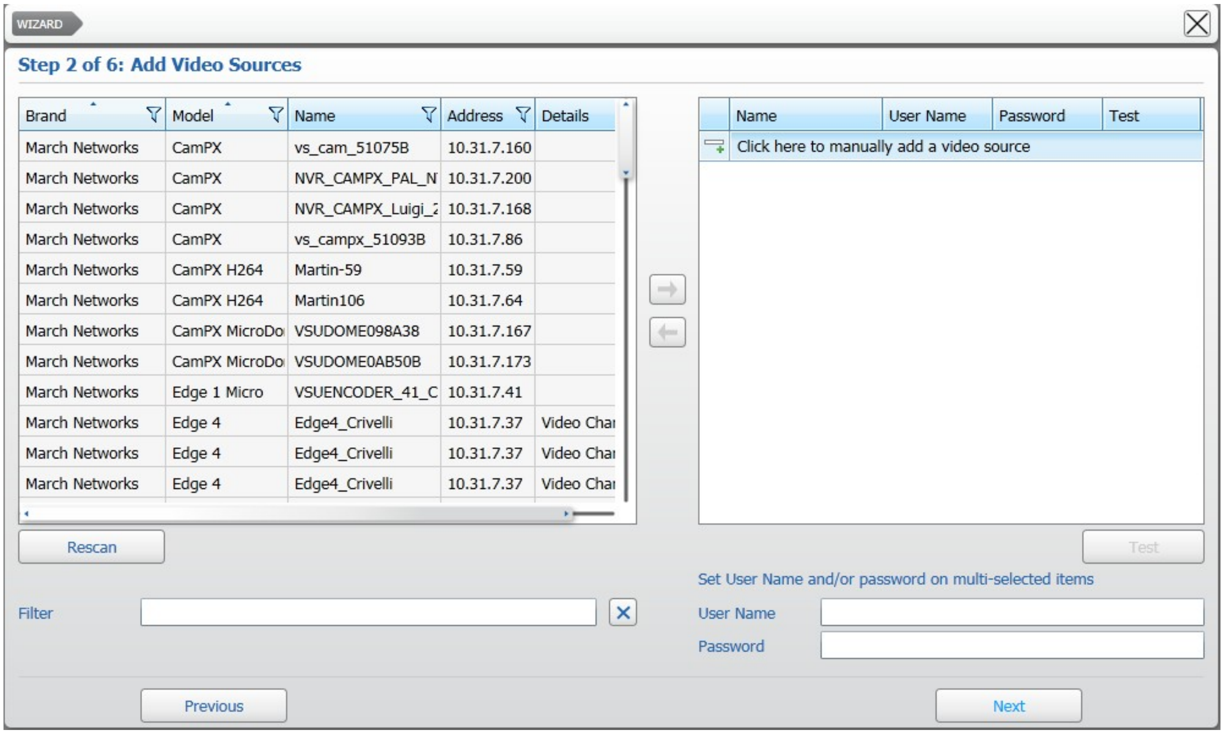
2 In the **Administrator Password** field, enter a new password for the *admin* account.
3 Enter the new password again in the **Confirm Password** field.
4 Click **Next** to save the changes and move to the next page.

Step 2: Adding IP Cameras

The **Add Video Sources** page allows you to add IP video channels to the Command Recording Software using the integrated network discovery tool or manually entering their network parameters. The integrated network discovery tool automatically scans the Command Recording Software sub-net to search for IP devices, such as March Networks IP cameras and encoders, ONVIF-compliant devices, and several third party cameras.

Notes:

- To discover selected third-party cameras using the UPNP protocol, you must enable the **SSDP Discovery** service on the server where the Command Recording Software service is running. For more information, see “Enabling the SSDP Discovery Service” on page 28.
- The **Configuration Wizard** does not allow you to add cameras from different Command Recording Softwares, 6000 Series Hybrid NVRs, and 3000/4000/8000 Series recorders using the E-Pass functionality.



Step 2 of 6: Add Video Sources

Brand	Model	Name	Address	Details
March Networks	CamPX	vs_cam_51075B	10.31.7.160	
March Networks	CamPX	NVR_CAMPX_PAL_N	10.31.7.200	
March Networks	CamPX	NVR_CAMPX_Luigi_	10.31.7.168	
March Networks	CamPX	vs_campx_51093B	10.31.7.86	
March Networks	CamPX H264	Martin-59	10.31.7.59	
March Networks	CamPX H264	Martin106	10.31.7.64	
March Networks	CamPX MicroDo	VSUDOME098A38	10.31.7.167	
March Networks	CamPX MicroDo	VSUDOME0AB50B	10.31.7.173	
March Networks	Edge 1 Micro	VSUENCODER_41_C	10.31.7.41	
March Networks	Edge 4	Edge4_Crivelli	10.31.7.37	Video Chai
March Networks	Edge 4	Edge4_Crivelli	10.31.7.37	Video Chai
March Networks	Edge 4	Edge4_Crivelli	10.31.7.37	Video Chai

Name	User Name	Password	Test
Click here to manually add a video source			

To add IP cameras to the Command Recording Software

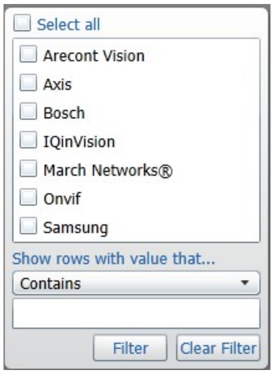
1. After you access the **Add Video Sources** page, the **Configuration Wizard** automatically performs a network scan to search for IP devices. To refresh the results, click **Rescan**.
2. Click on a column header to automatically sort the elements in the column list in ascending or descending alphabetical or numerical order.

   Note: Click on the column header again to change the order from ascending to descending or from descending to ascending.
3. If the list of scan results is large, you can also apply any of the following filters:

- **Camera Brand Filter**:

  a. Click the **Filter** icon in the **Brand** column.

     A menu appears.



  b. Select the check boxes corresponding to the camera brand you want to locate.

  c. Alternatively, you can configure a text filter by selecting the filter type from the list, and then entering the key word.

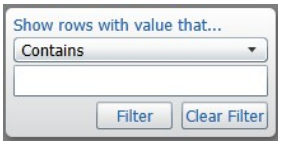
  d. Click **Filter** to apply the filter to the list.

     Tip: To remove the filter, click the **Filter** icon in the **Brand** column, and then click **Clear Filter**.

- **Name, Address, or Details Filter:**

  a. Click the **Filter** icon in the **Name**, **Address**, or **Details** column.

     A menu appears.



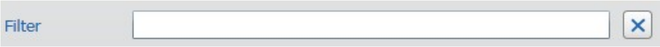
  b. To configure a text filter, select the filter type from the list, and then enter the key word.

c Click **Filter** to apply the filter to the list.

Tip: To remove the filter, click the **Filter** icon in the selected column, and then click **Clear Filter**.

- **Key Word Filter:**
  - Enter the key word in the **Filter** field.

    As you write the key word, the scan results are filtered.



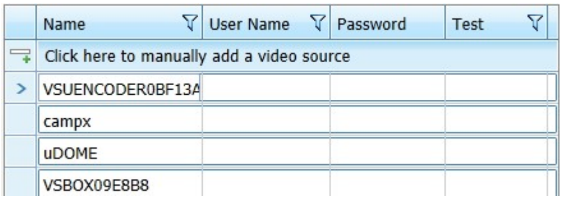
Filter

Tip: To remove the filter, click the ✕ button.

4 Select multiple cameras by keeping the **CTRL** key pressed and clicking additional cameras.

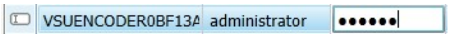
5 Click the ➡ button to add the cameras to the Command Recording Software.

The selected cameras appear in the camera list panel.



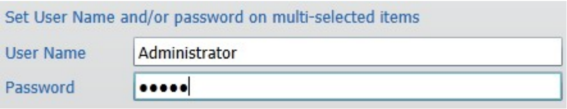
	Name	User Name	Password	Test
	Click here to manually add a video source			
>	VSUENCODER0BF13A			
	campx			
	uDOME			
	VSBOX09E8B8			

6 For each camera added to the Command Recording Software, enter the credentials required to access the video stream by clicking the **User Name** and **Password** fields.



VSUENCODER0BF13A	administrator	••••••

Tip: If two or more cameras share the same credentials, select them in the Command Recording Software cameras list panel by keeping the **CTRL** key pressed, and then enter the credentials in the **User Name** and **Password** fields located on the bottom of the page. The credentials are applied to the selected cameras.



Set User Name and/or password on multi-selected items

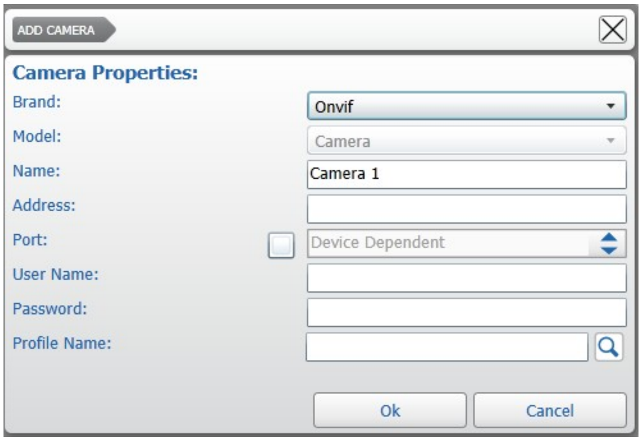
User Name: Administrator

Password: •••••

7 To manually add IP cameras to the Command Recording Software:

a Click the button in the camera list panel.

The **Add Camera** dialog box appears.



Camera Properties:

Brand: Onvif

Model: Camera

Name: Camera 1

Address:

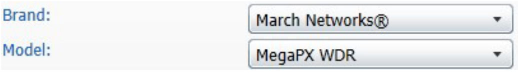
Port: □ Device Dependent

User Name:

Password:

Profile Name: 🔍

b Select the device **Brand** and the **Model** from the applicable list.



Brand: March Networks®

Model: MegaPX WDR

c Enter a **Name** for the device.

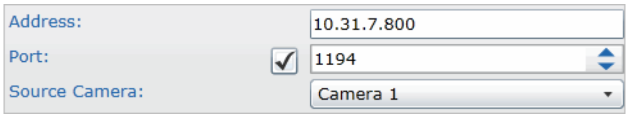
d Enter the IP **Address** of the device and select the **Port** check box to specify a communication port, if required.

e Enter the credentials (**User Name** and **Password**) required to access the video stream.

f To add a device that streams video from multiple connected cameras (such as an encoder, another Command Recording Software, or an NVR) select the video stream you want to add in the **Source Camera** list.

Notes:

- If you are adding an ONVIF compliant device, you are required to enter the ONVIF **Profile Name**. You can manually enter the profile, or click the 🔍 button to download the profile name from the camera.
- If you are adding **Generic** devices, you are also required to enter the URL of the video stream in the **Source Url** text box.



Address: 10.31.7.800

Port: ☑ 1194

Source Camera: Camera 1

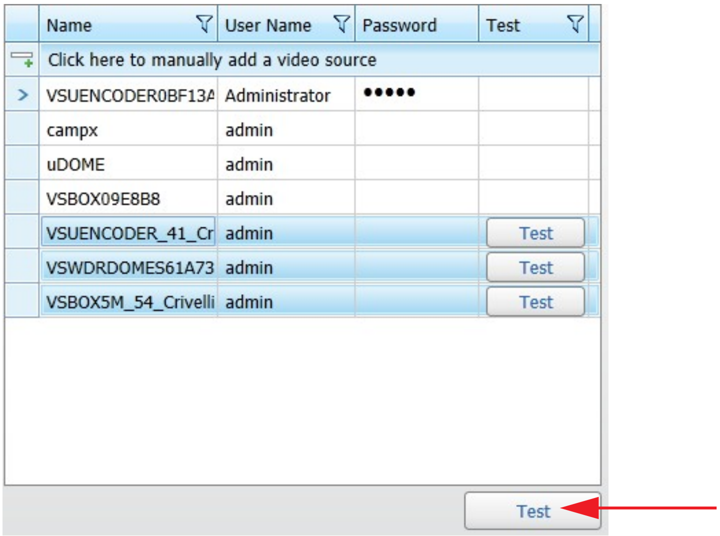
g Click **Ok** to add the camera to Command.

The camera appears in the camera list panel.

h Repeat step a to step g to manually add additional cameras to the Command Recording Software.

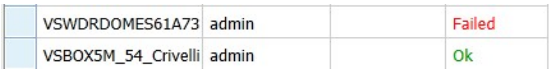
8 The **Configuration Wizard** also features a connectivity test for **Onvif** cameras: select all of the Onvif cameras in the cameras list panel, and then click the **Test** button.

Important: The ONVIF connectivity test is required to save the changes and move to the next page.



	Name	User Name	Password	Test
	Click here to manually add a video source			
>	VSUENCODER0BF13A	Administrator	●●●●●	
	campx	admin		
	uDOME	admin		
	VSBOX09E8B8	admin		
	VSUENCODER_41_Cr	admin		Test
	VSWDRDOMES61A73	admin		Test
	VSBOX5M_54_Crivelli	admin		Test

After a few seconds, the Command Recording Software performs the ONVIF connectivity test.



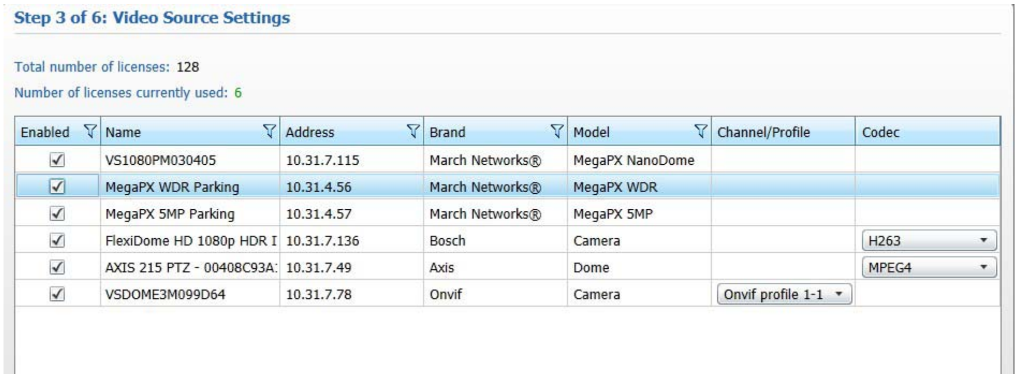
	VSWDRDOMES61A73	admin		Failed
	VSBOX5M_54_Crivelli	admin		Ok

9 Click **Next** to save the changes and move to the next page.

Step 3: Selecting Video Settings

The **Video Source Settings** page allows you enable/disable the added cameras, and configure the channel/profile and the video codec for ONVIF and selected third party cameras.

Note: The **Configuration Wizard** does not allow you to map the encoding profile of March Networks cameras. For more information, see "Editing IP Cameras" on page 161.



Step 3 of 6: Video Source Settings

Total number of licenses: 128

Number of licenses currently used: 6

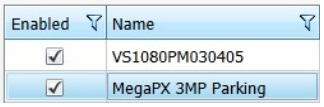
Enabled	Name	Address	Brand	Model	Channel/Profile	Codec
☑	VS1080PM030405	10.31.7.115	March Networks®	MegaPX NanoDome		
☑	MegaPX WDR Parking	10.31.4.56	March Networks®	MegaPX WDR		
☑	MegaPX 5MP Parking	10.31.4.57	March Networks®	MegaPX 5MP		
☑	FlexiDome HD 1080p HDR I	10.31.7.136	Bosch	Camera		H263 ▾
☑	AXIS 215 PTZ - 00408C93A:	10.31.7.49	Axis	Dome		MPEG4 ▾
☑	VSDOME3M099D64	10.31.7.78	Onvif	Camera	Onvif profile 1-1 ▾	

To select video settings

1 Click the row corresponding to the camera you want to configure.

2 In the **Enabled** column, clear the check box to disable the camera in Command.

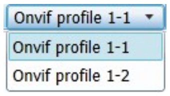
Note: While the camera is disabled, it still appears in the **Camera List** panel, but Command cannot connect to it and does not record its video.



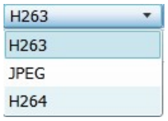
Enabled	Name
☑	VS1080PM030405
☑	MegaPX 3MP Parking

3 In the **Channel/Profile** column select the video channel or the Onvif profile from the list, if available.

Note: This option is available only for Onvif cameras and for selected third party cameras.



4 In the **Codec** column select the encoding profile for the camera, if available.

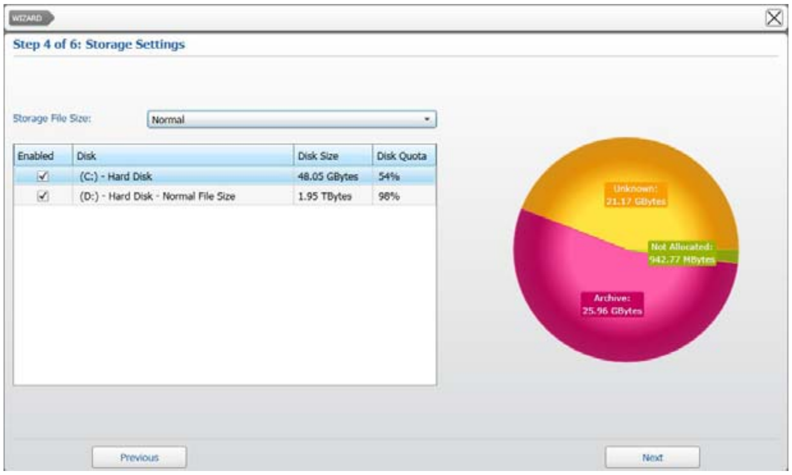


5 Repeat step 1 to step 4 to configure additional cameras.

6 Click **Next** to save the changes and move to the next page.

Step 4: Adding Storage Disks

The **Storage Settings** page allows you to add the system disks (including external USB drives) to the Command Recording Software to storage the video archive.



Step 4 of 6: Storage Settings

Storage File Size: Normal

Enabled	Disk	Disk Size	Disk Quota
☑	(C:) - Hard Disk	48.05 GBytes	54%
☑	(D:) - Hard Disk - Normal File Size	1.95 TBytes	98%

Important: If you plan to use Network Attached Storage (NAS) disks to archive video, you must disable all of the detected system disks, complete the configuration procedure with the **Configuration Wizard**, and then access the **Storage Configuration** page in Command Config. For more information about adding NAS disks, see “Adding or Importing Storage Disks” on page 137.

To add storage disks

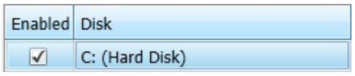
1 Select the storage group dimensions from the **Storage File Size** list:

- Select **Normal** if the storage total dimensions are under 30TB.
- Select **Large** if the storage total dimensions are over 30TB.

Tip: This option allows much faster storage mounting and management times with large storage dimensions.

2 Click the row corresponding to the disk you want to configure.

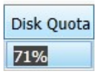
3 In the **Enabled** column, select/clear the check box to add/remove the storage disk to the Command Recording Software.



Enabled	Disk
☑	C: (Hard Disk)

Note: System disks are enabled by default, while external USB disks are disabled by default.

4 To modify the default disk allocation, click the **Disk Quota** field and enter a new allocation value for the disk. Press the **ENTER** key on your keyboard to confirm the changes.



Disk Quota
71%

5 Repeat step 1 to step 4 to add and configure additional storage disks.

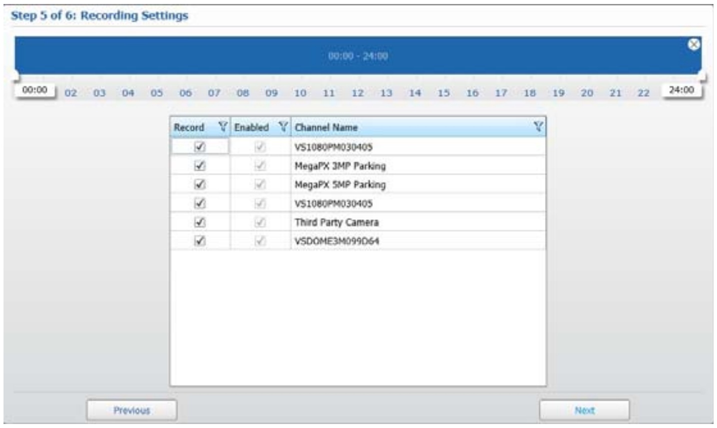
6 Click **Next** to save the changes and move to the next page.

Step 5: Configure Recording Settings

The **Recording Settings** page allows you to configure the following methods to record evidence:

- **Continuous recording** — Recording of evidence occurs 24 hours a day, seven days a week. For more information, see “To configure continuous recording” on page 57.
- **Programmed recording** — Recording only occurs on the times you specify. For more information, see “To configure programmed recording” on page 57.

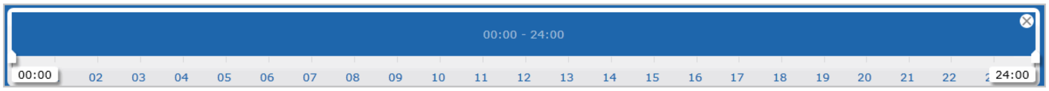
Note: The **Configuration Wizard** does not allow you to configure the **On-Event** recording method, specify dates for the **Programmed** recording, and enable/disable cameras.



Record	Enabled	Channel Name
☑	☑	VS1080PM030405
☑	☑	MegaPX 3MP Parking
☑	☑	MegaPX 5MP Parking
☑	☑	VS1080PM030405
☑	☑	Third Party Camera
☑	☑	VSDOME3M099D64

To configure continuous recording

1 Check that the entire timeline (24 hours) is selected.



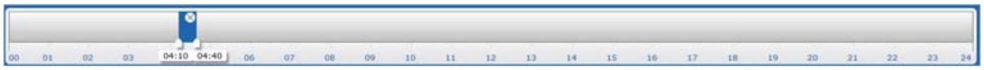
2 Clear the check boxes corresponding to the cameras you do not want to record.

3 Click **Next** to save the changes and move to the next page.

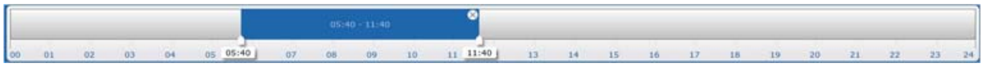
To configure programmed recording

1 To select a time interval using the timeline, do the following:

a Click and hold the left mouse button down at the desired start time.

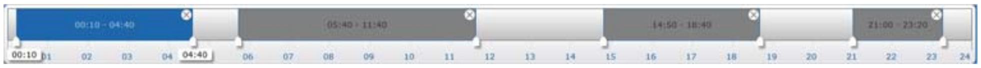


b Click and drag to define the length of the time interval.



Tip: To resize a time interval, click and drag the white tab at the beginning of at the ending of the interval. To move a time interval, click and drag inside the interval.

c You can set multiple time intervals for the same day.

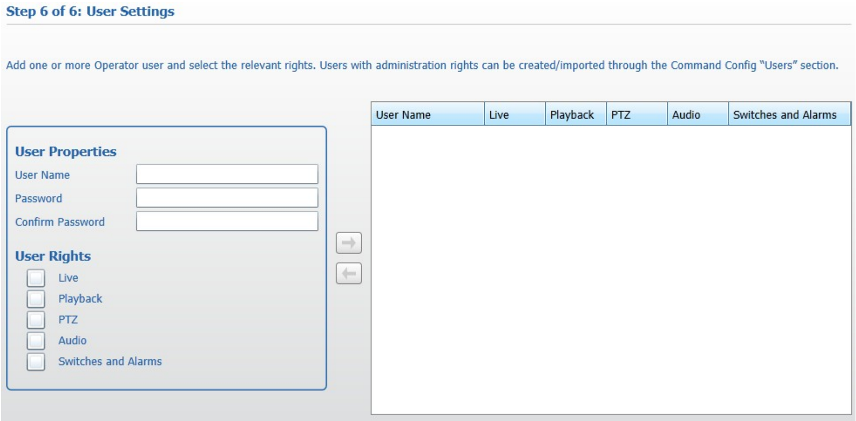


2 Clear the check boxes corresponding to the cameras you do <u>not</u> want to record.

3 Click **Next** to save the changes and move to the next page.

Step 6: Creating and Customizing Local User Profiles

The **User Settings** page allows you to create new local user profiles and customize them by assigning permissions over the main Command Recording Software functionalities.



Step 6 of 6: User Settings

Add one or more Operator user and select the relevant rights. Users with administration rights can be created/imported through the Command Config "Users" section.

User Properties

User Name

Password

Confirm Password

User Rights

☐ Live

☐ Playback

☐ PTZ

☐ Audio

☐ Switches and Alarms

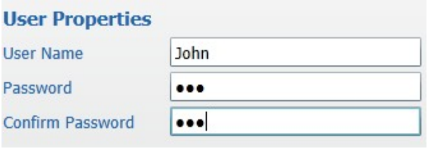
User Name	Live	Playback	PTZ	Audio	Switches and Alarms

Note: The **Configuration Wizard** does not allow you to assign permissions by schedule or by single resources, and add users or groups from a LDAP server.

To create and customize a local user profile

1 In the **User Properties** section, enter a **User Name** for the profile.

2 Enter a **Password** for the profile and enter it again in the **Confirm password** field.



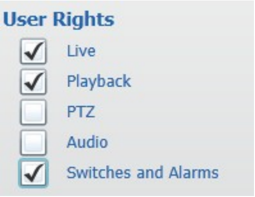
User Properties

User Name: John

Password: •••

Confirm Password: •••

3 In the **User Rights** section, select the check boxes corresponding to the permissions you want to assign to the profile.



User Rights

☑ Live

☑ Playback

☐ PTZ

☐ Audio

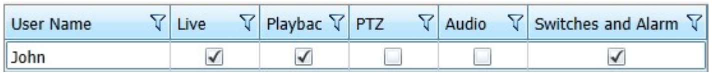
☑ Switches and Alarms

The permissions are described in the following table.

Permission	Action
Live	Select the **Live** check box to allow the user to view live video streams.
Playback	Select the **Playback** check box to allow the user to review recorded video evidence.
PTZ	Select the **PTZ** check box to allow the user to control PTZ cameras.
Audio	Select the **Audio** check box to allow the user to manage and configure audio channels for the cameras.
Switches and Alarms	Select the **Switches and Alarms** check box to allow the user to manage auxiliary channels and alarms.

4 Click the → button to create the user profile.

The user profiles appears in the user profile list panel.



User Name	Live	Playbac	PTZ	Audio	Switches and Alarm
John	☑	☑	☐	☐	☑

5 Repeat step 1 to step 4 to create additional user profiles.

6 To edit the permissions of a user profile, select or clear the check boxes corresponding to the permissions in the user profile list panel.

7 To edit the user’s credentials:

a Select the user profile in the user profile list panel.

b Click the ← button.

c Edit the user’s credentials in the **User Properties** section.

d Click the → button to apply the changes.

Note: The → button is enabled only if the passwords entered in **Password** and **Confirm Password** fields correspond.

8 Click **Finish** to save the changes and close the **Configuration Wizard**.

The process is complete and all of the configurations are applied to the Command Recording Software.

Congratulations!

Your Command Recording Software is now capable of recording, streaming live video, and playing back archived video evidence. For advanced system configuration, see chapters 5-17 of this Configuration Guide.

Chapter 5

Managing User Profiles

The **User Configuration** page allows you to create and customize local user profiles, LDAP user profiles and LDAP user groups. It also allows you to assign permissions to user profiles. User permissions limit what a user is allowed to access and configure.

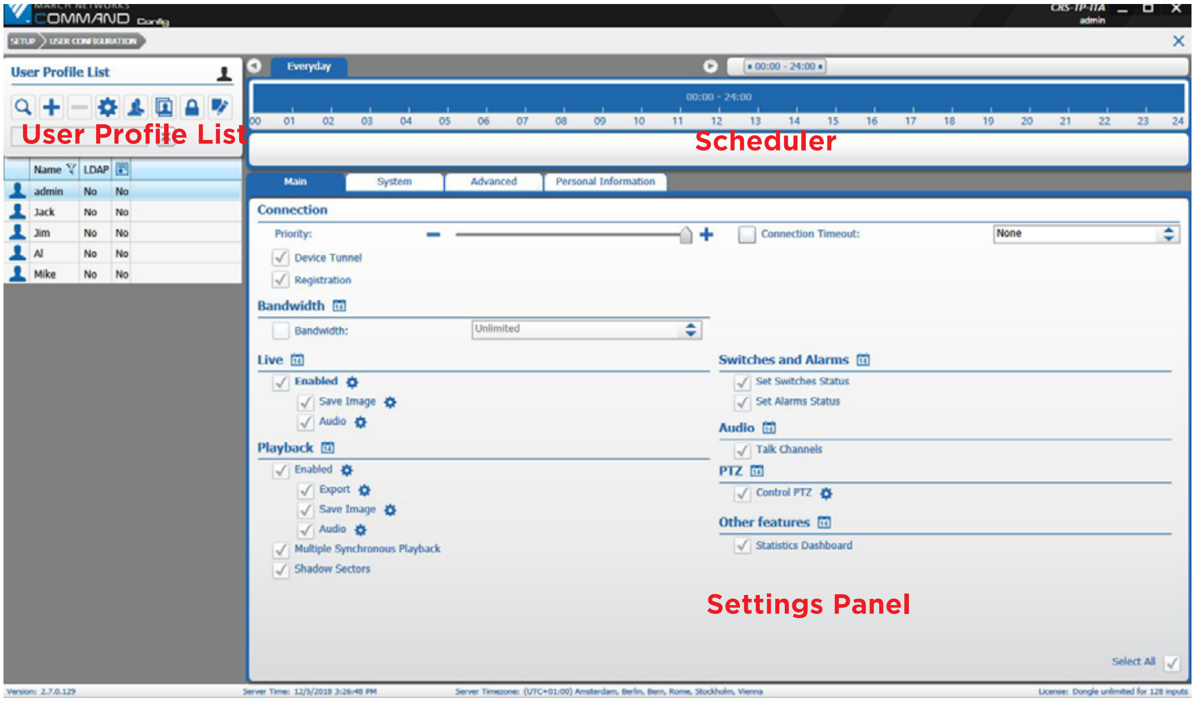
This chapter contains the following sections:

Overview

The **User Configuration** page allows you to create local user, import users from the LDAP service or import group of users from the LDAP service. It also allows you to assign permissions and schedules to user profiles.

To access the page, on the Command Config main page, under **User Management**, click **Users**.

The following illustration shows the **User Configuration** user interface.



Name	LDAP	
admin	No	No
Jack	No	No
Jim	No	No
Al	No	No
Mike	No	No

Connection

Priority:

☐ Connection Timeout: None

☑ Device Tunnel

☑ Registration

Bandwidth

☐ Bandwidth: Unlimited

Live

☑ Enabled

☑ Save Image

☑ Audio

Playback

☑ Enabled

☑ Export

☑ Save Image

☑ Audio

☑ Multiple Synchronous Playback

☑ Shadow Sectors

Switches and Alarms

☑ Set Switches Status

☑ Set Alarms Status

Audio

☑ Talk Channels

PTZ

☑ Control PTZ

Other features

☑ Statistics Dashboard

Select All ☑

Version: 2.7.0.129 Server Time: 12/5/2018 3:26:48 PM Server Timezone: (UTC+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna License: Dongle unlimited for 128 inputs

The **User Configuration** page is divided into three main areas.

1 **User Profile List** panel — Located at the top-left corner of the screen, it allows you to create, remove, duplicate and filter user profiles, duplicate Command Client user preferences, and configure extended login features for a user profile.

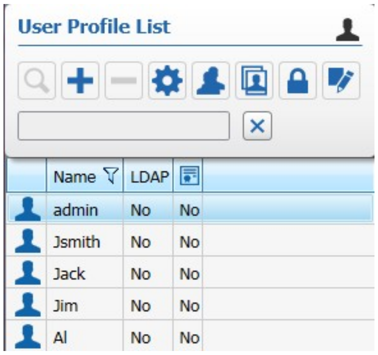
2 **Scheduler** — Located at the top of the screen, it allows you to set permissions based on day and time intervals.

3 **Settings** panel — Located at the bottom of the screen, it allows you to assign permissions to the user profiles.

User Profile List Panel

The **User Profile List** panel is located at the top-left corner of the screen. You can create, remove, duplicate and filter user profiles, and configure extended login features for a user profile using the **User Profile List** panel. The list displays the user profile's name, if the user profile is local or LDAP, and if an identification certificate is linked to the user profile. User groups are added to the **User Profile List** panel with a different icon.

The following table provides a description of the panel buttons.



User Profile List

	Name	LDAP	▤
👤	admin	No	No
👤	Jsmith	No	No
👤	Jack	No	No
👤	Jim	No	No
👤	Al	No	No

Button	Action
🔍	Imports a user profile or a user group from the LDAP service. **Note:** This button appears only if Command has established a successful connection to the LDAP server configured in the System Configuration page.
+	Creates a new user profile.
−	Removes the selected user profile from the Command Recording Software. **Note:** It is not possible to remove the *admin* user profile.
⚙	Opens the **Security Settings** dialog box.
👥	Duplicates the selected user profile.
▣	Duplicates Command Client's preferences and the **Personal** tree resources from a user profile to one or multiple user profiles.
🔒	Locks the selected user profile configuration.
✎	Opens the **Manage Camera Groups** dialog box.
▭ ☒	Filters the user profile list by entering text criteria.

Button	Action
▽	Filters data in the **Name** column.

Filtering in the User Profile List Panel

You can sort and filter the user profiles by text or by column. See the following sections for more details:

- "Filtering by Text" on page 63
- "Sorting in Columns" on page 64
- "Filtering in Columns" on page 64

Filtering by Text

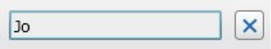
In the **User Profile List** panel, you can filter for a text string. The filter applies to all columns in the **User Profile List** panel.

When the text box field is empty, there is no active search and all users appear.

As you enter letters, characters, or numbers in the text box, the **User Profile List** panel automatically refreshes with the selected criteria.

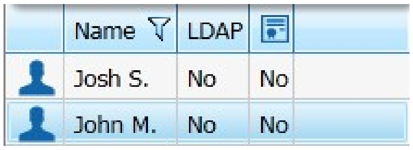
To filter by text in the User Profile List panel

1 On the **User Profile List** panel, enter the filter criteria in the text box.



Jo

The panel refresh to display only those users or groups that correspond to the filter criteria.



	Name ▽	LDAP	▣
👤	Josh S.	No	No
👤	John M.	No	No

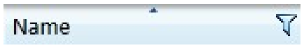
2 To remove the filter, click the ☒ button.

Sorting in Columns

You can alphabetically or numerically sort a column list (depending on the content of the list).

To sort in a column

1 Click on a column header to show the **Sort** icon.



2 Click the **Sort** icon to automatically sort the elements in the column list in ascending or descending alphabetical or numerical order.

Note: Click on the **Sort** icon again to change the order from ascending to descending or from descending to ascending.

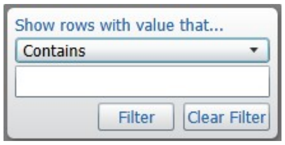
Filtering in Columns

You can filter data in the **Name** column list to show only specified list values.

To filter in a column

1 Select the **Name** column header and click the **Filter** icon.

The **Filter by text** dialog box appears.



2 For columns filtered by type, do one of the following:

- Select one or more check boxes.
- Click the **Select all** box to select all column elements.

As you select a check box, the column list displays only those switches details that match the specified filter criteria.

3 For columns filtered by text, do the following:

a Click the **Show rows with value that** drop-down list and select a filter expression.

Options include **Contains** and **Does not contain**.

b Enter a filter criteria in the text box.

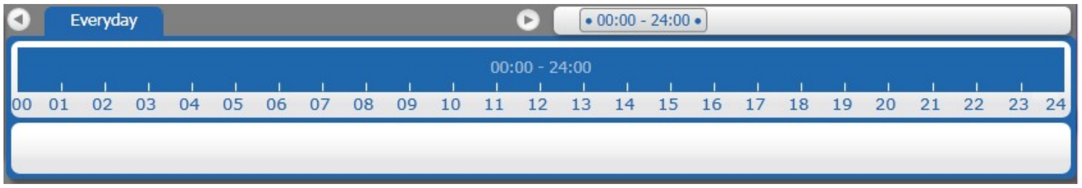
c Click **Filter** to apply the filter to the list.

The column list displays only those switches details that match the specified filter criteria.

Tip: To remove the filter, click the **Filter** icon in the column, and then click **Clear Filter**.

Scheduler

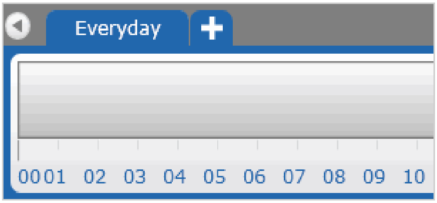
The **Scheduler** is located at the top of the screen. You can set permissions based on day and time intervals.



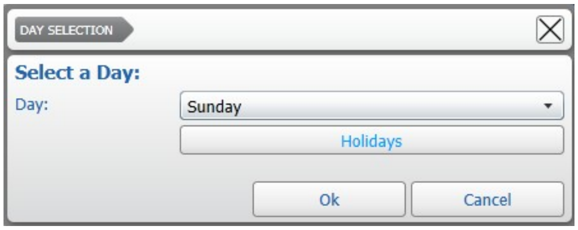
To create a schedule

1 In the **User Configuration** page, do one of the following:

- To configure the user permissions for every day, use the default **Everyday** tab.
- To configure the user permissions for a specific day of the week/month, click the plus tab + to create a new tab for a specific day.



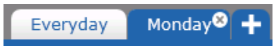
The **Day Selection** dialog box appears.



Day: Sunday

Select a day from the list and click **Ok**.

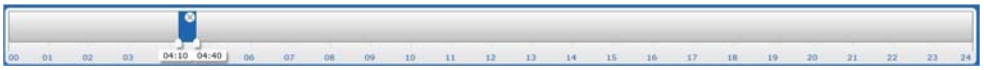
The tab for the selected day is added to the list.



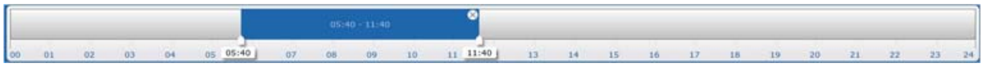
Note: When schedules conflict (for example, the **Everyday** tab is configured from 10 A.M., while the **Monday** tab is configured from 8 A.M.), Command follows an internal priority list. The priority, starting from top to bottom, is: Holiday, 1st/10th/15th day of the month, Single day of the week, Everyday.

2 To select a time interval for that day using the timeline, do the following:

- Click and hold the left mouse button down at the desired start time.

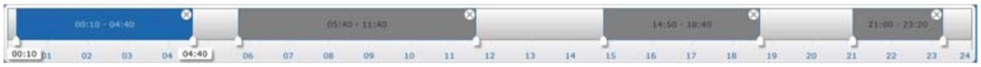


- Click and drag to define the length of the time interval.



Tip: To resize a time interval, click and drag the white tab at the beginning of at the ending of the interval. To move a time interval, click and drag inside the interval.

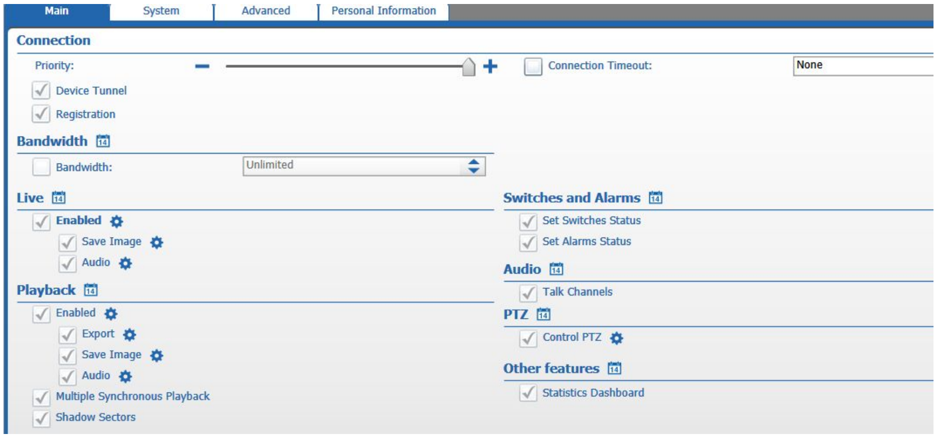
- You can set multiple time intervals for the same day. Every time interval on the time line has its own schedule. Click a time interval to select it or hold down the **SHIFT** key to select multiple intervals.



Settings Panel

The **Settings Panel** is located at the bottom of the screen. You can manage and assign permissions to user profiles using the **Settings Panel**.The **Settings Panel** contains four tabs:

- **Main** — where you can assign permissions on the main Command Recording Software features.



Connection

Priority:

□ Connection Timeout: None

☑ Device Tunnel

☑ Registration

Bandwidth

□ Bandwidth: Unlimited

Live

☑ Enabled
  ☑ Save Image
  ☑ Audio

Playback

☑ Enabled
  ☑ Export
  ☑ Save Image
  ☑ Audio

☑ Multiple Synchronous Playback

☑ Shadow Sectors

Switches and Alarms

☑ Set Switches Status

☑ Set Alarms Status

Audio

☑ Talk Channels

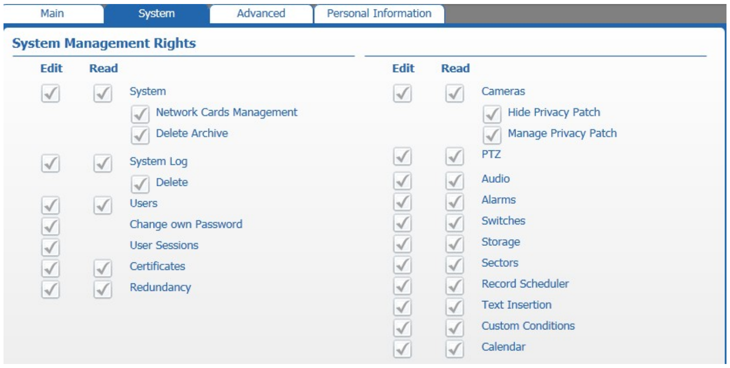
PTZ

☑ Control PTZ

Other features

☑ Statistics Dashboard

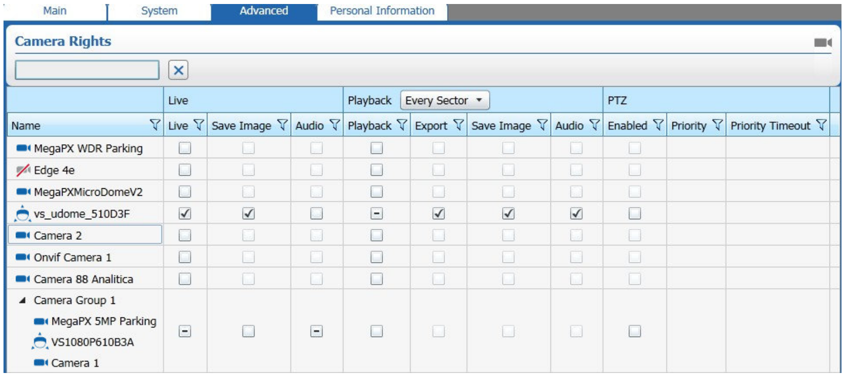
- **System** — where you can assign permissions on specific Command Config pages and configurations.



System Management Rights

Edit	Read		Edit	Read	
☑	☑	System	☑	☑	Cameras
		☑ Network Cards Management			☑ Hide Privacy Patch
		☑ Delete Archive			☑ Manage Privacy Patch
☑	☑	System Log	☑	☑	PTZ
		☑ Delete	☑	☑	Audio
☑	☑	Users	☑	☑	Alarms
☑		Change own Password	☑	☑	Switches
☑		User Sessions	☑	☑	Storage
☑	☑	Certificates	☑	☑	Sectors
☑	☑	Redundancy	☑	☑	Record Scheduler
			☑	☑	Text Insertion
			☑	☑	Custom Conditions
			☑	☑	Calendar

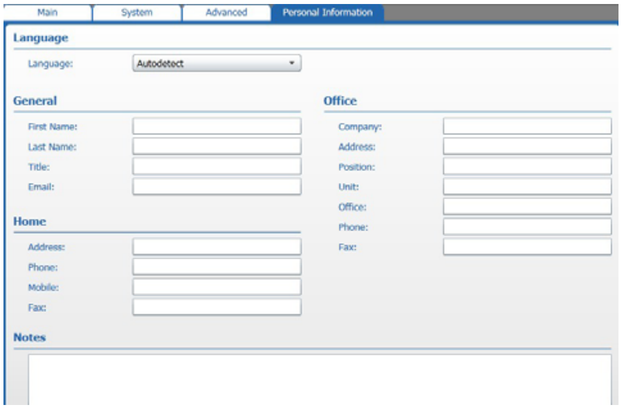
- **Advanced** — where you can assign permissions on single cameras or group of cameras.



Camera Rights

	Live			Playback Every Sector				PTZ		
Name	Live	Save Image	Audio	Playback	Export	Save Image	Audio	Enabled	Priority	Priority Timeout
MegaPX WDR Parking	☐	☐	☐	☐	☐	☐	☐	☐		
Edge 4e	☐	☐	☐	☐	☐	☐	☐	☐		
MegaPXMicroDomeV2	☐	☐	☐	☐	☐	☐	☐	☐		
vs_udome_510D3F	☑	☑	☐	⊟	☑	☑	☑	☐		
Camera 2	☐	☐	☐	☐	☐	☐	☐	☐		
Onvif Camera 1	☐	☐	☐	☐	☐	☐	☐	☐		
Camera 88 Analitica	☐	☐	☐	☐	☐	☐	☐	☐		
Camera Group 1	⊟	☐	⊟	☐	☐	☐	☐	☐		
MegaPX 5MP Parking										
VS1080P610B3A										
Camera 1										

- **Personal Information** — where you can set the interface language for the user profile and enter the user's details.



Language

Language: Autodetect

General

First Name:

Last Name:

Title:

Email:

Home

Address:

Phone:

Mobile:

Fax:

Office

Company:

Address:

Position:

Unit:

Office:

Phone:

Fax:

Notes

Changing the Administrator Password

To protect the security of your network, we recommend that you change the administrator password as soon as possible.

Notes:

- The system administrator can also change the password from the Command Config (see "Changing the Password From the Login page" on page 33) and Command Client login pages.
- The system administrator (*admin*) account has full access rights on the Command Recording Software. The *admin* profile is unique for every March Networks application.
- When you install the software for the first time, a blank password (no password) is the default value for the *admin* user profile. The *admin* user profile is a default profile that has access to all configuration. You cannot delete the admin profile.
- If you are viewing the application directly after installation, the only available profile is the *admin* user profile.

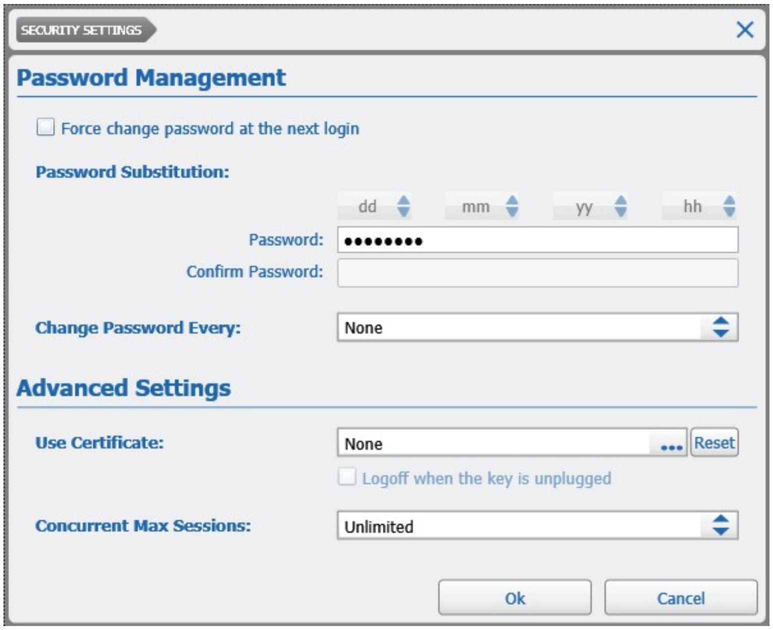
- To enhance protection for the *admin* user profile, you can configure automatic password changes. For more information, see “Configuring Extended Features for a User Profile” on page 74.
- You can also set a limit of concurrent sessions for the *admin* user profile. For more information, see “Configuring Extended Features for a User Profile” on page 74.
- The admin account is subject to the password policy configured on the **System Settings** page. For more information, see "Configuring the Password Policy" on page 123.

To change the administrator password

1 On the **User Configuration** page, select the admin user profile in the **User Profile List** panel.

2 Click the ⚙ button.

The **Security Settings** dialog box appears.



Password Management

□ Force change password at the next login

Password Substitution:

dd mm yy hh

Password: ••••••••

Confirm Password:

Change Password Every: None

Advanced Settings

Use Certificate: None ••• Reset

□ Logoff when the key is unplugged

Concurrent Max Sessions: Unlimited

3 In the **Password Management** section, enter a new password in the **Password** field.

4 Enter again the new password in the **Confirm Password** field.

Tip: The dialog box warns if the passwords do not match or if the new password does not respect the password policy configured in the **System** page.

5 Click **Ok** to confirm the password change.

6 Click the 💾 button to save and apply the changes.

Creating Local User Profiles

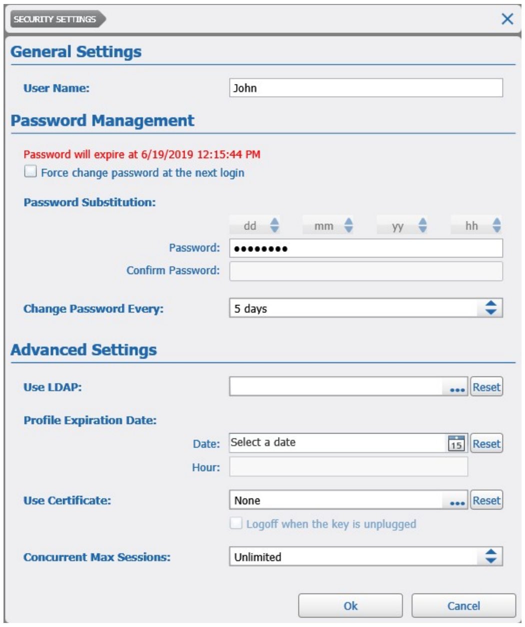
You can create local user profiles and customize them by adding permissions according to the specific day of the week or particular events. When you create user profiles, you can set the login credentials and specific security features, and specify customized permissions for the user, according to their role in the organization. For example, a control room operator should be able to view live and recorded video, and export recorded video but not be able to modify settings regarding cameras, storage, and recording schedules.

Note: The extended security feature for a user profile are described in the section “Configuring Extended Features for a User Profile” on page 74.

To create a new user profile

1 On the **User Configuration** page, click the + button to create a new user profile.

The **Security Settings** dialog box appears.



SECURITY SETTINGS

General Settings

User Name: John

Password Management

Password will expire at 6/19/2019 12:15:44 PM

☐ Force change password at the next login

Password Substitution:

dd mm yy hh

Password: ••••••••

Confirm Password:

Change Password Every: 5 days

Advanced Settings

Use LDAP:

Profile Expiration Date:

Date: Select a date

Hour:

Use Certificate: None

☐ Logoff when the key is unplugged

Concurrent Max Sessions: Unlimited

2 In the **General Settings** section, enter a **User Name** for the profile

3 In the **Password Management** section, enter a the password for the user profile in the **Password** field.

4 Enter again the new password in the **Confirm Password** field.

Tip: The dialog box warns if the passwords do not match or if the new password does not respect the password policy configured in the **System** page.

5 Click **Ok** to confirm the password change.

The new profile appears in the **User Profile List** panel.

6 Click the 💾 button to save and apply the changes.

Configuring LDAP Authentication for Local User Profiles

Command is compatible with LDAP servers, and allows you to configure LDAP authentication for local user accounts based on an LDAP user list. When a user account attempts to connect to Command, it automatically establishes a connection to the LDAP server to check and authenticate the user's credentials. Active Directory servers are useful to enforce password management policies (for example, password strengths, password expiration, and mandatory password change at first login in the domain) to all the elements of your video surveillance system.

Notes:

- You must configure a valid LDAP server in the **System Configuration** page before you can configure the LDAP authentication. For more information, see "To configure LDAP settings" on page 115. If a valid LDAP is not configured, the **Use LDAP** option does not appear in the **Security Settings** dialog box.
- After you configure LDAP authentication, the user can log on to the Command Recording Software using one of the following LDAP parameters as user name: **Username**, **Common Name**, and **Account Name**.
- If the user is member of an LDAP user group added to the Command Recording Software, the user has all of the permissions configured for the user profiles and the user group.
- If an LDAP user group is selected instead of an LDAP user, the local user account switches to a user group, and all of the group members can log on to the Command Recording Software using their LDAP credentials.

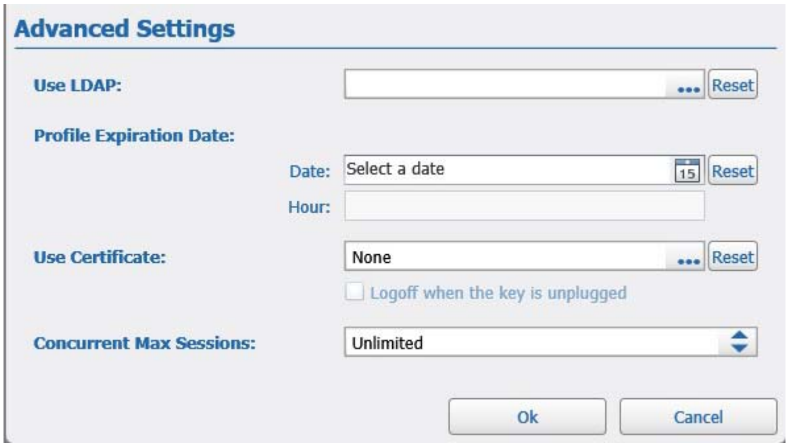
To configure LDAP authentication for a local user profile

1 On the **User Configuration** page, select a local user profile in the **User Profile List** panel.

2 Click the ⚙ button

The **Security Settings** dialog box appears.

Note: The the **Use LDAP** option appears only if Command has established a successful connection to the LDAP server configured in the **System Configuration** page. For more information, see "To configure LDAP settings" on page 115.



Advanced Settings

Use LDAP:

Profile Expiration Date:

Date: Select a date

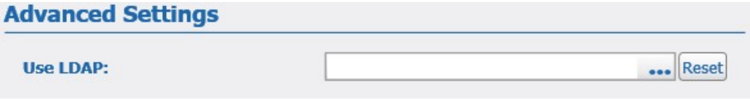
Hour:

Use Certificate: None

□ Logoff when the key is unplugged

Concurrent Max Sessions: Unlimited

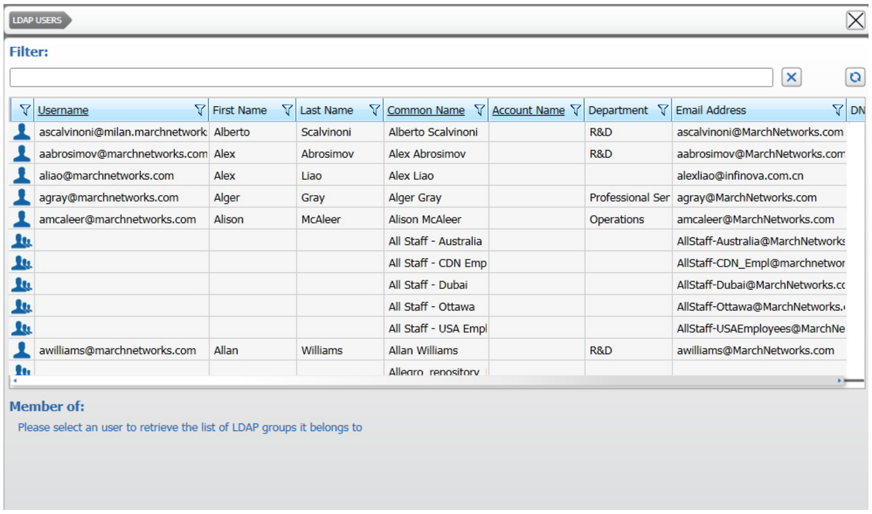
3 In the **Adavanced Settings** section, click the ••• button near the **Use LDAP** option to select to import the LDAP user from the list of users available on the LDAP server.



Advanced Settings

Use LDAP:

The **LDAP Users** dialog box appears.



Filter:

	Username	First Name	Last Name	Common Name	Account Name	Department	Email Address	DN
👤	ascalvinoni@milan.marchnetwork	Alberto	Scalvinoni	Alberto Scalvinoni		R&D	ascalvinoni@MarchNetworks.com	
👤	aabrosimov@marchnetworks.com	Alex	Abrosimov	Alex Abrosimov		R&D	aabrosimov@MarchNetworks.com	
👤	aliao@marchnetworks.com	Alex	Liao	Alex Liao			alexliao@infinova.com.cn	
👤	agray@marchnetworks.com	Alger	Gray	Alger Gray		Professional Ser	agray@MarchNetworks.com	
👤	amcaleer@marchnetworks.com	Alison	McAleer	Alison McAleer		Operations	amcaleer@MarchNetworks.com	
👥				All Staff - Australia			AllStaff-Australia@MarchNetworks	
👥				All Staff - CDN Emp			AllStaff-CDN_Empl@marchnetwor	
👥				All Staff - Dubai			AllStaff-Dubai@MarchNetworks.cc	
👥				All Staff - Ottawa			AllStaff-Ottawa@MarchNetworks.	
👥				All Staff - USA Empl			AllStaff-USAEmployees@MarchNe	
👤	awilliams@marchnetworks.com	Allan	Williams	Allan Williams		R&D	awilliams@MarchNetworks.com	
👥				Allegro_repository				

Member of:

Please select an user to retrieve the list of LDAP groups it belongs to

4 Do one of the following:

- Manually search for the user corresponding to the Command user profile in the LDAP users list.
- Filter the results by entering a search string:

a Enter the search string in the **Filter** field.

The results are instantly filtered.

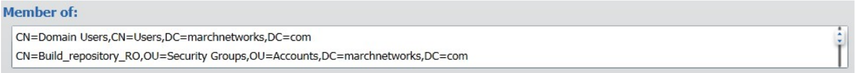
b To refresh the search results, click the ↻ button.

c To remove the filter, click the ✕ button.

5 Select the user corresponding to the Command user profile in the list and click **Ok**.

Notes:

- The text box below the list reports the LDAP user groups the user is member of.



Member of:

CN=Domain Users,CN=Users,DC=marchnetworks,DC=com
CN=Build_repository_RO,OU=Security Groups,OU=Accounts,DC=marchnetworks,DC=com

- To disable LDAP authentication click the **Reset** button.

6 Click **Ok** to save and apply the changes, and close the dialog box.

7 Click the 💾 button to save and apply the changes.

Adding User Profiles from the LDAP Service

Command is compatible with LDAP servers, and allows you to add user profiles based on an LDAP user list. When a LDAP user profile attempts to connect to Command, it automatically establishes a connection to the LDAP server to check and authenticate the user's credentials.

Notes:

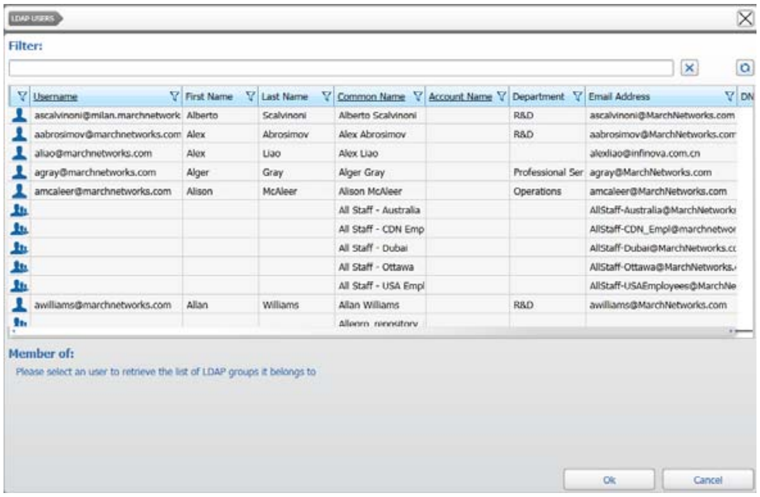
- You must configure a valid LDAP server in the **System Configuration** page before you can add a user from the LDAP service. For more information, see "To configure LDAP settings" on page 115. If a valid LDAP is not configured, the 🔍 button does not appear in the **User Profile List** panel.
- After you add a user from the LDAP service, the user can log on to the Command Recording Software using one of the following LDAP parameters as user name: **Username**, **Common Name**, and **Account Name**.
- If the user is member of an LDAP user group added to the Command Recording Software, the user has all of the permissions configured for the user profiles and the user group.

To add a user from the LDAP service

1 In the **User Profile List**, click the 🔍 button.

Note: The 🔍 button appears only if Command has established a successful connection to the LDAP server configured in the **System Configuration** page. For more information, see "To configure LDAP settings" on page 115

The **LDAP Users** dialog box appears.



	Username	First Name	Last Name	Common Name	Account Name	Department	Email Address	DN
👤	ascalvinoni@milan.marchnetwork	Alberto	Scalvinoni	Alberto Scalvinoni		R&D	ascalvinoni@MarchNetworks.com	
👤	aabrosimov@marchnetworks.com	Alex	Abrosimov	Alex Abrosimov		R&D	aabrosimov@MarchNetworks.com	
👤	aliao@marchnetworks.com	Alex	Liao	Alex Liao			alexliao@infinova.com.cn	
👤	agray@marchnetworks.com	Alger	Gray	Alger Gray		Professional Ser	agray@MarchNetworks.com	
👤	amcaleer@marchnetworks.com	Alison	McAleer	Alison McAleer		Operations	amcaleer@MarchNetworks.com	
👥				All Staff - Australia			AllStaff-Australia@MarchNetwork	
👥				All Staff - CDN Emp			AllStaff-CDN_Empl@marchnetwor	
👥				All Staff - Dubai			AllStaff-Dubai@MarchNetworks.cc	
👥				All Staff - Ottawa			AllStaff-Ottawa@MarchNetworks.	
👥				All Staff - USA Empl			AllStaff-USAEmployees@MarchNe	
👤	awilliams@marchnetworks.com	Allan	Williams	Allan Williams		R&D	awilliams@MarchNetworks.com	
👥				Allegro repository				

Please select an user to retrieve the list of LDAP groups it belongs to

2 Do one of the following:

- Manually search for the user profile in the LDAP users list.
- Filter the results by entering a search string:

a Enter the search string in the **Filter** field.

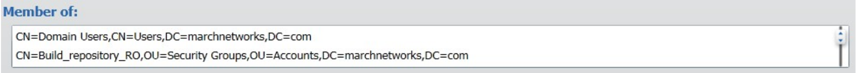
The results are instantly filtered.

b To refresh the search results, click the ⟳ button.

c To remove the filter, click the ✕ button.

3 Select the user you want to add to Command and click **Ok**.

Note: The text box below the list reports the LDAP user groups the user is member of.



Member of:

CN=Domain Users,CN=Users,DC=marchnetworks,DC=com
CN=Build_repository_RO,OU=Security Groups,OU=Accounts,DC=marchnetworks,DC=com

The user is added to the **User Profile List**.

4 Configure permissions for the new user profile. For more information, see “Assigning Permissions to User Profiles and User Groups” on page 79.

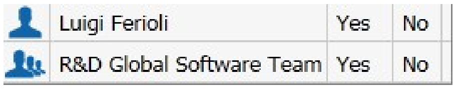
5 Click the 💾 button to save and apply the changes.

Adding User Groups from the LDAP Service

Command is compatible with LDAP servers, and allows you to add user groups based on an LDAP user list. Any user groups imported from the LDAP server are read-only. Any alterations to the group or members of the group must be made through the LDAP server. After you import the group, you assign permissions for the group and the permissions are automatically assigned to all of the LDAP user accounts that are members of the group. Active Directory servers are useful to enforce password management policies (for example, password strengths, password expiration, and mandatory password change at first login in the domain) to all the elements of your video surveillance system.

Notes:

- You must configure a valid LDAP server in the **System Configuration** page before you can add a user from the LDAP service. For more information, see “To configure LDAP settings” on page 115. If a valid LDAP is not configured, the 🔍 button does not appear in the **User Profile List** panel.
- User groups are added to the **User Profile List** panel with a different icon.



👤	Luigi Ferioli	Yes	No
👥	R&D Global Software Team	Yes	No

User Profile
User Group

- An LDAP user group cannot log on to the Command Recording Software (a user group does not have a login user name).
- Any members of the LDAP user group can log on to the Command Recording Software (unless the user has been banned from the Command Recording Software; see “Banning Connections from Command” on page 101) using one of the following LDAP parameters as user name: **Username**, **Common Name**, and **Account Name**.
- If the user is member of an LDAP user group added to the Command Recording Software, the user has all of the permissions configured for the user profiles and the user group.

To add a user group from the LDAP service

1 In the **User Profile List**, click the 🔍 button.

Note: The 🔍 button appears only if Command has established a successful connection to the LDAP server configured in the **System Configuration** page. For more information, see "To configure LDAP settings" on page 115

The **LDAP Users** dialog box appears.

2 Do one of the following:

- Manually search for the user group in the LDAP users list.
- Filter the results by entering a search string:

a Enter the search string in the **Filter** field.

The results are instantly filtered.

b To refresh the search results, click the ↻ button.

c To remove the filter, click the ✕ button.

3 Select the group you want to add to Command and click **Ok**.

The user group is added to the **User Profile List**.

4 Configure permissions for the user group. The permissions are applied to all of the members of the user group. For more information, see "Assigning Permissions to User Profiles and User Groups" on page 79.

5 Click the 💾 button to save and apply the changes.

Configuring Extended Features for a User Profile

You can configure extended features for a user profile so that:

- A user profile automatically expires after a configured time period (does not apply to the default admin user profile)
- A user must change the password at the next login (also see "Changing the Password From the Login page" on page 33)
- A user must change the password after a configured time period (also see "Changing the Password From the Login page" on page 33)
- A user profile automatically inserts the current year, month, day, or hour into its password, adding an additional level of system security.

  Important: These extended features are disabled for LDAP users and LDAP user groups.
- A user must plug a USB token/smartcard containing an identification certificate into the client to log on to the Command Recording Software.

  Important: Identification certificates are disabled for LDAP user groups.
- A user cannot log on to the Command Recording Software after the set limit of concurrent user session has been reached.

Notes:

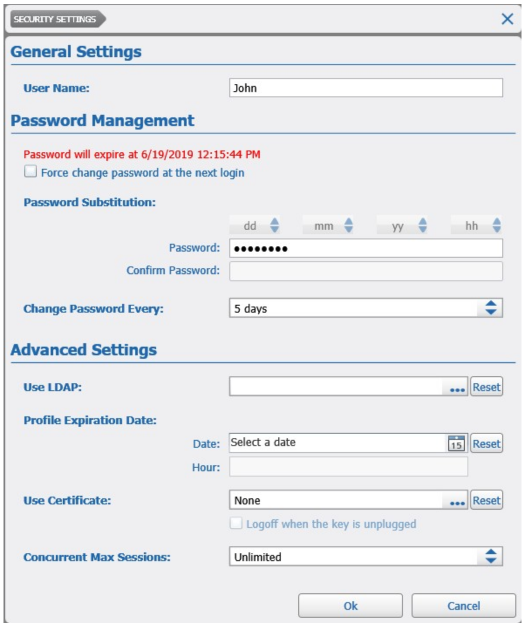
- You can also set a specific password policy on the **System Settings** page. For more information, see "Configuring the Password Policy" on page 123.
- Local user profiles can also change the password from the Command Config (see "Changing the Password From the Login page" on page 33) and Command Client login pages.

To configure the extended user features

1. On the **User Configuration** page, select a user profile in the **User Profile List** panel.
2. Click the ⚙ button

   The **Security Settings** dialog box appears.

   Note: The profile expiration and LDAP features are disabled for the admin profile.



SECURITY SETTINGS

General Settings

User Name: John

Password Management

Password will expire at 6/19/2019 12:15:44 PM

□ Force change password at the next login

Password Substitution:

dd mm yy hh

Password: ••••••••

Confirm Password:

Change Password Every: 5 days

Advanced Settings

Use LDAP: ... Reset

Profile Expiration Date:

Date: Select a date Reset

Hour:

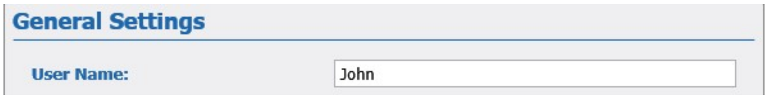
Use Certificate: None ... Reset

□ Logoff when the key is unplugged

Concurrent Max Sessions: Unlimited

Ok Cancel

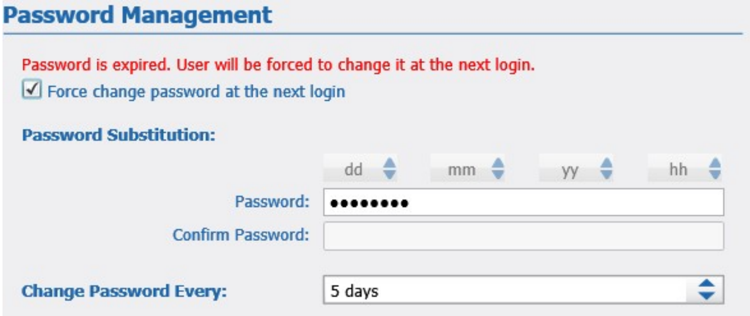
3. In the **General Settings** section, enter a new name in the **User Name** field, if needed.



General Settings

User Name: John

4 In the **Password Management** section, select the **Force change password at the next login** check box to force the user to create a new password the next time he logs on to the server using the Command Config (see “Changing the Password From the Login page” on page 33) or Command Client applications.



Password Management

Password is expired. User will be forced to change it at the next login.

☑ Force change password at the next login

Password Substitution:

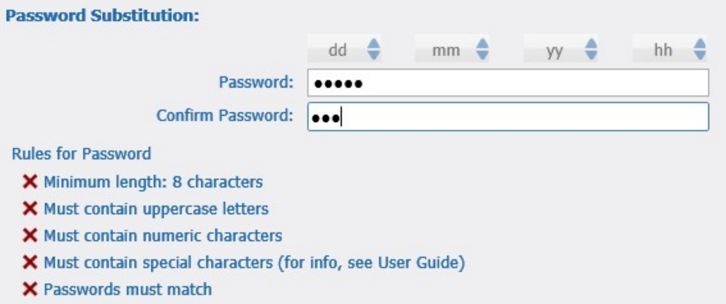
Password: ●●●●●●●●

Confirm Password:

Change Password Every: 5 days

5 To change the password for the user account, enter the new password in the **Password** field, and then enter the new password a second time in the **Confirm Password** field.

Tip: The dialog box warns if the passwords do not match or if the new password does not respect the password policy configured in the **System** page.



Password Substitution:

Password: ●●●●●

Confirm Password: ●●●

Rules for Password

✗ Minimum length: 8 characters

✗ Must contain uppercase letters

✗ Must contain numeric characters

✗ Must contain special characters (for info, see User Guide)

✗ Passwords must match

6 If you want to configure an automatic password change according to a custom parameter (year, month, day, or hour), use the buttons in the **Password Substitution** section:

a In the **Password** field, click where you want to insert the parameter.

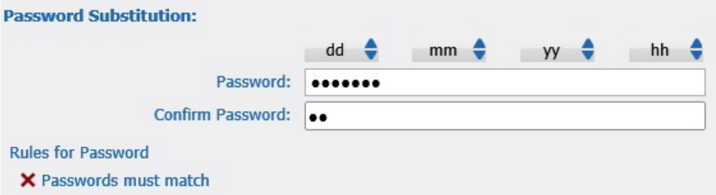
b Click the arrows in the parameters (**y = year**; **m = month**; **d = day**; **h = hour**) button to select the number of values that will be added to the password.

For example: If you select *yy* in the button corresponding to the *year* parameter, Command automatically adds the last two digits of the current year in the password.

The following table provides an explanation of the parameter buttons in the password. The last two columns provide an example of how a custom password (in this case the password is *March* and the key parameter is inserted after the “r”) changes on November 5, 2013 at 9.00 A.M. and on June 15, 2015 at 6.00 P.M. You can also combine two or more substitutions together.

Button	Action	Ex.1 (11/5/ 2013; 9 A.M.)	Ex.2 (6/15/ 2015; 6 P.M.)
yy (year)	The program automatically adds the last digits of the current year at the insertion point.	Mar13ch	Mar15ch
mm (month)	The program automatically adds the current month number at the insertion point.	Mar11ch	Mar06ch
dd (day)	The program automatically adds the current day number at the insertion point.	Mar05ch	Mar15ch
hh (hour)	The program automatically adds the current hour (24-hour mode) number at the insertion point.	Mar09ch	Mar18ch

c Enter the password with the added parameters in the **Confirm Password** field.

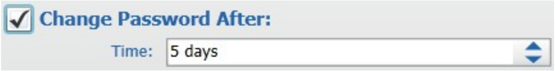


Password: •••••••

Confirm Password: ••

✗ Passwords must match

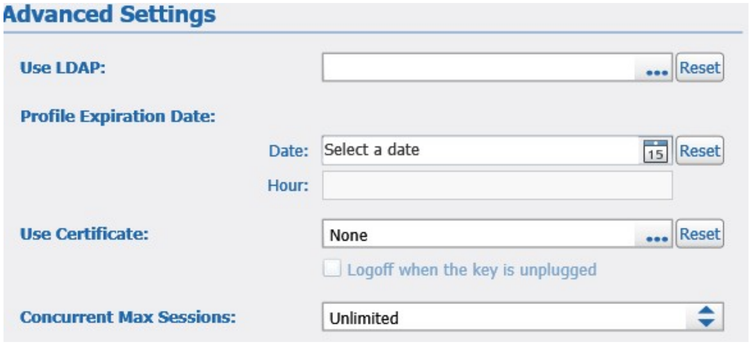
7 If you want to force the user to create a new password after the password expiration **Time**, click the **Change Password After** arrows to select the expiration time. After the time is expired the user is forced to create a new password the next time he logs on to the server using the Command Config (see “Changing the Password From the Login page” on page 33) or Command Client applications.



☑ Change Password After:

Time: 5 days

8 In the **Advanced Settings** section, if you want to activate the profile for a limited amount of time, select the specify the profile expiration **Date** and **Hour** in the **Profile Expiration Date** section.



Advanced Settings

Use LDAP: ••• Reset

Profile Expiration Date:

Date: Select a date 15 Reset

Hour:

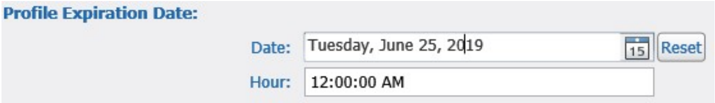
Use Certificate: None ••• Reset

□ Logoff when the key is unplugged

Concurrent Max Sessions: Unlimited

Notes:

- An expired profile is deactivated, but not deleted. The profile can be activated again by clearing the **Profile Expiration Date** check box.



Profile Expiration Date:

Date: Tuesday, June 25, 2019 15 Reset

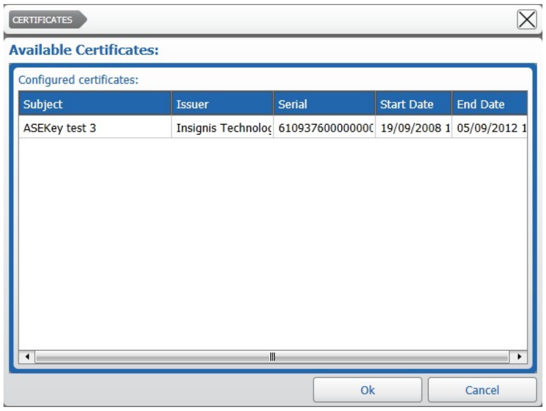
Hour: 12:00:00 AM

- To disable the feature click the **Reset** button.

9 If you want to enforce the presence of an identification certificate for logging on to the Command Recording Software and configuring the recording device, do the following:

a Click the ••• button to select the certificate.

The **Certificates** dialog box appears.



Available Certificates:

Configured certificates:

Subject	Issuer	Serial	Start Date	End Date
ASEKey test 3	Insignis Technolog	61093760000000(	19/09/2008 1	05/09/2012 1

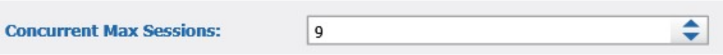
b Select a certificate and click **Ok**.

Note: You must install a valid identification certificate on the Command Recording Software to apply this option. For more information, see “Configuring Identification Certificates” on page 104.

c (Optional) Select the **Logoff when the key is unplugged** check box to automatically disconnect the user from the Command Recording Software when the USB token or smartcard reader containing the certificate is not plugged into the client.

Note: To disable the feature click the **Reset** button.

10 If you want to set a limit of concurrent sessions for the user profile, select enter the maximum number of allowed concurrent sessions in the **Concurrent Max Sessions** field.



Concurrent Max Sessions: 9

Notes:

- Every connection to the Command Recording Software using the Command Config, Command Client, and SiteManager represents a different concurrent user session.
- To disable the feature click the **Reset** button.

11 Click **Ok** to save and apply the changes, and close the dialog box.

12 Click the 💾 button to save and apply the changes.

Assigning Permissions to User Profiles and User Groups

You can assign permissions to a local or LDAP user profile, or an LDAP user group to restrict what that user (or the members of the user group) is allowed to configure. You can set permissions based on day and time intervals, or permissions that are valid only after specific events.

Important Notes:

- When the Command Recording Software is registered on a Command Enterprise Server and the same user is configured on both Command Enterprise and also locally on Command Recording Software devices, the user may choose to access the devices directly via Command Recording Software or collectively via Command Enterprise. When connecting directly to devices, only the locally defined Command Recording Software user rights will be applied for a particular user. When connecting via Command Enterprise, Enterprise user rights are applied first, followed by locally defined Command Recording Software user rights on a specific device. This allows device local Command Recording Software user rights to further refine rights of an Enterprise user on a particular device. If the Enterprise user is not defined locally on a particular device, there will be no further refinement available and only Enterprise rights will be applied.
- If an LDAP user is also member of an LDAP user group added to the Command Recording Software, the user has all of the permissions configured for the user profiles and the user group.

This section covers the following tasks:

- “Setting Day and Time Intervals for Permissions” on page 80
- “Setting Specific Conditions for Permissions” on page 80
- “Assigning Permissions Over Command Recording Software Features” on page 81
- “Assigning System Permissions” on page 85
- “Creating and Managing Group of Cameras” on page 88
- “Assigning Permissions Over Specific Cameras” on page 91
- “Setting Language and Entering Personal Details” on page 93

Setting Day and Time Intervals for Permissions

You can set permissions based on day and time intervals.

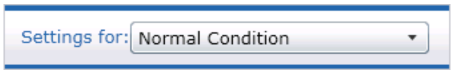
Note: Only the permissions included in sections with the 📅 icon (see “Assigning Permissions Over Command Recording Software Features” on page 81) are dependent from the configured date and time intervals.

To configure day and time intervals for permissions

1 On the **User Configuration** page, select a user profile or a user group in the **User Profile List** panel.

2 Set a schedule for the user profile/group as described in the **Scheduler** section (see “Scheduler” on page 65).

3 The **Settings for** list (below the time line) allows you to set permissions that are valid only after a specific event occurs. In this procedure you are setting permissions based on day and time, so leave this list set to **Normal Condition**. For instructions on setting permissions for specific events, see “Setting Specific Conditions for Permissions” on page 80.



Settings for: Normal Condition

4 Assign the permissions that you want to apply during that day and time interval, as described in:

   - “Assigning Permissions Over Command Recording Software Features” on page 81
   - “Assigning System Permissions” on page 85
   - “Assigning Permissions Over Specific Cameras” on page 91

5 Click the 💾 button to save and apply the changes.

Setting Specific Conditions for Permissions

You can set permissions that are activated only after specific conditions are met, such as when the status of an alarm changes. This is useful to set permissions that are activated only for a short time, granting a user profile or a user group more powers to respond to events such as alarms.

WARNING: The permissions specified for specific conditions override all the other permissions.

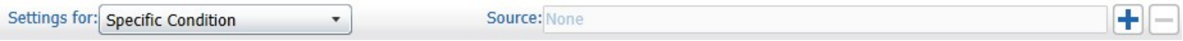
To set specific conditions for permissions

1 On the **User Configuration** page, select a user profile or a user group in the **User Profile List** panel.

2 Set a schedule for the user profile as described in the **Scheduler** section (see “Scheduler” on page 65).

3 Select **Specific Condition** from the **Settings for** list (under the time line).

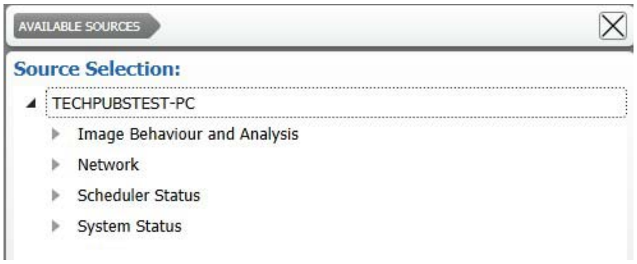
The **Source** field appears beside the **Settings for** list.



Settings for: Specific Condition ▾ Source: None + −

4 Click the + button to select a specific event as the source.

The **Available Sources** dialog box appears.



AVAILABLE SOURCES

Source Selection:

- TECHPUBSTEST-PC
  - Image Behaviour and Analysis
  - Network
  - Scheduler Status
  - System Status

5 Select a condition from the **Source Selection** list and click **Ok**.

6 Assign the permissions that you want to apply when that specific condition occurs.

7 For more information see:

- “Assigning Permissions Over Command Recording Software Features” on page 81
- “Assigning System Permissions” on page 85
- “Assigning Permissions Over Specific Cameras” on page 91

8 Click the 💾 button to save and apply the changes.

Assigning Permissions Over Command Recording Software Features

After you have set the day and time interval (see “Setting Day and Time Intervals for Permissions” on page 80) or the specific conditions for when you want the permissions to apply (see “Setting Specific Conditions for Permissions” on page 80), you can set the connection priority, and advanced permissions for that day and time interval or specific condition. Setting the connection priority is useful to limit the bandwidth usage according to the user’s role in the organization.

Notes:

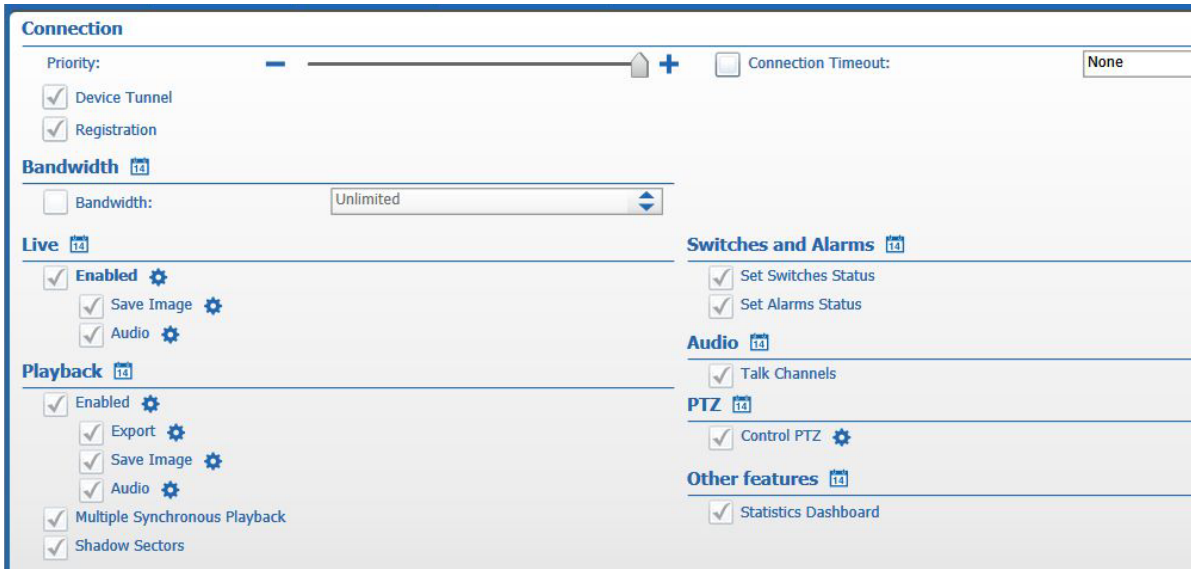
- The above settings are applied to the Command Config and Command Client interfaces, and to the SiteManager application.
- The 📅 icon near a section indicates that the permissions in the section are dependent from the configured date and time intervals (see “Setting Day and Time Intervals for Permissions” on page 80).

To assign permissions over Command Recording Software features

1 On the **User Configuration** page, select a user profile or a user group in the **User Profile List** panel.

2 Either click a tab that defines the day and time interval you want to set permissions for, or ensure that **Specific Condition** is displayed in the **Settings for** list, below the timeline.

3 Click the **Main** tab.



Connection

Priority: − +

□ Connection Timeout: None

☑ Device Tunnel

☑ Registration

Bandwidth

□ Bandwidth: Unlimited

Live

☑ Enabled

☑ Save Image

☑ Audio

Playback

☑ Enabled

☑ Export

☑ Save Image

☑ Audio

☑ Multiple Synchronous Playback

☑ Shadow Sectors

Switches and Alarms

☑ Set Switches Status

☑ Set Alarms Status

Audio

☑ Talk Channels

PTZ

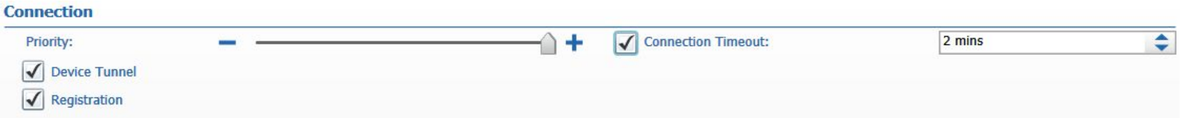
☑ Control PTZ

Other features

☑ Statistics Dashboard

Note: After you have selected the time interval from the timeline, that interval is displayed over the scheduler, so that you can check the time interval you are setting permissions for.

4 In the **Connection** section, select the connection **Priority** for the profile by moving the slider. This value must be set according to the network bandwidth capacity and the profile importance and permissions.



Connection

Priority: − +

☑ Connection Timeout: 2 mins

☑ Device Tunnel

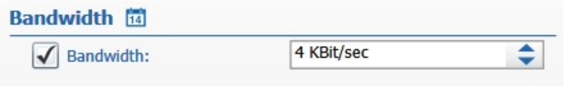
☑ Registration

5 Select the **Connection Timeout** check box if you want the user profile/group to disconnect from the server after the specified number of minutes.

6 Select the **Device Tunnel** check box if you want the user profile/group to access the cameras setup page using Command Config (see “Configuring the Security Settings” on page 26).

7 Select the **Registration** check box if you want the user profile/group to be able to register the Command Recording Software to a Command Enterprise Server from Command Config (see “Managing the Registration to Command Enterprise” on page 119).

8 In the **Bandwidth** section, select the **Bandwidth** check box to set the maximum bandwidth allowed for the profile/group while using the SiteManager application to connect to the Command Recording Software.

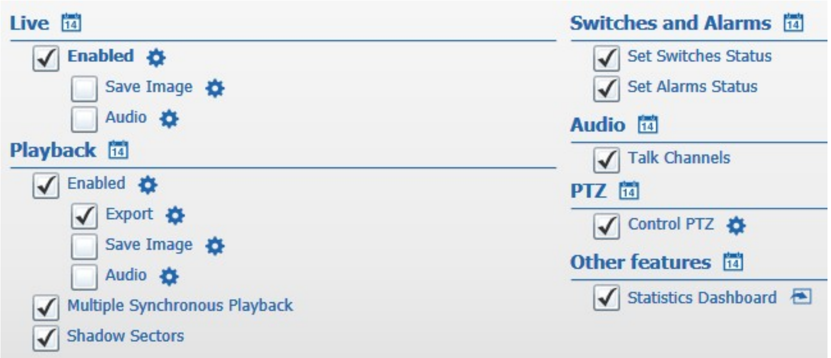


Bandwidth

☑ Bandwidth: 4 KBit/sec

9 To assign permissions over the main Command Recording Software features, do one of the following:

- Select the **Select all** check box to allow the user profile/group to access all of the resources added to the recording device.
- Select or clear the single check boxes to assign individual permissions. The specific permissions are described in the following table.



Live

☑ Enabled ⚙

□ Save Image ⚙

□ Audio ⚙

Playback

☑ Enabled ⚙

☑ Export ⚙

□ Save Image ⚙

□ Audio ⚙

☑ Multiple Synchronous Playback

☑ Shadow Sectors

Switches and Alarms

☑ Set Switches Status

☑ Set Alarms Status

Audio

☑ Talk Channels

PTZ

☑ Control PTZ ⚙

Other features

☑ Statistics Dashboard

Permission	Parameters	Action
Live	Enabled	Select the **Enabled** check box to allow the user profile/ group to view live video streams. **Note:** This action automatically selects all cameras in the **Advanced** tab. Click the ⚙ button or the **Advanced** tab to assign permissions based on specific cameras.
	Save Image	Select the **Save Image** check box to allow the user profile/group to export still images of live video streams using the SiteManager application. **Note:** This action automatically selects all cameras in the **Advanced** tab. Click the ⚙ button or the **Advanced** tab to assign permissions based on specific cameras.
	Audio	Select the **Audio** check box to allow the user profile/ group to listen to audio channels associated to live streams. **Note:** This action automatically selects all cameras in the **Advanced** tab. Click the ⚙ button or the **Advanced** tab to assign permissions based on specific cameras.

Permission	Parameters	Action
Switches and Alarms	Set Switches Status	Select the **Set Switches Status** check box to allow the user profile/group to manage auxiliary channels.
	Set Alarms Status	Select the **Set Alarms Status** check box to allow the user profile/group to manage alarms.
Playback	Enabled	Select the **Enabled** check box to allow the user profile/group to review recorded video evidence. **Note:** This action automatically selects all cameras in the **Advanced** tab. Click the ⚙ button or the **Advanced** tab to assign permissions based on specific cameras.
	Export	Select the **Export** check box to allow the user profile/group to export recorded video evidence. **Note:** This action automatically selects all cameras in the **Advanced** tab. Click the ⚙ button or the **Advanced** tab to assign permissions based on specific cameras.
	Save Image	Select the **Save Image** check box to allow the user profile/group to export still images of recorded video evidence using the SiteManager application. **Note:** This action automatically selects all cameras in the **Advanced** tab. Click the ⚙ button or the **Advanced** tab to assign permissions based on specific cameras.
	Audio	Select the **Audio** check box to allow the user profile/group to listen to audio channels associated to recorded video evidence. **Note:** This action automatically selects all cameras in the **Advanced** tab. Click the ⚙ button or the **Advanced** tab to assign permissions based on specific cameras.
	Multiple Synchronous Playback	Select the **Multiple Synchronous Playback** check box to allow the user profile/group to synchronize video playback using the multiple playback feature.
	Shadow Sectors	Select the **Shadow Sectors** check box to allow the user profile/group to manage the local storage of the cameras.
Audio	Talk Channels	Select the **Talk Channels** check box to allow the user profile/group to manage output (*talk*) audio channels.
PTZ	Control PTZ	Select the **Control PTZ** check box to allow the user profile/group to control PTZ cameras. **Note:** This action automatically selects all PTZ cameras in the **Advanced** tab. Click the ⚙ button or the **Advanced** tab to assign permissions based on specific PTZ cameras.

Permission	Parameters	Action
Other Features	Statistics Dashboard	Select the **Statistics Dashboard** check box to allow the user profile/group to access the **Statistics Dashboard** page (see “Accessing the Statistics Dashboard Page” on page 128). **Note:** You can directly launch the web browser and access the **Statistics Dashboard** by clicking the icon near the permission.

10 Click the button to save and apply the changes.

Assigning System Permissions

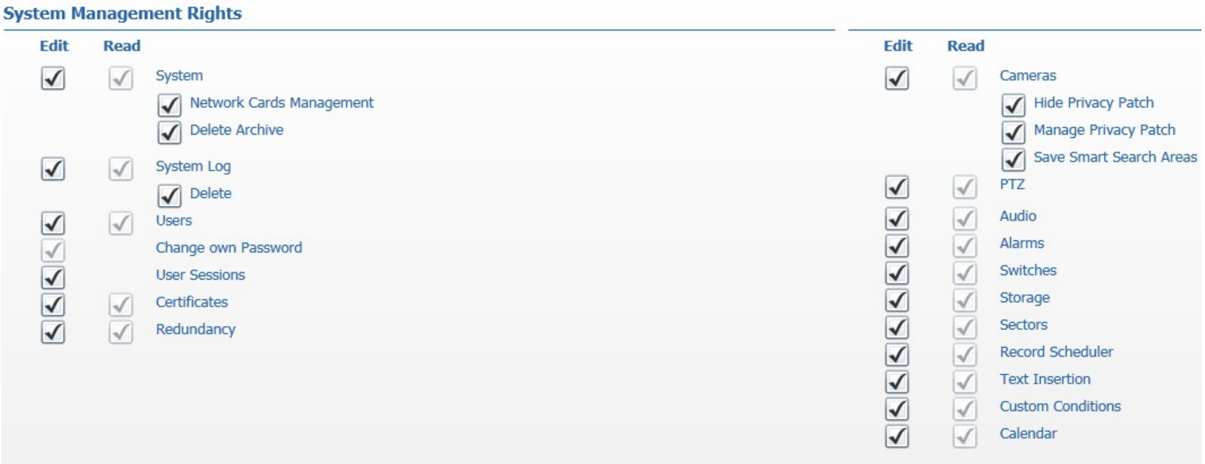
You can assign individual permissions on the user profiles or user groups using the **System** tab, so that users can only access designated pages in the Command Config interface and configure designated options.

To assign system permissions

1 On the **User Configuration** page, select a user profile or a user group in the **User Profile List** panel.

2 Either click a tab that defines the day and time interval you want to set permissions for, or ensure that **Specific Condition** is displayed in the **Settings for** list, below the timeline.

3 Click the **System** tab.



System Management Rights

Edit	Read	
☑	☑	System
		☑ Network Cards Management
		☑ Delete Archive
☑	☑	System Log
		☑ Delete
☑	☑	Users
☑		Change own Password
☑		User Sessions
☑	☑	Certificates
☑	☑	Redundancy

Edit	Read	
☑	☑	Cameras
		☑ Hide Privacy Patch
		☑ Manage Privacy Patch
		☑ Save Smart Search Areas
☑	☑	PTZ
☑	☑	Audio
☑	☑	Alarms
☑	☑	Switches
☑	☑	Storage
☑	☑	Sectors
☑	☑	Record Scheduler
☑	☑	Text Insertion
☑	☑	Custom Conditions
☑	☑	Calendar

4 Do one of the following:

- Select the **Select all** check box to allow the user profile/group to access all of the pages and configure all of the options.

- Select or clear the **Edit/Read** check boxes to assign the **System Management Rights** permissions, as described in the following table.

Permission	Action
System	Select the **System** check boxes to allow the user profile/group to view/edit the **System Configuration** options.
System - Network Cards Management	Select the **Network Cards Management** check box to allow the user profile/group to manage the recording device network options. For more information, see “Configuring System and Network Settings” on page 112.
System - Delete Archive	Select the **Delete Archive** check box to allow the user profile/group to delete recorded video evidence.
System Log	Select the **System Log** check boxes to allow the user profile/group to view/edit the **System Log Configuration** options.
System Log - Read System Log	Select the **Read System Log** check box to allow the user profile/group to read the log.
System Log - Delete	Select the **Delete** check box to allow the user profile/group to delete the log.
Users	Select the **Users** check boxes to allow the user profile/group to view/edit the **User Configuration** options.
Change Own Password	Select the **Change Own Password** check box to allow the user profile/group to change the password for his profile.
User Sessions	Select the **User Sessions** check box to allow the user profile/group to view and manage incoming connections to the recording device.
Certificates	Select the **Certificates** check boxes to allow the user profile/group to view/edit the **Certificate Configuration** options.
Redundancy	Select the **Redundancy** check boxes to allow the user profile/group to view/edit the **Redundancy Configuration** options.
Cameras	Select the **Cameras** check boxes to allow the user profile/group to view/edit the **Camera Configuration** options.
Cameras - Hide Privacy Patch	Select the **Hide Privacy Patch** check box to allow the user profile/group to show and hide configured privacy zones on cameras.
Cameras - Manage Privacy Patch	Select the **Manage Privacy Patch** check box to allow the user profile/group to create and edit privacy zones on cameras.
Cameras - Save Smart Search Area	Select the **Save Smart Search Area** check box to allow the user profile/group to save and edit motion areas for the Smart Search feature.

Permission	Action
PTZ	Select the **PTZ** check boxes to allow the user profile/group to view/edit PTZ cameras options.
Audio	Select the **Audio** check boxes to allow the user profile/group to view/edit the **Audio Configuration** options.
Alarms	Select the **Alarms** check boxes to allow the user profile/group to view/edit the **Alarm Configuration** options.
Switches	Select the **Switches** check boxes to allow the user profile/group to view/edit the **Switches Configuration** options.
Storage	Select the **Storage** check boxes to allow the user profile/group to view/edit the **Storage Configuration** options.
Sectors	Select the **Sectors** check boxes to allow the user profile/group to create and manage recording sectors.
Record Scheduler	Select the **Recording Scheduler** check boxes to allow the user profile/group to view/edit the cameras recording scheduler.
Text Insertion	Select the **Text Insertion** check boxes to allow the user profile/group to view/edit the **Text Insertion Configuration** options.
Custom Conditions	Select the **Custom Conditions** check boxes to allow the user profile/group to view/edit the **Custom Condition Configuration** options.
Calendar	Select the **Calendar** check boxes to allow the user profile/group to view/set planned holidays.

5 Click the 💾 button to save and apply the changes.

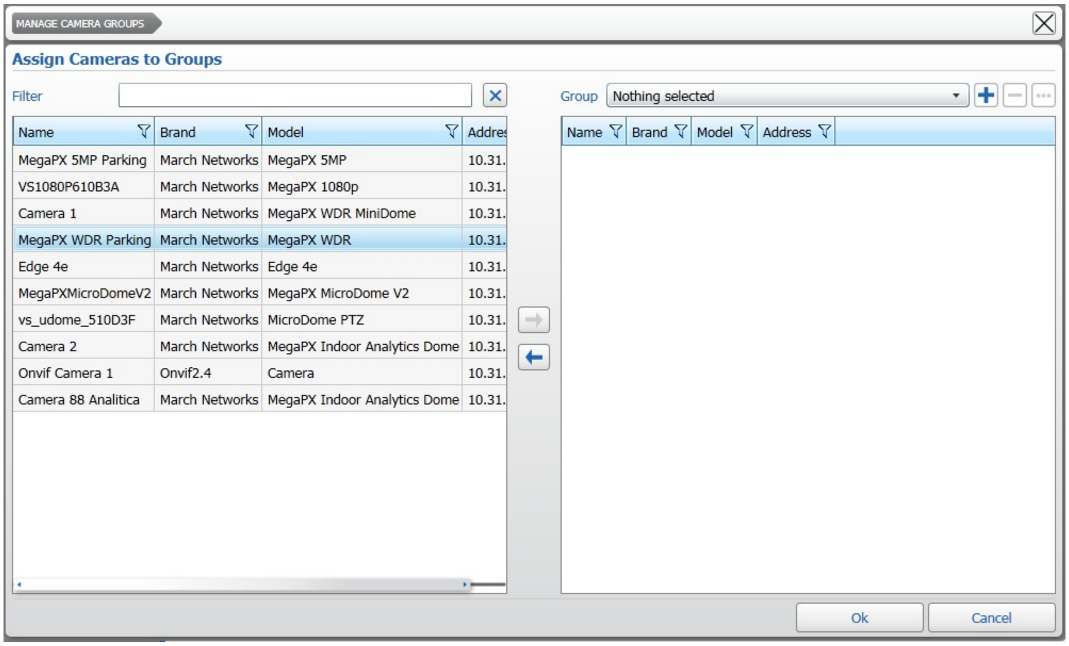
Creating and Managing Group of Cameras

The **User Configuration** page allows you to create group of cameras. The groups of cameras appear in the **Advanced** tab and you can assign permission over every camera included to the group.

To create group of cameras

1 On the **User Configuration** page, click the ✎ button to create and manage group of cameras.

The **Manage Camera Groups** dialog box appears.



MANAGE CAMERA GROUPS

Assign Cameras to Groups

Filter:

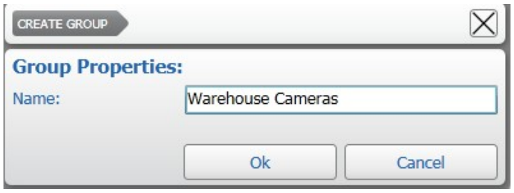
Group: Nothing selected

Name	Brand	Model	Addres
MegaPX 5MP Parking	March Networks	MegaPX 5MP	10.31.
VS1080P610B3A	March Networks	MegaPX 1080p	10.31.
Camera 1	March Networks	MegaPX WDR MiniDome	10.31.
MegaPX WDR Parking	March Networks	MegaPX WDR	10.31.
Edge 4e	March Networks	Edge 4e	10.31.
MegaPXMicroDomeV2	March Networks	MegaPX MicroDome V2	10.31.
vs_udome_510D3F	March Networks	MicroDome PTZ	10.31.
Camera 2	March Networks	MegaPX Indoor Analytics Dome	10.31.
Onvif Camera 1	Onvif2.4	Camera	10.31.
Camera 88 Analitica	March Networks	MegaPX Indoor Analytics Dome	10.31.

Name	Brand	Model	Address

2 Click the ✚ button to create a new group.

The **Create Group** dialog box appears.



CREATE GROUP

Group Properties:

Name: Warehouse Cameras

3 Enter a descriptive **Name** for the group and click **Ok**.

The group of cameras is added to the **Group** list.

4 Click on a column header to automatically sort the elements in the column list in ascending or descending alphabetical or numerical order.

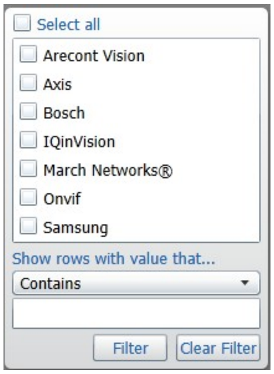
Note: Click on the column header again to change the order from ascending to descending or from descending to ascending.

5 If the list of cameras is large, you can also apply any of the following filters:

- **Camera Brand or Model Filter**:

a Click the **Filter** icon in the **Brand** or **Model** columns.

A menu appears.



b Select the check boxes corresponding to the camera brand or model you want to locate.

c Alternatively, you can configure a text filter by selecting the filter type from the list, and then entering the key word.

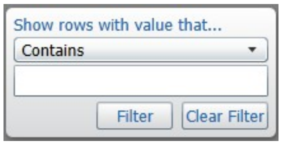
d Click **Filter** to apply the filter to the list.

Tip: To remove the filter, click the **Filter** icon in the **Brand** column, and then click **Clear Filter**.

- **Name or Address Filter:**

a Click the **Filter** icon in the **Name** or **Address** column.

A menu appears.



b To configure a text filter, select the filter type from the list, and then enter the key word.

c Click **Filter** to apply the filter to the list.

Tip: To remove the filter, click the **Filter** icon in the selected column, and then click **Clear Filter**.

- **Key Word Filter:**

  - Enter the key word in the **Filter** field.

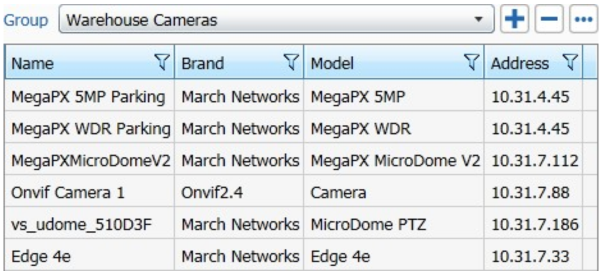
  As you write the key word, the scan results are filtered.

Tip: To remove the filter, click the ✕ button.

6 Select multiple cameras in the by keeping the **CTRL** key pressed and clicking additional cameras.

7 Click the ➡ button to add the cameras to the group.

The selected cameras appear in the camera list panel.



Group: Warehouse Cameras

Name	Brand	Model	Address
MegaPX 5MP Parking	March Networks	MegaPX 5MP	10.31.4.45
MegaPX WDR Parking	March Networks	MegaPX WDR	10.31.4.45
MegaPXMicroDomeV2	March Networks	MegaPX MicroDome V2	10.31.7.112
Onvif Camera 1	Onvif2.4	Camera	10.31.7.88
vs_udome_510D3F	March Networks	MicroDome PTZ	10.31.7.186
Edge 4e	March Networks	Edge 4e	10.31.7.33

8 Click **Ok** to close the dialog box.

9 Click the 💾 button to save and apply the changes.

To rename a group of cameras

1 On the **User Configuration** page, click the ✎ button to create and manage group of cameras.

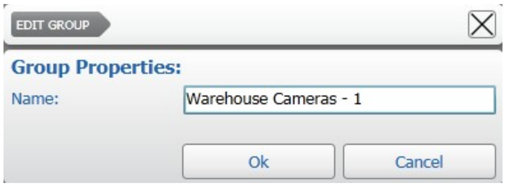
The **Manage Camera Groups** dialog box appears.

2 Select a group of cameras from the **Group** list.

3 Click the ••• button.

The **Edit Group** dialog box appears.

4 Enter a new **Name** for the group and click **Ok**.



Group Properties:

Name: Warehouse Cameras - 1

5 Click **Ok** close the dialog box.

6 Click the 💾 button to save and apply the changes.

To manage a group of cameras

1 On the **User Configuration** page, click the ✎ button to create and manage group of cameras.

The **Manage Camera Groups** dialog box appears.

2 Select a group of cameras from the **Group** list.

3 Add cameras to the group by selecting the cameras in the list and clicking the ➡ button.

4 Remove cameras from the group by selecting the cameras under the group and clicking the ⬅ button.

5 Click **Ok** close the dialog box.

6 Click the 💾 button to save and apply the changes.

To delete a group of cameras

1 On the **User Configuration** page, click the 📝 button to create and manage group of cameras.

The **Manage Camera Groups** dialog box appears.

2 Select a group of cameras from the **Group** list.

3 Click the − button.

The group is deleted.

4 Click **Ok** close the dialog box.

5 Click the 💾 button to save and apply the changes.

Assigning Permissions Over Specific Cameras

You can assign permissions over specific cameras or group of cameras using the **Advanced** tab, so that users can only access designated live or recorded videos form the selected cameras.

Note: Before assigning permissions over cameras, it is recommended that you create one or more group of cameras, as described in the previous section.

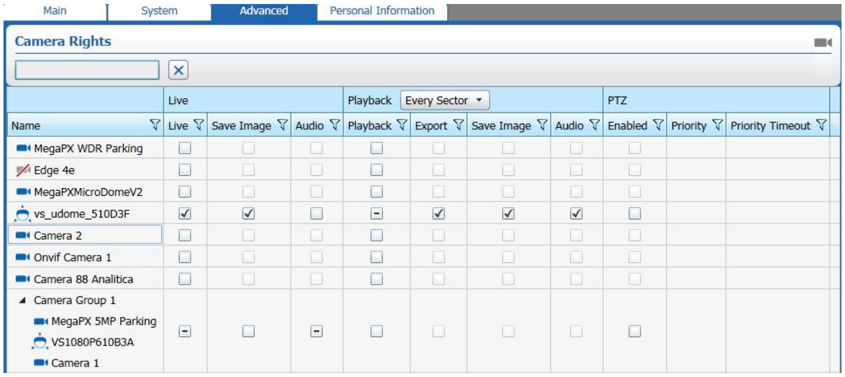
To set permissions over specific cameras

1 On the **User Configuration** page, select a user profile or a user group in the **User Profile List** panel.

2 Either click a tab that defines the day and time interval you want to set permissions for, or ensure that **Specific Condition** is displayed in the **Settings for** list, below the timeline.

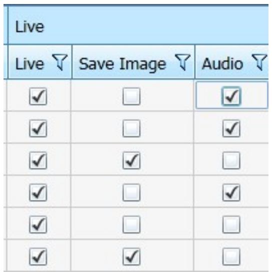
3 Click the **Advanced** tab.

Tip: Alternatively, you can access the tab by clicking the ⚙ button near a permission in the **Main** tab.



	Live			Playback Every Sector				PTZ		
Name	Live	Save Image	Audio	Playback	Export	Save Image	Audio	Enabled	Priority	Priority Timeout
MegaPX WDR Parking	□	□	□	□	□	□	□	□		
Edge 4e	□	□	□	□	□	□	□	□		
MegaPXMicroDomeV2	□	□	□	□	□	□	□	□		
vs_udome_510D3F	☑	☑	□	⊟	☑	☑	☑	□		
Camera 2	□	□	□	□	□	□	□	□		
Onvif Camera 1	□	□	□	□	□	□	□	□		
Camera 88 Analitica	□	□	□	□	□	□	□	□		
Camera Group 1 MegaPX 5MP Parking VS1080P610B3A Camera 1	⊟	□	⊟	□	□	□	□	□		

4 On the **Live** column, select the check boxes corresponding to the cameras or group of cameras to assign permissions associated with viewing live video streamed by those cameras. The **Save Image** and **Audio** check boxes are now available.



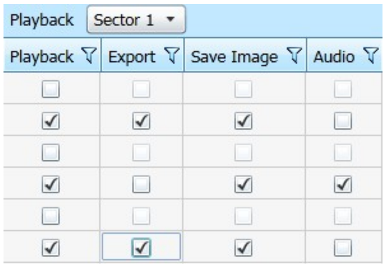
Live

Live	Save Image	Audio
☑	☐	☑
☑	☐	☑
☑	☑	☐
☑	☐	☑
☑	☐	☐
☑	☑	☐

5 Assign the camera permissions in the **Live** section.

Permission	Action
Live - Save Image	Select the **Save Image** check box to allow the user profile/ group to export still images of the camera’s live video stream using the SiteManager application.
Live - Audio	Select the **Audio** check box to allow the user profile/group to manage input audio channels associated to the camera.

6 In the **Playback** section, select a recording sector from the **Sectors** list to assign permissions over the video evidence recorded in that sector.



Playback Sector 1

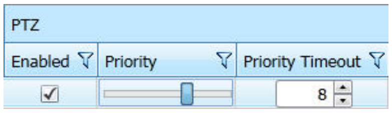
Playback	Export	Save Image	Audio
☐	☐	☐	☐
☑	☑	☑	☐
☐	☐	☐	☐
☑	☐	☑	☑
☐	☐	☐	☐
☑	☑	☑	☐

7 On the **Playback** column, select the check boxes corresponding to the cameras or group of cameras to assign permissions associated with the video evidence recorded from those cameras. The **Save Image**, **Export** and **Audio** check boxes are now available.

8 Assign the camera permissions in the **Playback** section.

Permission	Action
Playback - Save Image	Select the **Save Image** check box to allow the user to export still images of recorded video evidence using the SiteManager application.
Playback - Export	Select the **Export** check box to allow the user to export recorded video evidence.
Playback - Audio	Select the **Audio** check box to allow the user to listen to audio channels associated to recorded video evidence.

9. In the **PTZ Section** and on the **Enabled** column, select the check boxes corresponding to the PTZ cameras (or every PTZ camera added to a group of cameras) to allow the user to control their movement. The **Priority** slider and the **Priority Timeout** box are now available.



PTZ

Enabled	Priority	Priority Timeout
☑		8

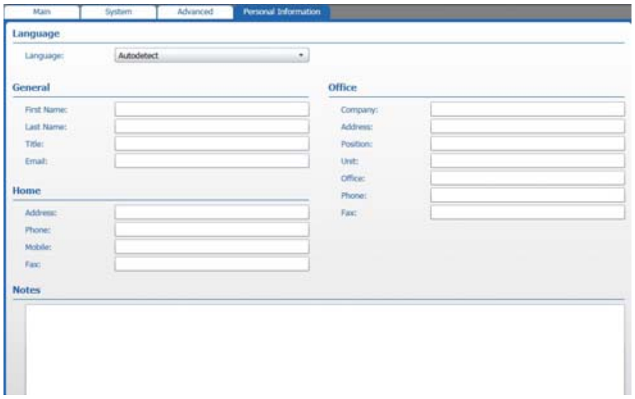
10. Select the connection **Priority** for the camera by moving the slider. You can also configure a **Priority Timeout** for the camera: after the time specified has passed, the camera loses its priority settings.
11. Click the 🖫 button to save and apply the changes.

Setting Language and Entering Personal Details

You can change the interface language and optionally enter the user's or the user group's details using the **Personal Information** tab.

To set the language and enter personal details

1. On the **User Configuration** page, select a user profile or a user group in the **User Profile List** panel.
2. Click the **Personal Information** tab.



Language: Autodetect

3. Select the interface **Language** from the list.

   Note: By selecting **Autodetect**, the Command Config interface automatically applies the language based on the OS configurations.
4. In the **General**, **Office**, **Home**, and **Notes** sections, edit the user's details as needed.

   Note: The user details are optional and do not affect the user's permission levels.
5. Click the 🖫 button to save and apply the changes.

Creating User Profiles Using Templates

After creating a local user profile, or adding a user profile/group from the LDAP service, you can use it as a template to create additional profiles or add profiles/group from the LDAP service. The new profile/group has the same settings and permissions as the profile/group used as a template. You can then customize the new user profile/group as much as you want.

Note: You can also use the *admin* profile as a template: by doing so you can create two or more user profiles with full administration powers (including creating and configuring user profiles) over the Command Recording Software configurations.

Select your configuration:

- "To create a user profile using a local user as a template" on page 94
- "To add a user profile using an LDAP user profile or an LDAP user group as a template" on page 94

To create a user profile using a local user as a template

1 On the **User Configuration** page, select a local user profile in the **User Profile List** panel.

2 Click the 👤 button to create a new local user profile that features the same settings and permissions as the profile used as a template.

The **New User** dialog box appears.

3 Enter the **User Name** for the profile

4 Enter the **Password** for the profile and enter it again it in the **Confirm password** field.

Note: The number of asterisks does not represent the actual number of characters.

5 Click **Ok** to confirm the profile creation. The new profile appears in the **User Profile List**. The user profile features the same settings and permissions as the profile used as a template.

6 Customize the profile by assigning new permissions. For more information, see"Assigning Permissions to User Profiles and User Groups" on page 79.

7 Click the 💾 button to save and apply the changes.

To add a user profile using an LDAP user profile or an LDAP user group as a template

1 On the **User Configuration** page, select an LDAP user profile or LDAP user group in the **User Profile List** panel.

2 Click the 👤 button to add a new user profile or user group from the LDAP service that features the same settings and permissions as the profile/group used as a template.

The **LDAP Users** dialog box appears.

3 Search for the user profile or user group in the list, as described in "Adding User Profiles from the LDAP Service" on page 72 and "Adding User Groups from the LDAP Service" on page 73.

4 Click **Ok** to add the profile/group to the Command Recording Software. The profile/group appears in the **User Profile List**. and features the same settings and permissions as the profile/group used as a template.

5 Customize the profile/group by assigning new permissions. For more information, see“Assigning Permissions to User Profiles and User Groups” on page 79.

6 Click the button to save and apply the changes.

Duplicating and Resetting the Command Client User Preferences

Command Config allows you to duplicate the Command Client user preferences from a user profile to one or multiple user profiles. It also allows you to reset the Command Client user preferences for a user profile and delete all of the resources from his **Personal** tree. For more information about the Command Client user preferences and how to populate the user’s Personal tree, see the *Command Client User Guide*, available for download from the March Networks Partner Portal and official websites.

Note: This operation has no effect on the user profiles settings and permissions.

In particular Command Config allows you to duplicate:

- The Command Client user preferences (including language)
- The interface layout saved by the user
- The resources added to the user’s Personal tree

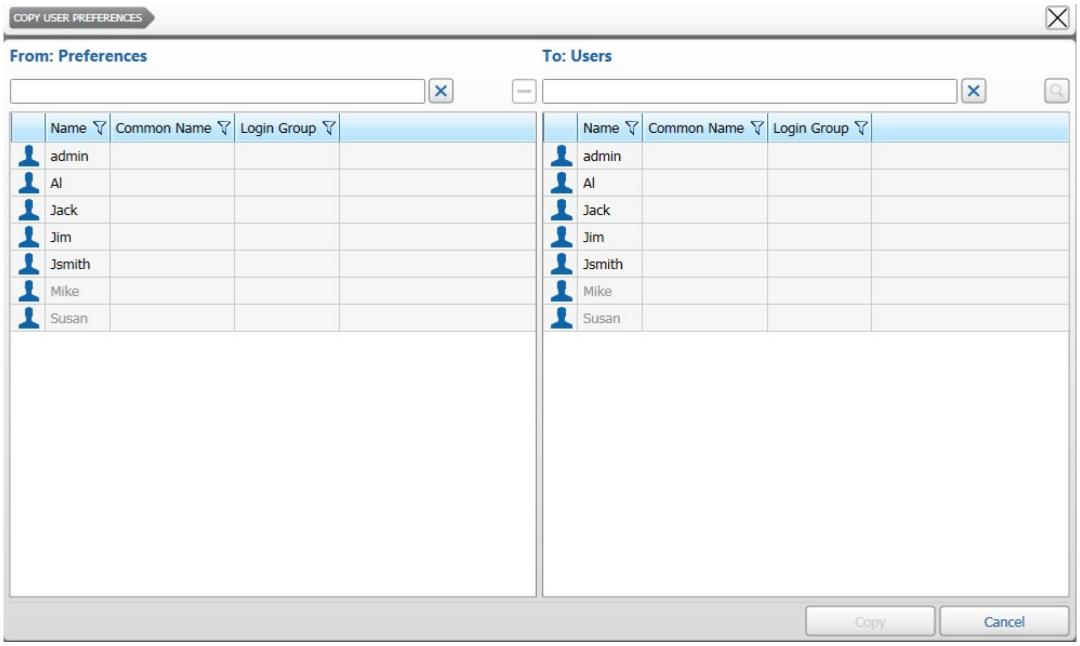
Select your configuration:

- “To duplicate the Command Client user preferences” on page 95
- “To reset the Command Client user preferences” on page 97

To duplicate the Command Client user preferences

1 On the **User Configuration** page click the button in the **User Profiles List** panel.

The **Copy User Preferences** dialog box appears.



From: Preferences

Name	Common Name	Login Group
admin		
Al		
Jack		
Jim		
Jsmith		
Mike		
Susan		

To: Users

Name	Common Name	Login Group
admin		
Al		
Jack		
Jim		
Jsmith		
Mike		
Susan		

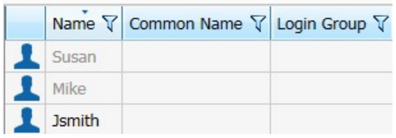
2 In the **From: Preferences** section select the user profile, whose Command Client user preferences you want to duplicate.

Tip: You can filter the user profiles list using the search bar and the filter buttons.

3 In the **To: Users section**, select the recipient user profile for the Command Client user preferences or select multiple user profiles by pressing the **CTRL** key.

Notes:

- User profiles who never logged on to Command Client are grayed.



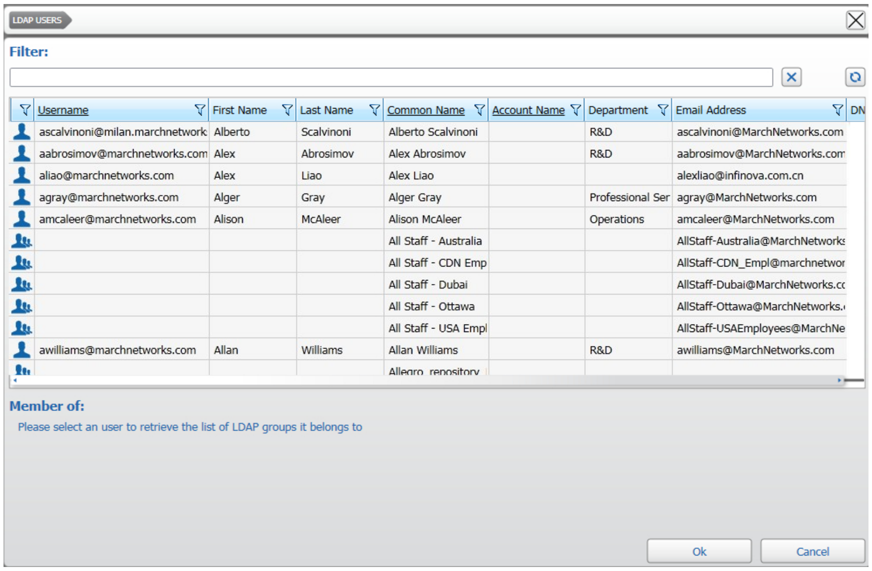
	Name	Common Name	Login Group
👤	Susan		
👤	Mike		
👤	Jsmith		

- You can also add to the list user profiles who are part of an LDAP user group but do not have a Command Recording Software user profile. This is useful if you want to duplicate the Command Client user preferences only to some of the users in the group.

  To add user profiles to the list from an LDAP group:

a Click the 🔍 button in the **To: Users** section.

The **LDAP Users** dialog box appears.



	Username	First Name	Last Name	Common Name	Account Name	Department	Email Address	DN
👤	ascalvinoni@milan.marchnetwork	Alberto	Scalvinoni	Alberto Scalvinoni		R&D	ascalvinoni@MarchNetworks.com	
👤	aabrosimov@marchnetworks.com	Alex	Abrosimov	Alex Abrosimov		R&D	aabrosimov@MarchNetworks.com	
👤	aliao@marchnetworks.com	Alex	Liao	Alex Liao			alexliao@infinova.com.cn	
👤	agray@marchnetworks.com	Alger	Gray	Alger Gray		Professional Ser	agray@MarchNetworks.com	
👤	amcaleer@marchnetworks.com	Alison	McAleer	Alison McAleer		Operations	amcaleer@MarchNetworks.com	
👥				All Staff - Australia			AllStaff-Australia@MarchNetworks	
👥				All Staff - CDN Emp			AllStaff-CDN_Empl@marchnetwor	
👥				All Staff - Dubai			AllStaff-Dubai@MarchNetworks.cc	
👥				All Staff - Ottawa			AllStaff-Ottawa@MarchNetworks.	
👥				All Staff - USA Empl			AllStaff-USAEmployees@MarchNe	
👤	awilliams@marchnetworks.com	Allan	Williams	Allan Williams		R&D	awilliams@MarchNetworks.com	
👥				Allegro_repository				

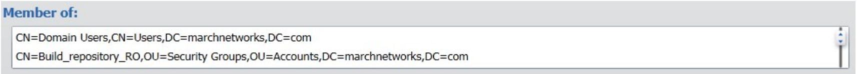
Member of:

Please select an user to retrieve the list of LDAP groups it belongs to

b Filter the LDAP user list using the search bar and the filter buttons.

c Select the user you want to add to the list and click **Ok**.

Note: The text box below the list reports the LDAP user groups the user is member of.



Member of:

CN=Domain Users,CN=Users,DC=marchnetworks,DC=com
CN=Build_repository_RO,OU=Security Groups,OU=Accounts,DC=marchnetworks,DC=com

The user is added to the user profiles in the **To: Users** section.

d Repeat steps a-c to add additional user profiles to the list.

4 Click **Copy**.

A warning dialog box appears.

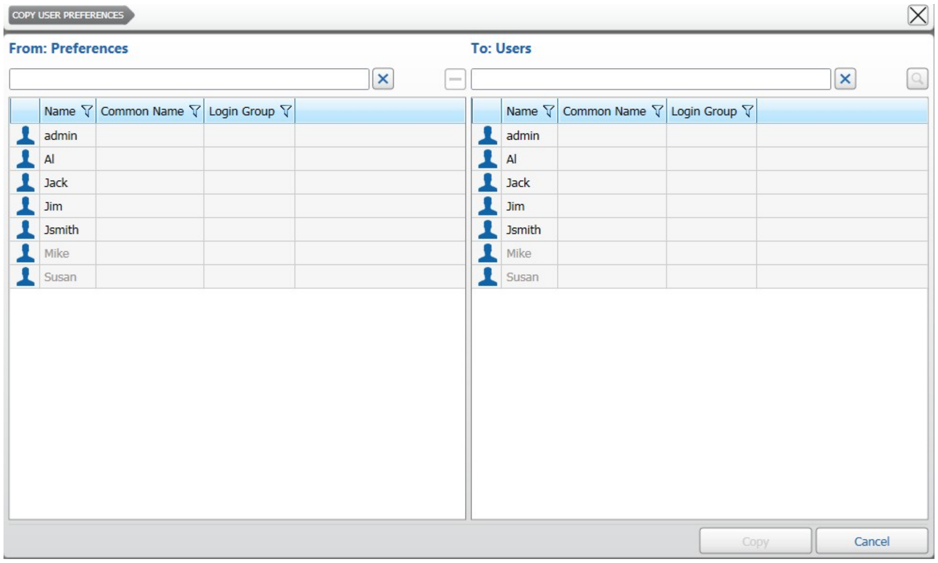
5 Click **Yes**.

The Command Client user preferences are applied to the selected user profiles.

To reset the Command Client user preferences

1 In the **User Configuration** page click the 👤 button in the **User Profiles List** panel.

The **Copy User Preferences** dialog box appears.



From: Preferences

Name	Common Name	Login Group
admin		
Al		
Jack		
Jim		
Jsmith		
Mike		
Susan		

To: Users

Name	Common Name	Login Group
admin		
Al		
Jack		
Jim		
Jsmith		
Mike		
Susan		

2 In the **From: Preferences** section select the user profile, whose Command Client user preferences you want to reset to the default settings, or select multiple user profiles by pressing the **CTRL** key.

3 Click the ▬ button.

A warning dialog box appears.

4 Click **Yes**.

The Command Client user preferences are rest to the default settings and the user profile is grayed in the list.

Locking User Profiles

You can lock user profiles or user groups to avoid any modification to the permissions assigned.

To lock a user profile

1 On the **User Configuration** page, select a user profile or a user group in the **User Profile List** panel.

2 Click the 🔒 button to lock the user profile/group.

The lock symbol appears on the profile icon.

3 Click the 💾 button to save and apply the changes.

Deleting User Profiles

If you no longer need a user profile or a user group, you can delete it from the profile list.

Notes:

- You cannot delete the *admin* user profile.
- When you delete an LDAP user group, all of the members of the group which have not been added to the Command Recording Software as single LDAP user profiles cannot log on to the server anymore.
- When you delete an LDAP user group, the members of the group which are have been added as single LDAP user profiles keep only the permissions configured for the profile.

To delete a user profile or a user group

1 On the **User Configuration** page, select a user profile or a user group in the **User Profile List** panel.

2 Click the ▬ button to delete the profile/group.

A **Warning** dialog box appears.

3 Click **Yes** to confirm the profile/group deletion.

4 Click the 💾 button to save and apply the changes.

Chapter 6

Managing User Sessions and Network Connections

You can check which user profiles are currently connected to a Command Recording Software through the **User Sessions** page. You can also instantly disconnect a user profile, assign temporary permissions, or ban an IP address.

This chapter contains the following sections:

- "Disconnecting User Profiles" on page 100
- "Setting Temporary Permissions" on page 100
- "Banning Connections from Command" on page 101

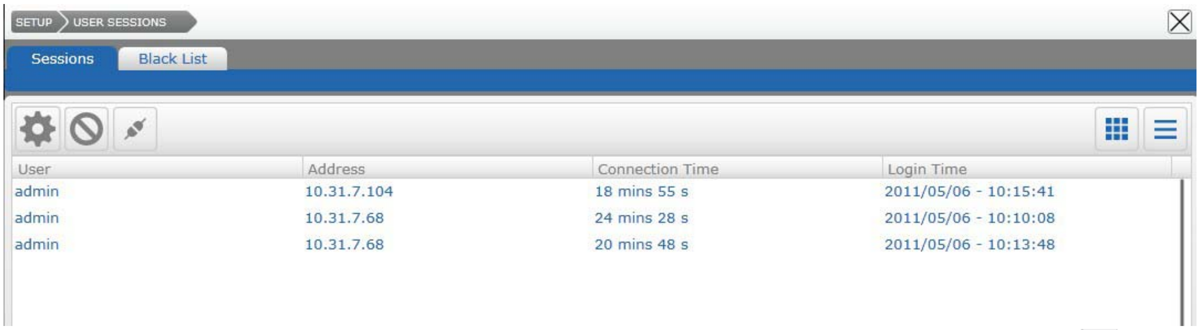
Disconnecting User Profiles

The **User Sessions** page allows you to view the user profiles connected to a Command Recording Software and then force their disconnection from the server.

To disconnect a user profile

1 On the Command Config main page, under **User Management**, click **User Sessions**.

The **User Sessions** page appears, where you can view the user profiles currently connected to a Command Recording Software.



User	Address	Connection Time	Login Time
admin	10.31.7.104	18 mins 55 s	2011/05/06 - 10:15:41
admin	10.31.7.68	24 mins 28 s	2011/05/06 - 10:10:08
admin	10.31.7.68	20 mins 48 s	2011/05/06 - 10:13:48

Tip: You can switch the view mode by clicking the **Thumbnails** ▦ or **Details** ☰ button.

2 Select a user profile.

3 Click the 🔌 button to instantly disconnect the user profile from the server.

Note: The user is not banned and can reconnect to the server afterwards.

Setting Temporary Permissions

On the **User Sessions** page, you can configure a full set of temporary permissions that are only applied to the current session.

Note: For LDAP user profiles that are members of an LDAP user group added to the Command Recording Software, it is not possible to configure a schedule.

To set a temporary permission

1 On the **User Sessions** page, select a connected user profile.

2 Click the ⚙ button to edit the user profile permissions for the current session.

The **Network Sessions Configuration** dialog box appears.

3 Edit the user profile permissions. For more information, see “Assigning Permissions to User Profiles and User Groups” on page 79.

The new permissions are applied only to the current session and are lost after the user profile disconnects from Command.

Banning Connections from Command

On the **User Sessions** page, you can permanently ban connections to a Command Recording Software if they connect from suspicious IP addresses. A connection is the combination of a user profile and its current IP address. You can ban a specific IP address or a range of IP addresses at the same time.

Note: The ban is applied to the Command Config and Command Client interfaces, and to the SiteManager application.

The **User Session** page also allows you to remove the temporary lock on local and LDAP user profiles after too many failed login attempts. For more information about configuring the temporary lock, see "Managing the Command Recording Software" on page 24.

Select your configuration:

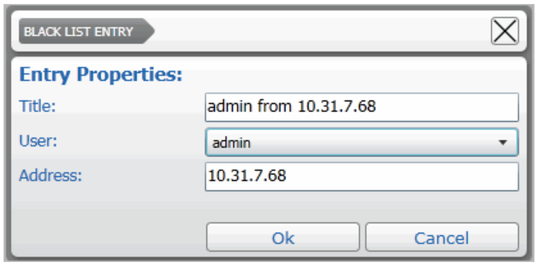
- "To ban a connection from Command" on page 101
- "To ban an IP address or a range of IP addresses" on page 102
- "To remove the temporary lock from local and LDAP user profiles" on page 103

To ban a connection from Command

1 On the **User Sessions** page, select a connected user profile.

2 Click the 🛇 button.

The **Blacklist Entry** dialog box appears.



Title: admin from 10.31.7.68

User: admin

Address: 10.31.7.68

Command automatically fills the **Title** and **Address** fields.

3 Select a specific local **User** from the list, if required.

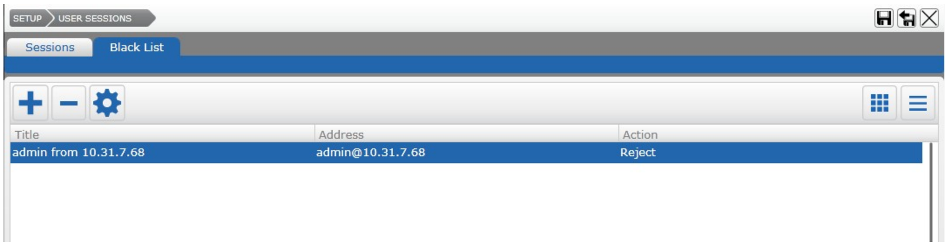
Notes:

- Select **All** to ban every user connecting from the specified IP Address.
- For LDAP user or user groups, you must manually enter the LDAP user name.

4 Review and edit the information as required and click **Ok** to ban the connection.

Command automatically switches to the **Black List** tab and the banned connection is added to the list.

WARNING: A banned connection results in the user being unable to connect from the banned IP address. However, the user can to connect to a Command Recording Software from a different IP address.



Title	Address	Action
admin from 10.31.7.68	admin@10.31.7.68	Reject

5 Select the banned connection and do any of the following:

- Click the − button to remove the ban from the connection.
- Click the ⚙ button to open the **Blacklist Entry** dialog box and edit the ban information.
- Click the 🔒 button to lock the ban configuration.

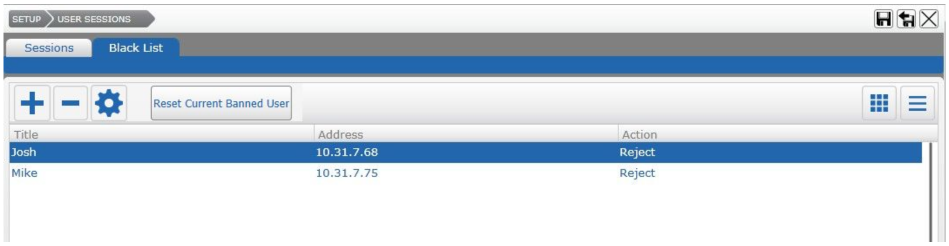
6 To manually ban a connection, click the + button and repeat step 4 to step 5.

7 Click the 💾 button to save and apply the changes.

To ban an IP address or a range of IP addresses

1 Click the **Black List** tab.

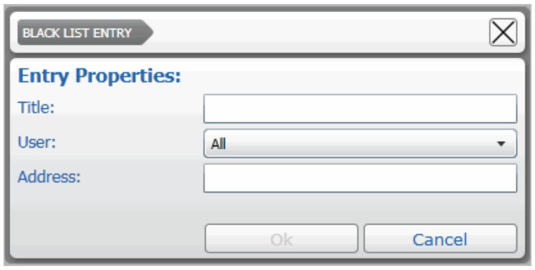
The list of banned connections appears.



Title	Address	Action
Josh	10.31.7.68	Reject
Mike	10.31.7.75	Reject

2 Click the + button.

The **Blacklist Entry** dialog box appears.



Entry Properties:

Title:

User: All

Address:

3 In the **Title** box, enter a name for the entry.

4 Select a specific user from the **User** list, or select **All** to ban every user connecting from the specified IP Address.

5 In the **Address** box, enter the IP address you want to ban.

Tip: You can also ban a range of IP addresses by replacing the first or last digits with an asterisk (*). For example, by typing 198.162.50.* in the **Address** text box, all the IP addresses beginning with 198.162.50 are banned from connecting to a Command Recording Software.

6 Click **Ok** to confirm the changes.

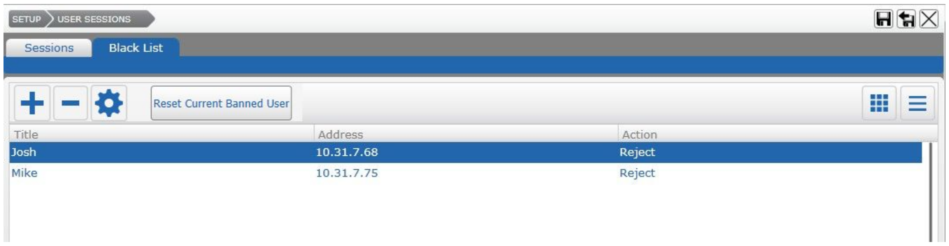
The banned IP address is added to the list.

7 Click the 💾 button to save and apply the changes.

To remove the temporary lock from local and LDAP user profiles

1 Click the **Black List** tab.

The list of locked user profiles appears.



Title	Address	Action
Josh	10.31.7.68	Reject
Mike	10.31.7.75	Reject

2 Select the locked user profile.

3 Click the **Reset Current Banned User** button.

The user account is unlocked and can log on to the Command Recording Software.

Note: The **Reset Current Banned User** button has no effect on banned user accounts and banned IP addresses.

Chapter 7

Configuring Identification Certificates

You can enhance the security of the Command Recording Software by adding identification certificates on the **Certificate Configuration** page. Identification certificates are included in specific USB tokens or smartcards. Certificates can be linked to the Command Recording Software connection (via Command Config, Command Client, and SiteManager) or to specific features.

For example, if you require an identification certificate for the connection to the Command Recording Software, you can only log on with an appropriate USB token/ smartcard inserted on the client. You can also configure identification certificates for the primary Command features, such as archive encryption, video playback, export, and Command configuration.

For more information about associating identification certificates to user profiles, see "Creating Local User Profiles" on page 69.

Important: The configurations included in the **Certificate Configuration** page are applied to every Command Recording Software user account. Identification certificates are not supported on Mac OS X systems.

This chapter contains the following sections:

- "Importing Identification Certificates" on page 105
- "Associating Command Features to Identification Certificates" on page 107
- "Removing and Deleting Identification Certificates" on page 108

Importing Identification Certificates

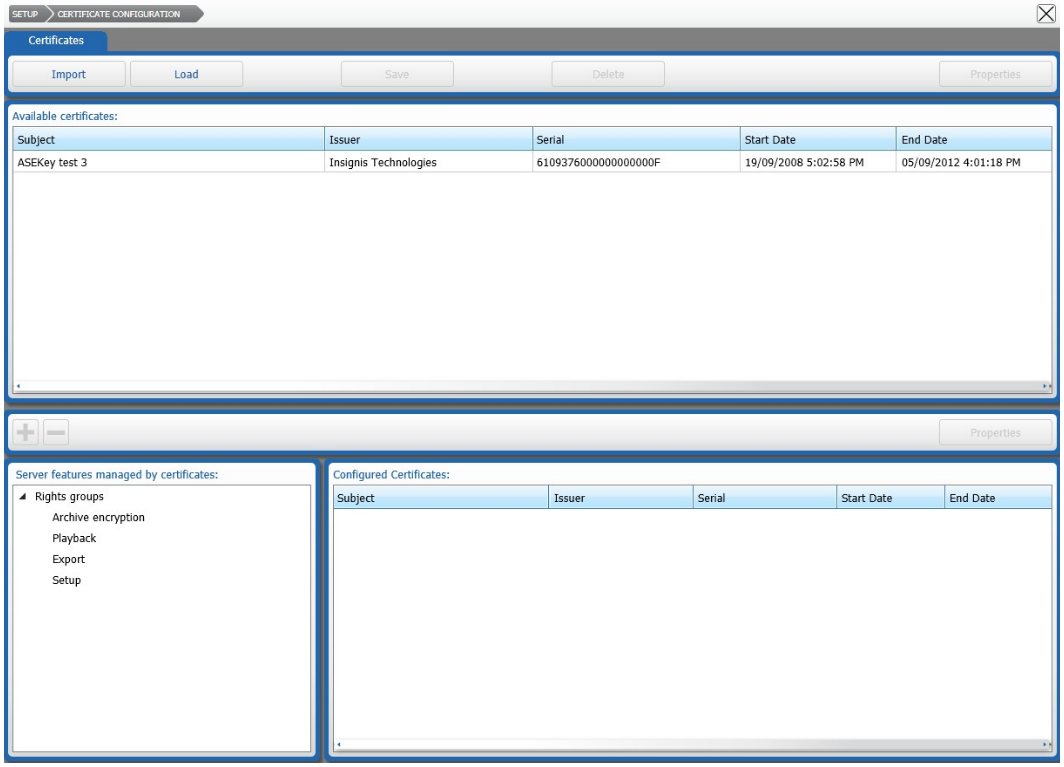
You can enhance the security of Command by importing identification certificates. Before adding an identification certificate to Command, you must import it from a USB token/smartcard. For more information about identification certificates management, see the documentation accompanying the smartcard/USB token management software.

To import an identification certificate

1 Insert the USB token/smartcard containing the identification certificate into the client.

2 On the Command Config main page, under **User Management**, click **Certificates**.

The **Certificate Configuration** page appears.



Available certificates:

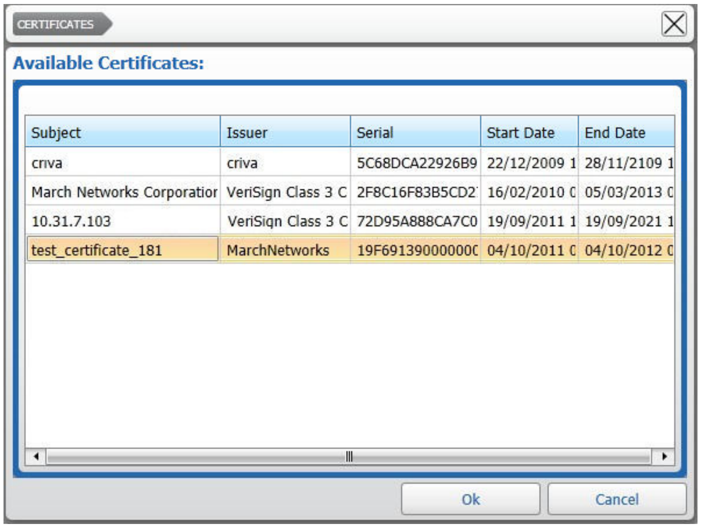
Subject	Issuer	Serial	Start Date	End Date
ASEKey test 3	Insignis Technologies	6109376000000000000F	19/09/2008 5:02:58 PM	05/09/2012 4:01:18 PM

Configured Certificates:

Subject	Issuer	Serial	Start Date	End Date

3 Click **Import**.

The **Certificates** dialog box appears.



Available Certificates:

Subject	Issuer	Serial	Start Date	End Date
criva	criva	5C68DCA22926B9	22/12/2009 1	28/11/2109 1
March Networks Corporatior	VeriSign Class 3 C	2F8C16F83B5CD2	16/02/2010 0	05/03/2013 0
10.31.7.103	VeriSign Class 3 C	72D95A888CA7C0	19/09/2011 1	19/09/2021 1
test_certificate_181	MarchNetworks	19F69139000000	04/10/2011 0	04/10/2012 0

4 Select a certificate in the list and click **Ok**.

The certificate is added to the server.

5 Click the 💾 button to save and apply the changes.

Exporting and Uploading Identification Certificates

After you import the identification certificate on the Command Recording Software, you can save it on the client and use it to configure other Command Recording Softwares or 7532 Hybrid NVRs on the network. This is useful to configure Command Recording Softwares or 7532 Hybrid NVRs without plugging the USB token/smartcard on the client.

To export an identification certificate

1 On the **Certificates Configuration** page, select a certificate in the **Available certificates** section.

2 Click **Save.**

The **Save As** dialog box appears.

3 Navigate to the folder where you want to save the identification certificate, enter a name for the certificate file, and then click **Ok**.

The identification certificate is saved locally in the selected folder.

To upload an exported certificate

1 On the **Certificates Configuration** page, click **Load**.

The **Open** dialog box appears.

2 Navigate to the folder where the identification certificate file you want to upload is located, and click **Open**.

The identification certificate is uploaded to the Command Recording Software.

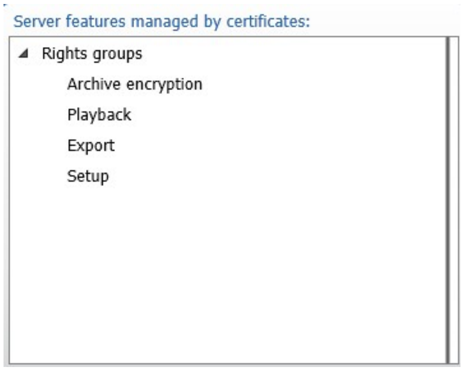
Associating Command Features to Identification Certificates

You can now configure identification certificates for the primary Command features, such as archive encryption, video playback, export, and Command setup.

To associate Command features to an identification certificate

1 On the **Certificate Configuration** page, select a certificate in the **Available certificates** section.

2 Select a rights group under **Server features managed by certificates**. Every group (**Archive encryption**, **Playback**, **Export**, **Setup**) represents a key Command feature.



Server features managed by certificates:

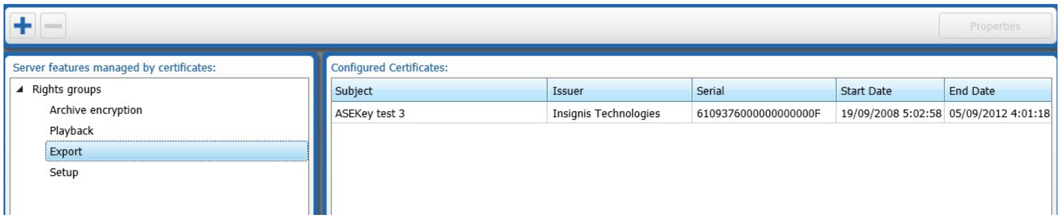
◢ Rights groups
- Archive encryption
- Playback
- Export
- Setup

The groups are described in the following table.

Group	Result
Archive encryption	The video archive is encrypted. The user must plug the USB token/smartcard into the client to access archived video evidence. **Note:** The Command Recording Software encrypts only videos archived after the certificate configuration.
Playback	The playback functionality is locked. The user must plug the USB token/smartcard into the client to review archived video evidence.
Export	The export functionality is locked. The user must plug the USB token/smartcard into the client to export archived video evidence.
Setup	The Command Recording Software configurations are locked. The user must plug the USB token/smartcard into the client to configure the Command Recording Software.

3 Click the + button

The certificate is associated to the selected group.



Server features managed by certificates:

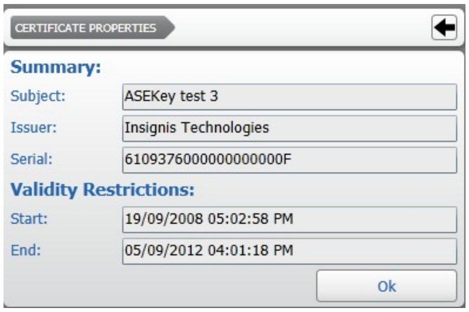
- Rights groups
  - Archive encryption
  - Playback
  - Export
  - Setup

Configured Certificates:

Subject	Issuer	Serial	Start Date	End Date
ASEKey test 3	Insignis Technologies	6109376000000000000F	19/09/2008 5:02:58	05/09/2012 4:01:18

4 Select the uploaded certificate and click **Properties**.

The **Certificate Properties** dialog box appears.



Summary:

Subject: ASEKey test 3

Issuer: Insignis Technologies

Serial: 6109376000000000000F

Validity Restrictions:

Start: 19/09/2008 05:02:58 PM

End: 05/09/2012 04:01:18 PM

5 Repeat steps 2-4 to link the certificate to associate additional Command features to identification certificates.

6 Click the 🖫 button to save and apply the changes.

Removing and Deleting Identification Certificates

If a certificate is no longer required, you can remove it from a group of features. You can also delete the identification certificate from the Command Recording Software.

To remove an identification certificate from a group of features

1 On the **Certificate Configuration** page, select a rights group with the certificate you want to remove.

2 Select the certificate and click the − button.

3 Click the 🖫 button to save and apply the changes.

To delete an identification certificate from the Command Recording Software

1 On the **Certificate Configuration** page, select a certificate in the **Configured certificates** section.

2 Click **Delete**.

A **Warning** dialog box appears.

3 Click **Yes** to confirm the certificate deletion.

4 Click the 🖫 button to save and apply the changes.

Chapter 8

Configuring System Settings

You can use the **System Configuration** page to configure the following system settings for a Command Recording Software.

Important Note: Most of the Command Recording Software network settings must be directly configured on the server. If you need to modify any major settings (time and date, DST, internal IP addresses, DNS, and gateways), consult your network administrator.

This chapter contains the following sections:

Accessing the System Configuration

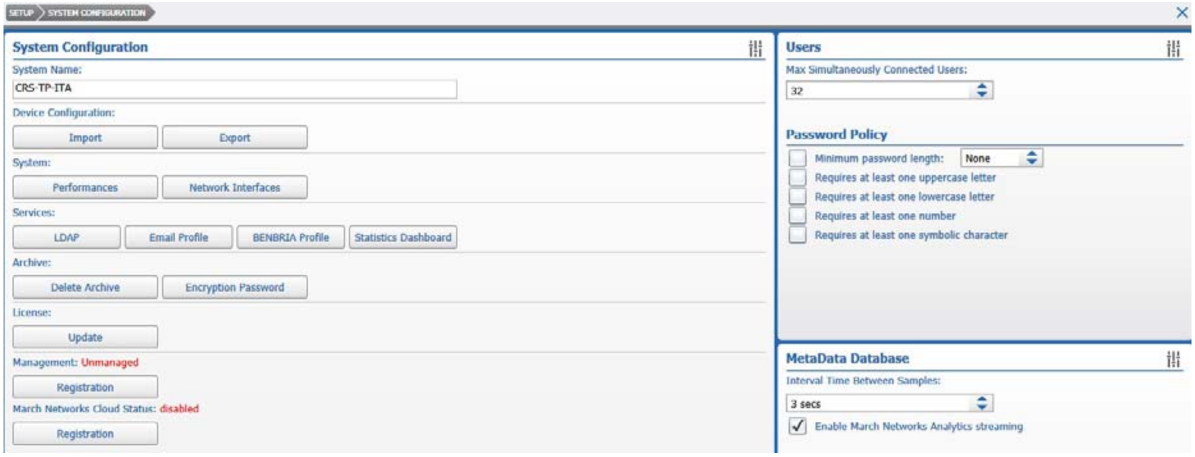
You can customize your Command Recording Software in the Command system by using the **System Configuration** page.

Important: The **License Update** button is used only for USB dongle licensing.

To access the system configuration

1 On the Command Config main page, under **General Settings**, click **System**.

The **System Configuration** page appears.



System Configuration

System Name: CRS-TP-ITA

Device Configuration:

System:

Services:

Archive:

License:

Management: Unmanaged

March Networks Cloud Status: disabled

Users

Max Simultaneously Connected Users: 32

Password Policy

□ Minimum password length: None

□ Requires at least one uppercase letter

□ Requires at least one lowercase letter

□ Requires at least one number

□ Requires at least one symbolic character

MetaData Database

Interval Time Between Samples: 3 secs

☑ Enable March Networks Analytics streaming

2 In the **System Name** box, enter a name for the Command Recording Software.

Note: March Networks applications identify the Command Recording Software by this name.

3 Click the 💾 button to save and apply the changes.

Exporting and Importing Configuration Settings

On the **System Configuration** page, you can export and import configuration settings from and to other Command Recording Softwares.

WARNING: Importing the configuration from a different Command Recording Software deletes the current configuration. The storage configuration cannot be exported or imported. Recording cannot start until a new storage group is configured. It is not possible to import the configuration from a Command Recording Software 2.9 to a lower version. If you plan to apply the same configuration to different Command Recording Softwares, you must first upgrade every Command Recording Software in the system to version 2.9 (64-bit version). For more information about upgrading the Command Recording Software, see “Upgrading Command Recording Software” on page 21.

To export configuration settings

1 In the **Configuration Settings** section, click **Export** to save the current system configuration settings in an XML file.

A **Warning** dialog box appears.

2 To confirm that you are ready to export the configuration, click **Yes**.

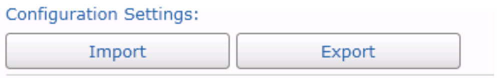
The **Save As** dialog box appears.

3 Navigate to the folder where you want to save the configuration settings, enter a name for the configuration settings file, and then click **Ok**.

An XML file with all the configuration settings of your current system is saved in the location you chose.

To import configuration settings

1 In the **Configuration Settings** section, click **Import** to load the configuration settings from another Command Recording Software or system.



The **Open** dialog box appears.

2 Navigate to the folder where the XML configuration settings file you want to import is located, and click **Open**.

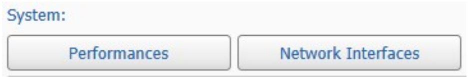
A **Warning** dialog box appears.

3 To confirm that you are ready to import the configuration, click **Yes**.

The new configuration settings are applied to your current system.

Configuring System and Network Settings

You can view performance information for the Command Recording Software you are connected to and configure the network settings.



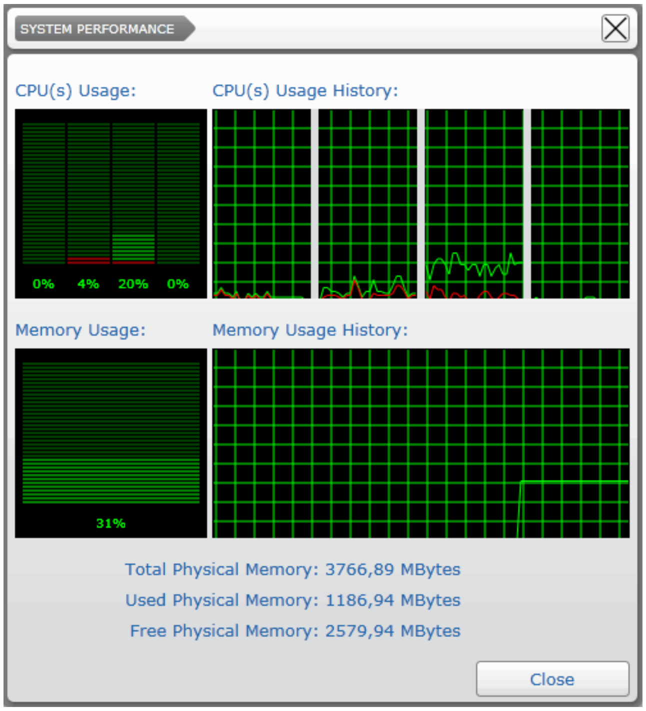
Select your configuration:

- "To view the performance details" on page 112
- "To configure the network settings" on page 113

To view the performance details

1 In the **System** section of the **System Configuration** page, click **Performances**.

The **System Performance** dialog box appears, where you can view the CPU usage history, the memory usage history, and the amount of total, used, and free physical memory available.



Total Physical Memory: 3766,89 MBytes

Used Physical Memory: 1186,94 MBytes

Free Physical Memory: 2579,94 MBytes

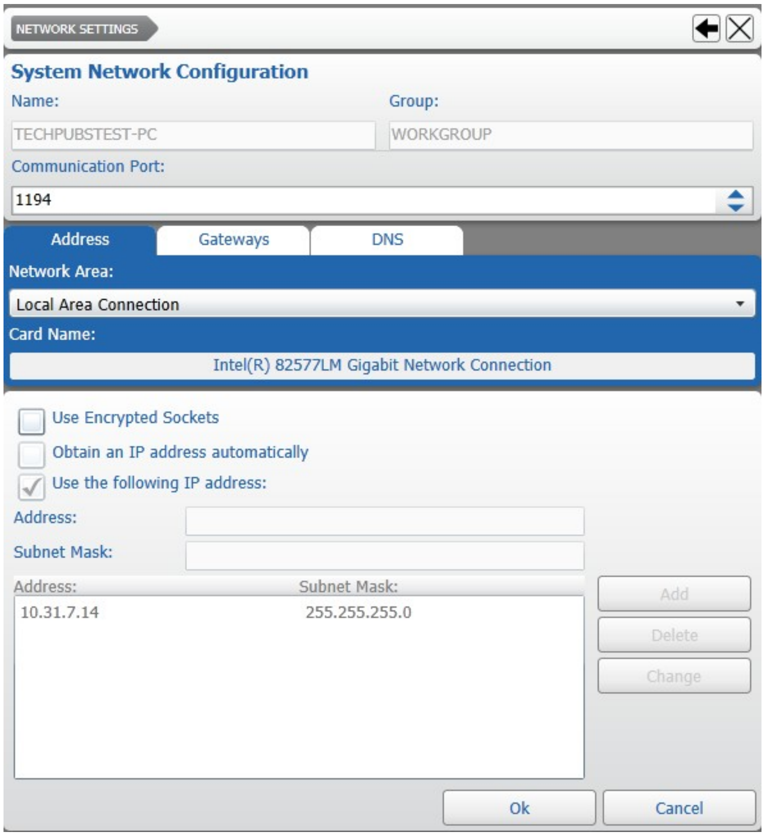
2 Click **Close**.

To configure the network settings

1 In the **System** section of the **System Configuration** page, click **Network Interfaces** to view the network configuration of your Command Recording Software and to configure settings such as the server communication port.

Important Note: Most of the Command Recording Software network and time settings must be directly configured on the server. If you need to modify any major settings (internal IP addresses, DNS, and gateways), consult your network administrator.

The **Network Settings** dialog box appears.



System Network Configuration

Name: TECHPUBSTEST-PC

Group: WORKGROUP

Communication Port: 1194

Network Area: Local Area Connection

Card Name: Intel(R) 82577LM Gigabit Network Connection

□ Use Encrypted Sockets

□ Obtain an IP address automatically

☑ Use the following IP address:

Address:

Subnet Mask:

Address:	Subnet Mask:
10.31.7.14	255.255.255.0

2 Select a new **Communication Port**.

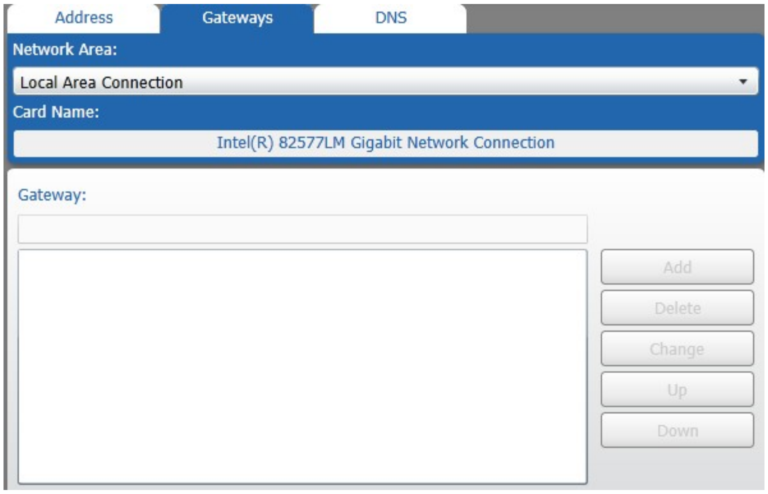
Note: The default communication port is 1194.

3 Select a **Network Area** from the list.

4 To automatically encrypt transmitted data, select the **Use Encrypted Sockets** check box.

5 Click the **Gateways** tab to view information about the connection gateways.

Note: These settings are not available on Command Recording Softwares and must be configured on the server by the network administrator.

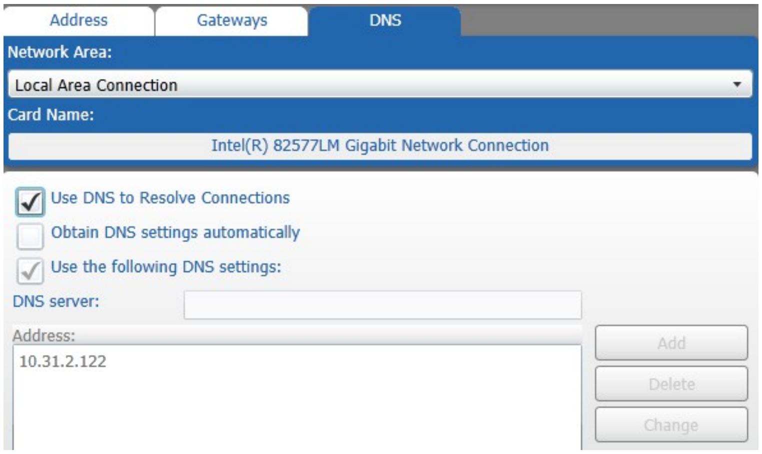


Network Area: Local Area Connection

Card Name: Intel(R) 82577LM Gigabit Network Connection

Gateway:

6 Click the **DNS** tab and select the **Use DNS To Resolve Connections** check box to allow the DNS server to manage incoming connections and identify the incoming clients.



Network Area: Local Area Connection

Card Name: Intel(R) 82577LM Gigabit Network Connection

☑ Use DNS to Resolve Connections

□ Obtain DNS settings automatically

☑ Use the following DNS settings:

DNS server:

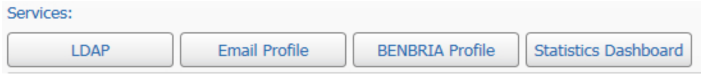
Address:
10.31.2.122

7 Click **Update** to apply the changes.

Configuring Services

In the **Services** section of the **System Configuration** page you can configure the LDAP settings, the email profile, the **System Overview** page, the BENBRIA profile for your Command Recording Software.

Note: For more information on the **System Overview** page, see “Accessing the Statistics Dashboard Page” on page 128.



Select your configuration:

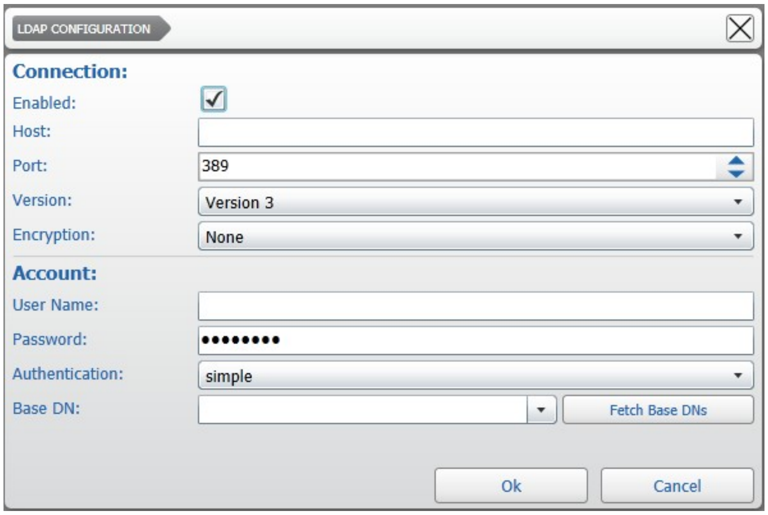
- “To configure LDAP settings” on page 115
- “To configure the email profile” on page 116
- “To configure the BENBRIA profile” on page 116
- “To configure the Statistics Dashboard page” on page 117

To configure LDAP settings

1 Click **LDAP** to configure the connection to an LDAP server.

Note: These settings are required if you want to configure LDAP authentication for user accounts based on the user list of the LDAP server. For more information, see “Configuring LDAP Authentication for Local User Profiles” on page 70.

The **LDAP Configuration** dialog box appears.



Enabled: ☑
Host:
Port: 389
Version: Version 3
Encryption: None
User Name:
Password: ••••••••
Authentication: simple
Base DN:

2 In the **Connection** section, select the **Enabled** check box to activate LDAP authentication.

3 Enter the LDAP server’s IP Address in the **Host** box.

4 Select the LDAP server’s communication **Port**.

5 Select the LDAP protocol **Version** from the list.

6 Select the LDAP protocol **Encryption** mode from the list, if required.

7 In the **Account** section, enter the credentials (**User Name** and **Password**) required to access the user list on the LDAP server.

8 Select the account **Authentication** mode from the list, according to the server's configuration. Options include **Simple** and **SASL**.

9 Click **Fetch Base DNs** and select the server's Distinguished Name (DN) string from the **Base DN** list.

Tip: You can also manually enter the DN string by clicking in the **Base DN** field.

10 Click **Ok**.

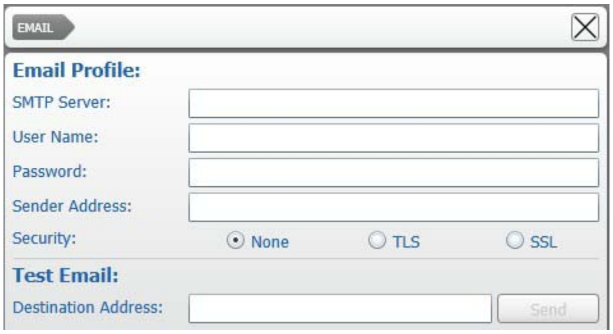
11 Click the 💾 button to save and apply the changes.

To configure the email profile

1 Click **Email Profile** to configure an SMTP server for outgoing messages.

Note: These settings are required if you want to configure the Command Recording Software to automatically send an e-mail after an alarm is triggered. For more information, see "Setting Automatic Alarm Notifications" on page 222.

The **Email** dialog box appears.



EMAIL

Email Profile:

SMTP Server:

User Name:

Password:

Sender Address:

Security: ● None ○ TLS ○ SSL

Test Email:

Destination Address:

2 Enter the **SMTP Server** address, the mail account credentials (**User Name** and **Password**), and the **Sender** e-mail **Address**.

Note: The number of dots does not represent the actual number of characters.

3 Click a **Security** setting according to the SMTP server's configuration. Options include **None**, **TLS**, and **SSL**.

4 Click **Ok**.

5 Click the 💾 button to save and apply the changes.

Tip: To send a test e-mail, enter an address in the **Destination Address** field, and then click **Send**.

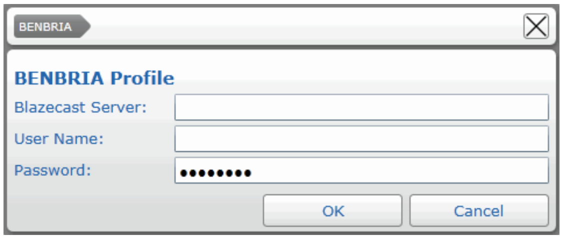
To configure the BENBRIA profile

1 Click **BENBRIA Profile** to configure the interaction between Command and the Benbria Blazecast® notification system.

Important: A valid user profile on a Benbria Blazecast is required to configure this option.

Note: These settings are required to automatically generate notifications and alerts based on alarms triggered by the Command Recording Software. For more information, see "To set automatic notifications to Benbria Blazecast servers" on page 226.

The **BENBRIA** dialog box appears.



BENBRIA

BENBRIA Profile

Blazecast Server:

User Name:

Password: ••••••••

2 Enter the IP Address of the **Blazecast Server**.

3 Enter the login credentials (**User Name** and **Password**) for the Blazecast server.

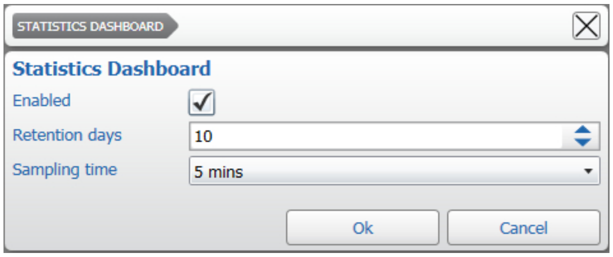
4 Click **Ok**.

5 Click the 💾 button to save and apply the changes.

To configure the Statistics Dashboard page

1 Click **Statistics Dashboard** to configure the statistics that appear in the **Statistics Dashboard** page.

The **Statistics Dashboard** dialog box appears.



STATISTICS DASHBOARD

Statistics Dashboard

Enabled ☑

Retention days 10

Sampling time 5 mins

2 Select the **Enabled** check box to enable the **Statistics Dashboard** page.

3 In the **Retention Days** field, configure the time interval after which statistics are removed from the Command Recording Software database.

4 Select a time interval from the **Sampling Time** list to configure how frequently data are sampled by the Command Recording Software.

5 Click **Ok**.

6 Click the 💾 button to save and apply the changes.

Managing Archived Video

In the **Services** section of the **System Configuration** page you can delete all or a specified part of the archived video evidence recorded by your Command Recording Software, enable video encryption for the remote export on a USB stick connected directly to the server, and configure the password to play the exported video evidence using Command Player.

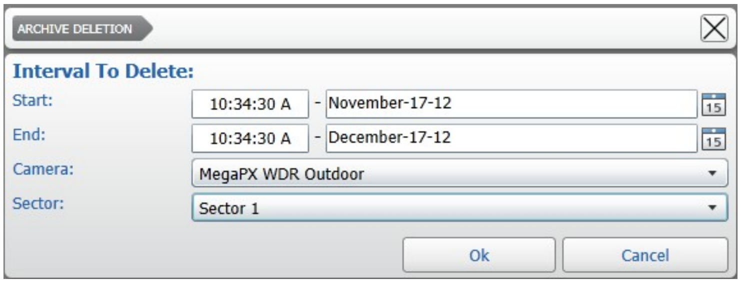
Select your configuration:

- "To delete archived video" on page 118
- "To encrypt video evidence for remote USB export" on page 118

To delete archived video

1 In the **Archive** section of the **System Configuration** page, click **Delete Archive** to delete a specified interval of the video evidence recorded.

The **Archive Deletion** dialog box appears.



ARCHIVE DELETION

Interval To Delete:

Start: 10:34:30 A - November-17-12

End: 10:34:30 A - December-17-12

Camera: MegaPX WDR Outdoor

Sector: Sector 1

2 Define the time interval of the video evidence that you want to delete by configuring the **Start** and **End** options.

Tip: Click the 📅 button to select the date from a calendar.

3 Select a recorded camera from the **Camera** list.

Note: Select **All** to delete all the video evidence recorded in the specified time interval.

4 Select a recording sector camera from the **Sector** list.

Note: Select **All** to delete all the video evidence recorded in the specified time interval.

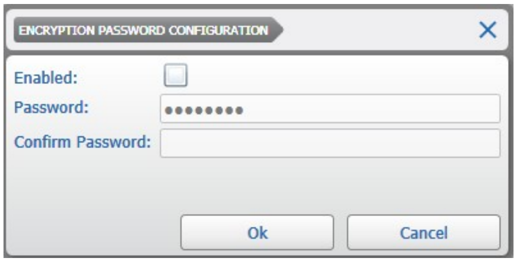
5 Click **Ok** to delete the specified video evidence and close the dialog box.

6 Click the 💾 button to save and apply the changes.

To encrypt video evidence for remote USB export

1 In the **Archive** section of the **System Configuration** page, click **Encryption Password**.

The **Encryption Password Configuration** dialog box appears.



ENCRYPTION PASSWORD CONFIGURATION

Enabled: □

Password: ••••••••

Confirm Password:

2 Select the **Enabled** check box to enable the archive encryption for the remote export on a USB stick connected directly to the server.

3 In the **Password** field, enter the password required to play the exported video evidence using Command Player.

4 Enter again the password in the **Confirm Password** field.

5 Click **Ok** to close the dialog box.

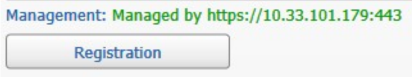
6 Click the 💾 button to save and apply the changes.

Managing the Registration to Command Enterprise

You can use the **System Configuration** page to register the Command Recording Software to a Command Enterprise Server or unregister a Command Recording Software from a Command Enterprise Server.

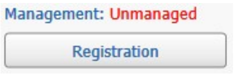
Important Notes:

- Only user profiles with the **Registration** permission can see the **Management** section and unregister a Command Recording Software (see "Assigning Permissions Over Command Recording Software Features" on page 81).
- Before registering your Command Recording Software to a Command Enterprise Server, ensure that the CES has enough channel licenses for all the Command Recording Software video channels. Unlicensed channels are automatically disabled, but continue recording as scheduled. When you apply a license to the channel, you can access the video evidence archived when the channel was disabled.
- After you unregister the Command Recording Software from the Command Enterprise Server, you must plug the USB dongle or register to a different Command Enterprise server to apply a new license.
- The button changes according to the initial state.



Management: Managed by https://10.33.101.179:443

Registered to a Command Enterprise Server



Management: Unmanaged

Unregistered

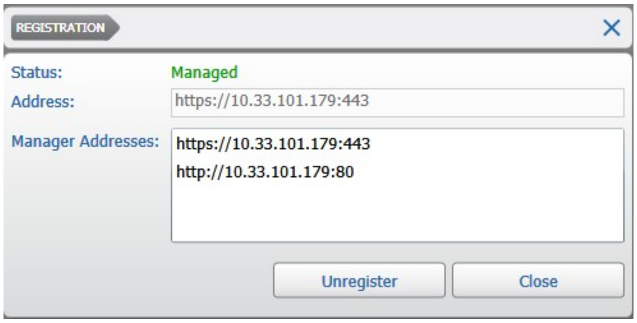
Select your configuration:

- "To unregister from a Command Enterprise Server" on page 119
- "To register to a Command Enterprise Server" on page 120

To unregister from a Command Enterprise Server

1 In the **Management** section of the **System Configuration** page, click **Registration**.

The **Registration** dialog box appears.



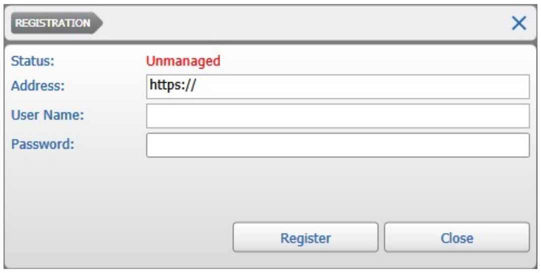
Status: Managed

Address: https://10.33.101.179:443

Manager Addresses:
https://10.33.101.179:443
http://10.33.101.179:80

2 Click **Unregister**.

After several seconds, the Command Recording Software performs the procedure and the status switches to **Unmanaged**.



Status: Unmanaged
Address: https://
User Name:
Password:

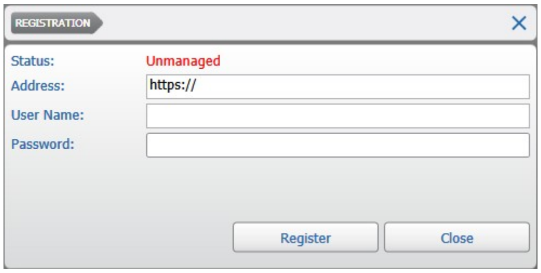
3 Click **Close** to close the dialog box.

4 Click the 💾 button to save and apply the changes.

To register to a Command Enterprise Server

1 In the **Management** section of the **System Configuration** page, click **Registration**.

The **Registration** dialog box appears.



Status: Unmanaged
Address: https://
User Name:
Password:

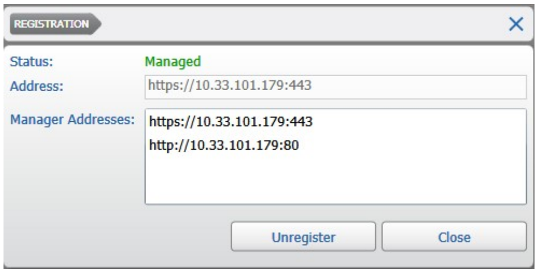
2 In the **Address** field, enter “https://” followed by the IP address or host name of the Command Enterprise Serve, followed by “:” and the communication port, if different from the default one (443):

https://<CEShostname>:<CESport>.

3 Log on to the CES with a valid **User** name and **Password**.

4 Click **Unregister**.

After several seconds, the Command Recording Software performs the procedure, the status switches to **Managed** and the available addresses for the CES appear in the **Manager Addresses** field.



Status: Managed
Address: https://10.33.101.179:443
Manager Addresses: https://10.33.101.179:443
http://10.33.101.179:80

5 Click **Close** to close the dialog box.

6 Click the 💾 button to save and apply the changes.

Registering to the March Networks Cloud Service

You can use the **System Configuration** page to register a Command Recording Software to the March Networks Cloud service. By doing so, you can view live video evidence from a Command Recording Software on mobile devices such as smartphones and tablets.

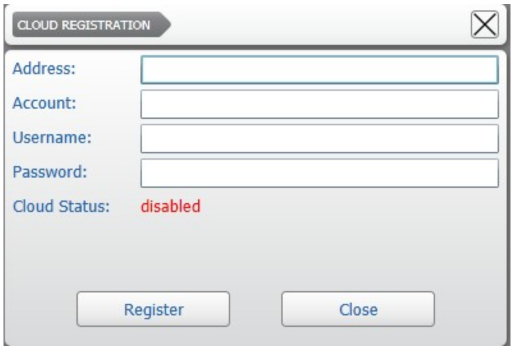
Important: Before registering a Command Recording Software to the March Networks Cloud service, you must subscribe to the service and create a valid account. For more information, contact your local March Networks Sales representative.

Note: After you register to the March Networks Cloud service, you must enable the cameras you want to view on the mobile devices. For more information, see “Editing IP Cameras” on page 161.

To register to the March Networks Cloud service

1 In the **March Networks Cloud Status** section of the **System Configuration** page, click **Registration**.

The **Cloud Registration** dialog box appears.



Cloud Status: disabled

2 Enter the March Networks Cloud server IP address or host name in the **Address** box.

3 Enter the March Networks Cloud **Account** name.

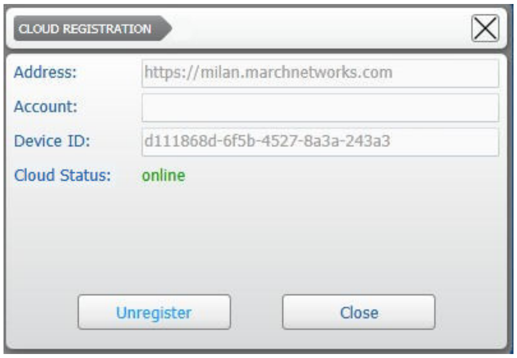
4 Enter the March Networks Cloud account credentials in the **Username** and **Password** boxes.

5 Click **Register** to register the Command Recording Software to the March Networks Cloud service.

6 Click **Close** to return to the **System Configuration** page.

After a few seconds the Command Recording Software connects to the March Networks Cloud service.

Tip: To unregister the Command Recording Software from the service, click again **Registration**, and then click **Unregister**.

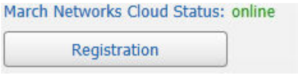


Address: https://milan.marchnetworks.com

Account:

Device ID: d111868d-6f5b-4527-8a3a-243a3

Cloud Status: online


March Networks Cloud Status: online

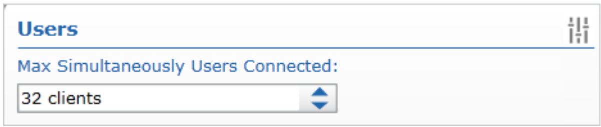
Defining the Number of Connected Users

You can use the **System Configuration** page to define the number of users who can connect to the Command Recording Software simultaneously.

Important: This configuration refers to the number of users per connection type: for example, if you set four as the maximum number of users that can be connected to the Command Recording Software at the same time, this means that up to four users can connect to the Command Recording Software using the Command Config or Command Client interfaces, and another four users can connect to the Command Recording Software using SiteManager.

To define the number of connected users

1 In the **Users** section, select the number of users (clients) that can be connected to the Command Recording Software at the same time in the **Max Simultaneously Connected Users** box.



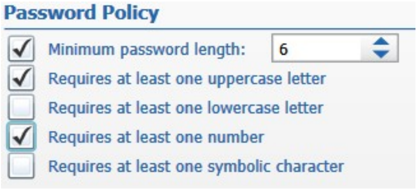
Max Simultaneously Users Connected: 32 clients

2 Click the 💾 button to save and apply the changes.

Configuring the Password Policy

You can use the **System Configuration** page to configure a password policy: in this way you can increase the security of your system by forcing user to create password that respect the options configured in the **Password Policy** section.

Note: If the password for a user profile does not respect the new password policy, the policy is enforced the next time the user logs on to the server using the Command Config (see “Changing the Password From the Login page” on page 33) or Command Client applications.



Password Policy

☑ Minimum password length: 6

☑ Requires at least one uppercase letter

□ Requires at least one lowercase letter

☑ Requires at least one number

□ Requires at least one symbolic character

To configure the password policy

1 In the **Password Policy** section, do any of the following:

- Select the **Minimum password length** check box and then enter or select a value to set the minimum number of characters for the password.
- Select the **Requires at least one uppercase letter** check box to force the use one or more than one uppercase letters in the password.
- Select the **Requires at least one lowercase letter** check box to force the use one or more than one lowercase letters in the password.
- Select the **Requires at least one number** check box to force the use one or more than one numbers in the password.
- Select the **Requires at least one symbolic character** check box to force the use one or more than one special characters in the password.

  Note: The list of allowed special characters includes:

  !”#$%&’()*+,-./:;<=>?@[\]^_`{|}~

2 Click the 💾 button to save and apply the changes.

The next time a user tries to log on to the server using the Command Config (see “Changing the Password From the Login page” on page 33) or Command Client applications, the policy is enforced and the user must change the password for his profile if his password does not respect the new password policy.

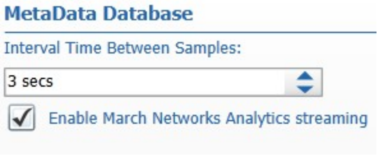
Configuring Metadata Databases

You can use the System Configuration page to configure how often the Command Recording Software collects information about video analytics. This information is used for the Metadata Search on the SiteManager application. For more information, see the *SiteManager User Guide*, available on the Software DVD or from the March Networks Partner Portal and official websites.

Tip: If the SiteManager software is not in use, you can also disable metadata streams: this may be useful to decrease the CPU workload.

To configure the metadata database

1 In the **Metadata Database** section, select how often the Command Recording Software collects information about video analytics in the **Interval Time Between Samples** box.



MetaData Database

Interval Time Between Samples:

3 secs

☑ Enable March Networks Analytics streaming

2 Click the 💾 button to save and apply the changes.

To disable metadata streams

1 In the **Metadata Database** section, clear the **Enable March Networks Analytics Streaming** to disable Metadata streams from devices with the VideoSphere Analytics activated.

2 Click the 💾 button to save and apply the changes.

3 Do one of the following:

- Access the **Camera Configuration** page, disable all of the video analytics capable cameras in the **Camera List** panel, and then click the 💾 button. Re-enable the cameras and click the 💾 button. For more information, see “Disabling a Camera” on page 193.
- Access the **Command Management** interface on the server and click the ▶ button to restart the Command Recording Software service. For more information, see “Managing the Command Recording Software” on page 24.

4 Repeat steps 1-3 to re-enable the metadata streams.

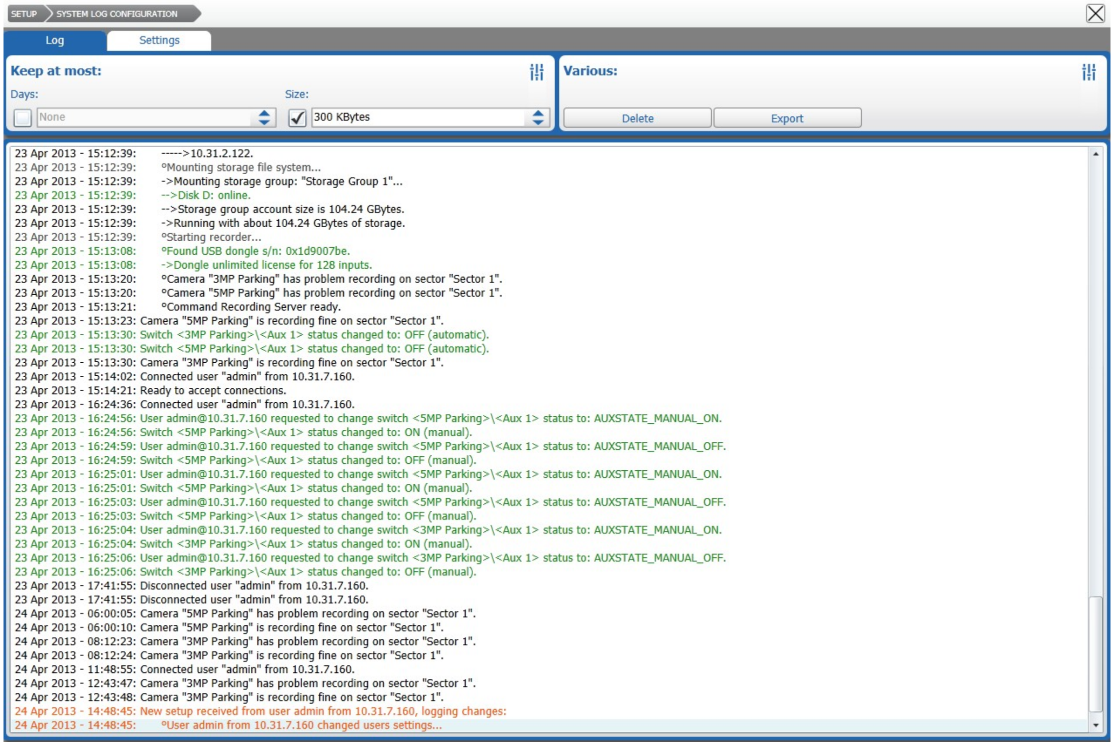
Viewing and Managing System Logs

Command Config features an intuitive, text-based system log that highlights all of the main actions performed on the Command Recording Software with different colors. For example, video exports are indicated with green, setup changes with orange, and unauthorized log on attempts with red.

To view and manage the system log

1. On the Command Config main page, under **General Settings**, click **System Log**.

The **System Log Configuration** page appears.



Keep at most:

Days: ☐ None

Size: ☑ 300 KBytes

Various:

```
23 Apr 2013 - 15:12:39:     ----->10.31.2.122.
23 Apr 2013 - 15:12:39:     °Mounting storage file system...
23 Apr 2013 - 15:12:39:     ->Mounting storage group: "Storage Group 1"...
23 Apr 2013 - 15:12:39:     -->Disk D: online.
23 Apr 2013 - 15:12:39:     -->Storage group account size is 104.24 GBytes.
23 Apr 2013 - 15:12:39:     ->Running with about 104.24 GBytes of storage.
23 Apr 2013 - 15:12:39:     °Starting recorder...
23 Apr 2013 - 15:13:08:     °Found USB dongle s/n: 0x1d9007be.
23 Apr 2013 - 15:13:08:     ->Dongle unlimited license for 128 inputs.
23 Apr 2013 - 15:13:20:     °Camera "3MP Parking" has problem recording on sector "Sector 1".
23 Apr 2013 - 15:13:20:     °Camera "5MP Parking" has problem recording on sector "Sector 1".
23 Apr 2013 - 15:13:21:     °Command Recording Server ready.
23 Apr 2013 - 15:13:23: Camera "5MP Parking" is recording fine on sector "Sector 1".
23 Apr 2013 - 15:13:30: Switch <3MP Parking>\<Aux 1> status changed to: OFF (automatic).
23 Apr 2013 - 15:13:30: Switch <5MP Parking>\<Aux 1> status changed to: OFF (automatic).
23 Apr 2013 - 15:13:30: Camera "3MP Parking" is recording fine on sector "Sector 1".
23 Apr 2013 - 15:14:02: Connected user "admin" from 10.31.7.160.
23 Apr 2013 - 15:14:21: Ready to accept connections.
23 Apr 2013 - 16:24:36: Connected user "admin" from 10.31.7.160.
23 Apr 2013 - 16:24:56: User admin@10.31.7.160 requested to change switch <5MP Parking>\<Aux 1> status to: AUXSTATE_MANUAL_ON.
23 Apr 2013 - 16:24:56: Switch <5MP Parking>\<Aux 1> status changed to: ON (manual).
23 Apr 2013 - 16:24:59: User admin@10.31.7.160 requested to change switch <5MP Parking>\<Aux 1> status to: AUXSTATE_MANUAL_OFF.
23 Apr 2013 - 16:24:59: Switch <5MP Parking>\<Aux 1> status changed to: OFF (manual).
23 Apr 2013 - 16:25:01: User admin@10.31.7.160 requested to change switch <5MP Parking>\<Aux 1> status to: AUXSTATE_MANUAL_ON.
23 Apr 2013 - 16:25:01: Switch <5MP Parking>\<Aux 1> status changed to: ON (manual).
23 Apr 2013 - 16:25:03: User admin@10.31.7.160 requested to change switch <5MP Parking>\<Aux 1> status to: AUXSTATE_MANUAL_OFF.
23 Apr 2013 - 16:25:03: Switch <5MP Parking>\<Aux 1> status changed to: OFF (manual).
23 Apr 2013 - 16:25:04: User admin@10.31.7.160 requested to change switch <3MP Parking>\<Aux 1> status to: AUXSTATE_MANUAL_ON.
23 Apr 2013 - 16:25:04: Switch <3MP Parking>\<Aux 1> status changed to: ON (manual).
23 Apr 2013 - 16:25:06: User admin@10.31.7.160 requested to change switch <3MP Parking>\<Aux 1> status to: AUXSTATE_MANUAL_OFF.
23 Apr 2013 - 16:25:06: Switch <3MP Parking>\<Aux 1> status changed to: OFF (manual).
23 Apr 2013 - 17:41:55: Disconnected user "admin" from 10.31.7.160.
23 Apr 2013 - 17:41:55: Disconnected user "admin" from 10.31.7.160.
24 Apr 2013 - 06:00:05: Camera "5MP Parking" has problem recording on sector "Sector 1".
24 Apr 2013 - 06:00:10: Camera "5MP Parking" is recording fine on sector "Sector 1".
24 Apr 2013 - 08:12:23: Camera "3MP Parking" has problem recording on sector "Sector 1".
24 Apr 2013 - 08:12:24: Camera "3MP Parking" is recording fine on sector "Sector 1".
24 Apr 2013 - 11:48:55: Connected user "admin" from 10.31.7.160.
24 Apr 2013 - 12:43:47: Camera "3MP Parking" has problem recording on sector "Sector 1".
24 Apr 2013 - 12:43:48: Camera "3MP Parking" is recording fine on sector "Sector 1".
24 Apr 2013 - 14:48:45: New setup received from user admin from 10.31.7.160, logging changes:
24 Apr 2013 - 14:48:45:     °User admin from 10.31.7.160 changed users settings...
```

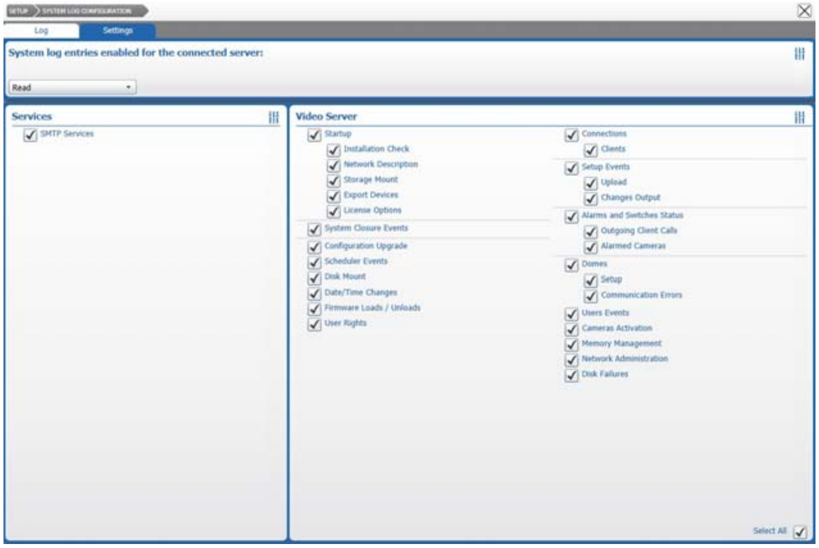
2. In the **Keep at Most** section, select the check box corresponding to one of the following log management methods:
   - **Days** — When a log exceeds the specified number of days, the system automatically starts deleting the oldest entries.
   - **Size** — When a log exceeds the maximum file size specified, the system automatically starts deleting the oldest entries.
3. In the **Various** section, click **Delete** to clear the current log file.
4. In the **Various** section, click **Export** to save the current log as a text file.

   The **Save As** dialog box appears.

   Navigate to the folder where you want to save the text file and click **Save**.

5 To customize the log contents, click the **Settings** tab.

The system log settings page appears.



System log entries enabled for the connected server:

Read

Services

☑ SMTP Services

Video Server

☑ Startup
- ☑ Installation Check
- ☑ Network Description
- ☑ Storage Mount
- ☑ Export Devices
- ☑ License Options

☑ System Closure Events

☑ Configuration Upgrade
☑ Scheduler Events
☑ Disk Mount
☑ Date/Time Changes
☑ Firmware Loads / Unloads
☑ User Rights

☑ Connections
- ☑ Clients

☑ Setup Events
- ☑ Upload
- ☑ Changes Output

☑ Alarms and Switches Status
- ☑ Outgoing Client Calls
- ☑ Alarmed Cameras

☑ Domes
- ☑ Setup
- ☑ Communication Errors

☑ Users Events
☑ Cameras Activation
☑ Memory Management
☑ Network Administration
☑ Disk Failures

Select All ☑

6 In the **System log entries enabled for the connected server** section, select one of the following log view modes from the list:

- **Read** — The log automatically filters the irrelevant information.
- **Write** — The log is unfiltered.

7 In the **Services** and **Video Server** sections, select the check boxes corresponding to the information you want to appear in the system log.

Tip: You can select or clear all the check boxes by clicking **Check All** or **Uncheck All** in the **Select** section.

8 Click the 💾 button to save and apply the changes.

Specifying Planned Holidays Using the Timeline

While not a mandatory task, configuring planned holidays in Command Config is useful when you want to set special rules for user profiles and recording policies for days when your organization is closed. You can specify holidays by accessing any of the pages that involve the use of the timeline.

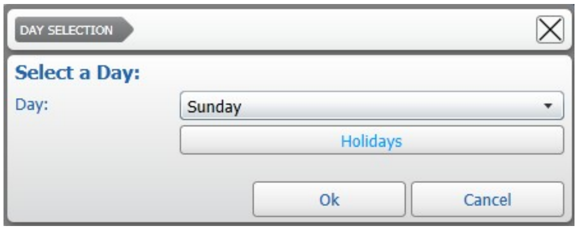
To specify planned holidays

1 On the Command Config main page, click any of the following sections to access a timeline:

- **Users**
- **Alarms**
- **Auxes**
- **Scheduler**

2 Click the + tab above the time line.

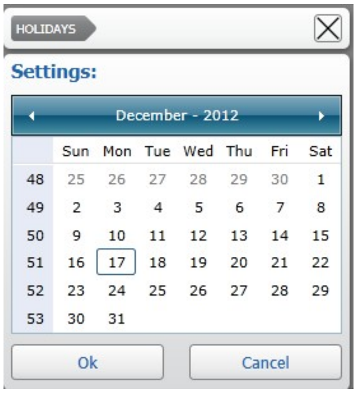
The **Day Selection** dialog box appears.



Day: Sunday

3 Click **Holidays**.

The **Holidays** dialog box appears.



December - 2012

	Sun	Mon	Tue	Wed	Thu	Fri	Sat
48	25	26	27	28	29	30	1
49	2	3	4	5	6	7	8
50	9	10	11	12	13	14	15
51	16	17	18	19	20	21	22
52	23	24	25	26	27	28	29
53	30	31					

4 To select a month, click the arrow buttons.

5 To designate a day as a holiday, click a day or multiple days in the calendar table.

Note: When a day is set as a holiday, it changes color from gray to blue.

6 Click **Done** to confirm the changes.

You can now set special rules for accounts and recording policies for days when your organization is closed by selecting **Holiday** from the **Day** list.

Accessing the Statistics Dashboard Page

The **Statistics Dashboard** page allows you to access useful charts and data related to the system performance, recording performance, and incoming and outcoming bitrate. The data can also be exported to an excel file and the charts can be downloaded for offline view, allowing you to send them to the March Networks Technical Support for analysis in case of performance problems.

Important Notes:

- To enable and configure the **Statistics Dashboard** page, access the **System Configuration** page and click the **Statistics Dashboard** button in the **Services** section. For more information, see “To configure the Statistics Dashboard page” on page 117.
- Offline charts are compatible with the Google Chrome web browser only.

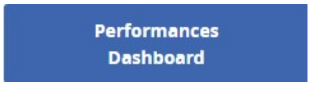
Select your configuration:

- “To access the Statistics Dashboard page” on page 128
- “To perform a query and manage charts” on page 129
- “To download an offline copy of the charts” on page 133

To access the Statistics Dashboard page

1 Do one of the following:

- In the **Address** bar of a Web browser, enter http://<*serverhostname*>. When the landing page appears, click the **Performances Dashboard** button.



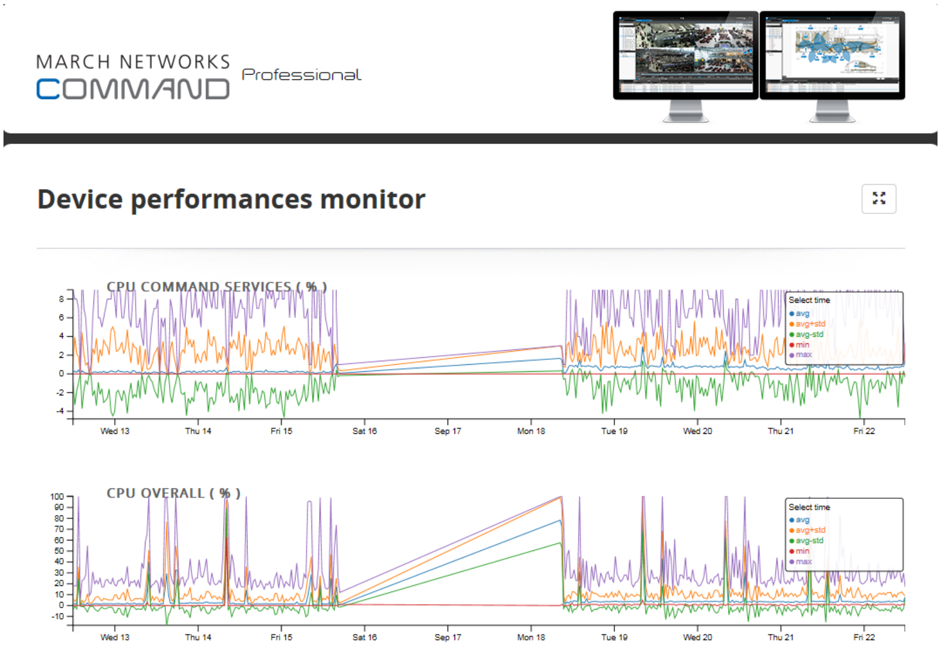
- On the Command Config main page, under **System Monitoring**, click **Statistics Dashboard**. A new browser window opens.

2 When prompted, log on to the Command Recording Software with a valid **User** name and **Password**.

Note: The **System Overview** permission must be assigned to your user profile to access the page. For more information, see “Assigning Permissions Over Command Recording Software Features” on page 81.

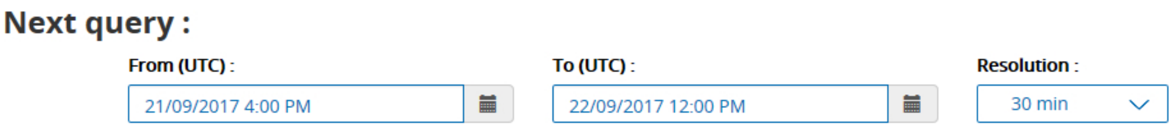
The **System Overview** page appears showing charts about the CPU and memory usage.

3 Click the ⛶ button to resize the web page.



To perform a query and manage charts

1 To specify the query start time and date, click the 📅 button in the **From (UTC)** field.



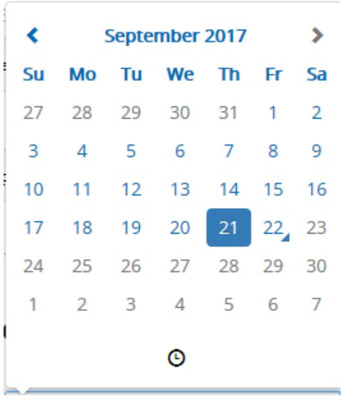
Next query :

From (UTC) : 21/09/2017 4:00 PM

To (UTC) : 22/09/2017 12:00 PM

Resolution : 30 min

The date selector appears.

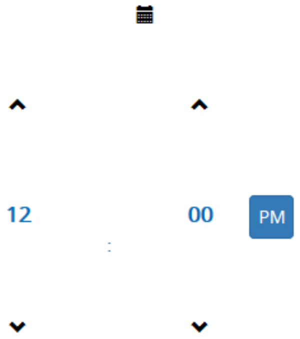


‹ September 2017 ›

Su	Mo	Tu	We	Th	Fr	Sa
27	28	29	30	31	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
1	2	3	4	5	6	7

2 Select the starting date and click the 🕒 button.

The time selector appears.

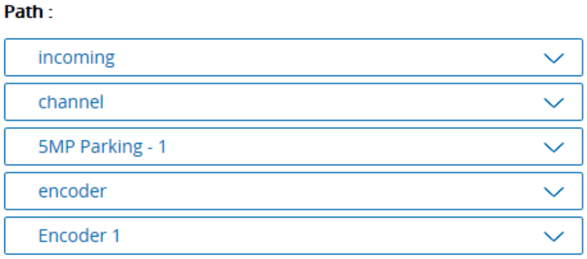


3 Select the starting time and click anywhere to close the date and time selector.

4 Click the 📅 button in the **To (UTC)** field to select the ending time and date.

5 Select the data granularity from the **Resolution** list.

6 Select the type of chart you want to display from the **Path** list. According to the number of options selected, different charts are displayed.


Path :

incoming

channel

5MP Parking - 1

encoder

Encoder 1

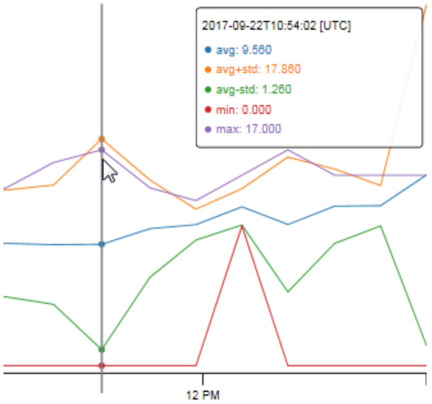
The different charts are described in the following table.

Chart	Path	Description
Incoming - All Video Channels	Incoming -> Query	These charts display statistics about the incoming **Video**, **Audio**, **Metadata**, **Shadow Archive**, and **Recovery** data for all of the video channels.
Incoming - All Encoding Profiles of a Video Channel	Incoming - Channel - <Videoch.> -> Query	These charts display statistics about the incoming **Audio**, **Metadata**, and **Shadow Archive** for all of the encoding profiles of the selected video channel.
Incoming - Encoding Profile of a Video Channel	Incoming - Channel - <Videoch.> - <Encoder> -> Query	These charts display statistics about the incoming **Bitrate** and **Frame Rate** for the selected encoding profile.
Usage	Usage -> Query	This chart displays statistics about the outcoming data (from the Command Recording Software to clients).

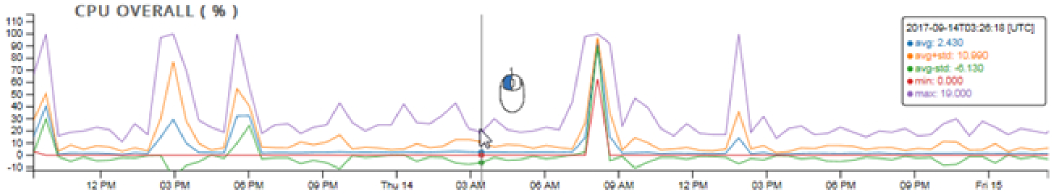
Chart	Path	Description
Recording - All Video Channels	Recording -> Query	This chart displays statistics about the amount of data (in KB/s) recorded by the Command Recording Software.
Recording - Partition of a Storage Group	Recording - Group - <Storagegr.> - Partition - <P.name> -> Query	These charts display statistic about the amount of data (in KB/s) recorded by a partition of a storage group on the Command Recording Software and the recording latency.
Recording - Video Channel	Recording - Channel - <Videoch.> - Sector - <Sectornum.> ->Query	These charts display statistic about the amount of data (in KB/s) recorded on a sector for a video channel and the archive retention time for that sector.
System	System - Info	Displays the amount of RAM installed on the server.

7 You can perform the following actions on the charts:

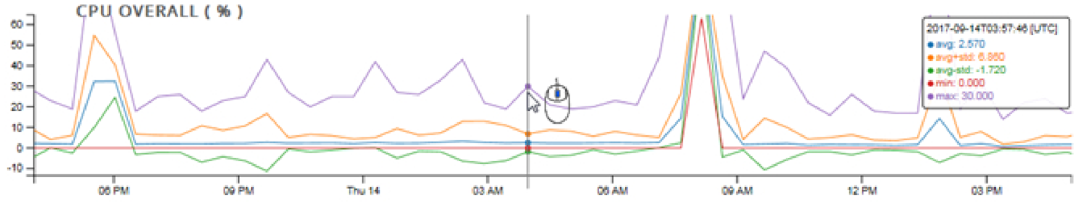
- Move the mouse cursor on the chart to display the values corresponding to the cursor position.



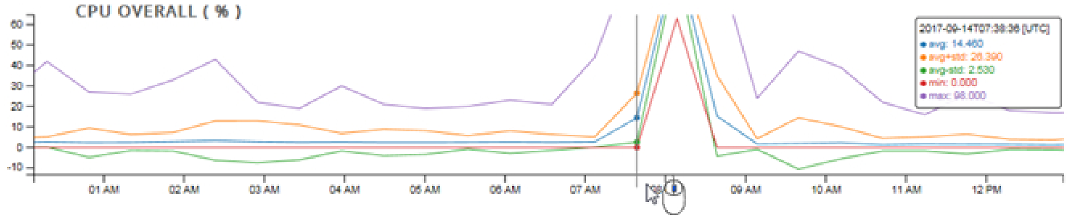
- To move a chart, click anywhere on the chart and drag the mouse.



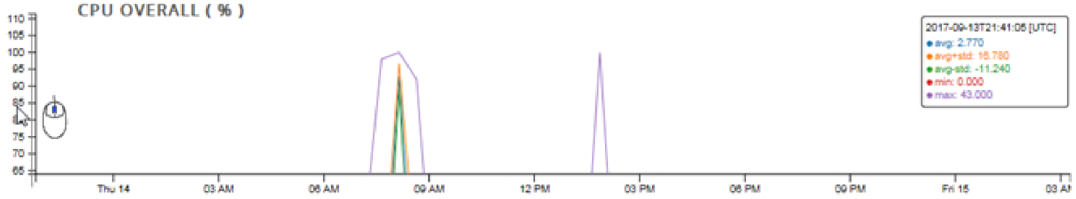
- To zoom a chart, move the mouse cursor on the chart and roll the mouse wheel.



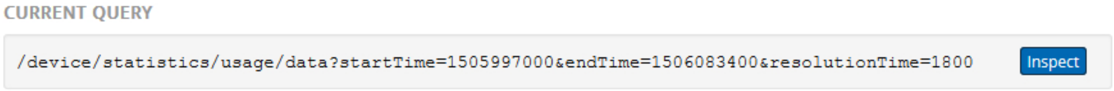
- To modify the scale for the horizontal axis, move the mouse cursor on the axis and roll the mouse wheel.



- To modify the scale for the vertical axis, move the mouse cursor on the axis and roll the mouse wheel.



8 Click **Inspect** to open a new tab containing raw data. You can then select and copy the data, and then import them in an Excel sheet.



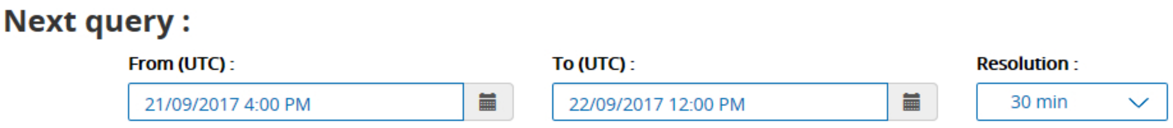
CURRENT QUERY

`/device/statistics/usage/data?startTime=1505997000&endTime=1506083400&resolutionTime=1800`

Important Note: The page opens in a new tab inside the browser. Depending on the configuration, some browsers may block the new tab. For information, see the online help of your browser.

To download an offline copy of the charts

1 To specify the query start time and date, click the 📅 button in the **From (UTC)** field.



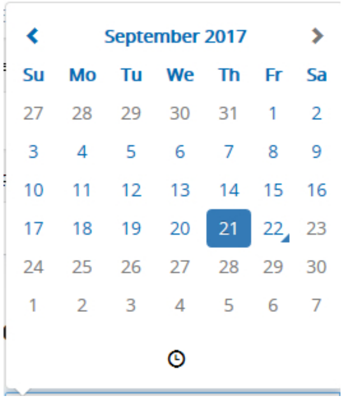
Next query :

From (UTC) : 21/09/2017 4:00 PM

To (UTC) : 22/09/2017 12:00 PM

Resolution : 30 min

The date selector appears.

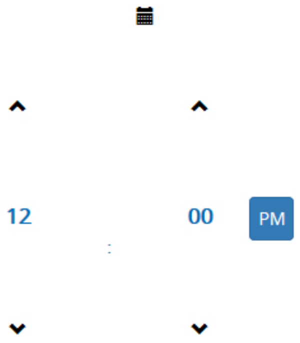


September 2017

Su	Mo	Tu	We	Th	Fr	Sa
27	28	29	30	31	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
1	2	3	4	5	6	7

2 Select the starting date and click the 🕒 button.

The time selector appears.



3 Select the starting time and click anywhere to close the date and time selector.

4 Click the 📅 button in the **To (UTC)** field to select the ending time and date.

5 Select the data granularity from the **Resolution** list.

6 Click the **Download** button.

The charts for the selected time frame are downloaded in .zip format. In case of issues you can either send the file to the March Networks Technical Support for analysis, or view it using the Google Chrome web browser.

To view the offline copy of the charts:

a Extract the zip archive in a directory of your choice.

b Open the Windows Command Processor (cmd.exe) and enter the following command line:

```
start chrome --allow-file-access-from-files
```

The Google Chrome web browser starts.

c Drag the index.html file from the folder to the Google Chrome window.

The offline version of the **Statistics Dashboard** page appears.

d Select the type of chart you want to display from the **Path** list, as described in the previous section (see “To perform a query and manage charts” on page 129).

Chapter 9

Creating Storage Groups

The **Storage Configuration** page allows you to manage the storage groups and the storage disks where your evidence is stored. This includes adding, removing, mounting, and configuring storage disks.

By default, the Command Recording Software has no storage disks configured. Before adding cameras and recording video evidence, you must configure one or more storage disks for the Command Recording Software.

Important Note: For more information about storage disposal, data encryption and privacy-related policies, download the *Data Protection and Privacy Application Note* from the March Networks Partner Portal.

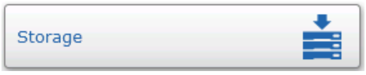
This chapter contains the following sections:

Creating Storage Groups

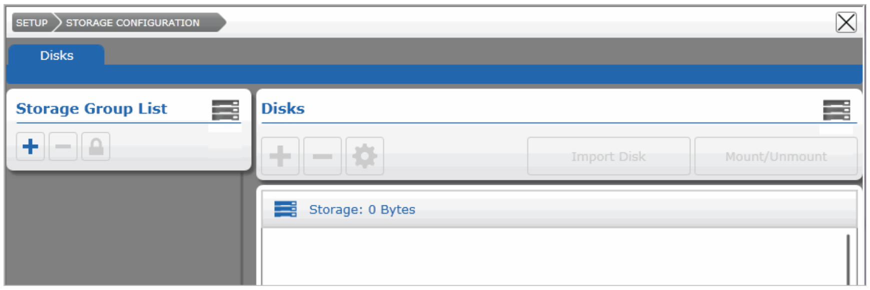
You can use storage groups to organize your storage disks. Storage groups are useful to decrease the workload of a storage disk.

To create a storage group

1 On the Command Config main page, under **Recording Management**, click **Storage**.



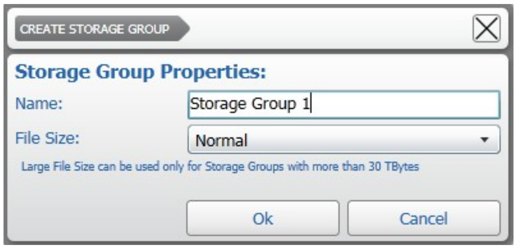
The **Storage Configuration** page appears.



Storage: 0 Bytes

2 In the **Storage Group List** section, click the + button to create a new group of storage disks.

The **Create Storage Group** dialog box appears.



Name: Storage Group 1

File Size: Normal

Large File Size can be used only for Storage Groups with more than 30 TBytes

3 Enter a custom name for the storage group.

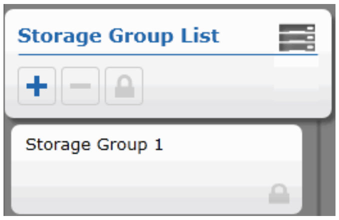
4 Select the storage group dimensions from the **File Size** list:

- Select **Normal** if the storage total dimensions are under 30TB.
- Select **Large** if the storage total dimensions are over 30TB.

Tip: This option allows much faster storage mounting and management times with large storage dimensions.

5 Click **Ok**.

The new storage group appears in the list.



Storage Group 1

6 Repeat step 2 to step 5 to create additional storage groups.

Note: You can delete a storage group, including all of the storage disks included in the group, by selecting it in the list and by clicking the − button or clicking the (**X**) button that appears in the upper right corner of the storage group. Command asks whether you want to delete the allocated disk space. The disk space contains all the video evidence stored on the disk. If you delete the disk space, the video evidence is deleted from the disk you are deleting as well.

Tip: You can also click the 🔒 button to lock the storage group and prevent any modification to it.

Adding or Importing Storage Disks

To ensure evidence is stored, you must add storage disks to storage groups by specifying the local or network disks on which you want to store evidence.

Important Notes:

- Command Recording Software can start recording on a storage group only after all of the disk added to the storage grouped have been mounted.
- It is recommended that you clean the storage disk before adding it to the Command Recording Software.

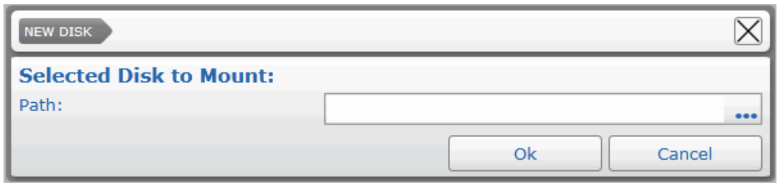
To add or import a storage disk

1 Click a storage group in the list.

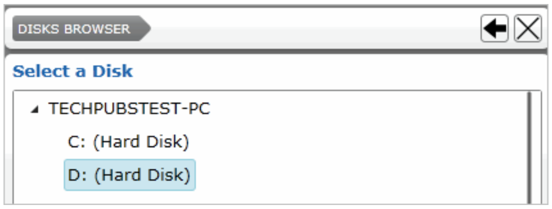
2 In the **Disks** section, click the + button.

Note: You can also click **Import Disk** to share a disk mounted on another Command Recording Software.

The **New Disk** dialog box appears.



3 Enter the disk **Path** (such as **D:\** or **\\networkdisk\Recording\**), or click the ... button to select a local disk from the **Disk Browser** dialog box.

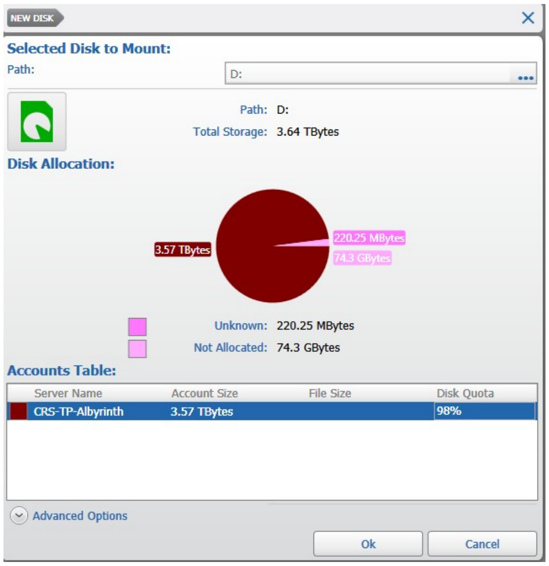


Notes:

- Do <u>NOT</u> mount the storage disk where the Command Recording Software is installed.
- For network disks, it is required to enter the disks credentials.

4 Click **Ok**.

The **Disk Properties** dialog box appears.



Selected Disk to Mount:

Path: D:

Path: D:

Total Storage: 3.64 TBytes

Disk Allocation:

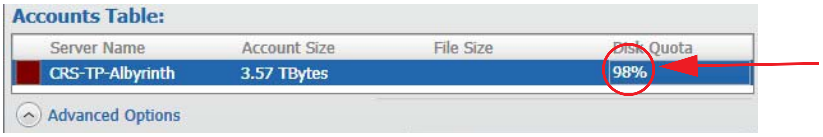
Unknown: 220.25 MBytes

Not Allocated: 74.3 GBytes

Accounts Table:

	Server Name	Account Size	File Size	Disk Quota
■	CRS-TP-Albyrinth	3.57 TBytes		98%

5 To modify the default disk allocation, select the disk in the **Accounts Table** section, and then click the **Disk Quota** value and enter a new allocation value for the disk. Press the **ENTER** key on your keyboard to confirm the changes.



Accounts Table:

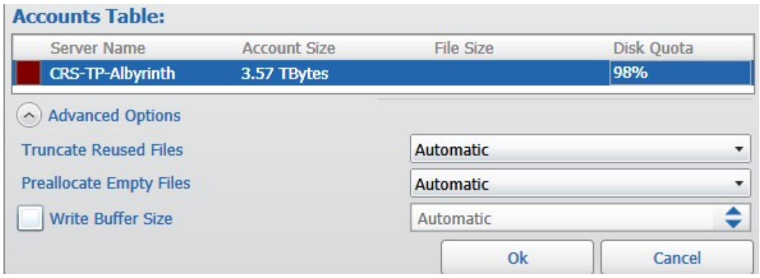
	Server Name	Account Size	File Size	Disk Quota
■	CRS-TP-Albyrinth	3.57 TBytes		98%

Notes:

- You must allocate more than 10 GB, otherwise Command cannot start recording.
- You can modify the disk allocation at any time by clicking the ⚙ button (see “Managing Storage Disks” on page 140).

6 (Optional) Click the **Advanced Options** button to configure how the CRS stores the video and data received from cameras, in particular to optimize the video archive on network storage.

Note: The **Advanced Options** must be configured by expert users. It is recommended that you contact the March Networks Technical Support before modifying the default configurations.



Accounts Table:

	Server Name	Account Size	File Size	Disk Quota
■	CRS-TP-Albyrinth	3.57 TBytes		98%

Truncate Reused Files: Automatic

Preallocate Empty Files: Automatic

□ Write Buffer Size: Automatic

7 The **Truncate Reused** file list allows you to select how the CRS allocates the new files when the storage disk is full.

Options include **Automatic** (the CRS automatically manages the file allocation), **True** (the CRS removes the contents of old files without deleting them - recommended for local storage), or **False** (the CRS overwrites the new files - recommended for network storage).

8 The **Preallocate Empty Files** file list allows you to select how the CRS allocates the storage space for the video archive according to the configured disk **Quota**.

Options include **Automatic** (the CRS automatically manages the space allocation), **True** (the CRS preallocates the storage space - recommended for local storage), or **False** (the CRS does not preallocate the storage space - recommended for network storage).

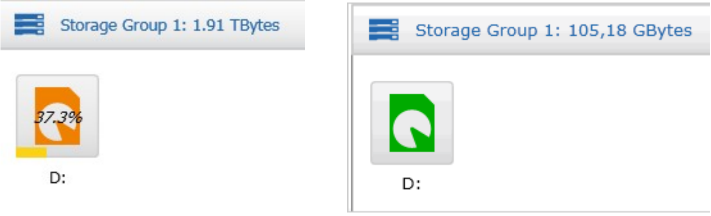
9 Select the **Write Buffer Size** check box and then enter or select a buffer value (in KB/s) to adjust the writing speed of data on the disc.

Notes:

- For local storage the write buffer is disabled and managed through the system cache, while for network storage the default buffer is 56 KB/s.
- The maximum allowed value is 512 KB/s.

10 Click **Ok**.

The disk icon appears in the **Storage Configuration** page. When the icon turns from orange to green the storage is available.



Note: Depending on the disk dimensions and the network status, this task could take several minutes.

11 To add additional storage disks, repeat step 1 to step 10.

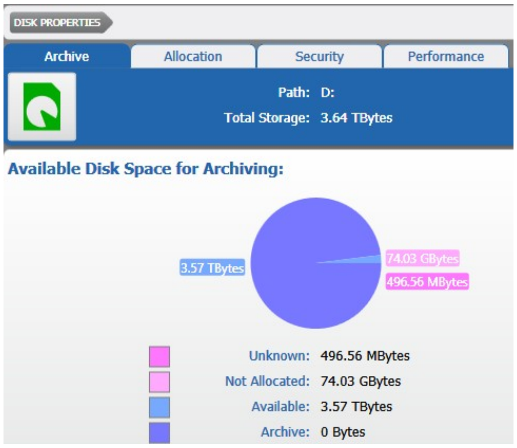
Managing Storage Disks

After adding a storage disk to Command, you can use the **Disk Properties** page to view a summary of the storage, allocate a particular amount of storage for the disk, manage the security settings, and review the disk's performance.

To manage a storage disk

1 Select a configured storage disk button and click the ⚙ button.

The **Disk Properties** dialog box appears. In the **Archive** tab you can view information about the available disk space.



Path: D:
Total Storage: 3.64 TBytes

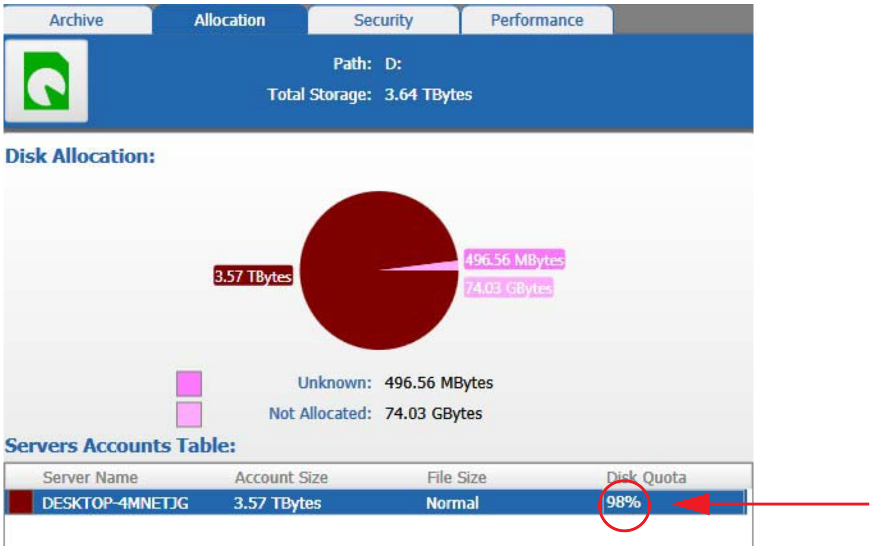
Available Disk Space for Archiving:

▨	Unknown:	496.56 MBytes
▨	Not Allocated:	74.03 GBytes
▨	Available:	3.57 TBytes
▨	Archive:	0 Bytes

2 Click the **Allocation** tab to modify the default disk allocation.

3 Select the disk in the **Server Accounts Table** section, and then click the **Disk Quota** value and enter a new allocation value for the disk. Press the **ENTER** key on your keyboard to confirm the changes.

Note: You can also modify the **Advanced Options** to configure how the CRS stores the video and data received from cameras, as described in "Adding or Importing Storage Disks" on page 137.



Path: D:
Total Storage: 3.64 TBytes

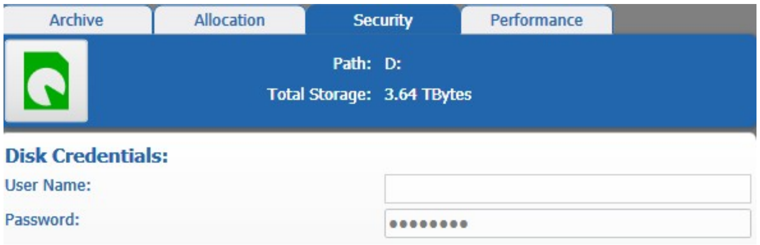
Disk Allocation:

▨	Unknown:	496.56 MBytes
▨	Not Allocated:	74.03 GBytes

Servers Accounts Table:

	Server Name	Account Size	File Size	Disk Quota
■	DESKTOP-4MNETJG	3.57 TBytes	Normal	98%

4 Click the **Security** tab to modify the credentials (**User Name** and **Password**) required to access the disk.



Path: D:

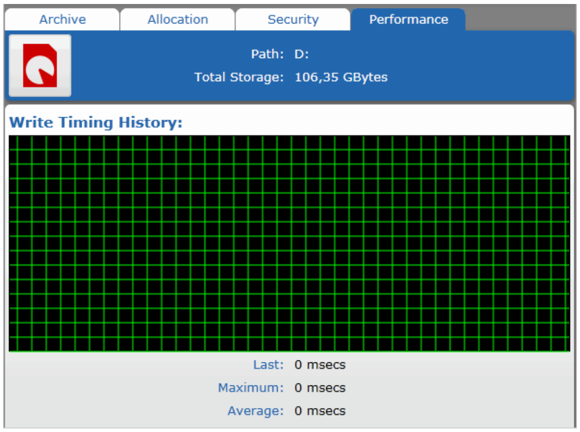
Total Storage: 3.64 TBytes

Disk Credentials:

User Name:

Password: ••••••••

5 Click the **Performance** tab to view real time graphics about the disk performance.



Path: D:

Total Storage: 106,35 GBytes

Write Timing History:

Last: 0 msecs

Maximum: 0 msecs

Average: 0 msecs

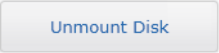
6 Click **Ok** to confirm the changes.

Disabling Storage Disks

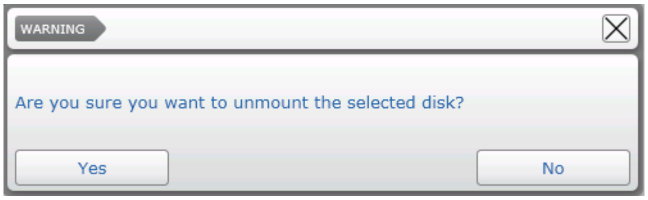
If you no longer need a configured storage disk but you do not want to permanently delete it, you can temporarily disable the disk.

To disable a storage disk

1 Select a configured storage disk and click **Unmount Disk**.



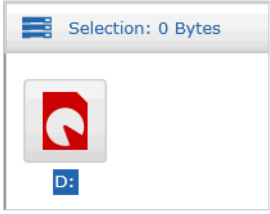
A **Warning** dialog box appears.



Are you sure you want to unmount the selected disk?

2 Click **Yes** to temporarily disable the storage disk.

The disk icon turns red.



3 You can re-enable the storage disk by clicking **Mount Disk**.

A confirmation window appears.

4 Click **Yes** to enable the storage disk.

The disk icon turns orange and then green.

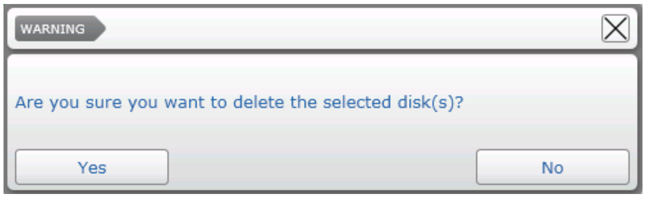
Deleting Storage Disks

If you no longer need a configured storage disk, you can delete the disk from the Command Recording Software.

To delete a storage disk

1 Select a configured storage disk button and click the − button.

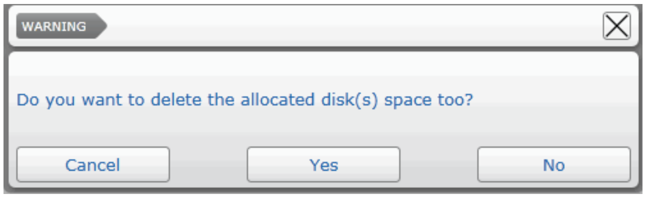
A **Warning** dialog box appears.



Are you sure you want to delete the selected disk(s)?

2 Click **Yes** to confirm the deletion of the storage disk.

A second **Warning** dialog box appears, asking whether you want to delete the disk space.



Do you want to delete the allocated disk(s) space too?

Note: The allocated disk space contains all the video evidence stored on the disk. If you delete the disk space, the video evidence is deleted from the disk you are deleting as well.

3 Click one of the following:

- **Yes** — Removes the video evidence from the disk.
- **No** — Maintains the video evidence on the disk.
- **Cancel** — Stops the deletion process.

Chapter 10

Managing Cameras with Command

You can add IP video channels to the Command Recording Software on the **Camera Configuration** page. You can add any March Networks IP camera or encoder to Command, as well as a number of compatible third-party and Onvif cameras. Using the E-Pass functionality, you can also add video channels from 3000/4000/8000 Series recorders and from a different Command recording platform (Command Recording Software, Command Lite, 7532 Hybrid NVR, and 6000 Series Hybrid NVR). You can also map additional encoding profiles, create and edit Onvif profiles, configure options about the video display quality, set privacy patches on the cameras, manage PTZ cameras, and save preset views and guard tours for PTZ cameras.

Notes:

- If you plan to add a third-party camera to Command, consult the *Supported Devices List* available on the March Networks Website (www.marchnetworks.com) in the Command Professional section. Multi-encoding is supported on March Networks IP cameras and on selected third-party cameras.
- Before you add Onvif-compliant cameras to the NVR, ensure that both the recorder and the cameras are set to the same time (an NTP server is recommended).
- If you are using a Command Enterprise server to manage configurations of the cameras added tot he Command Recording Software using the Mass Management feature, you must not add the same camera twice using its native protocol and the ONVIF protocol.
- Command Recording Software supports panomorph lenses and the ImmerVision Enables® technology. The **Panomorph** option in the **Settings** tab can be selected only if the camera mounts a registered panomorph lens. For more information, visit the ImmerVision Website (www.immervision.com) and see “Editing General Settings” on page 162**.**

  ImmerVision Enables and the ImmerVision Enables logo are trademarks of ImmerVision Canada Inc.
  Copyright 2000-2019 ImmerVision Canada Inc.

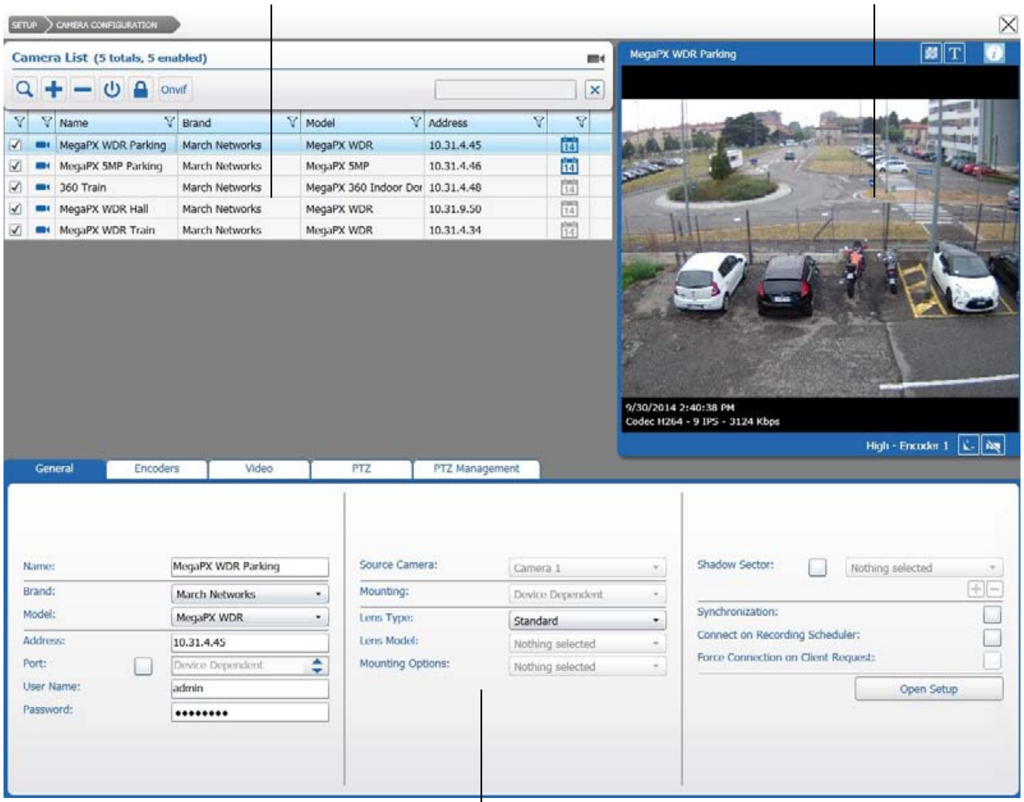
This chapter contains the following sections:

Overview

The **Camera Configuration** page allows you to add IP video channels to the Command Recording Software, add privacy patches to the images, and enable/configure PTZ cameras.

To access the page, on the Command Config main page, under **Device Management**, click **Cameras**.

The following image shows the **Camera Configuration** user interface.



Camera List (5 totals, 5 enabled)

		Name	Brand	Model	Address	
☑		MegaPX WDR Parking	March Networks	MegaPX WDR	10.31.4.45	14
☑		MegaPX 5MP Parking	March Networks	MegaPX 5MP	10.31.4.46	14
☑		360 Train	March Networks	MegaPX 360 Indoor Doı	10.31.4.48	14
☑		MegaPX WDR Hall	March Networks	MegaPX WDR	10.31.9.50	14
☑		MegaPX WDR Train	March Networks	MegaPX WDR	10.31.4.34	14

9/30/2014 2:40:38 PM
Codec H264 - 9 IPS - 3124 Kbps

Name: MegaPX WDR Parking
Brand: March Networks
Model: MegaPX WDR
Address: 10.31.4.45
Port: □ Device Dependent
User Name: admin
Password: ●●●●●●●●

Source Camera: Camera 1
Mounting: Device Dependent
Lens Type: Standard
Lens Model: Nothing selected
Mounting Options: Nothing selected

Shadow Sector: □ Nothing selected
Synchronization: □
Connect on Recording Scheduler: □
Force Connection on Client Request: □

The **Camera Configuration** page is divided into three main areas.

4 **Camera List** panel — Located at the top-left corner of the screen, it allows you to add, remove, filter, and select IP cameras.

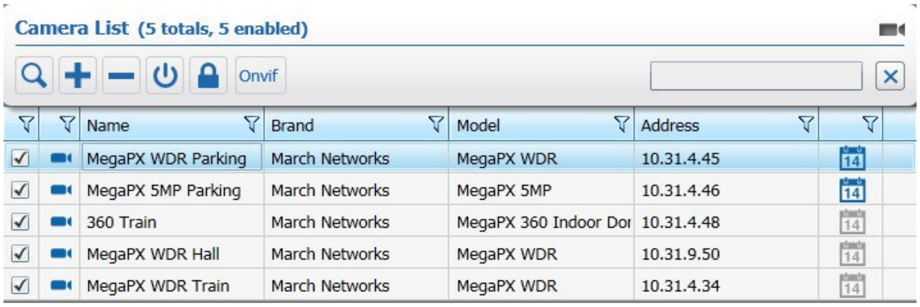
Note: A simplified version of this panel can be found also on the **Scheduler**, **Alarms**, and **Audio** pages.

5 **Video Preview** window — Located at the top-right corner of the screen, it displays the video stream of the currently selected camera.

6 **Settings** panel — Located at the bottom of the screen, it allows you to edit IP cameras, map encoding profiles, adjust video settings, and enable and configure PTZ cameras.

Camera List Panel

The **Camera List** panel is located at the top-left corner of the screen. You can add, remove, filter, and select IP cameras using the **Camera List** panel. A simplified version of this panel can also be found on the **Scheduler**, **Alarms**, and **Audio** pages.



Camera List (5 totals, 5 enabled)

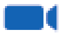
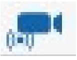
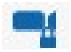
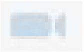
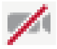
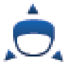
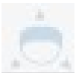
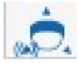
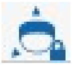
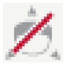
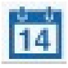
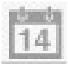
		Name	Brand	Model	Address	
☑		MegaPX WDR Parking	March Networks	MegaPX WDR	10.31.4.45	14
☑		MegaPX 5MP Parking	March Networks	MegaPX 5MP	10.31.4.46	14
☑		360 Train	March Networks	MegaPX 360 Indoor Doı	10.31.4.48	14
☑		MegaPX WDR Hall	March Networks	MegaPX WDR	10.31.9.50	14
☑		MegaPX WDR Train	March Networks	MegaPX WDR	10.31.4.34	14

The following table provides a description of the panel buttons.

Button	Action
🔍	Launches a Network Scan.
+	Adds an IP camera to the Command Recording Software.
−	Removes the selected IP camera from the Command Recording Software.
⏻	Enables/disables the selected cameras.
🔒	Locks the camera configuration.
□ ☒	Filters the camera list by entering text criteria.
▽	Filters data in a column.
☑	Enables/disables the selected camera.
Onvif	Opens the **Onvif Device Configurator**. **Note:** The button appears only if Onvif-compliant (profile S) cameras had been added to the Command Recording Software.

Camera List Panel Resources

The following resource icons appear in the **Camera List** panel:

Icon	Description
	Camera
	Camera - Audio enabled
	Camera - Locked
	Camera - Disabled
	Camera - Disconnected
	PTZ camera
	PTZ camera - Disabled
	PTZ camera - Audio enabled
	PTZ camera - Locked
	PTZ camera - Disconnected
	The camera is scheduled to record. **Note:** Hover the mouse pointer over the icon to view information about the recording schedule.
	The camera is not scheduled to record.

Filtering in the Camera Configuration Page

You can sort and filter the cameras by text or by column. See the following sections for more details:

- “Filtering by Text” on page 149
- “Sorting in Columns” on page 149
- “Filtering in Columns” on page 150

Filtering by Text

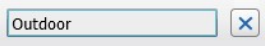
In the **Camera List** panel and in the **Camera Discovery** dialog box, you can filter for a text string. The filter applies to all columns in the list.

When the text box field is empty, there is no active search and all resources appear.

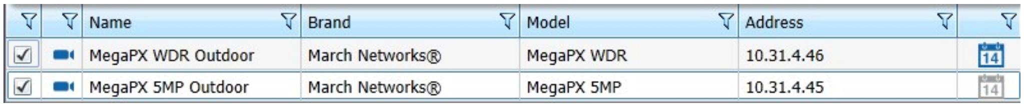
As you enter letters, characters, or numbers in the text box, the list automatically refreshes with the selected criteria.

To filter by text

1 On the **Camera List** panel or in the **Camera Discovery** dialog box, enter the filter criteria in the text box.



The list refresh to display only those cameras that correspond to the filter criteria.



		Name	Brand	Model	Address	
☑		MegaPX WDR Outdoor	March Networks®	MegaPX WDR	10.31.4.46	14
☑		MegaPX 5MP Outdoor	March Networks®	MegaPX 5MP	10.31.4.45	14

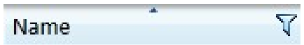
2 To remove the filter, click the ✕ button.

Sorting in Columns

You can alphabetically or numerically sort a column list (depending on the content of the list).

To sort in a column

1 Click on a column header to show the **Sort** ▴ icon.



2 Click the **Sort** icon to automatically sort the elements in the column list in ascending or descending alphabetical or numerical order.

Note: Click on the **Sort** icon again to change the order from ascending to descending or from descending to ascending.

Filtering in Columns

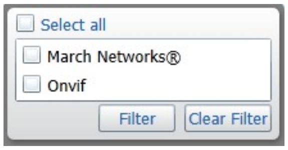
You can filter data in a column list to show only specified list values.

To filter in a column

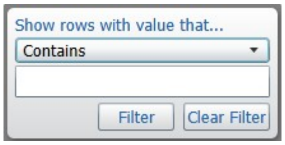
1 Select a column header and click the **Filter** icon.

The **Filter** dialog box appears. According to the selected column, you can apply filters by type or by text.

Filter by Type



Filter by Text



2 For columns filtered by type, do one of the following:

- Select one or more check boxes.
- Click the **Select all** box to select all column elements.

As you select a check box, the column list displays only those device details that match the specified filter criteria.

3 For columns filtered by text, do the following:

a Click the **Show rows with value that** drop-down list and select a filter expression.

Options include **Contains** and **Does not contain**.

b Enter a filter criteria in the text box.

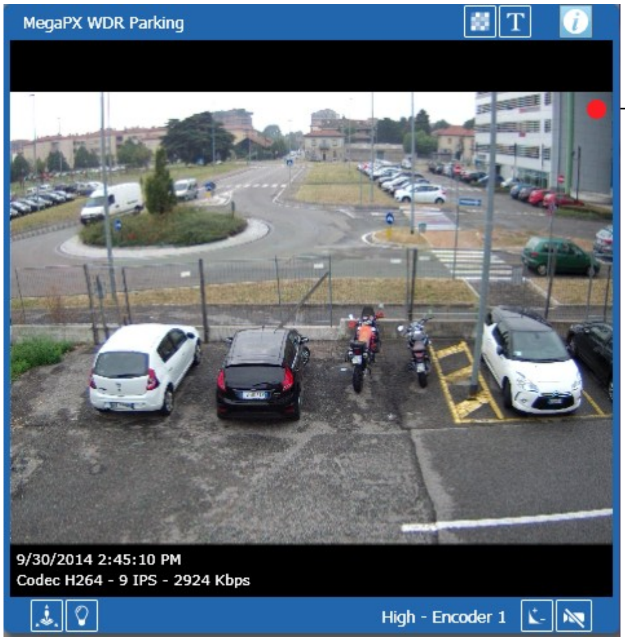
c Click **Filter** to apply the filter to the list.

The column list displays only those device details that match the specified filter criteria.

Tip: To remove the filter, click the **Filter** icon column, and then click **Clear Filter**.

Video Preview Window

The **Video Preview** window is located on the top-right corner of the **Camera Configuration** page and displays live video of the camera selected in the **Camera List** panel. If the Command Recording Software is currently recording the camera, the recording indicator appears on the window.



MegaPX WDR Parking

9/30/2014 2:45:10 PM
Codec H264 - 9 IPS - 2924 Kbps

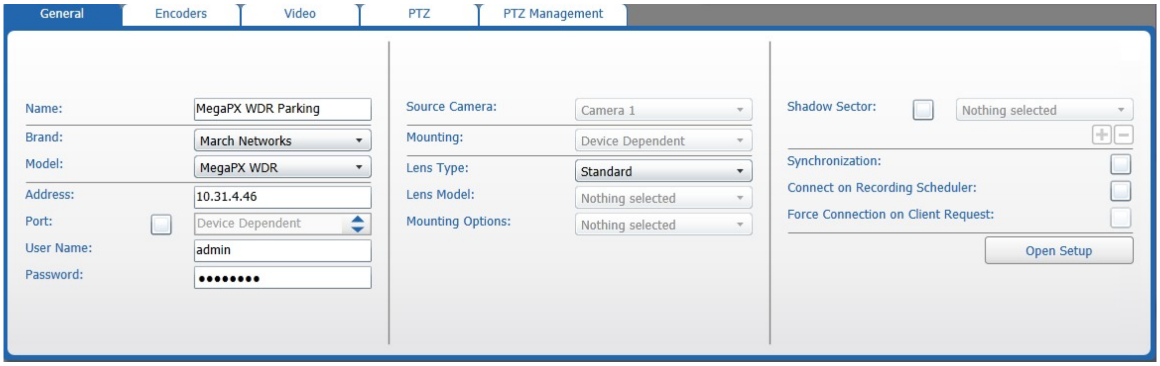
The following table describes the buttons available on the **Video Preview** toolbar.

Button	Action
▦	Hides privacy patches on the camera stream. **Note:** This is a local setting and it is not applied to the Command Recording Software.
T	Hides text overlay on the camera steam. **Note:** This is a local setting and it is not applied to the Command Recording Software.
i	Displays the encoding profile, frame rate and data rate on the camera stream. **Note:** This is a local setting and it is not applied to the Command Recording Software.
🕹	Opens the PTZ Control panel. **Note:** This icon is available for PTZ cameras only.
💡	Opens the PTZ Switches panel. **Note:** This icon is available for PTZ cameras with selected PTZ protocols only.
	Activates the wiper functionality. **Note:** This icon is available for PTZ cameras with selected PTZ protocols only.
Encoder 1	Opens the encoding profile selection list.
	Disable live video streaming to the **Video Preview** window for all of the available cameras.

Settings Panel

The **Settings Panel** is located at the bottom of the screen. You can manage and configure the video channels using the panel. The **Settings Panel** contains five tabs:

- **General** — where you can edit IP cameras and activate the Shadow Archiving functionality.

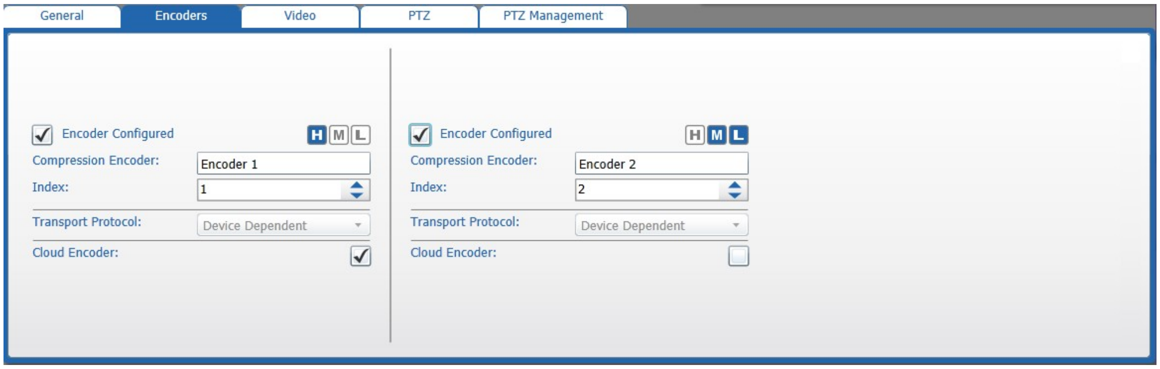


Name: MegaPX WDR Parking
Brand: March Networks
Model: MegaPX WDR
Address: 10.31.4.46
Port: □ Device Dependent
User Name: admin
Password: ••••••••

Source Camera: Camera 1
Mounting: Device Dependent
Lens Type: Standard
Lens Model: Nothing selected
Mounting Options: Nothing selected

Shadow Sector: □ Nothing selected
Synchronization: □
Connect on Recording Scheduler: □
Force Connection on Client Request: □

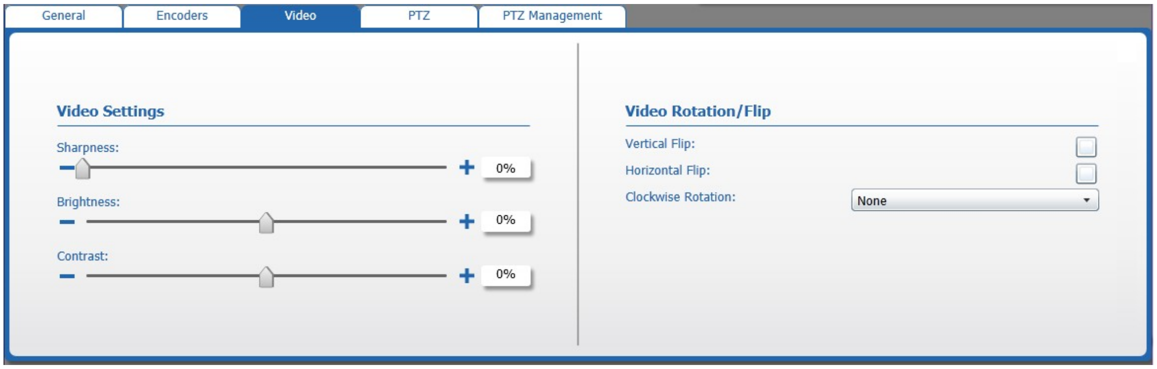
- **Encoders** — where you can configure the encoding profiles for the cameras added to the Command Recording Software, and send them to the March Networks Cloud service.



☑ Encoder Configured
Compression Encoder: Encoder 1
Index: 1
Transport Protocol: Device Dependent
Cloud Encoder: ☑

☑ Encoder Configured
Compression Encoder: Encoder 2
Index: 2
Transport Protocol: Device Dependent
Cloud Encoder: □

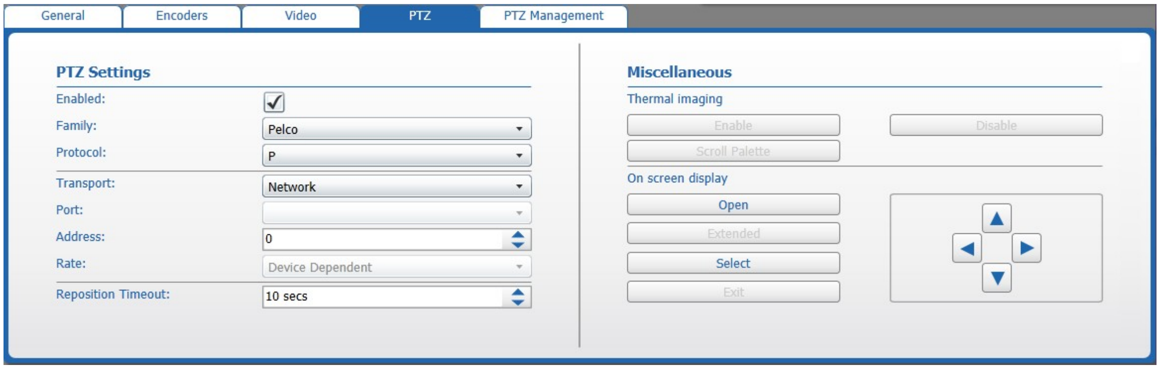
- **Video** — where you can adjust video settings for the video stream, and mirror/rotate the images.



Video Settings
Sharpness: 0%
Brightness: 0%
Contrast: 0%

Video Rotation/Flip
Vertical Flip: □
Horizontal Flip: □
Clockwise Rotation: None

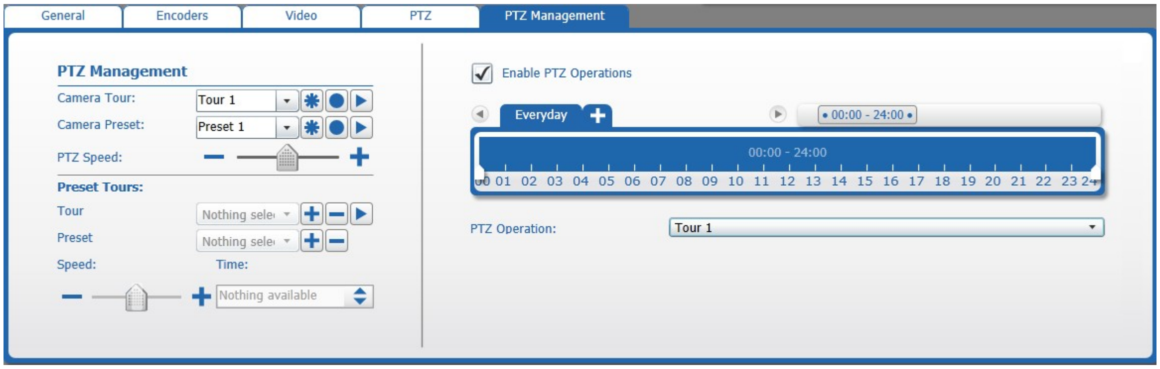
- **PTZ** — where you can enable the PTZ functionality, configure the PTZ protocol, and access advanced PTZ functionalities.



PTZ Settings
Enabled: ☑
Family: Pelco
Protocol: P
Transport: Network
Port:
Address: 0
Rate: Device Dependent
Reposition Timeout: 10 secs

Miscellaneous
Thermal imaging
On screen display

- **PTZ Management** — where you can configure preset, tour, preset tours, and schedule PTZ actions.



PTZ Management

Camera Tour: Tour 1

Camera Preset: Preset 1

PTZ Speed:

Tour: Nothing sele

Preset: Nothing sele

Speed:

Nothing available

☑ Enable PTZ Operations

• 00:00 - 24:00 •

PTZ Operation: Tour 1

Adding IP Cameras

The **Camera Configuration** page, allows you to add IP cameras to the Command Recording Software using the network discovery tool or manually entering their network parameters.

Select your configuration:

- “Adding IP Cameras Using the Network Discovery Tool” on page 154
- “Adding Cameras from a Different March Networks Recording Platform (E-Pass)” on page 157.
- “Manually Adding IP Cameras to Command” on page 160

Adding IP Cameras Using the Network Discovery Tool

The integrated network discovery tool allows you to scan your network for IP devices, such as March Networks IP cameras, encoders and recorders, Onvif-compliant devices, and several third party cameras. This tool lets you automatically configure network parameters, logon keys, and add multiple cameras to Command at the same time.

Important: You must enable the **SSDP Discovery** service on the server where the Command Recording Software service is running, to discover selected third party cameras using the UPNP protocol. For more information, see “Enabling the SSDP Discovery Service” on page 28.

Note: If you plan to add a third-party camera to Command, consult the consult the *Command: Supported Devices List* available on the March Networks Website in the Command Professional section.

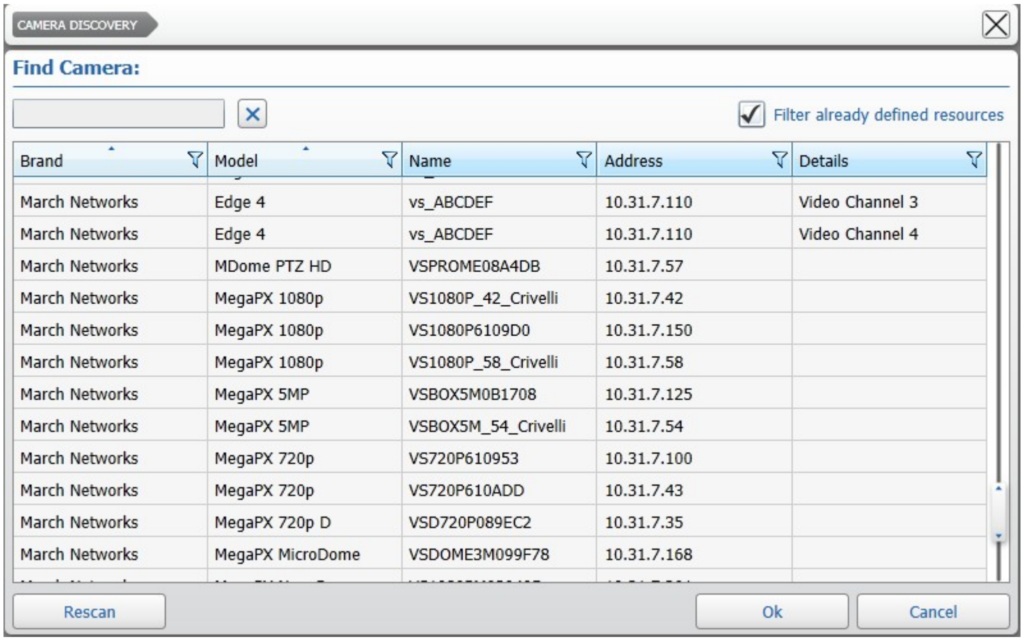
Using the network discovery tool, you can scan for devices and add:

- A single IP camera. For more information, see “To scan the network and add a single IP camera” on page 155.
- Multiple IP cameras. For more information, see “To scan the network and add multiple IP cameras” on page 156.

To scan the network and add a single IP camera

1 On the **Camera Configuration** page, click the 🔍 button in the **Camera List** panel to launch the network scan.

The scan results appear in the **Cameras Discovery** dialog box.



Brand	Model	Name	Address	Details
March Networks	Edge 4	vs_ABCDEF	10.31.7.110	Video Channel 3
March Networks	Edge 4	vs_ABCDEF	10.31.7.110	Video Channel 4
March Networks	MDome PTZ HD	VSPROME08A4DB	10.31.7.57	
March Networks	MegaPX 1080p	VS1080P_42_Crivelli	10.31.7.42	
March Networks	MegaPX 1080p	VS1080P6109D0	10.31.7.150	
March Networks	MegaPX 1080p	VS1080P_58_Crivelli	10.31.7.58	
March Networks	MegaPX 5MP	VSBOX5M0B1708	10.31.7.125	
March Networks	MegaPX 5MP	VSBOX5M_54_Crivelli	10.31.7.54	
March Networks	MegaPX 720p	VS720P610953	10.31.7.100	
March Networks	MegaPX 720p	VS720P610ADD	10.31.7.43	
March Networks	MegaPX 720p D	VSD720P089EC2	10.31.7.35	
March Networks	MegaPX MicroDome	VSDOME3M099F78	10.31.7.168	

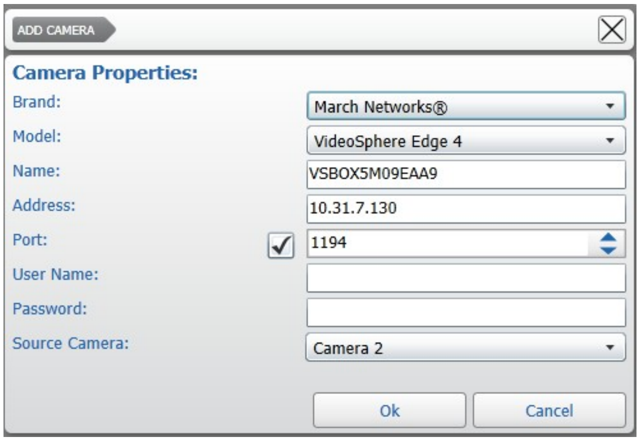
Tip: Click **Rescan** to refresh the results.

2 If the list of scan results is large, you can filter it by text or by column or sort the result by column. For more information, see “Filtering in the Camera Configuration Page” on page 149.

Tip: To filter the cameras already added to the Command Recording Software, select the **Filter already defined resources** check box.

3 Select an available device and click **Ok**.

The **Add Camera** dialog box appears.



Brand:	March Networks®
Model:	VideoSphere Edge 4
Name:	VSBOX5M09EAA9
Address:	10.31.7.130
Port:	☑ 1194
User Name:	
Password:	
Source Camera:	Camera 2

4 Check the device settings and enter the credentials (**User Name** and **Password**) required to access the video stream.

5 If the video stream belongs to a device capable of multiple channels (for example an Edge 4 encoder), select the video channel you want to add from the **Source Camera** list.

6 Click **OK** to add the camera.

The camera appears in the **Camera List** panel.

Note: You can rename the camera by holding the mouse button on the camera's name in the panel. After typing the new name, press **ENTER** to confirm.

7 Repeat step 1 to step 6 to add additional cameras to Command.

8 Click the 💾 button to save and apply the changes.

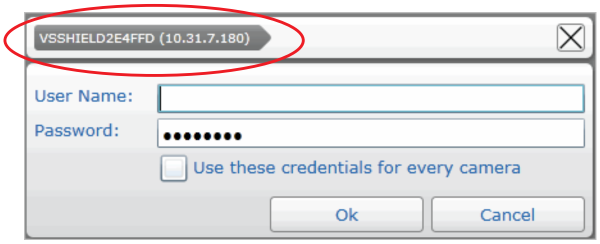
To scan the network and add multiple IP cameras

1 On the **Camera Configuration** page, perform a network scan as described in "To scan the network and add a single IP camera" on page 155.

2 Select multiple cameras by pressing the **CTRL** key and clicking additional cameras. You can select a camera from a single device, or you can expand additional devices and select cameras from multiple devices.

3 Click **Ok**.

The **Credentials** dialog box appears. In the upper left corner of the window you can read the device name and IP address.



VSSHIELD2E4FFD (10.31.7.180)

User Name:

Password: ••••••••

□ Use these credentials for every camera

4 Enter the credentials (**User Name** and **Password**) required to access the device.

5 Clear the **Use these credentials for every camera** check box and click **Ok**.

Note: You can only select this option if every device shares the same credentials.

6 Enter the credentials for the other devices as they appear on the screen.

All of the selected cameras are added simultaneously to Command.

7 Click the 💾 button to save and apply the changes.

Adding Cameras from a Different March Networks Recording Platform (E-Pass)

Command allows you to add video channels from a different Command Recording Software, or analog and IP cameras from 6700 Series, 8000 Series, 9000 Series, RideSafe, RideSafe GT, and RideSafe RT recorders. By doing so, the Command Recording Software can work as a backup machine for other March Networks recording platforms.

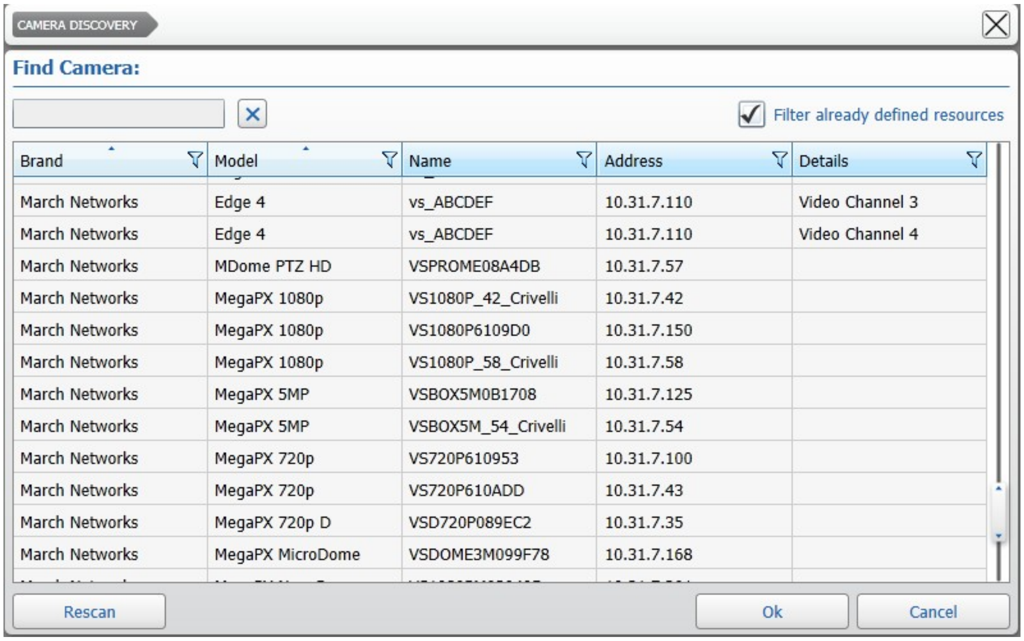
Important Notes:

- 6400 Series Hybrid NVRs are recognized as **6000 Series** model, while 6700 Series Hybrid NVRs are recognized as **Command Recording Software/7000 Series** model.
- This section is only applicable if all of your recording platforms in the system have been upgraded to the latest software version.

To add cameras from a different March Networks recording platform

1 On the **Cameras Configuration** page, click the 🔍 button to launch the network scan.

The scan results appear in the **Cameras Discovery** dialog box.



Brand	Model	Name	Address	Details
March Networks	Edge 4	vs_ABCDEF	10.31.7.110	Video Channel 3
March Networks	Edge 4	vs_ABCDEF	10.31.7.110	Video Channel 4
March Networks	MDome PTZ HD	VSPROME08A4DB	10.31.7.57	
March Networks	MegaPX 1080p	VS1080P_42_Crivelli	10.31.7.42	
March Networks	MegaPX 1080p	VS1080P6109D0	10.31.7.150	
March Networks	MegaPX 1080p	VS1080P_58_Crivelli	10.31.7.58	
March Networks	MegaPX 5MP	VSBOX5M0B1708	10.31.7.125	
March Networks	MegaPX 5MP	VSBOX5M_54_Crivelli	10.31.7.54	
March Networks	MegaPX 720p	VS720P610953	10.31.7.100	
March Networks	MegaPX 720p	VS720P610ADD	10.31.7.43	
March Networks	MegaPX 720p D	VSD720P089EC2	10.31.7.35	
March Networks	MegaPX MicroDome	VSDOME3M099F78	10.31.7.168	

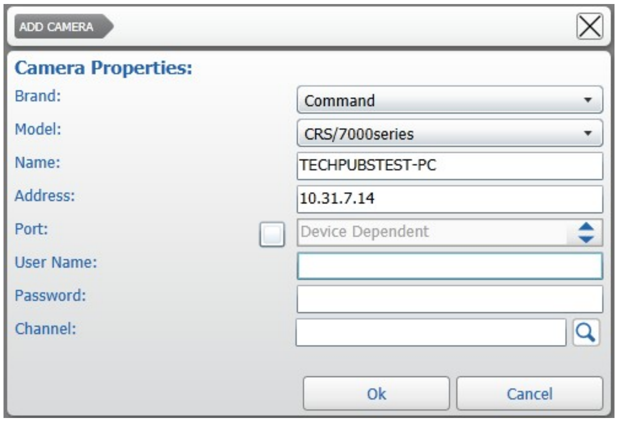
2 On the **Model** column header, click the **Filter** ▽ icon.

3 Select the **Command Recording Software/7000 Series, 6000 Series**, and/or the **R5** check boxes**.**

The results are instantly filtered.

4 Select the recording platform where the camera has been added and click **Ok**.

The **Add Camera** dialog box appears.



Camera Properties:

Brand: Command

Model: CRS/7000series

Name: TECHPUBSTEST-PC

Address: 10.31.7.14

Port: □ Device Dependent

User Name:

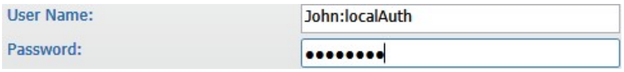
Password:

Channel:

5 Select the **Port** check box to specify a communication port, if required.

6 In the **User Name** text box, do one of the following:

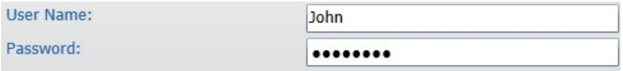
- If you are adding a camera from a CRS or a 6700 Series recorder registered to a Command Enterprise Server, enter the username of a Command Enterprise user account.
- If you are adding a camera from a 8000 Series, 9000 Series or RideSafe recorder registered to a Command Enterprise Server, use the following syntax: *<CESuser>:localAuth*. For example, if the CES username is John: **John:localAuth**
- If the other recording platform is <u>not</u> registered on a Command Enterprise Server, enter the username of a local user account.



User Name: John:localAuth

Password: •••••••••

Visual Intelligence NVR Registered on a Command Enterprise Server



User Name: John

Password: ••••••••

Visual Intelligence NVR <u>Not</u> Registered on a Command Enterprise Server

7 Enter the **Password for the user account**.

Note: If the recording platform is registered to a Command Enterprise Server, you must use the password of the CES user account.

8 In the **Channel** text box, click the 🔍 button to connect to the Command Recording Software/NVR and download the list of available video channels.

After a few moments, the list of available video channels appears.

9 Select the video channel you want to add or select multiple cameras by pressing the **CTRL** key and clicking additional cameras.

10 Click **Ok** to add the cameras to Command.

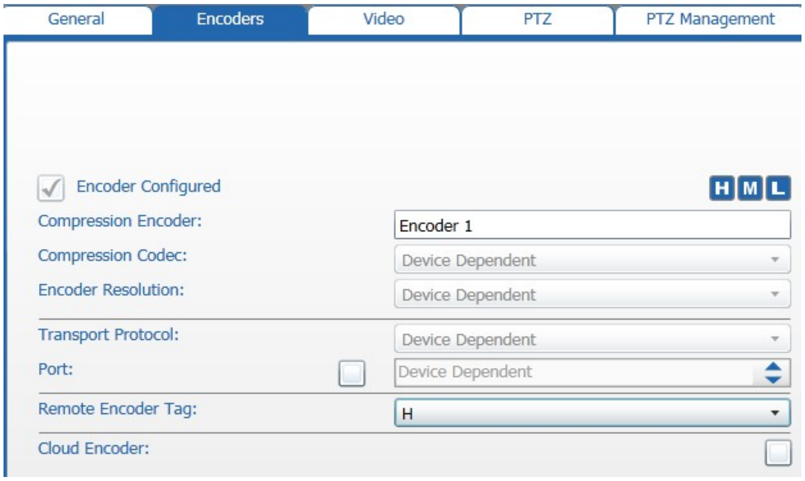
The cameras appear in the **Camera List** panel.

Note: You can rename the cameras by holding the mouse button on the cameras' name in the panel. After typing the new name, press **ENTER** to confirm.

11 Click the 💾 button to save and apply the changes.

12 Select the camera you just added from the **Camera List** panel.

13 Click the **Encoders** tab.



☑ Encoder Configured

Compression Encoder:	Encoder 1
Compression Codec:	Device Dependent
Encoder Resolution:	Device Dependent
Transport Protocol:	Device Dependent
Port: □	Device Dependent
Remote Encoder Tag:	H
Cloud Encoder:	□

14 Select the encoding profile you want to record from the **Remote Encoder Tag** list.

The **H**, **M**, and **L** options correspond to the tags assigned on the Command Recording Software/NVR.

Important Note: For Visual Intelligence Recorders (R5) the **H** option corresponds to the higher encoding profile and the **M** option to the lowest encoding profile (if enabled on the NVR). Select the **L** option to configure the NVR to send a static snapshot every five seconds.

15 Click the 💾 button to save and apply the changes.

16 Repeat step 1 to step 15 to add additional cameras from a different March Networks recording platform.

17 Click the 💾 button to save and apply the changes.

Manually Adding IP Cameras to Command

You can manually add IP cameras to Command by specifying network parameters.

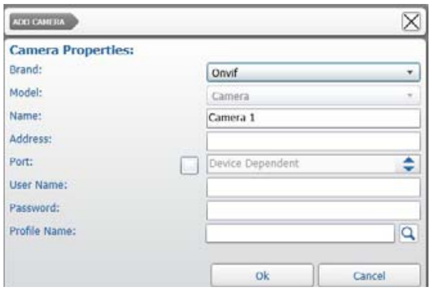
Notes:

- You must follow this procedure for third-party devices not recognized by the network discovery tool.
- For cameras added from a different March Networks recording platform (E-Pass), you must select **Command** from the **Brand** list and the type of recorder from the **Model** list. For more information about the E-Pass feature, see "Adding Cameras from a Different March Networks Recording Platform (E-Pass)" on page 157.

To manually add IP Cameras to Command

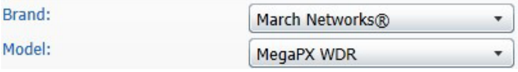
1 On the **Camera Configuration** page, click the + button.

The **Add Camera** dialog box appears.



Brand: Onvif
Model: Camera
Name: Camera 1
Address:
Port: □ Device Dependent
User Name:
Password:
Profile Name:

2 Select the device **Brand** and the **Model** from the applicable list.



Brand: March Networks®
Model: MegaPX WDR

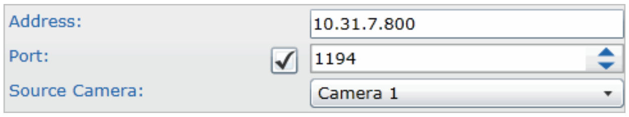
3 Enter a **Name** for the device.

4 Enter the IP **Address** of the device and select the **Port** check box to specify a communication port, if required.

5 Enter the credentials (**User Name** and **Password**) required to access the video stream.

6 To add a device that streams video from multiple connected cameras (such as an encoder, another Command Recording Software, or an NVR) select the video stream you want to add in the **Source Camera** list.

Note: If you are adding **Generic** devices, you must also enter the URL of the video stream in the **Source Url** text box.



Address: 10.31.7.800
Port: ☑ 1194
Source Camera: Camera 1

7 Click **Ok** to add the camera to Command.

The camera appears in the **Camera List** panel.

Note: You can rename the camera by holding the mouse button on the camera's name in the panel. After typing the new name, press **ENTER** to confirm.

8 Repeat step 1 to step 7 to add additional cameras to Command.

9 Click the 💾 button to save and apply the changes.

Editing IP Cameras

Most video stream configurations are device-dependent and must be applied directly from the setup interface of the IP camera. However, there are a number settings that you can configure on the **General** tab.

This section explains how to:

- Access The IP camera setup interface. For more information, see “Accessing the Setup Interface of an IP Camera” on page 161.
- Edit general setting for the camera, connection parameters, credentials, and the March Networks Cloud service. For more information, see “Editing General Settings” on page 162.
- Activate the Shadow Archiving feature. For more information, see “Activate and Manage Shadow Archive” on page 163.
- Activate the Connection On Demand feature. For more information, see “Activating the Connection on Demand Functionality” on page 168.

Note: The number and type of available settings are dependent on the brand and model of the device.

Accessing the Setup Interface of an IP Camera

The **Camera Configuration** page allows you to open the setup interface of a supported IP camera in a different tab of the browser.

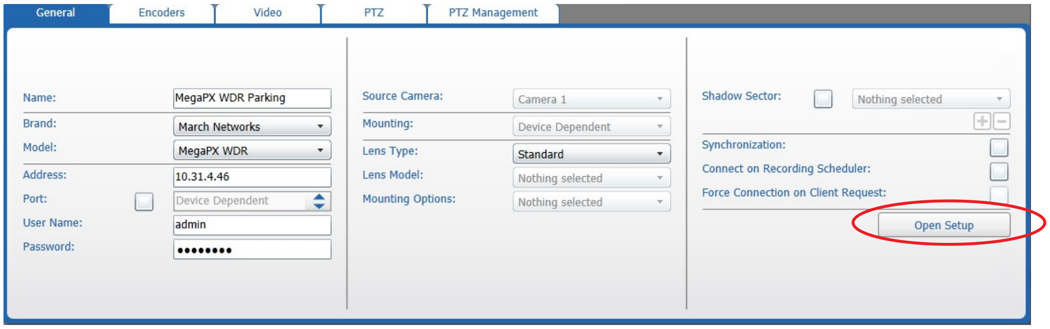
Notes:

- To access the setup interface of an IP camera, the user must possess the Device Tunneling permission. For more information, see “Assigning Permissions to User Profiles and User Groups” on page 79.
- The setup interface opens in a new tab inside the browser. Depending on the configuration, some browsers may block the new tab. For information, see the help online of your browser.
- The **Open Setup** button may have no effect on some third-party cameras, or may open a different interface. For example, on some Onvif-compliant cameras, the button opens the visualization interface, as the setup interface is reached through a different URL.
- For information about configuring a device using the setup interface, see the documentation accompanying the device. Some setup interfaces may require the use of a specific browser.

To access the IP camera setup interface

1. On the **Camera Configuration** page, select an IP camera in the **Camera List** panel.
2. Click the **General** tab.

3 Click **Open Setup**.



Name: MegaPX WDR Parking
Brand: March Networks
Model: MegaPX WDR
Address: 10.31.4.46
Port: □ Device Dependent
User Name: admin
Password: ••••••••
Source Camera: Camera 1
Mounting: Device Dependent
Lens Type: Standard
Lens Model: Nothing selected
Mounting Options: Nothing selected
Shadow Sector: □ Nothing selected
Synchronization: □
Connect on Recording Scheduler: □
Force Connection on Client Request: □

The setup interface for the IP camera appears.

Editing General Settings

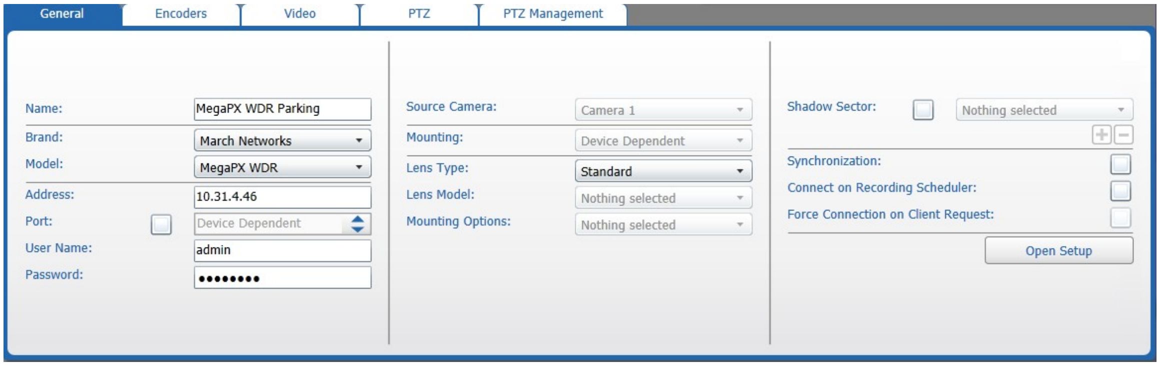
The **General** tab allows you to modify the details (including connection parameters and credentials) of an added IP camera.

Note: The **Panomorph** option in the **General** tab can be selected only if the camera mounts a registered panomorph lens. For more information, visit the ImmerVision Website (www.immervision.com).

To edit the general settings

1 On the **Camera Configuration** page, select a camera in the **Camera List** panel.

2 Click the **General** tab.

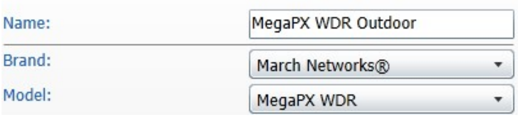


Name: MegaPX WDR Parking
Brand: March Networks
Model: MegaPX WDR
Address: 10.31.4.46
Port: □ Device Dependent
User Name: admin
Password: ••••••••
Source Camera: Camera 1
Mounting: Device Dependent
Lens Type: Standard
Lens Model: Nothing selected
Mounting Options: Nothing selected
Shadow Sector: □ Nothing selected
Synchronization: □
Connect on Recording Scheduler: □
Force Connection on Client Request: □

3 Enter a new custom name for the video channel in the **Name** field.

Tip: You can also rename a camera by double-clicking the **Name** field or by pressing the **F2** key in the **Camera List** panel.

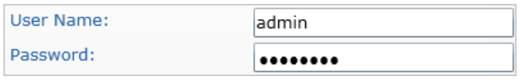
4 Select the device **Brand** and the **Model** from the applicable list.



Name: MegaPX WDR Outdoor
Brand: March Networks®
Model: MegaPX WDR

5 Edit the IP **Address** of the device and select the **Port** check box to select a communication port, if required.

6 Edit the credentials (**User Name** and **Password**) required to access the video stream, if required.



User Name:	admin
Password:	••••••••

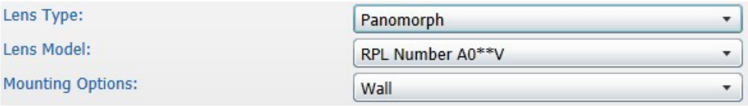
7 If the device streams video from multiple connected cameras, select an available video stream from the **Source Camera** list.

8 For selected third party cameras, select the camera's mounting position from the **Mounting** list.

9 (Optional) If panomorph lenses are installed on the camera, do the following:

a Select the **Panomorph** option from the **Lens Type** list.

The **Lens Model** and **Mounting Options** lists appear.



Lens Type:	Panomorph
Lens Model:	RPL Number A0**V
Mounting Options:	Wall

b Select the **Lens Model** from the list, if available.

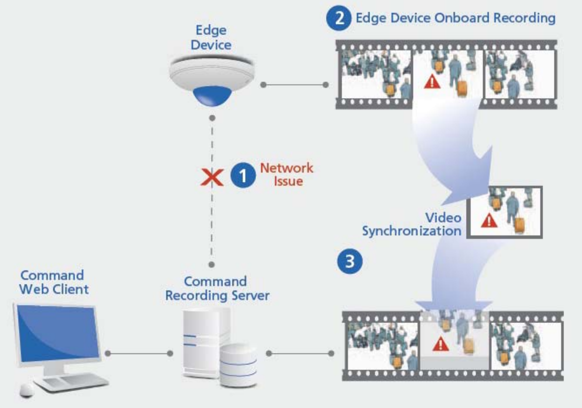
c Select the camera installation mode from the **Mounting Options** list.

Options include **Wall**, **Ceiling**, and **Ground**.

10 Click the 💾 button to save and apply the changes.

Activate and Manage Shadow Archive

The Shadow Archive™ is a feature that allows you to manage the local storage (for example SD cards) of a device by activating the shadow sector. Adding the shadow sector of a camera to Command allows you to manage the local storage of a device as part of Command Recording Software. It also allows you to activate automatic synchronization between the configured storage and the device's local storage.



Important Notes:

- You must activate local or direct recording by accessing the Web Setup interface of the device before enabling the Shadow Archive feature on Command. You must also synchronize the Command Recording Software date and time to the device. For optimal performance with the synchronization feature, it is recommended that you follow the guidelines included in the documentation (Configuration Guide and Release Notes) accompanying the device.
- The Shadow Archive technology is available on every March Networks edge device and on selected legacy edge devices.
- For ME4 cameras, it is strongly recommended that you configure the Daylight Saving Time settings to allow the cameras to synchronize to the Command Recording Software. For more information, see the documentation accompanying your ME4 camera.
- You can also activate the Shadow Archive feature for redundant machines, allowing you to automatically recover the missing archive on a monitored Command Recording Software. For more information, see “Setting Redundant Machines” on page 260.

To activate Shadow Sector

1. On the **Camera Configuration** page, select a compatible IP camera in the **Camera List** panel.
2. Click the **General** tab.
3. Select the **Shadow Sector** check box to add the device’s Shadow Archive to Command.
4. Click the 💾 button to save and apply the changes.

   You can now access the video evidence archived on the camera’s local storage using SiteManager.

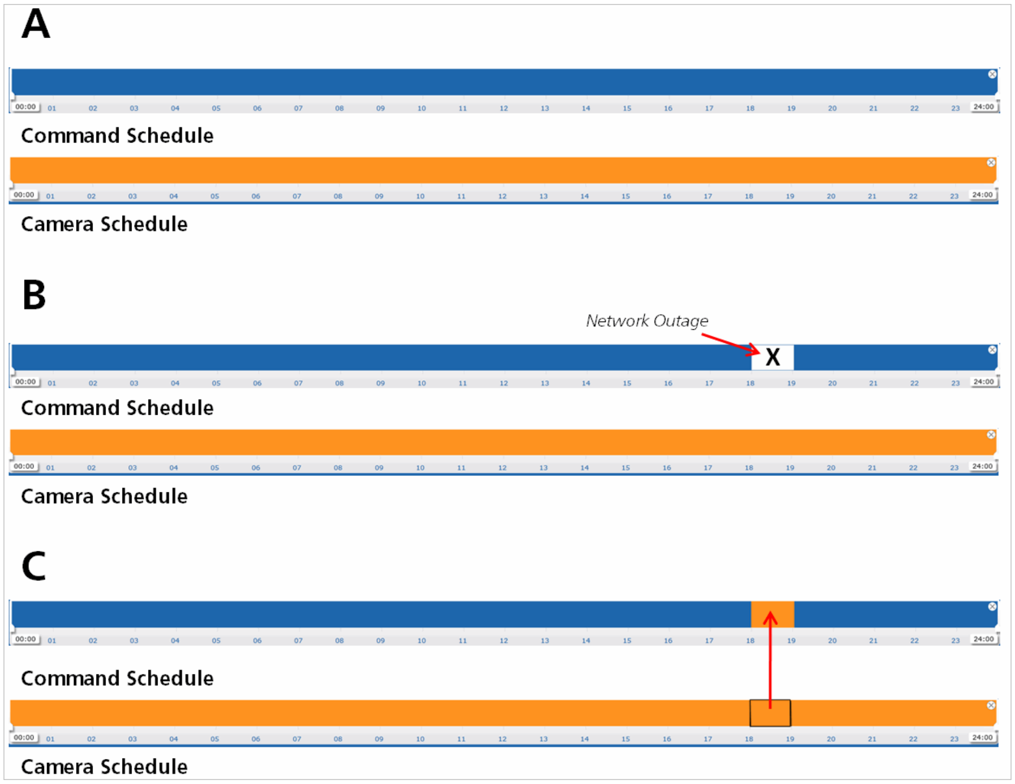
Activating the Automatic Synchronization Feature

After you activate the Shadow Archive on Command, you can configure the automatic synchronization feature. This feature allows Command to automatically recover missing video from the device after a network or server outage. When Command re-establishes its connection to the camera, it downloads the video evidence recorded by the camera during the outage.

For example: Command records video evidence from a camera 24 hours a day, and the camera is also set to record 24 hours a day on the onboard storage (**A**). Command cannot record from the camera from 6 P.M. to 7 P.M. due to a network outage, but the camera can and does continue recording (**B**). When the network connectivity is re-established, Command establishes a new connection to the camera and automatically recovers the missed video evidence from the camera for the 6-7 P.M. time interval (**C**).

Tip: March Networks cameras are also able to start recording after detecting a disconnection from the Command Recording Software server. For more information, see the specific camera’s documentation, available for download from the March Networks Partner Portal and official websites.

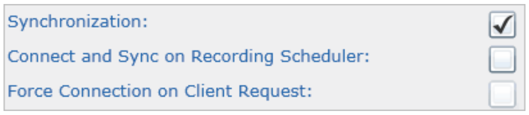
Automatic Synchronization



To activate the automatic synchronization feature

1 Add the Shadow Archive to Command as described in “To activate Shadow Sector” on page 164.

2 Select the **Synchronization** check box.



Synchronization: ☑
Connect and Sync on Recording Scheduler: ☐
Force Connection on Client Request: ☐

3 Click the 💾 button to save and apply the changes.

Command can now recover any missing video directly from the device after a network or server outage.

Activating Optional Synchronization Policies

In addition to automatic synchronization, Command offers two optional policies:

- **Connect and Sync on Recording Scheduler** policy
- **Force Connection on Client Request** policy

Important: You can also enable the two policies independently from the automatic synchronization feature to activate the **Connection-on-Demand** functionality. For more information, see “Activating the Connection on Demand Functionality” on page 168.

The **Connect and Sync on Recording Scheduler** policy interacts with the recording scheduler of Command, and allows you to limit the bandwidth usage on the network while a camera records 24 hours a day.

Note: It is recommended that you configure a valid recording schedule before activating this policy. This policy is applied to all of the recording schedules.

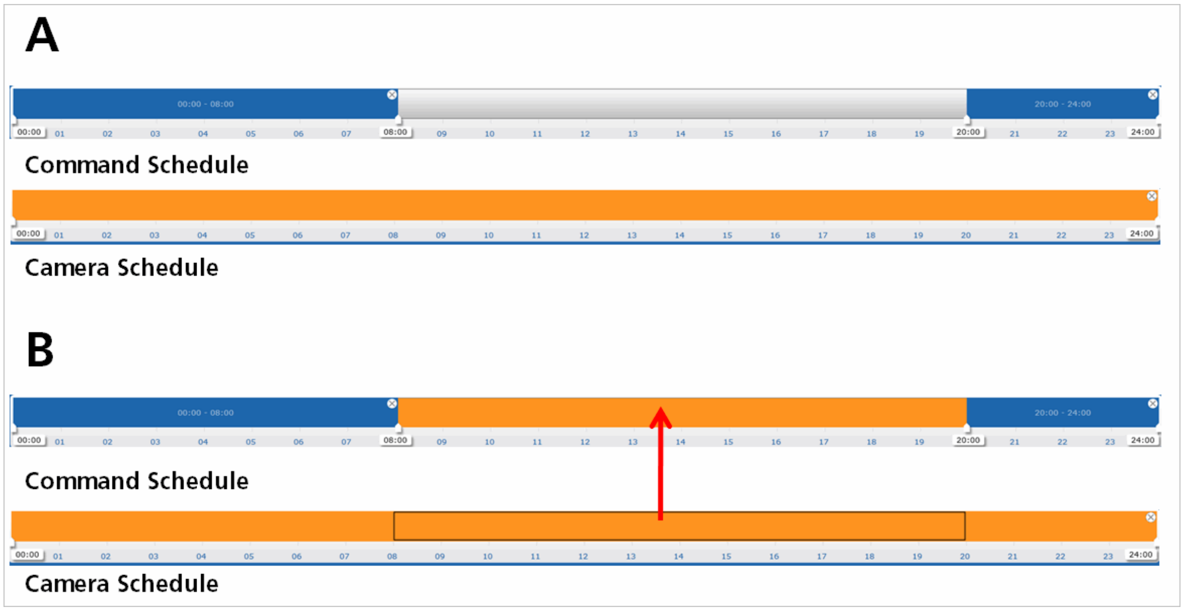
Important: When the **Connect and Sync on Recording Scheduler** policy is enabled and the **Force Connection on Client Request** policy is disabled, the Command Recording Software never connects to the camera outside of the schedule, including live viewing.

For example:

Command records video evidence from a camera from 8 P.M. to 8 A.M., but the camera is set to record 24 hours a day on the onboard storage (**A**). Command is connected to the camera only during the night, reducing bandwidth use during the day.

When the **Connect and Sync on Recording Scheduler** policy is enabled, Command automatically recovers the video evidence recorded by the camera during the day, after performing the connection to the camera at 8 P.M. (**B**). As a result, video for the whole day is available on Command even though Command was not connected to the camera between 8 A.M. and 8 P.M.

Connect and Sync on Recording Scheduler Policy



The **Force Connection on Client Request** policy interacts with client applications (such as Command Client and VideoSphere SiteManager) that connect to Command, and allows you to recover from the Shadow Archive only video evidence that has not been streamed to a client application. This policy is useful to avoid synchronizing not relevant video evidence already monitored by a user and to recover bandwidth and storage space. In addition, this policy is required to view live video outside of the recording schedule, and to force Command to instantly synchronize the video.

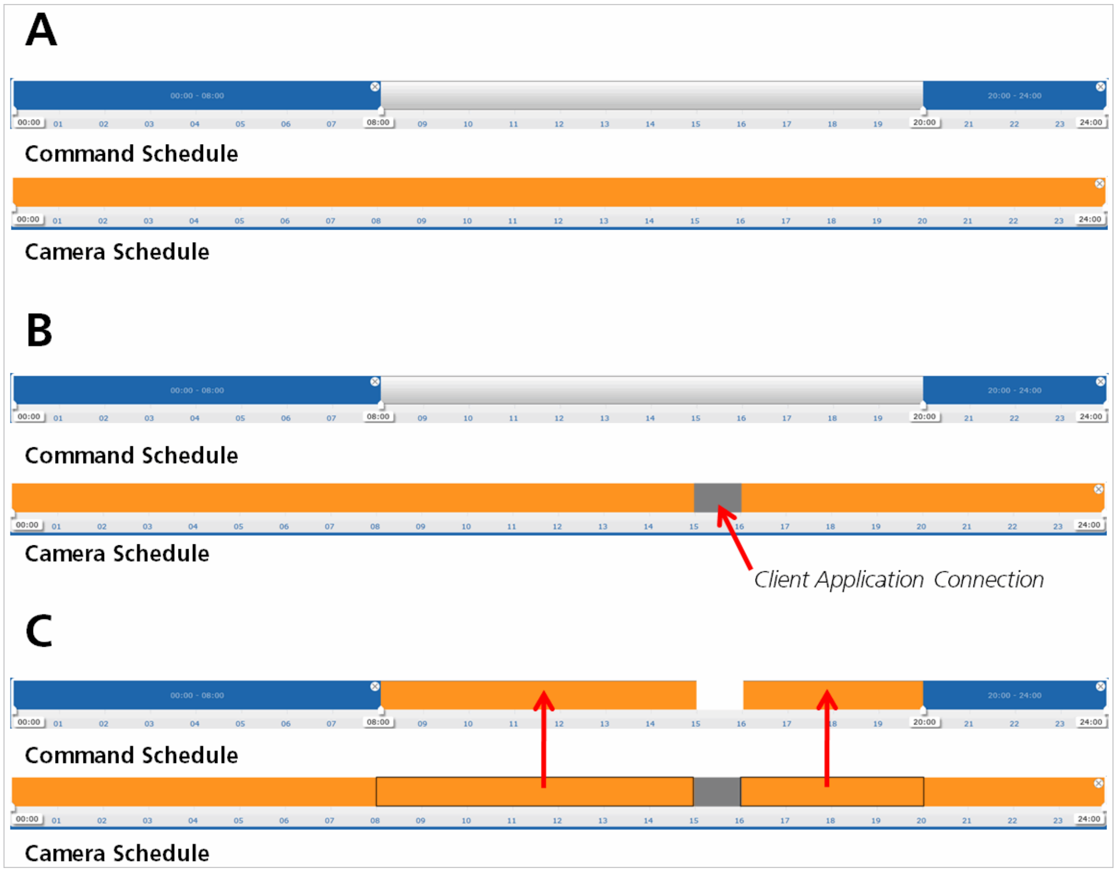
For example:

Command records video evidence from a camera from 8 P.M. to 8 A.M., but the camera is set to record 24 hours a day on the onboard storage and the **Connect and Sync on Recording Scheduler** policy has been enabled (**A**).

When the **Force Connection on Client Request** policy is enabled, Command detects when a client application requests live video from the camera, and instantly starts the video synchronization. Command also detects how long the client is connected to the camera and automatically excludes that video evidence from the automatic synchronization (**B**).

If a client application streamed live video from the camera from 3 P.M. to 4 P.M., Command automatically recovers the video evidence from the camera from 8 A.M. to 3 P.M. and from 4 P.M. to 8 P.M. (**C**).

Force Connection on Client Request Policy

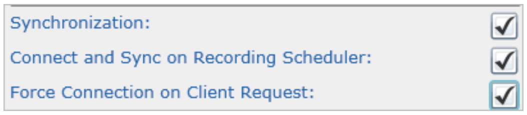


To activate optional synchronization policies

1 Add the Shadow Archive to Command and activate the automatic synchronization feature, as described in "To activate the automatic synchronization feature" on page 165.

2 Select the check boxes corresponding to the policies to enable them.

Note: The **Force Connection on Client Request** policy is dependent from the **Connect and Sync on Recording Scheduler** policy.



Synchronization: ☑
Connect and Sync on Recording Scheduler: ☑
Force Connection on Client Request: ☑

3 Click the 💾 button to save and apply the changes.

Activating the Connection on Demand Functionality

The Command recording platforms (Command Recording Software and Command Lite) support the *Connection on Demand* functionality. When a camera is added to the Command Recording Software, it streams video and data to the server for features such as recording, live video stream, pre and post alarm recording cache, and metadata from video analytics.

Connection on Demand is a functionality designed for installations with small bandwidth. This functionality allows you to limit the bandwidth usage by streaming live video from a camera added to the Command Recording Software only when a client application or interface (including Command Config, Command Client, and SiteManager) requests for it.

Important: You can activate the *Connection on Demand* functionality on any camera added to the Command Recording Software where automatic synchronization has not been enabled. The functionality is active only when the camera is not recording on the Command Recording Software.

To activate the Connection on Demand functionality

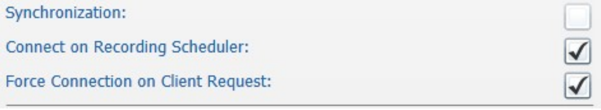
1 On the **Camera Configuration** page, select an IP camera in the **Camera List** panel.

2 Click the **Settings** tab.

3 Ensure the **Synchronization** check box is clear.

4 Select the **Connect on Recording Scheduler** check box.

5 Select the **Force Connection on Client Request** check box.



Synchronization: ☐
Connect on Recording Scheduler: ☑
Force Connection on Client Request: ☑

6 Click the 💾 button to save and apply the changes.

7 The camera now streams live video to the Command Recording Software only when a client application or interface (including Command Config, Command Client, and SiteManager) requests for it.

Managing Encoding Profiles

The **Encoders** tab allows you to configure the encoding profiles of a March Networks camera, allowing you to select profiles with different resolution, frame rate and bit rate according to the requirements. It also allows you to configure one or more encoding profiles for third party cameras, if supported by the camera brand and model.

This section explains how to:

- Configure the encoding profiles of March Networks cameras. For more information, see “Configure the Encoding Profiles of a March Networks Camera” on page 169.
- Configure the encoding profiles of selected third party cameras. For more information, see “Configuring the Encoding Profiles for Third Party Cameras” on page 171.
- Create and configure the encoding profiles of Onvif-compliant (Profile S) cameras. For more information, see “Creating and Editing Onvif Profiles” on page 173.

Configure the Encoding Profiles of a March Networks Camera

The **Encoders** tab allows you to configure the encoding profiles of a March Networks camera, allowing you to select profiles with different resolution, frame rate and bit rate according to the requirements.

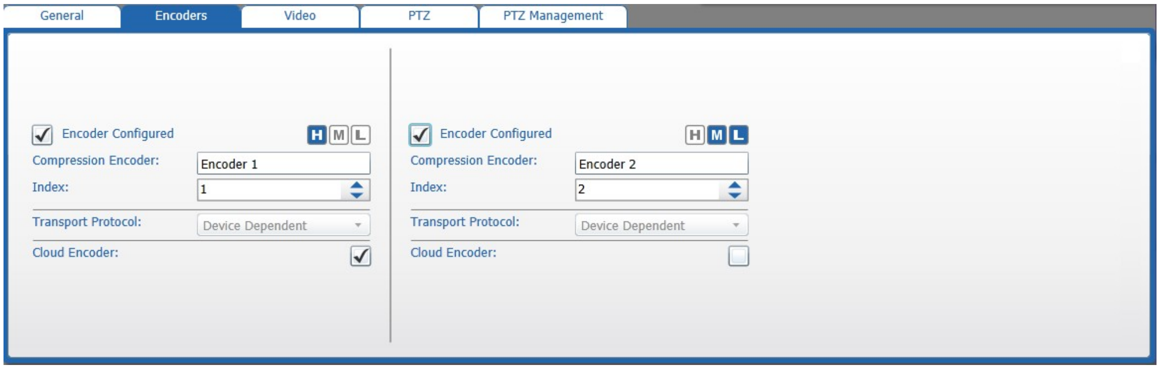
Notes:

- You can apply this procedure only if two or more encoding profiles are configured for the March Networks camera.
- For cameras added using the E-Pass feature, see “Adding Cameras from a Different March Networks Recording Platform (E-Pass)” on page 157.

To map the encoding profiles of a March Networks Camera

1. On the **Camera Configuration** page, select a March Networks camera in the **Camera List** panel.
2. Click the **General** tab.
3. Click **Open Setup** to access the setup interface for the device.
4. Check the number and configuration of the available encoding profiles and close the setup interface to return to Command Config.

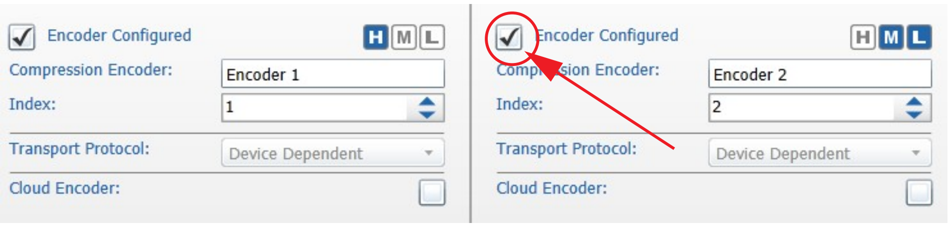
5 Click the **Encoders** tab.



☑ Encoder Configured
Compression Encoder: Encoder 1
Index: 1
Transport Protocol: Device Dependent
Cloud Encoder: ☑

☑ Encoder Configured
Compression Encoder: Encoder 2
Index: 2
Transport Protocol: Device Dependent
Cloud Encoder: □

6 To add an additional encoding profile, select the **Encoder Configured** check box for the second encoding profile.



☑ Encoder Configured
Compression Encoder: Encoder 1
Index: 1
Transport Protocol: Device Dependent
Cloud Encoder: □

☑ Encoder Configured
Compression Encoder: Encoder 2
Index: 2
Transport Protocol: Device Dependent
Cloud Encoder: □

7 Enter a name for the encoding profile in the **Compression on Encoder** text box.

8 Select the value corresponding to the encoding profile on the camera in the **Index** field.

9 Repeat step 6 to step 8 to add additional encoding profiles.

10 Assign the encoding profiles a tag corresponding to the video quality by clicking (**H**) High, (**M**) Medium, or (**L**) Low near each encoding profile. You can assign more than one tag to a single encoding profile.

H M L

11 (Optional) Select the **Cloud Encoder** check box for an encoding profile to send it to the March Networks Cloud service. If this option is not configured, the Command Recording Software does not send the camera's live video to the Cloud service.

Notes:

- Before you configure this option, you must register the Command Recording Software to the March Networks Cloud service. For more information see "Registering to the March Networks Cloud Service" on page 121.
- You must configure this option on every camera and every encoding profile you want to add to the March Networks Cloud service.
- Before you select the encoding profile, ensure that the video stream bitrate does not exceed your available bandwidth on the March Networks Cloud service.

12 Click the 💾 button to save and apply the changes.

Configuring the Encoding Profiles for Third Party Cameras

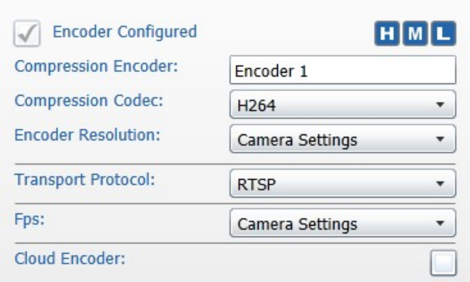
The **Encoders** tab allows you to configure the encoding profiles for third party cameras, if supported by the camera brand and model.

To configure the encoding profiles for a third party camera

1 On the **Camera Configuration** page, select a third party camera in the **Camera List** panel.

Important: This section is applicable only for third party cameras. The number of configurable options is dependent on the camera brand and model.

2 Click the **Encoders** tab.



☑ Encoder Configured

Compression Encoder: Encoder 1

Compression Codec: H264

Encoder Resolution: Camera Settings

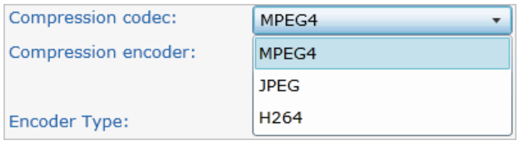
Transport Protocol: RTSP

Fps: Camera Settings

Cloud Encoder: □

3 Enter a name for the encoding profile in the **Compression Encoder** text box.

4 Select a **Compression codec** from the list, if applicable.

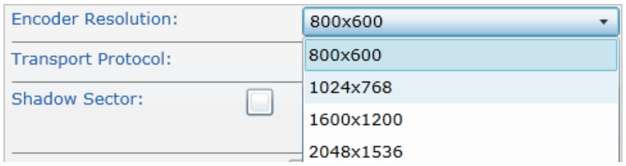


Compression codec: MPEG4

Compression encoder:

Encoder Type:

5 Select the video resolution from the **Encoder resolution** list, if applicable.

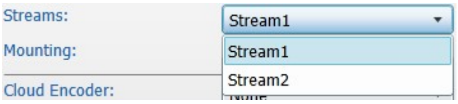


Encoder Resolution: 800x600

Transport Protocol:

Shadow Sector: □

6 Select a configured encoding profile from the **Streams** list.

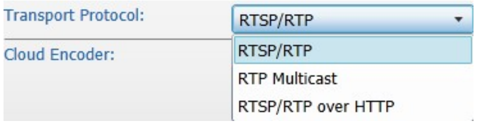


Streams: Stream1

Mounting:

Cloud Encoder:

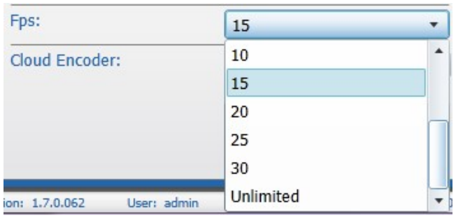
7 Select the **Transport protocol** from the list, if required.



Transport Protocol: RTSP/RTP

Cloud Encoder:

8 Select a frame rate from the **Fps** list, if applicable.



Fps: 15

10
15
20
25
30
Unlimited

Cloud Encoder:

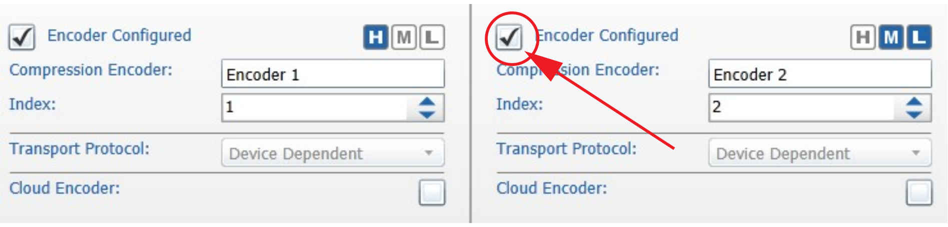
ion: 1.7.0.062 User: admin

9 (Optional) Select the **Cloud Encoder** check box for an encoding profile to send it to the March Networks Cloud service. If this option is not configured, the Command Recording Software does not send the camera's live video to the Cloud service.

Notes:

- Before you configure this option, you must register the Command Recording Software to the March Networks Cloud service. For more information see "Registering to the March Networks Cloud Service" on page 121.
- You must configure this option on every camera and every encoding profile you want to add to the March Networks Cloud service.
- Before you select the encoding profile, ensure that the video stream bitrate does not exceed your available bandwidth on the March Networks Cloud service.

10 If multi-encoding is supported for the third-party camera, select the **Encoder Configured** check box for the second encoding profile, and then repeat step 2 to step 9 to configure the encoding profile.



☑ Encoder Configured H M L
Compression Encoder: Encoder 1
Index: 1
Transport Protocol: Device Dependent
Cloud Encoder: □

☑ Encoder Configured H M L
Compression Encoder: Encoder 2
Index: 2
Transport Protocol: Device Dependent
Cloud Encoder: □

Note: Multi-encoding is supported only on specific third-party cameras. For a list of supported cameras, consult the latest *Command Release Notes* and the *Supported Devices List*, available on the March Networks official website.

11 Assign the encoding profiles a tag corresponding to the video quality by clicking (**H**) High, (**M**) Medium, or (**L**) Low near each encoding profile. You can assign more than one tag to a single encoding profile.

12 Click the 💾 button to save and apply the changes.

Creating and Editing Onvif Profiles

Command Recording Software is an Onvif-certified application that allows you to create and edit the Onvif profiles on March Networks and third-party cameras compliant to the Onvif Profile S specifications. The **Onvif Device Configurator** is a simple and intuitive interface that allows you to create new Onvif encoding profiles or customize existing ones.

Notes:

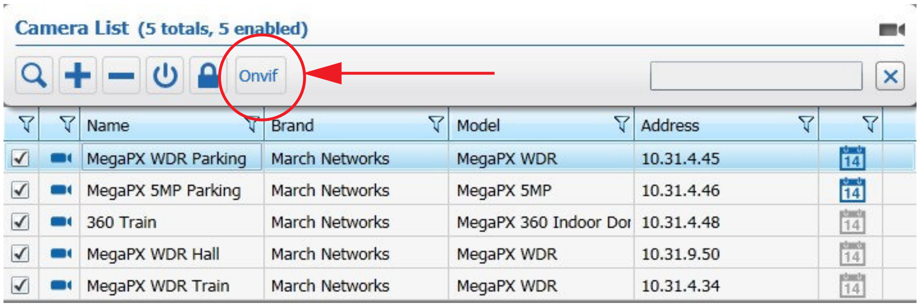
- The **Onvif Device Configurator** button appears only after one or more Onvif-compliant (Profile S) cameras has been added to the Command Recording Software.
- According to the camera in use, the **Onvif Device Configurator** may not allow to edit some parameters (for example, the compression codec or the bitrate value). To edit those parameters, access the IP camera setup interface, as described in “Accessing the Setup Interface of an IP Camera” on page 161.

Select your configuration:

- “To create a new Onvif profile” on page 173
- “To customize an Onvif profile” on page 175
- “To delete an Onvif profile” on page 176
- “To apply a customized profile to an Onvif camera” on page 176

To create a new Onvif profile

1 On the **Camera Configuration** page, click the **Onvif** button on the **Camera List** panel.

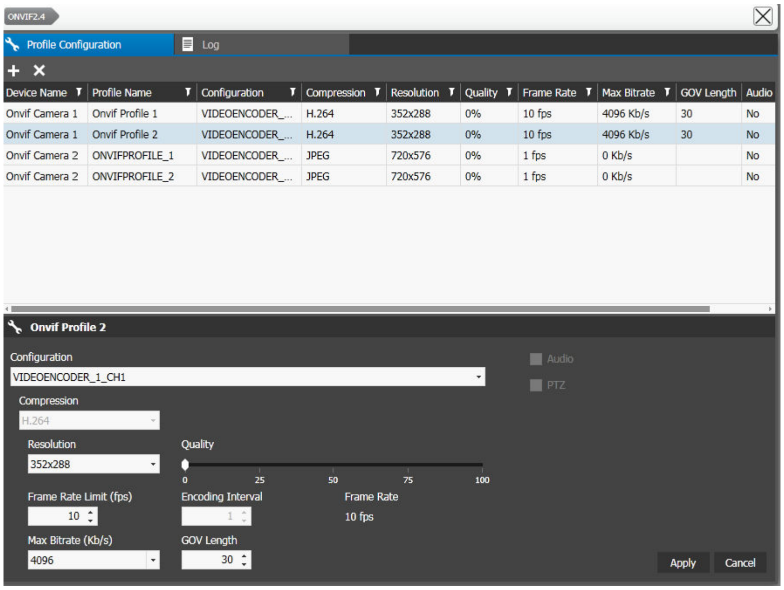


Camera List (5 totals, 5 enabled)

		Name	Brand	Model	Address	
☑		MegaPX WDR Parking	March Networks	MegaPX WDR	10.31.4.45	14
☑		MegaPX 5MP Parking	March Networks	MegaPX 5MP	10.31.4.46	14
☑		360 Train	March Networks	MegaPX 360 Indoor Dor	10.31.4.48	14
☑		MegaPX WDR Hall	March Networks	MegaPX WDR	10.31.9.50	14
☑		MegaPX WDR Train	March Networks	MegaPX WDR	10.31.4.34	14

The **Onvif Device Configurator** appears.

Note: If the Command Recording Software cannot connect to the Onvif cameras or download information about the configured Onvif profiles, the **Onvif Device Configurator** automatically switches to the **Log** tab, displaying information about the connection errors.



Device Name	Profile Name	Configuration	Compression	Resolution	Quality	Frame Rate	Max Bitrate	GOV Length	Audio
Onvif Camera 1	Onvif Profile 1	VIDEOENCODER_...	H.264	352x288	0%	10 fps	4096 Kb/s	30	No
Onvif Camera 1	Onvif Profile 2	VIDEOENCODER_...	H.264	352x288	0%	10 fps	4096 Kb/s	30	No
Onvif Camera 2	ONVIFPROFILE_1	VIDEOENCODER_...	JPEG	720x576	0%	1 fps	0 Kb/s		No
Onvif Camera 2	ONVIFPROFILE_2	VIDEOENCODER_...	JPEG	720x576	0%	1 fps	0 Kb/s		No

Onvif Profile 2

Configuration: VIDEOENCODER_1_CH1

Compression: H.264

Resolution: 352x288

Quality: 0

Frame Rate Limit (fps): 10

Encoding Interval: 1

Frame Rate: 10 fps

Max Bitrate (Kb/s): 4096

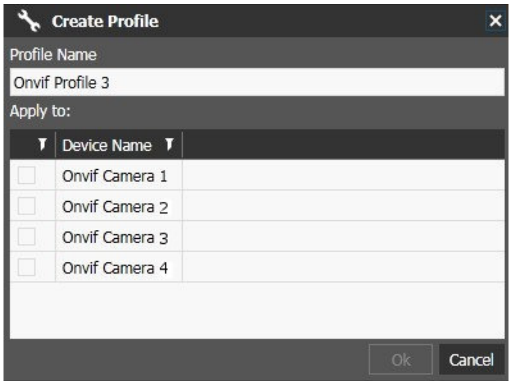
GOV Length: 30

□ Audio

□ PTZ

2 Click the + button.

The **Create Profile** dialog box appears.



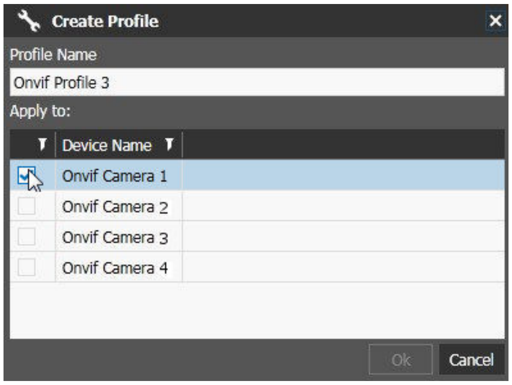
Profile Name: Onvif Profile 3

Apply to:

	Device Name
□	Onvif Camera 1
□	Onvif Camera 2
□	Onvif Camera 3
□	Onvif Camera 4

3 (Optional) Enter a custom name for the new profile in the **Profile Name** text box.

4 Select the check box corresponding to the Onvif camera where you want to create the new profile.



Create Profile

Profile Name: Onvif Profile 3

Apply to:

	Device Name
☑	Onvif Camera 1
□	Onvif Camera 2
□	Onvif Camera 3
□	Onvif Camera 4

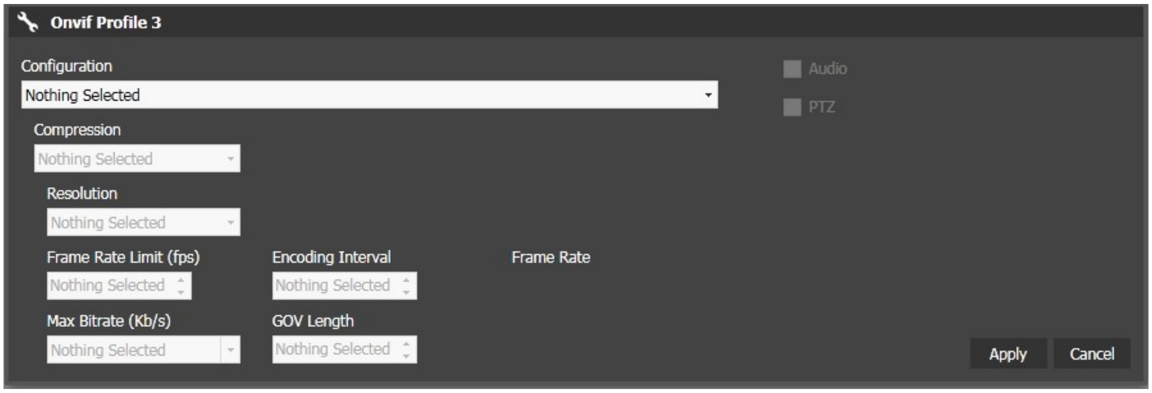
5 Click **Ok** to create the new Onvif profile.

The profile appears in the **Onvif Device Configurator**.

To customize an Onvif profile

1 In the **Onvif Device Configurator**, select an Onvif profile.

The profile configurations appear in the **Settings** panel.



Onvif Profile 3

Configuration: Nothing Selected

Compression: Nothing Selected

Resolution: Nothing Selected

Frame Rate Limit (fps): Nothing Selected

Encoding Interval: Nothing Selected

Frame Rate

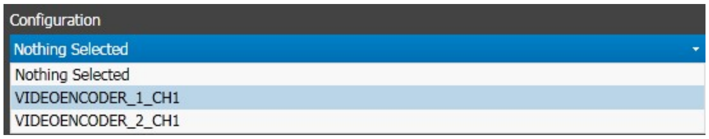
Max Bitrate (Kb/s): Nothing Selected

GOV Length: Nothing Selected

□ Audio

□ PTZ

2 Select an available encoding profile from the **Configuration** list.



Configuration

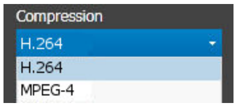
Nothing Selected

- Nothing Selected
- VIDEOENCODER_1_CH1
- VIDEOENCODER_2_CH1

3 Select the **Audio** check box to enable the camera’s output audio channel.

4 Select the **PTZ** check box to enable the PTZ functionality for the camera.

5 Select a compression codec from the **Compression** list.

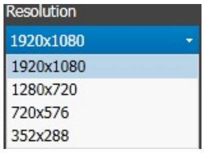


Compression

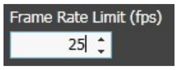
H.264

- H.264
- MPEG-4

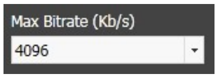
6 Select the video resolution from the **Resolution** list.


Resolution: 1920x1080

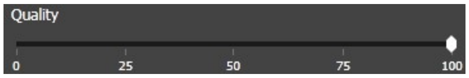
7 Enter or select the video frame rate in the **Frame Rate Limit** text box.


Frame Rate Limit (fps): 25

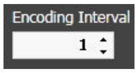
8 For H.264 compressions, select the highest bit rate allowed from the **Max Bitrate** list.


Max Bitrate (Kb/s): 4096

9 Move the **Quality** slider to configure the image quality.

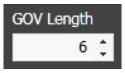


10 Enter or select the encoding interval range in the **Encoding Interval** text box. The encoding interval corresponds to the number of frames divided by the encoded frames. An encoding interval value of “1” means that every frame is encoded.


Encoding Interval: 1

11 Enter or select the I-frames interval in the **Gov Length** text box.

This option configures the interval in which the key frames (*I-Frames*) are coded. A value of 1 indicates that key frames are continuously generated. A value of 2 indicates that every two frames, one is a key frame, a value of 3 indicates that every three frames, one is a key frame, etc.


GOV Length: 6

12 Click the **Apply** button to save and apply the changes.

13 Click the ☒ button to close the **Onvif Device Configurator**.

To delete an Onvif profile

1 In the **Onvif Device Configurator**, select an Onvif profile.

2 Click the ✖ button to delete the Onvif profile.

The profile is deleted.

3 Click the ☒ button to close the **Onvif Device Configurator**.

To apply a customized profile to an Onvif camera

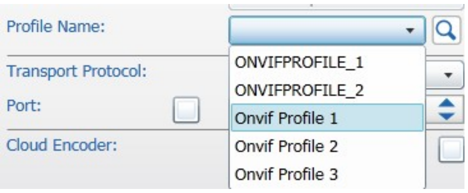
1 On the **Camera Configuration** page, select an Onvif-compliant camera in the **Camera List** panel.

2 Click the **Encoders** tab.

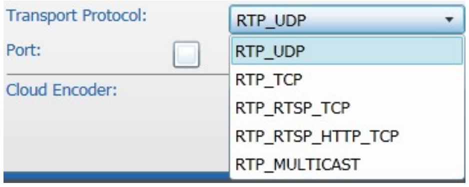
3 Enter a name for the encoding profile in the **Compression Encoder** text box.

4 In the **Profile Name** section, click the 🔍 button to download the profiles you created and edited for the camera.

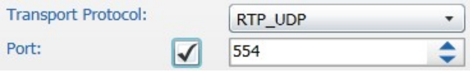
5 Select an **Onvif** profile from the **Profile Name** list.



6 Select the **Transport protocol** from the list, if required.



7 Select the **Port** check box to specify a communication port for the transport protocol, if required.



Transport Protocol: RTP_UDP

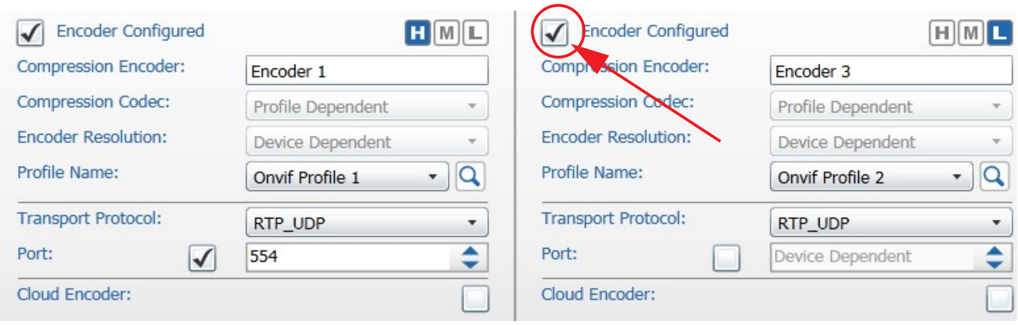
Port: ☑ 554

8 (Optional) Select the **Cloud Encoder** check box for an encoding profile to send it to the March Networks Cloud service. If this option is not configured, the Command Recording Software does not send the camera’s live video to the Cloud service.

Notes:

- Before you configure this option, you must register the Command Recording Software to the March Networks Cloud service. For more information see “Registering to the March Networks Cloud Service” on page 121.
- You must configure this option on every camera and every encoding profile you want to add to the March Networks Cloud service.
- Before you select the encoding profile, ensure that the video stream bitrate does not exceed your available bandwidth on the March Networks Cloud service.

9 To add an additional encoding profile, select the **Encoder Configured** check box for the second encoding profile, and then repeat step 2 to step 8 to configure the encoding profile.



☑ Encoder Configured — H M L

Compression Encoder:	Encoder 1
Compression Codec:	Profile Dependent
Encoder Resolution:	Device Dependent
Profile Name:	Onvif Profile 1
Transport Protocol:	RTP_UDP
Port: ☑	554
Cloud Encoder:	□

☑ Encoder Configured — H M L

Compression Encoder:	Encoder 3
Compression Codec:	Profile Dependent
Encoder Resolution:	Device Dependent
Profile Name:	Onvif Profile 2
Transport Protocol:	RTP_UDP
Port: □	Device Dependent
Cloud Encoder:	□

10 Assign the encoding profiles a tag corresponding to the video quality by clicking (**H**) High, (**M**) Medium, or (**L**) Low near each encoding profile. You can assign more than one tag to a single encoding profile.

H M L

11 Click the 💾 button to save and apply the changes.

Adjusting Video Settings

The **Video** tab allows you to apply slight modifications to the video streams in terms of sharpness, brightness and contrast, and rotate and mirror the streams.

This section explains how to:

- Post-process the video streams. For more information, see “Post-Processing the Video Streams” on page 179.
- Apply and configure privacy patches. For more information, see “Applying Privacy Patches” on page 180.

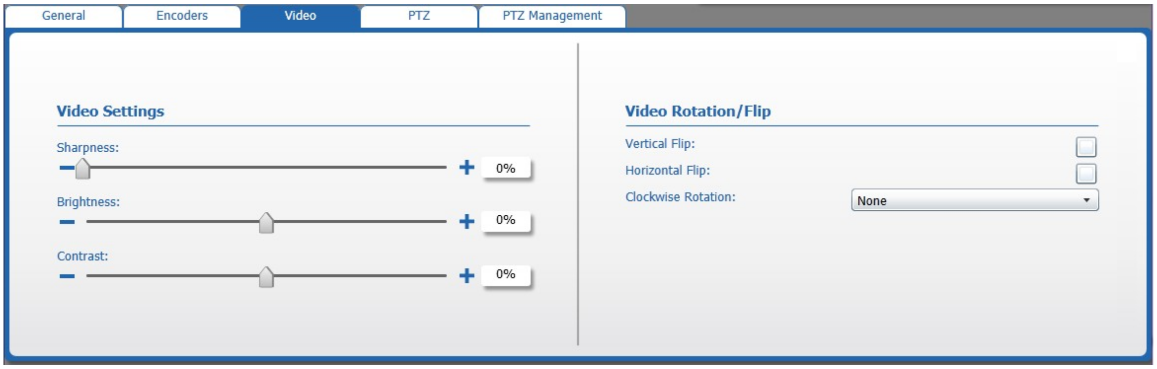
Post-Processing the Video Streams

The **Video** tab allows you to slightly adjust the sharpness, brightness, and contrast levels on the video streams. These settings are applied after the image has been sent to the Command Recording Software and are independent from the equivalent settings in the camera's setup interface. This tab also allows you to mirror or rotate the video stream.

To post-process the video streams

1 On the **Camera Configuration** page, select a camera in the **Camera List** panel.

2 Click the **Video** tab.



Sharpness: 0%

Brightness: 0%

Contrast: 0%

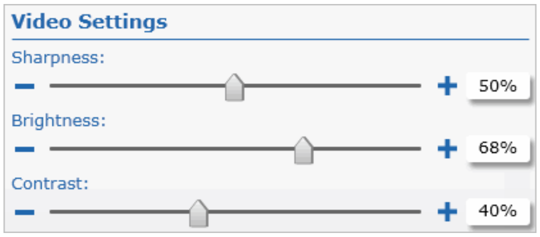
Vertical Flip: □

Horizontal Flip: □

Clockwise Rotation: None

3 Move the sliders in the **Video Settings** section for delicate modifications to the image **Sharpness**, **Brightness**, and **Contrast** levels.

The modifications are instantly applied to the image.

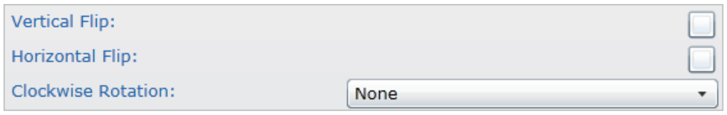


Sharpness: 50%

Brightness: 68%

Contrast: 40%

4 Select an angle from the **Clockwise Rotation** list to rotate the image, if required.



Vertical Flip: □

Horizontal Flip: □

Clockwise Rotation: None

5 Select the **Vertical Flip** check box to turn the image upside down, if required.

6 Select the **Horizontal Flip** check box to mirror the image, if required.

7 Click the 💾 button to save and apply the changes.

Applying Privacy Patches

You can apply one patch or multiple patches on a camera image to protect the privacy of people or objects captured by the camera image. The patches are managed by Command and not by the cameras (pseudonymization) and are applied to live and recorded videos. The privacy patches are added as additional metadata to the video by the Command Config application and are displayed on the Command Client and Command Player client applications. The patches can be removed only by user accounts with the specific permission on a Command Enterprise Server.

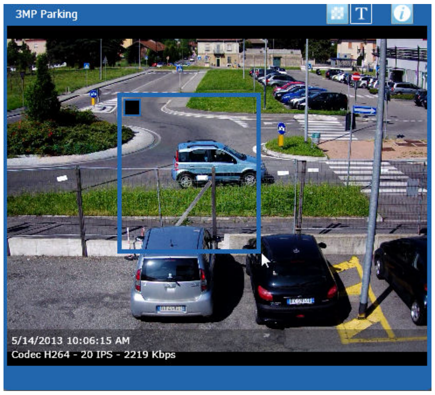
Notes:

- The privacy patch covers a specific portion of the image, regardless of changes to the field of view.
- The privacy patches are exported with the video on both the CME and MP4 video formats.
- To apply privacy patches on the cameras' sensors (achieving a complete anonymization of the masked area), consult the documentation accompanying your devices for instructions about how privacy patches are managed. This is particularly important with PTZ cameras, where privacy patches must follow changes in the field of view.

To apply privacy patches

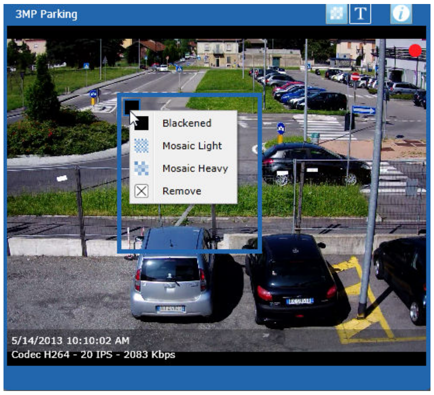
1. On the **Camera Configuration** page, select a camera in the **Camera List** panel.
2. Select the portion of the video stream that you want to cover by right-clicking and dragging in the image.

   Tip: You can create multiple privacy patches on the same video stream.



3 Click the **Edit** button on the upper left corner of the patch and select the privacy patch type.

Options include **Blackened**, **Mosaic Light**, and **Mosaic Heavy**.



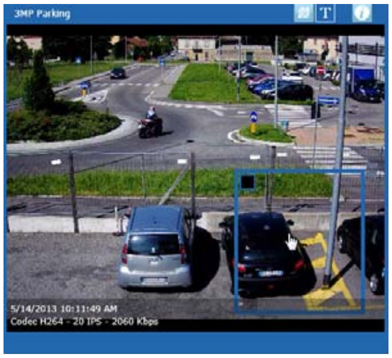
4 Click the 💾 button to save and apply the changes.

The patch is applied to the video stream.

5 To move a patch, do the following:

a Place the mouse cursor in the center of the patch.

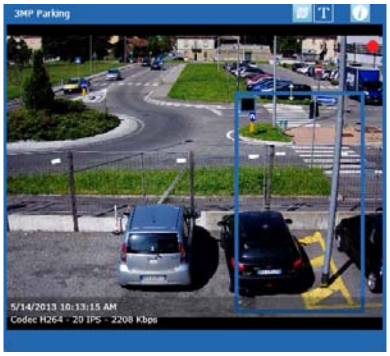
b Right-click and drag the patch to a new location.



6 To resize a patch, do the following:

a Place the mouse cursor over one of the borders or edges, until it becomes a double-edged arrow.

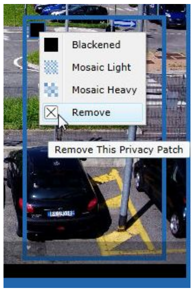
b With your mouse cursor over the arrow, click and drag to resize the patch.



7 To hide the patch on the **Video Preview** window, click the ▦ button on the toolbar.

Note: This is a local setting and it is not applied to the Command Recording Software.

8 To delete a patch, click the **Edit** button on the upper left corner of the patch and select **Remove**.



9 Click the 💾 button to save and apply the changes.

Managing PTZ Cameras

The **Camera Configuration** page allows you to enable PTZ cameras, configure the PTZ protocol, save presets, tours, and preset tours, and access advanced functionalities (if supported by the camera), such as auxiliary channels, thermal imaging, and OSD menus.

Note: To apply privacy patches on the PTZ cameras' sensors (achieving a complete anonymization of the masked area), consult the documentation accompanying your devices for instructions about how privacy patches are managed. This is particularly important with PTZ cameras, where privacy patches must follow changes in the field of view.

This section explains how to:

- Enable PTZ cameras in Command. For more information, see "Enabling PTZ Cameras" on page 183.
- Move PTZ cameras with the mouse or with the PTZ Control panel. For more information, see "Moving PTZ Cameras" on page 185.
- Accessing advanced functionalities (if supported by the camera), such as auxiliary channels, thermal imaging, and OSD menus. For more information, see "Accessing the Advanced Features on PTZ Cameras" on page 187.
- Save preset views, tours, preset tours, and schedule PTZ actions. For more information, see "Saving Preset Views and Tours" on page 188.

Enabling PTZ Cameras

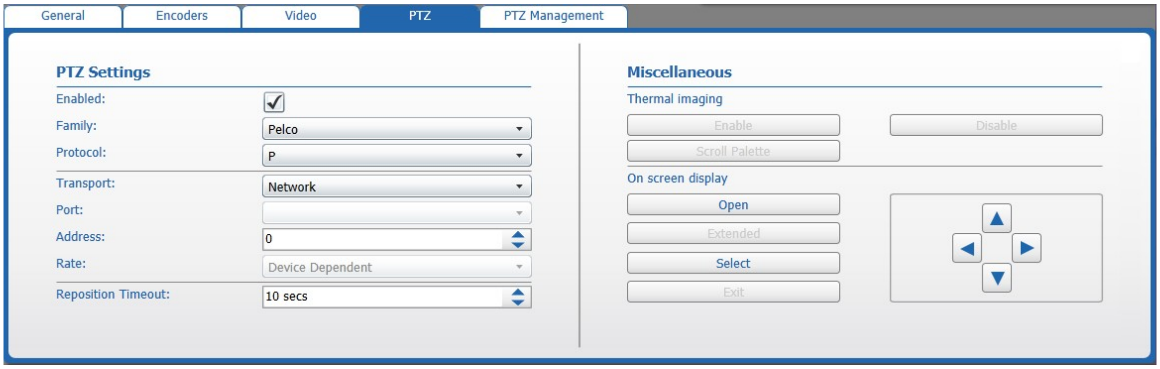
After adding a PTZ camera to Command, you must enable the PTZ functionality. Command automatically specifies the required parameters for March Networks PTZ cameras, but you must manually specify the parameters for analog and third-party PTZ cameras. After you enable the PTZ functionality, you can use the video preview window to move the camera with your mouse, and configure custom tours and preset views.

To enable PTZ functionality

1 On the **Camera Configuration** page, add a PTZ camera to Command.

For more information, see "Adding IP Cameras" on page 154.

2 Select the camera in the **Camera List** panel and click the **PTZ** tab.



PTZ Settings

Enabled: ☑

Family: Pelco

Protocol: P

Transport: Network

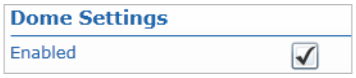
Port:

Address: 0

Rate: Device Dependent

Reposition Timeout: 10 secs

3 Select the **Enabled** check box to enable the PTZ functionality for the camera. The camera button in the list switches to the PTZ camera button.

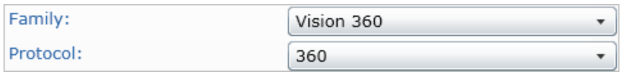


Dome Settings

Enabled ☑

Note: Command automatically specifies the required parameters for March Networks PTZ cameras, but you must manually specify the parameters for third-party PTZ cameras. The PTZ protocol configuration procedure (step 4 to step 9) is required for third-party PTZ cameras only. Consult the documentation accompanying your PTZ camera before you configure these settings.

4 Select the PTZ protocol **Family** and specific **Protocol** from the applicable list.

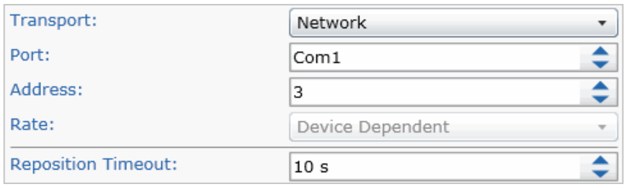


Family: Vision 360

Protocol: 360

Note: To enable PTZ cameras from a 3000/4000/8000 Series recorder, you must select **Command** from the **Family** list and select **R5** from the **Protocol** list.
To enable PTZ cameras from a different Command Recording Software or a 7532 Hybrid NVR, you must select **Command** from the **Family** list and select **Command Recording Software/7000 Series** from the **Protocol** list. The procedure described from step 5 to step 9 is not applicable for these PTZ cameras.

5 Select the data **Transport** mode (either **Network** or **Serial**) from the list.



Transport: Network

Port: Com1

Address: 3

Rate: Device Dependent

Reposition Timeout: 10 s

6 Select a camera communication **Port**.

7 Select the PTZ camera ID in the **Address** field.

8 Select the data **Rate** transfer from the list, if available.

9 Configure the **Reposition timeout**. When the time that you set is reached, the camera automatically returns to the default position.

10 Click the 💾 button to save and apply the changes.

Important: If PTZ control is not enabled after performing this procedure, it is recommended that you lower the **Address** value by 1 as a possible workaround.

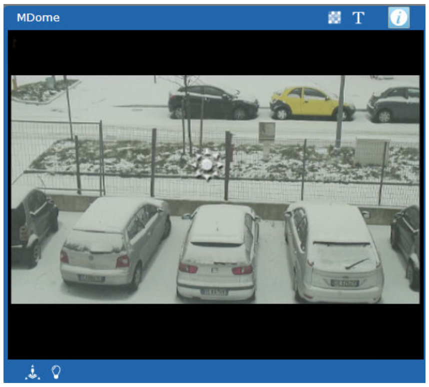
Moving PTZ Cameras

The video preview window allows you to move PTZ cameras using the mouse and the PTZ navigation pad.

To move a PTZ camera

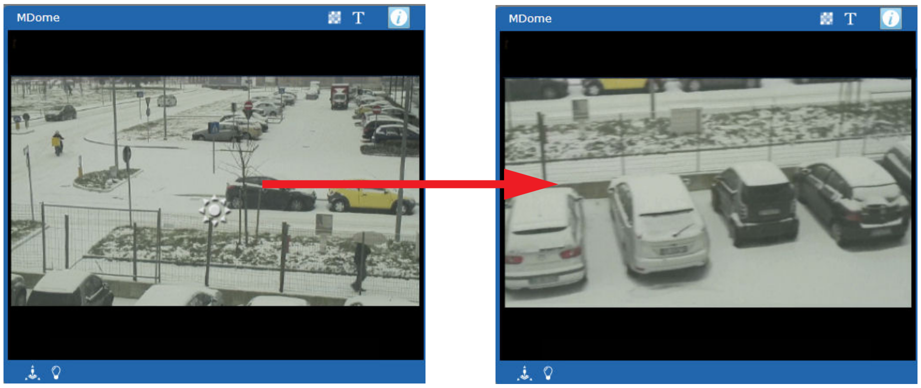
1. On the **Camera Configuration** page, select an enabled PTZ camera in the **Camera List** panel.
2. Move the pointer over the image and hold the mouse button.

   The pointer changes shape.



3. To move the camera, hold the left mouse button down and move the mouse.

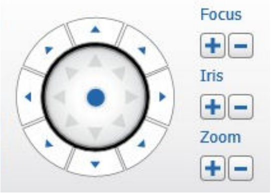
   The PTZ camera follows the mouse movement and speed.



Tip: Alternatively, you can move the PTZ camera using the PTZ Control panel:

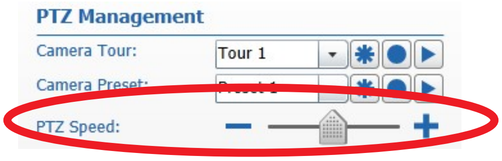
a. Click the button in the **Video Preview** window toolbar.

   The PTZ Control panel appears.



b To move the PTZ camera, click the arrow buttons on the navigation pad or move the pointer inside the navigation pad.

4 To configure the PTZ camera speed, click the **PTZ Management** tab, and then move the **PTZ Speed** slider.



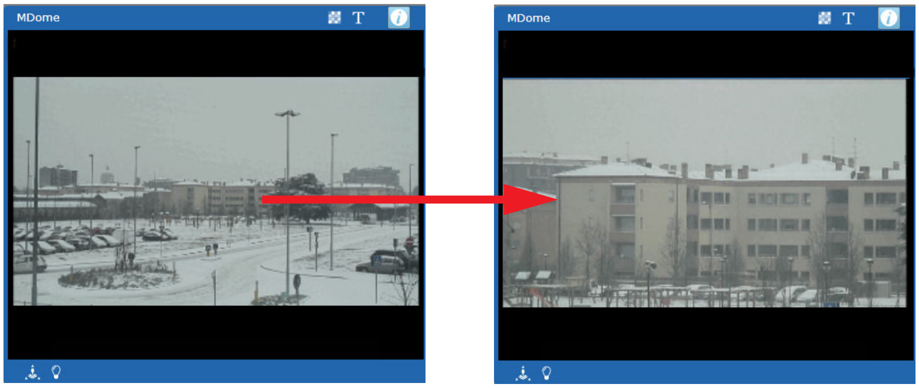
PTZ Management

Camera Tour: Tour 1

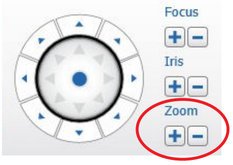
Camera Preset: Preset 1

PTZ Speed:

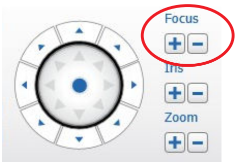
5 To zoom in or out, move the pointer over the image and roll the mouse wheel up (zoom in) and down (zoom out).



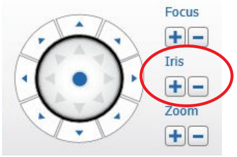
Tip: Alternatively, you can zoom in or out by clicking the **Zoom +** and **Zoom —** buttons on the PTZ control panel.



6 To adjust the camera's focus level, click the button in the **Video Preview** window toolbar, and then click the **Focus +** and **Focus —** buttons.



7 To adjust the camera's iris aperture, click the button in the **Video Preview** window toolbar, and then click the **Iris +** and **Iris —** buttons.



Note: Some PTZ cameras (such as PTZ cameras added using the E-Pass functionality) may not allow you to modify the focus level and the iris aperture.

Accessing the Advanced Features on PTZ Cameras

Command is able to access advanced features, such as auxiliary channel control, the PTZ camera's OSD page, and the camera wash and wiper functionality.

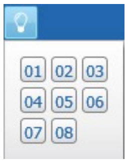
Important: These features are available only if the PTZ camera and its PTZ protocol support these features. Consult the documentation accompanying your PTZ camera before accessing the advanced features.

To access the advanced features on PTZ cameras

1 On the **Camera Configuration** page, select an enabled PTZ camera in the **Camera List** panel.

2 Click the button in the **Video Preview** window toolbar.

The **PTZ Switches** panel appears.

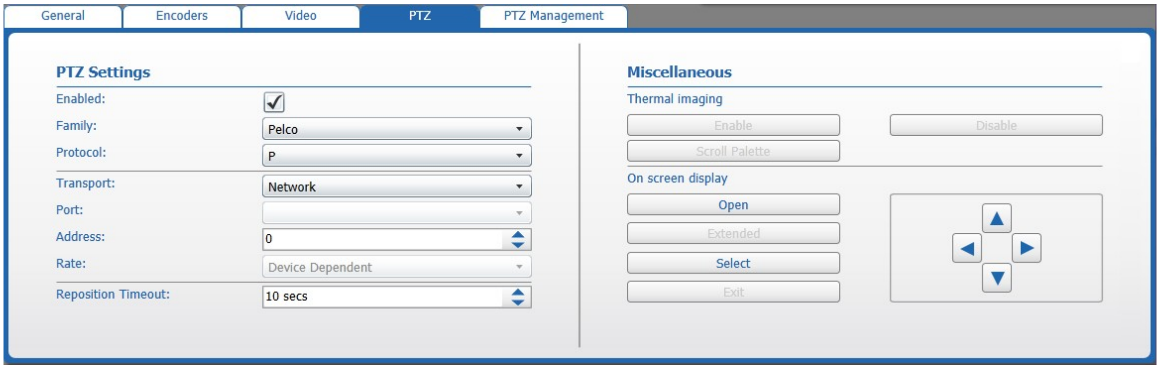


3 Click a number to activate the corresponding auxiliary channel on the camera.

Note: It is recommended to consult the documentation accompanying your PTZ camera before activating the auxiliary channels. To hide the panel, click anywhere on the **Camera Configuration** page.

4 Click the button in the **Video Preview** window toolbar to activate the wiper functionality.

5 Click the **PTZ** tab.



PTZ Settings

Enabled: ☑

Family: Pelco

Protocol: P

Transport: Network

Port:

Address: 0

Rate: Device Dependent

Reposition Timeout: 10 secs

Miscellaneous

Thermal imaging

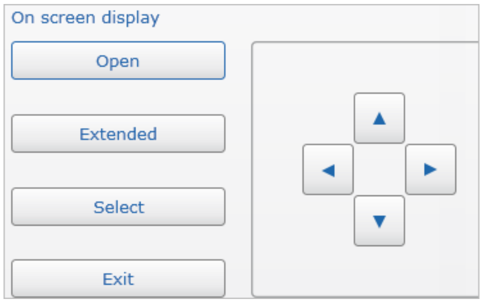
On screen display

6 In the **Thermal Imaging** section, click **Enable** to activate thermal imaging on the camera.

Tip: To disable thermal imaging, click **Disable**.

7 In the **Thermal Imaging** section, click **Scroll Palette** to manually select the color palette while thermal imaging is activated on the camera.

8 In the **On screen display** section do one of the following:
   - Click the **Open** button to access the camera's OSD page on the Video Preview window.
   - Click **Extended** to access the advanced version of the OSD page, if possible.



9 Use the navigation pad to navigate to the page options and click **Select** to confirm an option.

10 Click **Exit** to close the OSD page.

11 Click the 💾 button to save and apply the changes.

Saving Preset Views and Tours

Preset views are a combination of the current camera's position, optical zoom, and focus. These settings are saved on the camera so that you can instantly recall them.

PTZ tours are a series of pan, tilt, and zoom movements that are saved on the camera so that they can be instantly launched. You can create up to eight different tours for each camera, depending on the camera capabilities.

Preset tours are sequences of configured preset views that are saved on the Command Recording Software and that can be instantly launched.

Important: To create a preset tour, you must have saved at least two preset views for the PTZ camera. For more information, see “To save a preset view” on page 188.

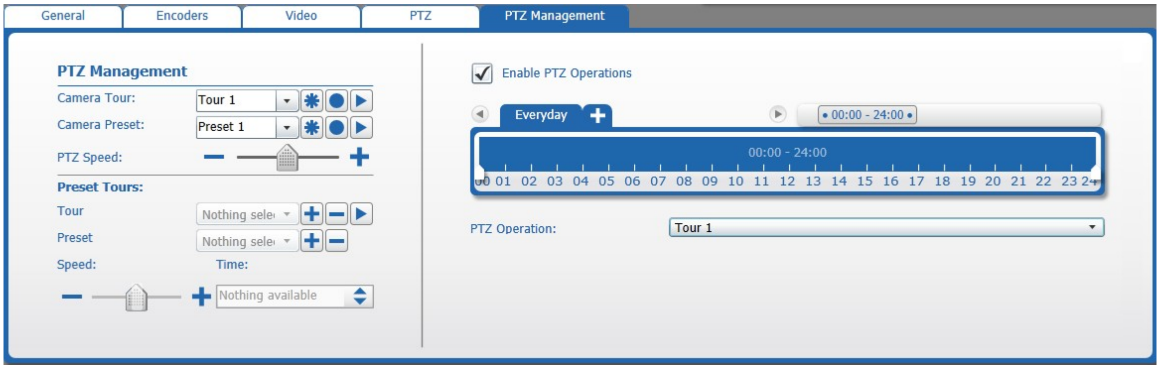
Command allows you to saving preset views, tours and preset tours for your PTZ cameras without opening the setup interface or On Screen Display (OSD) page, and without requiring the use of an external keyboard. It also allows you to schedule a PTZ action (preset, tour, or presets tour) for the camera.

Note: You cannot save presets or tours on PTZ cameras added using the E-Pass functionality. However, you can move the PTZ camera to an existing preset. The tour and preset tour functionalities are not supported on all of the March Networks PTZ cameras. For more information, see the documentation accompanying the PTZ camera.

To save a preset view

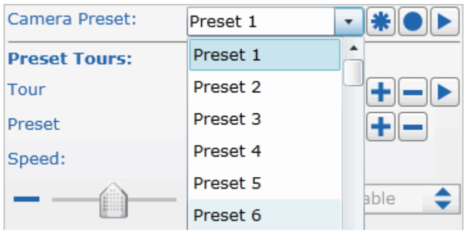
1 On the **Camera Configuration** page, select an enabled PTZ camera in the **Camera List** panel.

2 Click the **PTZ Management** tab.



Camera Tour: Tour 1
Camera Preset: Preset 1
PTZ Speed:
Tour: Nothing sele
Preset: Nothing sele
Time: Nothing available
☑ Enable PTZ Operations
PTZ Operation: Tour 1

3 Select a preset from the **Camera Preset** list.



4 Move the PTZ camera and adjust the zoom, focus, and iris controls as required.

5 Click the ● button to save the selection as a preset view.

6 (Optional) Click the ✱ to mark the preset view as a favorite.

Note: When you mark a preset as a favorite, a shortcut is added to the **Preset** menu on Command Client. You must mark a preset as a favorite to launch it using the March Networks Cloud service.

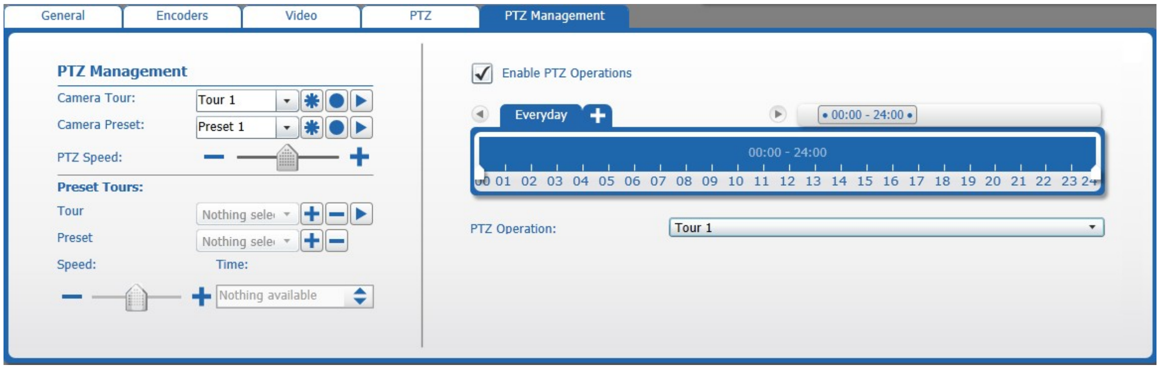
7 Repeat step 3 to step 6 to create additional preset views.

Note: To move the PTZ camera to a saved preset, select it from the list and click the ▶ button.

To save a tour

1 On the **Camera Configuration** page, select an enabled PTZ camera in the **Camera List** panel.

2 Click the **PTZ Management** tab.



Camera Tour: Tour 1
Camera Preset: Preset 1
PTZ Speed:
Tour: Nothing sele
Preset: Nothing sele
Time: Nothing available
☑ Enable PTZ Operations
PTZ Operation: Tour 1

3 Select a tour from the **Camera Tour** list.

Important: The number of programmable tours may change, according to the camera model and to the PTZ protocol. For legacy XDome PTZ and MiniDome PTZ cameras, the first four tours in the list are read-only tours that must be configured by accessing the camera's setup interface or OSD page.

4 Click the ● button to start recording the tour.

Note: While recording, the button is highlighted in red.

5 Move the PTZ camera.

Command captures all of the pan, tilt, and zoom movements.

6 When you are finished creating the tour, click the ● button again.

7 You can review the tour in the video preview window by clicking the ▶ button.

The PTZ camera starts moving.

8 Click the ✱ to mark the tour as a favorite.

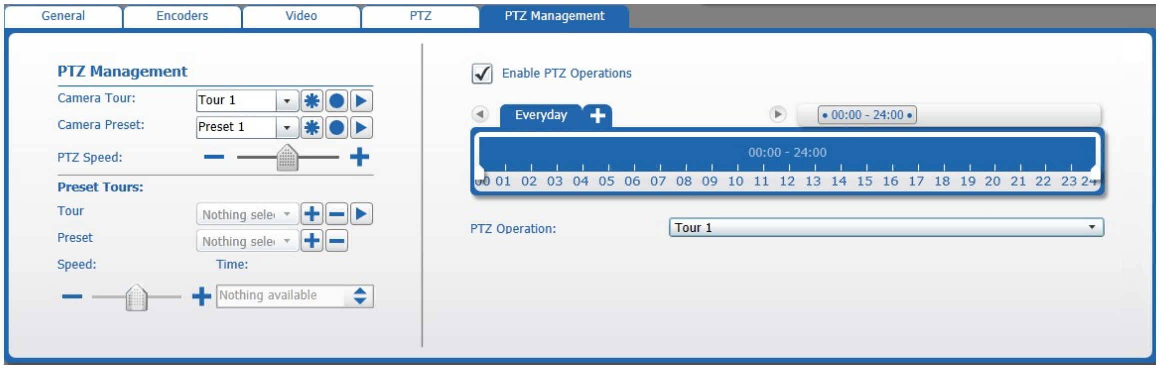
Note: When you mark a tour as a favorite, a shortcut is added to the **Tour** menu on Command Client. You must mark a tour as a favorite to launch it using the March Networks Cloud service.

9 Repeat step 3 to step 6 to create additional tours.

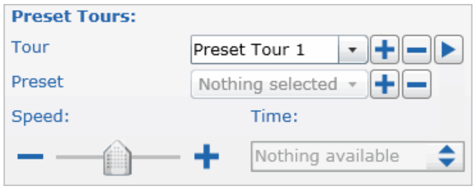
To configure a preset tour

1 On the **Camera Configuration** page, select an enabled PTZ camera select a camera in the **Camera List** panel.

2 Click the **PTZ Management** tab.

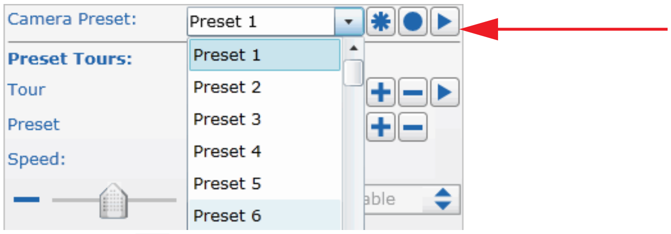


3 In the **Preset tours** section, click the ✚ button.
The preset tour appears in the list.



4 Select a preset view from the **Camera Preset** list in the **Navigation** section.

The camera moves towards the selected preset view.



Camera Preset: Preset 1

Preset Tours:

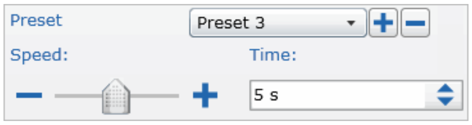
Tour

Preset

Speed:

5 Click the + button near the **Preset** list in the **Preset Tour** section to add the preset view to the tour and select the **Time** interval before moving to the next preset.

Tip: You can also configure the movement speed before moving to the next preset by moving the **Speed** slider, if supported by the camera.



Preset: Preset 3

Speed:

Time: 5 s

6 Repeat step 4 to step 5 to add other preset views to the preset tour.

Tip: You can remove a preset from the tour by selecting it from the list and clicking the − button.

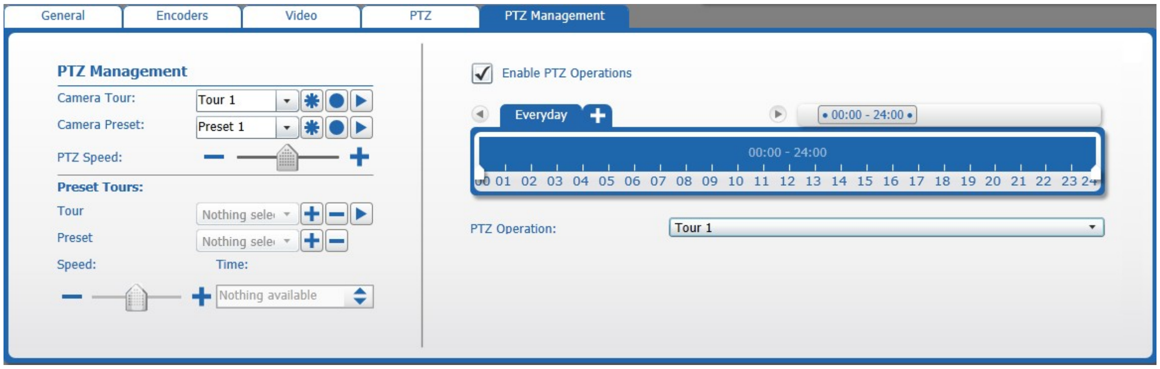
7 You can review the tour in the video preview window by clicking the ▶ button.

The PTZ camera starts moving.

To schedule a PTZ action

1 On the **Camera Configuration** page, select an enabled PTZ camera select a camera in the **Camera List** panel.

2 Click the **PTZ Management** tab.



PTZ Management

Camera Tour: Tour 1

Camera Preset: Preset 1

PTZ Speed:

Preset Tours:

Tour: Nothing sele

Preset: Nothing sele

Speed:

Time: Nothing available

☑ Enable PTZ Operations

PTZ Operation: Tour 1

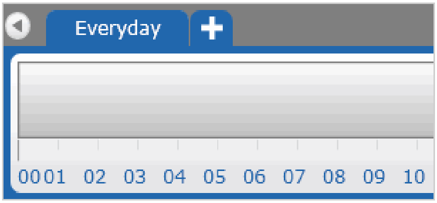
3 Select the **Enable PTZ Operations** check box.

☑ Enable PTZ Operations

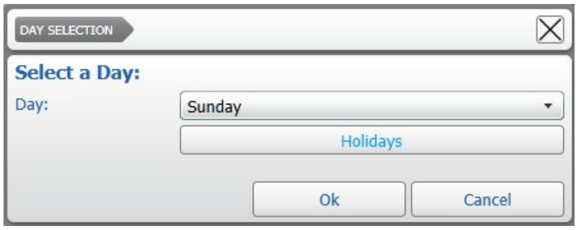
4 Do one of the following:

- To schedule the PTZ action for every day, use the default **Everyday** tab.

- To schedule the PTZ action for a specific day of the week/month, click the tab + to create a new tab for a specific day.



The **Day Selection** dialog box appears.

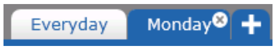

DAY SELECTION

Select a Day:

Day: Sunday

Select a day from the list and click **Ok**.

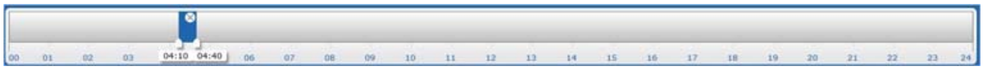
The tab for the selected day is added to the list.



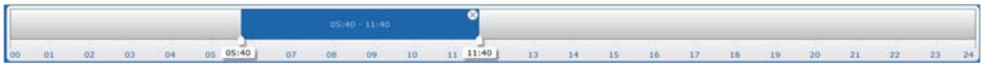
Note: When schedules conflict (for example, the **Everyday** tab is configured to record from 10 A.M., while the **Monday** tab is configured to record from 8 A.M.), Command follows an internal priority list. The priority, starting from top to bottom, is: Holiday, 1st/10th/15th day of the month, Single day of the week, Everyday.

5 To select a time interval for that day using the timeline, do the following:

- Click and hold the left mouse button down at the desired start time.

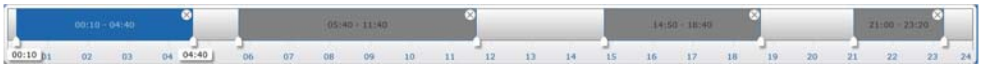


- Click and drag to define the length of the time interval.

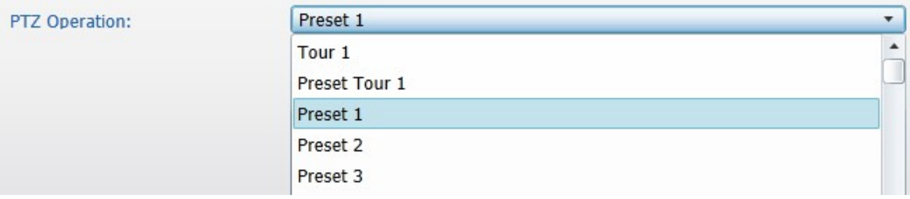


Tip: To resize a time interval, click and drag the white tab at the beginning of at the ending of the interval. To move a time interval, click and drag inside the interval.

- You can set multiple time intervals for the same day. Every time interval on the time line has its own schedule. Click a time interval to select it or hold down the **SHIFT** key to select multiple intervals.



6 Select a configured preset, tour, or preset tour from the **PTZ Operation** list.



PTZ Operation: Preset 1

Tour 1
Preset Tour 1
Preset 1
Preset 2
Preset 3

7 Click the 💾 button to save and apply the changes.

The PTZ camera is forced to perform the configured action according to the schedule.

Disabling a Camera

You can temporarily disable a camera in Command. While disabled, the Command Recording Software cannot connect to the camera and does not record its video.

To disable a camera

1 On the **Camera Configuration** page, select the camera you want to disable in the **Camera List** panel.

2 Click the ⏻ button to disable the camera.

Tip: You can also disable a camera by clearing the check box corresponding to the camera in the **Camera List** panel.

3 Click the 💾 button to save and apply the changes.

Note: You can enable the camera again by selecting it and clicking the ⏻ button, or by selecting the camera's check box.

Deleting IP Cameras

If you no longer need an IP camera, you can delete it from the camera list.

To delete an IP camera

1 On the **Camera Configuration** page, select the camera you want to delete in the **Camera List** panel.

2 Click the − button to remove the camera.

A confirmation dialog box appears.

3 Click **Yes** to confirm the camera deletion.

Click the 💾 button to save and apply the changes.

Viewing Live Video Using RTSP Streaming

You can also view live video using a media player application compatible with RTSP streaming (such as VLC®).

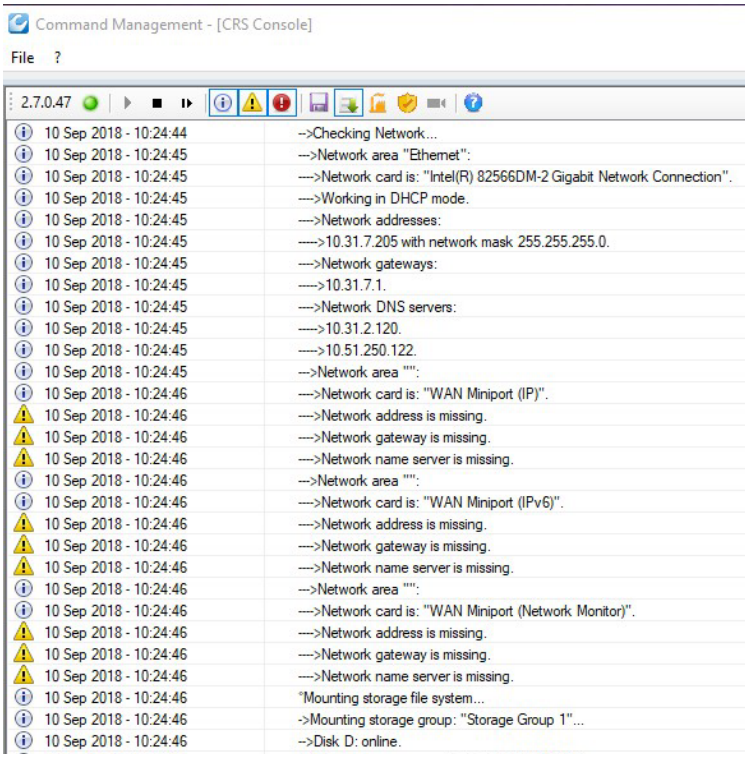
Notes:

- The privacy patches configured with Command Config are not added to the video when a channel is streamed using the RTSP protocol.
- Before launching the media player streaming, ensure the video channel is currently enabled and connected to the Command Recording Software. Disabled or disconnected channels may cause the media player application to crash.

To view live video using RTSP streaming

1 On the server’s **Start** menu, point to **March Networks**, and then click **Command Recording Software Management**.

The **Command Management** console appears.

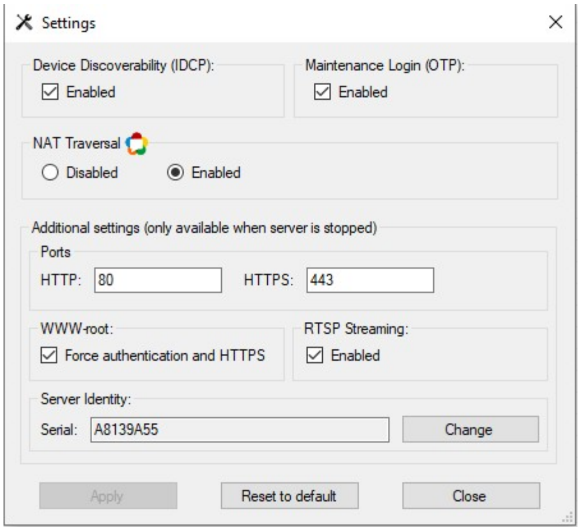


```
10 Sep 2018 - 10:24:44    -->Checking Network...
10 Sep 2018 - 10:24:45    --->Network area "Ethernet":
10 Sep 2018 - 10:24:45    ---->Network card is: "Intel(R) 82566DM-2 Gigabit Network Connection".
10 Sep 2018 - 10:24:45    ---->Working in DHCP mode.
10 Sep 2018 - 10:24:45    ---->Network addresses:
10 Sep 2018 - 10:24:45    ----->10.31.7.205 with network mask 255.255.255.0.
10 Sep 2018 - 10:24:45    ---->Network gateways:
10 Sep 2018 - 10:24:45    ----->10.31.7.1.
10 Sep 2018 - 10:24:45    ---->Network DNS servers:
10 Sep 2018 - 10:24:45    ----->10.31.2.120.
10 Sep 2018 - 10:24:45    ----->10.51.250.122.
10 Sep 2018 - 10:24:45    --->Network area "":
10 Sep 2018 - 10:24:46    ---->Network card is: "WAN Miniport (IP)".
10 Sep 2018 - 10:24:46    ---->Network address is missing.
10 Sep 2018 - 10:24:46    ---->Network gateway is missing.
10 Sep 2018 - 10:24:46    ---->Network name server is missing.
10 Sep 2018 - 10:24:46    --->Network area "":
10 Sep 2018 - 10:24:46    ---->Network card is: "WAN Miniport (IPv6)".
10 Sep 2018 - 10:24:46    ---->Network address is missing.
10 Sep 2018 - 10:24:46    ---->Network gateway is missing.
10 Sep 2018 - 10:24:46    ---->Network name server is missing.
10 Sep 2018 - 10:24:46    --->Network area "":
10 Sep 2018 - 10:24:46    ---->Network card is: "WAN Miniport (Network Monitor)".
10 Sep 2018 - 10:24:46    ---->Network address is missing.
10 Sep 2018 - 10:24:46    ---->Network gateway is missing.
10 Sep 2018 - 10:24:46    ---->Network name server is missing.
10 Sep 2018 - 10:24:46    °Mounting storage file system...
10 Sep 2018 - 10:24:46    ->Mounting storage group: "Storage Group 1"...
10 Sep 2018 - 10:24:46    -->Disk D: online.
```

2 Click the ■ button to stop the Command Recording Software service.

3 Click the 🛡 button.

The **Security Settings** dialog box appears.



Settings

Device Discoverability (IDCP): ☑ Enabled

Maintenance Login (OTP): ☑ Enabled

NAT Traversal: ○ Disabled ● Enabled

Additional settings (only available when server is stopped)

Ports

HTTP: 80 HTTPS: 443

WWW-root: ☑ Force authentication and HTTPS

RTSP Streaming: ☑ Enabled

Server Identity:

Serial: A8139A55

4 In the **RTSP Streaming** section, ensure that the **Enabled** check box is selected.

5 Click the ▶ button to start the Command Recording Software service.

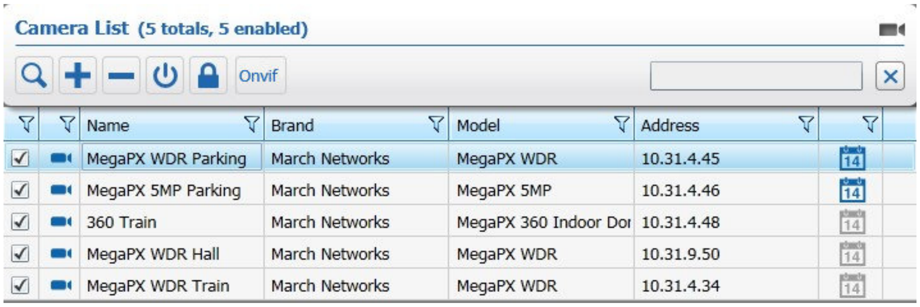
6 Close the console and log on to the Command Recording Software using the Command Config application.

7 Click **Cameras**.

The **Cameras Configuration** page appears.

8 Check which video channels are currently enabled and active.

Note: Trying to view a disabled or disconnected camera using the RTSP protocol may cause the media player application to crash.



Camera List (5 totals, 5 enabled)

		Name	Brand	Model	Address	
☑	■	MegaPX WDR Parking	March Networks	MegaPX WDR	10.31.4.45	14
☑	■	MegaPX 5MP Parking	March Networks	MegaPX 5MP	10.31.4.46	14
☑	■	360 Train	March Networks	MegaPX 360 Indoor Doı	10.31.4.48	14
☑	■	MegaPX WDR Hall	March Networks	MegaPX WDR	10.31.9.50	14
☑	■	MegaPX WDR Train	March Networks	MegaPX WDR	10.31.4.34	14

9 Open a web browser and enter:

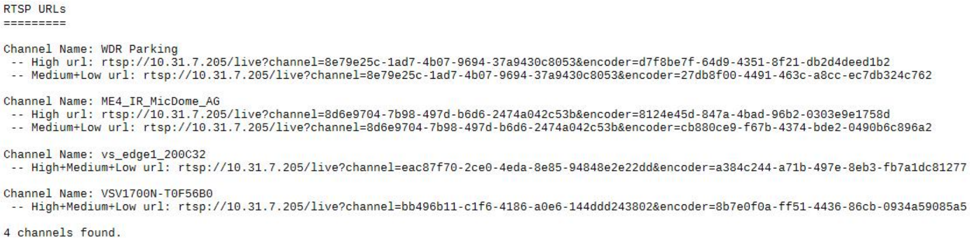
https://<*serverhostname*>/rtsp

10 On the warning page, click **Continue to this website**.

The authentication dialog box appears.

11 Log on with a valid **User** name and **Password**.

The RTSP URLs page appears.



```
RTSP URLs
=========

Channel Name: WDR Parking
 -- High url: rtsp://10.31.7.205/live?channel=8e79e25c-1ad7-4b07-9694-37a9430c8053&encoder=d7f8be7f-64d9-4351-8f21-db2d4deed1b2
 -- Medium+Low url: rtsp://10.31.7.205/live?channel=8e79e25c-1ad7-4b07-9694-37a9430c8053&encoder=27db8f00-4491-463c-a8cc-ec7db324c762

Channel Name: ME4_IR_MicDome_AG
 -- High url: rtsp://10.31.7.205/live?channel=8d6e9704-7b98-497d-b6d6-2474a042c53b&encoder=8124e45d-847a-4bad-96b2-0303e9e1758d
 -- Medium+Low url: rtsp://10.31.7.205/live?channel=8d6e9704-7b98-497d-b6d6-2474a042c53b&encoder=cb880ce9-f67b-4374-bde2-0490b6c896a2

Channel Name: vs_edge1_200C32
 -- High+Medium+Low url: rtsp://10.31.7.205/live?channel=eac87f70-2ce0-4eda-8e85-94848e2e22dd&encoder=a384c244-a71b-497e-8eb3-fb7a1dc81277

Channel Name: VSV1700N-T0F56B0
 -- High+Medium+Low url: rtsp://10.31.7.205/live?channel=bb496b11-c1f6-4186-a0e6-144ddd243802&encoder=8b7e0f0a-ff51-4436-86cb-0934a59085a5

4 channels found.
```

12 Copy the URL corresponding to the video channel and encoding profile you want to stream using the RTSP protocol.

13 Launch the RTSP-compatible media player application of your choice.

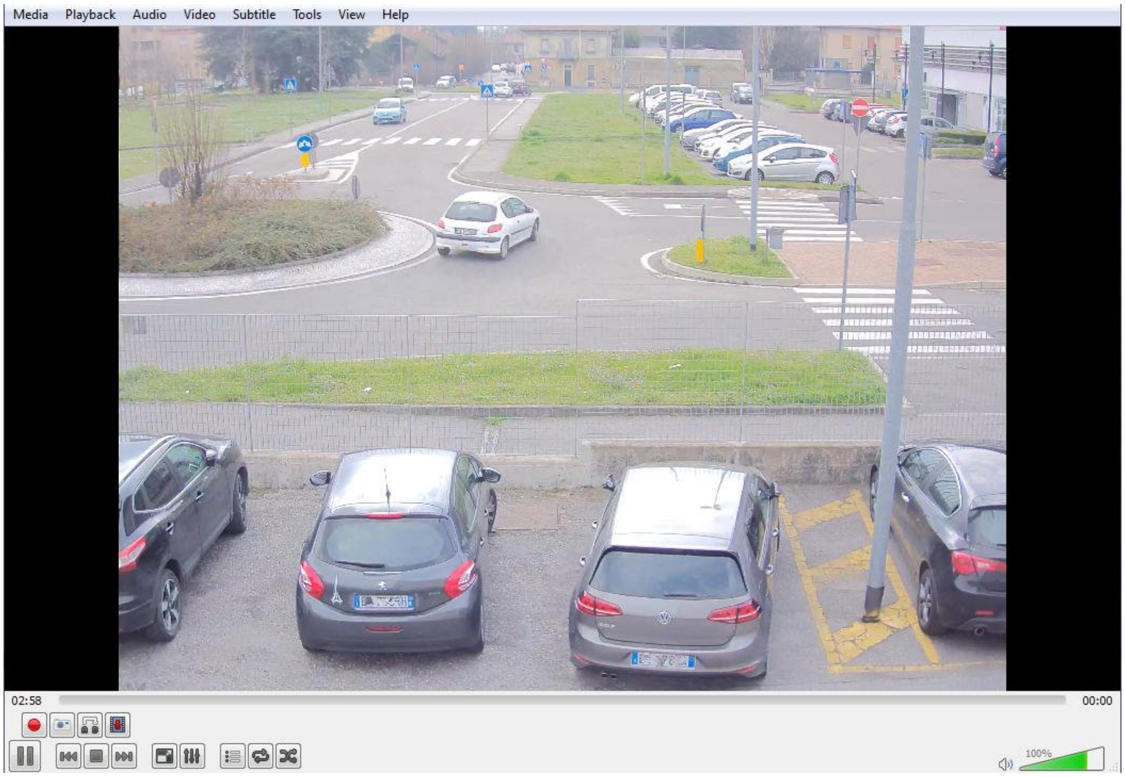
14 When prompted, paste the URL and click **OK**.

An authentication dialog box appears.

15 Log on with a valid **User** name and **Password**.

Note: The user account must have the **Live** user right for the selected channel.

After a few seconds, live video from the selected channel and encoding profile appears on the application.



Chapter 11

Creating Recording Schedules

On the **Scheduler Configuration** page, you can create a number of recording sectors and configure them in terms of storage, space, and cameras for different purposes (such as continuous recording, programmed recording, and on-event recording).

Important: When Command connects to a camera from a 3000/4000/8000 Series recorder, the Command Recording Software becomes the primary recording machine. Otherwise, when Command disconnects from the camera, the DVR automatically switches the retention policy from the configured **Minimal Retention Period** to **Long Term Retention Period**. For more information, see the *Administrator Console User Manual* available for download from the March Networks Partner Portal and official websites.

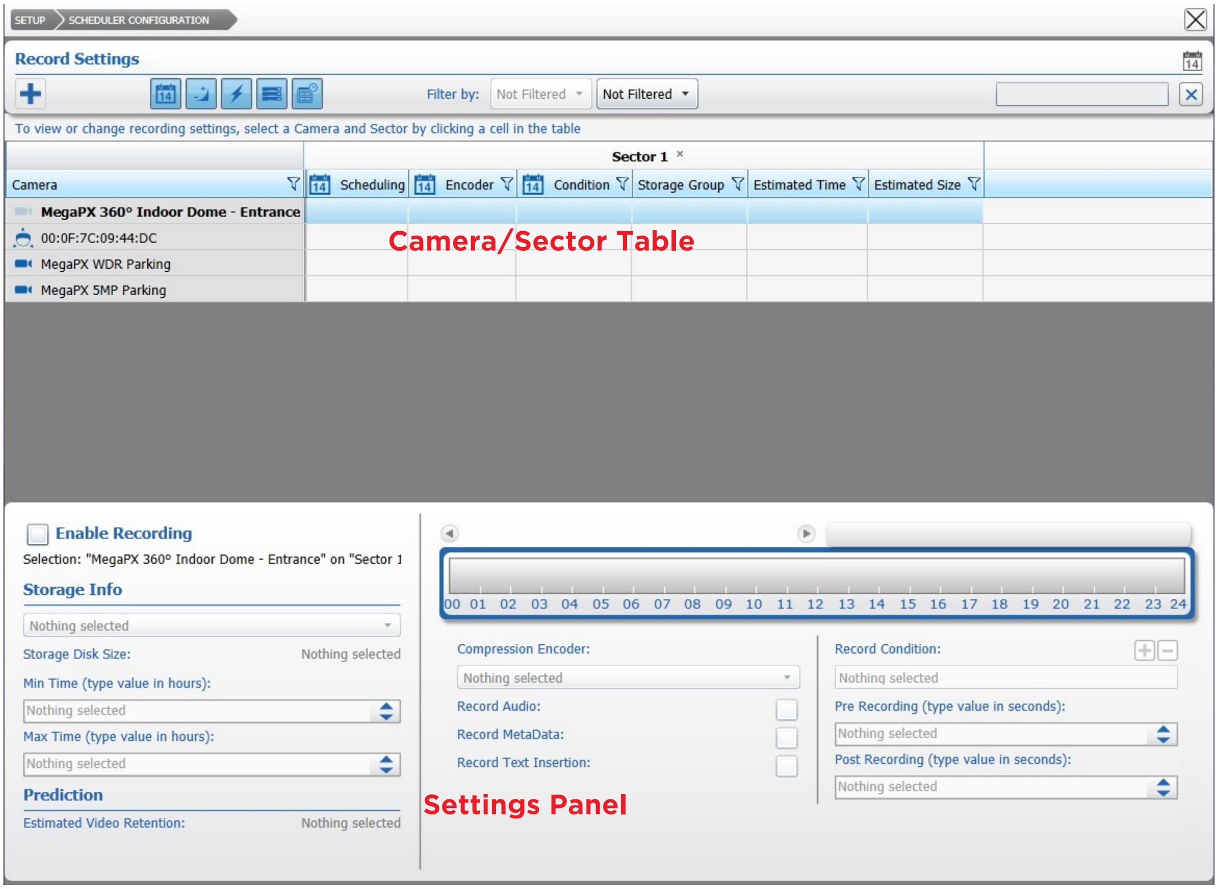
This chapter contains the following sections:

Overview

The **Scheduler Configuration** page allows you to create recording sectors and configure recording schedules using an intuitive interface.

To access the page, on the Command Config main page, under **Recording Management**, click **Scheduler**.

The following illustration shows the **Recording Configuration** user interface.



To view or change recording settings, select a Camera and Sector by clicking a cell in the table

	Sector 1 ×					
Camera	Scheduling	Encoder	Condition	Storage Group	Estimated Time	Estimated Size
MegaPX 360° Indoor Dome - Entrance						
00:0F:7C:09:44:DC						
MegaPX WDR Parking						
MegaPX 5MP Parking						

Camera/Sector Table

□ Enable Recording

Selection: "MegaPX 360° Indoor Dome - Entrance" on "Sector 1

Storage Info

Nothing selected

Storage Disk Size: Nothing selected

Min Time (type value in hours): Nothing selected

Max Time (type value in hours): Nothing selected

Prediction

Estimated Video Retention: Nothing selected

Compression Encoder: Nothing selected

Record Audio: □

Record MetaData: □

Record Text Insertion: □

Record Condition: Nothing selected

Pre Recording (type value in seconds): Nothing selected

Post Recording (type value in seconds): Nothing selected

Settings Panel

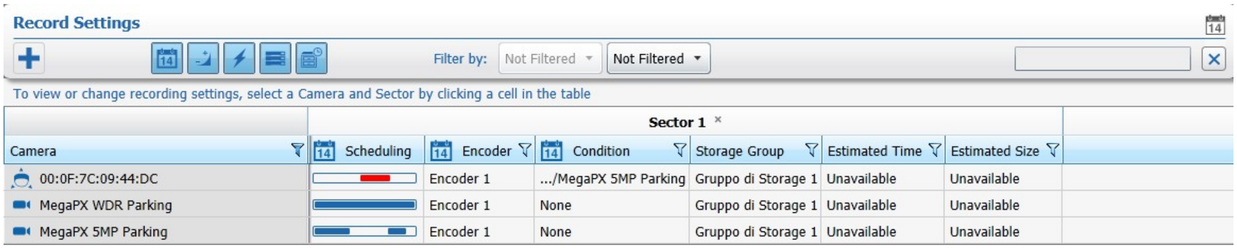
The **Recording Configuration** page is divided into two main areas.

1 **Camera/Sector** table — Located at the top of the screen, it allows you to create recording sectors, and select combinations of cameras and recording sectors to configure recording. It also allows you to see the recording configurations for every camera at a glance.

2 **Settings** panel — Located at the bottom of the screen, it allows you to manage and configure the recording schedules and options.

Camera/Sector Table

The **Camera/Sector** table is located at the top of the screen. You can create recording sectors, and then select combinations of cameras and recording sectors to configure recording. You can also see the recording configurations for every camera at a glance.



Record Settings

Filter by: Not Filtered ▾ Not Filtered ▾

To view or change recording settings, select a Camera and Sector by clicking a cell in the table

	Sector 1 ×					
Camera	Scheduling	Encoder	Condition	Storage Group	Estimated Time	Estimated Size
00:0F:7C:09:44:DC		Encoder 1	.../MegaPX 5MP Parking	Gruppo di Storage 1	Unavailable	Unavailable
MegaPX WDR Parking		Encoder 1	None	Gruppo di Storage 1	Unavailable	Unavailable
MegaPX 5MP Parking		Encoder 1	None	Gruppo di Storage 1	Unavailable	Unavailable

The following table provides a description of the toolbar buttons.

Button	Action
+	Creates a new recording sector.
14	Shows/hides the **Scheduling** column.
	Shows/hides the **Encoder** column.
⚡	Shows/hides the **Condition** column.
☰	Shows/hides the **Storage Group** column.
	Shows/hides the **Estimated Time** and **Estimated Size** columns.
Everyday ▾	Shows only the schedules correspondent to the selected days.
□ ☒	Filters the **Camera/Sector** table by entering text criteria.
▽	Filters data in a column.

Filtering in the Camera/Sector Table

You can sort and filter the table by text or by column, or you can display only the relevant columns and rows in the table. See the following sections for more details:

- "Filtering by Text" on page 200
- "Sorting in Columns" on page 200
- "Filtering in Columns" on page 201
- "Displaying Selected Columns and Schedules" on page 201

Filtering by Text

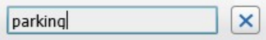
In the **Camera/Sector** table, you can filter for a text string. The filter applies to all columns and rows in the table.

When the text box field is empty, there is no active search and all resources appear.

As you enter letters, characters, or numbers in the text box, the table automatically refreshes with the selected criteria.

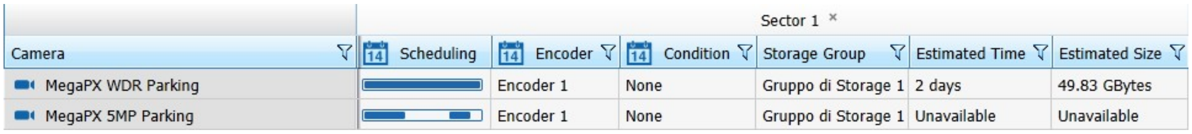
To filter by text

1 In the **Camera/Sector** table, enter the filter criteria in the text box.



parking ✕

The list refresh to display only those cameras that correspond to the filter criteria.



	Sector 1					
Camera	Scheduling	Encoder	Condition	Storage Group	Estimated Time	Estimated Size
MegaPX WDR Parking		Encoder 1	None	Gruppo di Storage 1	2 days	49.83 GBytes
MegaPX 5MP Parking		Encoder 1	None	Gruppo di Storage 1	Unavailable	Unavailable

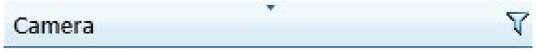
2 To remove the filter, click the ✕ button.

Sorting in Columns

You can alphabetically or numerically sort a column list (depending on the content of the list).

To sort in a column

1 Click on a column header to show the **Sort** ▲ icon.



2 Click the **Sort** icon to automatically sort the elements in the column list in ascending or descending alphabetical or numerical order.

Note: Click on the **Sort** icon again to change the order from ascending to descending or from descending to ascending.

Filtering in Columns

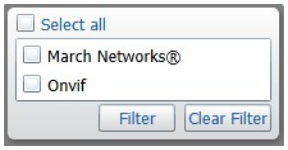
You can filter data in a column list to show only specified list values.

To filter in a column

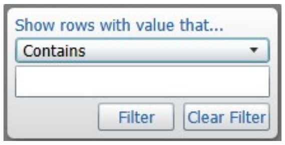
1. Select a column header and click the **Filter** icon.

   The **Filter** dialog box appears. According to the selected column, you can apply filters by type or by text.

   Filter by Type

   Filter by Text

2. For columns filtered by type, do one of the following:
   - Select one or more check boxes.
   - Click the **Select all** box to select all column elements.

   As you select a check box, the column list displays only those device details that match the specified filter criteria.

3. For columns filtered by text, do the following:

   a. Click the **Show rows with value that** drop-down list and select a filter expression.

      Options include **Contains** and **Does not contain**.

   b. Enter a filter criteria in the text box.

   c. Click **Filter** to apply the filter to the list.

      The column list displays only those device details that match the specified filter criteria.

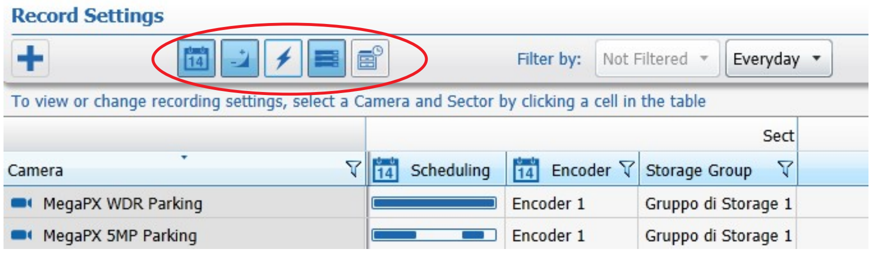
      Tip: To remove the filter, click the **Filter** icon in the column, and then click **Clear Filter**.

Displaying Selected Columns and Schedules

You can display only the relevant columns in the table by using the filter buttons. You can also display only the schedule correspondent to a specific schedule day, selected from the **Filter by** list in the **Camera/Sector** table toolbar.

To display selected columns and rows

1. In the **Camera/Sector** table toolbar click one or more filter buttons to show or hide the correspondent columns.

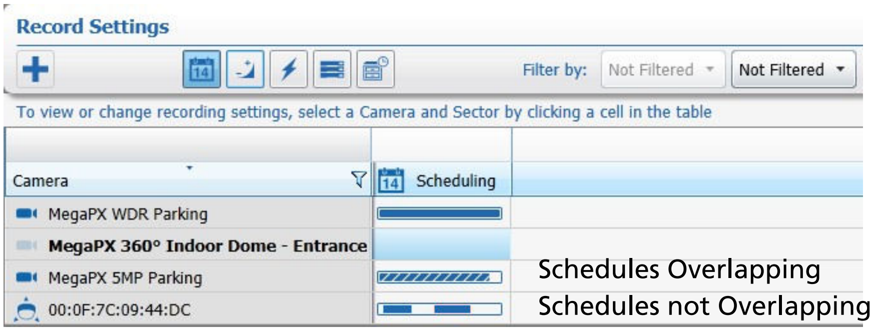


To view or change recording settings, select a Camera and Sector by clicking a cell in the table

Camera	Scheduling	Encoder	Storage Group
MegaPX WDR Parking		Encoder 1	Gruppo di Storage 1
MegaPX 5MP Parking		Encoder 1	Gruppo di Storage 1

2 Select a schedule day from the **Filter by** list to display only the correspondent schedules.

Note: By selecting the **Not Filtered** option, all of the schedules are displayed in the **Scheduling** column.



Record Settings

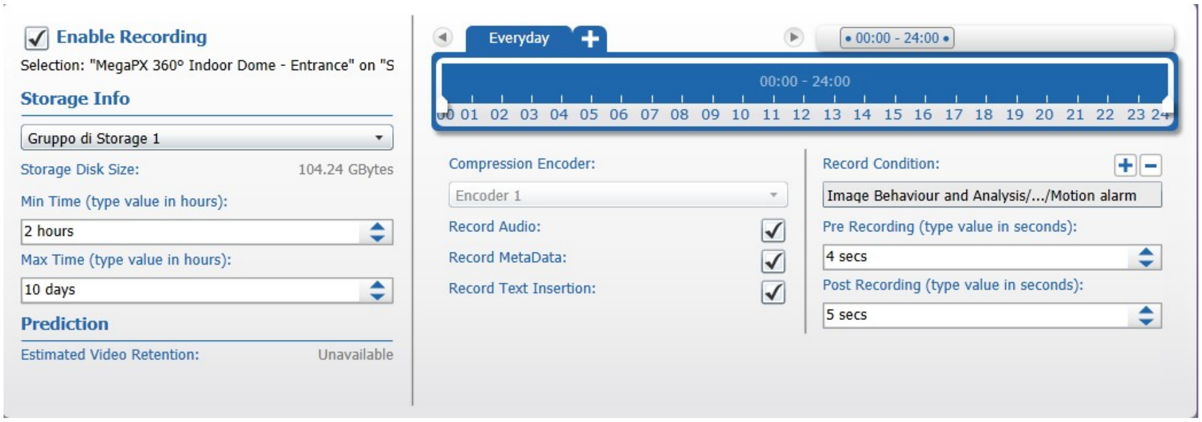
Filter by: Not Filtered | Not Filtered

To view or change recording settings, select a Camera and Sector by clicking a cell in the table

Camera	Scheduling
MegaPX WDR Parking	
MegaPX 360° Indoor Dome - Entrance	
MegaPX 5MP Parking	Schedules Overlapping
00:0F:7C:09:44:DC	Schedules not Overlapping

Settings Panel

The **Settings Panel** is located at the bottom of the screen and includes the scheduler. You can manage and configure the recording schedules and options using the **Settings Panel**.



☑ Enable Recording

Selection: "MegaPX 360° Indoor Dome - Entrance" on "S

Storage Info

Gruppo di Storage 1

Storage Disk Size: 104.24 GBytes

Min Time (type value in hours): 2 hours

Max Time (type value in hours): 10 days

Prediction

Estimated Video Retention: Unavailable

Everyday | 00:00 - 24:00

Compression Encoder: Encoder 1

Record Audio: ☑

Record MetaData: ☑

Record Text Insertion: ☑

Record Condition: Image Behaviour and Analysis/.../Motion alarm

Pre Recording (type value in seconds): 4 secs

Post Recording (type value in seconds): 5 secs

Creating Recording Sectors

By default, the Command Recording Software creates the first recording sector, **Sector 1**, automatically allocating storage space for every camera enabled for recording, according to the video resolution and bitrate. If you plan to apply the same recording conditions to every camera (for example the continuous recording of all resources) and you don't need to split the archive between different storage groups, you don't need to configure other recording sectors.

Optionally, you can create recording sectors to:

- Store evidence in different storage groups, based on the camera or recording method that is used to capture the evidence. For example, you can create one sector to store continuously recorded evidence with low resolution and frame rate, and you can create another sector to store evidence with maximum resolution and frame rate captured when alarm events occur.
- Allocate storage space based on the requirements of each recording sector.
- Specify how long evidence is retained for each sector on the disk. For example, you can retain alarm-related evidence longer than continuously recorded evidence.
- Create a mirror of one or more recording sectors to create a backup copy of recorded video evidence.

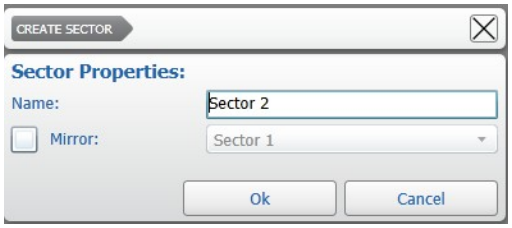
You can perform the following actions on a sector:

- Create a new sector. For more information, see "To create a recording sector" on page 203.
- Mirror an existing recording sector. For more information, see "Click the button to save and apply the changes." on page 204.
- Delete a recording sector. For more information, see "To delete a recording sector" on page 204.

To create a recording sector

1 On the **Scheduler Configuration** page, click the + button.

The **Create Sector** dialog box appears.



CREATE SECTOR

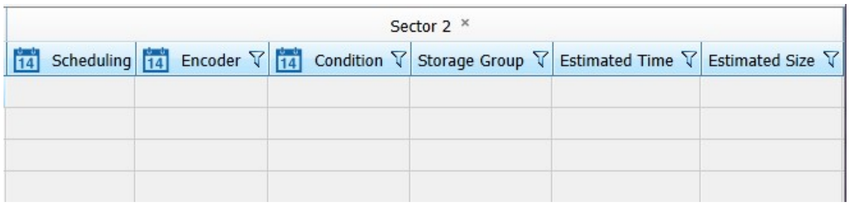
Sector Properties:

Name: Sector 2

□ Mirror: Sector 1

2 Enter a **Name** and click **Ok** to create a new recording sector.

All of the columns corresponding to the new recording sector are added to the **Camera/Sector** table.



Note: You can rename the sector by holding the mouse button on the sector name. After typing the new name, press **ENTER** to confirm.

3 Repeat step 1 to step 2 to create additional recording sectors.

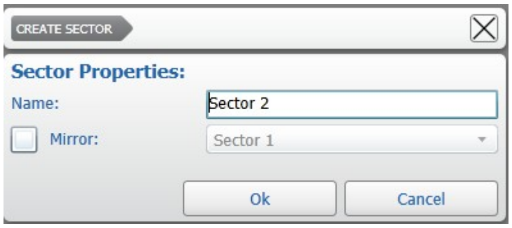
4 Click the 💾 button to save and apply the changes.

To mirror a recording sector

1 On the **Scheduler Configuration** page, create and a configure one or more recording schedules on a sector. For more information, see “Evidence Recording Methods” on page 205.

2 Click the ✚ button.

The **Create Sector** dialog box appears.



CREATE SECTOR

Sector Properties:

Name: Sector 2

□ Mirror: Sector 1

3 Select the **Mirror** check box.

4 Select a configured recording **Sector** from the list.

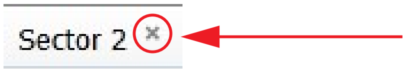
5 Click **OK**.

6 All of the columns corresponding to the mirror sector are added to the **Camera/ Sector** table. The columns display the same schedules as the mirrored sector.

7 Click the 💾 button to save and apply the changes.

To delete a recording sector

1 On the **Scheduler Configuration** page, click the (**X**) button that appears near the sector name.



A **Warning** dialog box appears.

2 Click **Yes** to confirm the sector deletion.

3 Click the 💾 button to save and apply the changes.

Evidence Recording Methods

You can choose one of the following methods to record evidence:

- **Continuous recording** — Recording of evidence occurs 24 hours a day, seven days a week. For more information, see "Configuring Continuous Recording" on page 205.
- **Programmed recording** — Recording only occurs on the dates and times you specify. For more information, see "Configuring Programmed Recording" on page 207.
- **On-event recording** — Recording only occurs when an event happens. For example, evidence is recorded when an alarm occurs, there is a network problem, or a particular user logs on to Command. For more information, see "Configuring On-Event Recording" on page 210.

Configuring Continuous Recording

The continuous recording method allows you to record the selected cameras 24 hours a day, 7 days a week.

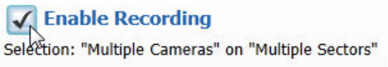
To configure continuous recording

1 On the **Scheduler Configuration** page, select one or more cells in the **Camera/Sector** table, corresponding to the cameras you want to record and to the sector where you want to record video evidence.

Tip: You can select multiple cells by holding down the **CTRL** or **SHIFT** key. To select all of the cameras and sectors, click a cell and press the **CTRL** + **A** keys.

Important: When Command connects to a camera from a 3000/4000/8000 Series recorder, the Command Recording Software becomes the primary recording machine. Otherwise, when Command disconnects from the camera, the DVR automatically switches the retention policy from the configured **Minimal Retention Period** to **Long Term Retention Period**. For more information, see the *Administrator Console User Manual* available for download from the March Networks Partner Portal and official websites.

2 In the **Settings** panel, select the **Enable Recording** check box.

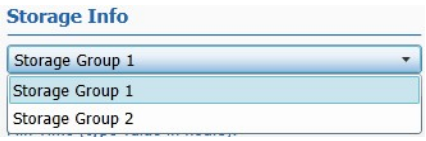


☑ Enable Recording

Selection: "Multiple Cameras" on "Multiple Sectors"

The cameras are set for recording.

3 Select the storage group from the **Storage Info** list.



Storage Info

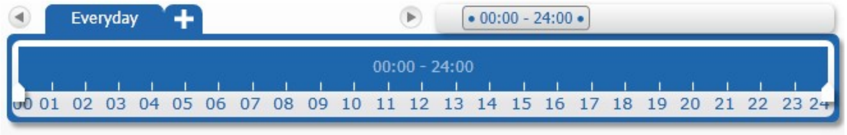
Storage Group 1

Storage Group 1

Storage Group 2

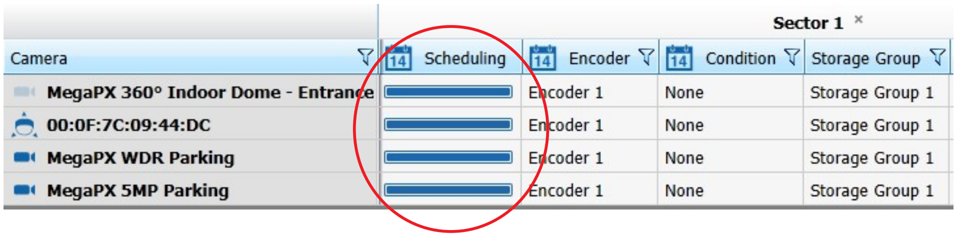
Note: For more information about adding and managing storage disks, see "Adding or Importing Storage Disks" on page 137.

4 Ensure the entire timeline (24 hours) is selected in the scheduler.



5 Click the 💾 button to save and apply the changes.

The schedule appears in the **Camera/Sector** table.



	Sector 1			
Camera	Scheduling	Encoder	Condition	Storage Group
MegaPX 360° Indoor Dome - Entrance	▬	Encoder 1	None	Storage Group 1
00:0F:7C:09:44:DC	▬	Encoder 1	None	Storage Group 1
MegaPX WDR Parking	▬	Encoder 1	None	Storage Group 1
MegaPX 5MP Parking	▬	Encoder 1	None	Storage Group 1

Customizing Camera Recording Options

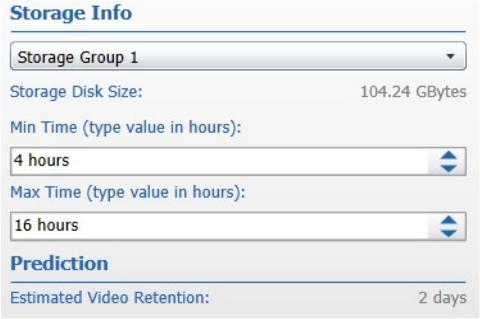
You can configure specific options for individual cameras, for example by removing audio from the video.

Note: You can customize recording options for every recording method.

To customize camera recording options

1 On the **Scheduler Configuration** page, select one or more cells in the **Camera/Sector** table.

2 In the **Settings** panel, in the **Storage Info** section, configure the **Min Time** and **Max Time** options.



Storage Info

Storage Group 1

Storage Disk Size: 104.24 GBytes

Min Time (type value in hours): 4 hours

Max Time (type value in hours): 16 hours

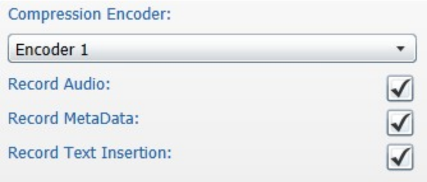
Prediction

Estimated Video Retention: 2 days

These options allow you to specify optional policies for the video evidence retention on the storage disk:

- The **Min Time** option specifies the minimum time the video evidence of a camera must remain in storage. Only video evidence older than the time interval specified can be purged from the storage.
- The **Max Time** option specifies the maximum time the video evidence of a camera can remain in storage. The video evidence older than the time interval specified is automatically purged from the storage.

3 Select an encoding profile from the **Compression Encoder** list, if applicable.



Compression Encoder:

Encoder 1

Record Audio: ☑

Record MetaData: ☑

Record Text Insertion: ☑

4 Select the **Record Audio** check box to add the audio track to the video evidence, if applicable.

5 Select the **Record Metadata** check box to add the analytics metadata to the video evidence, if applicable.

6 Select the **Record Text Insertion** check box to add overlay text to the video evidence, if applicable.

7 Repeat step 1 to step 6 to customize the recording options for other cameras.

8 Click the 💾 button to save and apply the changes.

Configuring Programmed Recording

The programmed recording method allows you to record selected cameras at set times and dates.

You can perform the following actions:

- Configure a programmed recording schedule. For more information, see “To configure programmed recording” on page 207.
- Delete a programmed recording schedule. For more information, see “To delete a programmed recording schedule” on page 209.

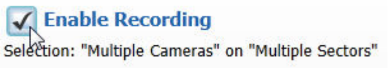
To configure programmed recording

1 On the **Scheduler Configuration** page, select one or more cells in the **Camera/Sector** table, corresponding to the cameras you want to record and to the sector where you want to record video evidence.

Tip: You can select multiple cells by holding down the **CTRL** or **SHIFT** key. To select all of the cameras and sectors, click a cell and press the **CTRL** + **A** keys.

Important: When Command connects to a camera from a 3000/4000/8000 Series recorder, the Command Recording Software becomes the primary recording machine. Otherwise, when Command disconnects from the camera, the DVR automatically switches the retention policy from the configured **Minimal Retention Period** to **Long Term Retention Period**. For more information, see the *Administrator Console User Manual* available for download from the March Networks Partner Portal and official websites.

2 In the **Settings** panel, select the **Enable Recording** check box.

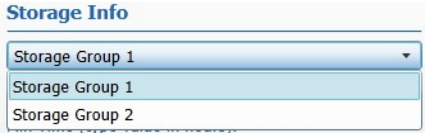


☑ Enable Recording

Selection: "Multiple Cameras" on "Multiple Sectors"

The cameras are set for recording.

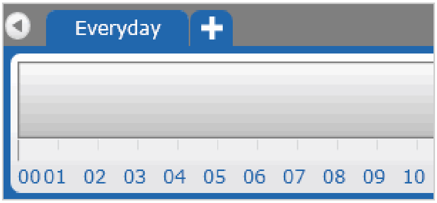
3 Select the storage group from the **Storage Info** list.



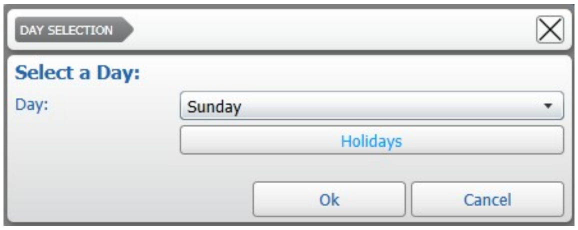
Note: For more information about adding and managing storage disks, see “Adding or Importing Storage Disks” on page 137.

4 Do one of the following:

- To program recording for every day, use the default **Everyday** tab.
- To configure the scheduler for a specific day of the week/month, click the tab + to create a new tab for a specific day.

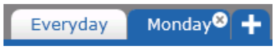


The **Day Selection** dialog box appears.



Select a day from the list and click **Ok**.

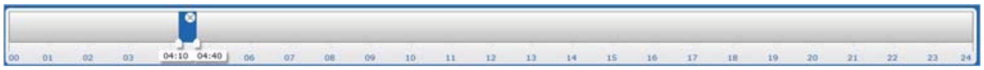
The tab for the selected day is added to the list.



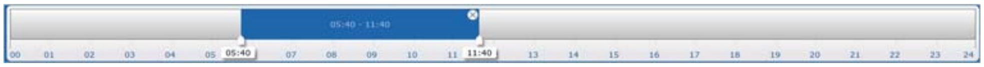
Note: When recording schedules conflict (for example, the **Everyday** tab is configured to record from 10 A.M., while the **Monday** tab is configured to record from 8 A.M.), Command follows an internal priority list. The priority, starting from top to bottom, is: Holiday, 1st/10th/15th day of the month, Single day of the week, Everyday.

5 To select a time interval for that day using the timeline, do the following:

- Click and hold the left mouse button down at the desired start time.

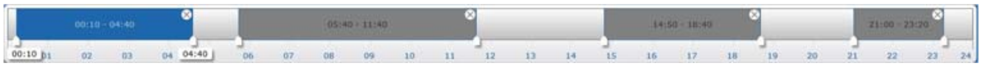


- Click and drag to define the length of the time interval.



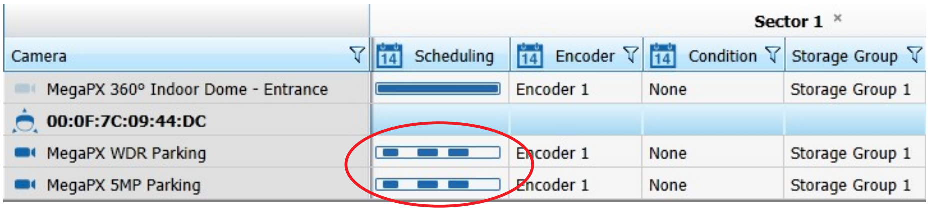
Tip: To resize a time interval, click and drag the white tab at the beginning of at the ending of the interval. To move a time interval, click and drag inside the interval.

- You can set multiple time intervals for the same day. Every time interval on the time line has its own recording schedule. Click a time interval to select it or hold down the **SHIFT** key to select multiple intervals.



6. Click the 💾 button to save and apply the changes.
7. Customize the recording options for individual cameras. For more information, see “Customizing Camera Recording Options” on page 206.

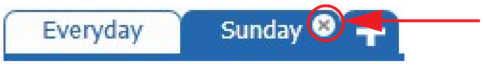
   The schedule appears in the **Camera/Sector** table.



	Sector 1 ×			
Camera	Scheduling	Encoder	Condition	Storage Group
MegaPX 360° Indoor Dome - Entrance		Encoder 1	None	Storage Group 1
00:0F:7C:09:44:DC				
MegaPX WDR Parking		Encoder 1	None	Storage Group 1
MegaPX 5MP Parking		Encoder 1	None	Storage Group 1

To delete a programmed recording schedule

1. On the **Scheduler Configuration** page, select one or more cells in the **Camera/Sector** table, corresponding to the cameras and sectors configured with the programmed recording schedule.
2. In the **Settings** panel, click the (**X**) button that appears on the upper right corner of the day tab.



   A confirmation dialog box appears.

3. Click **Yes** to confirm the schedule deletion.
4. Click the 💾 button to save and apply the changes.

Configuring On-Event Recording

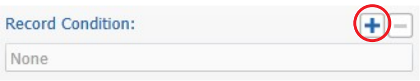
The on-event recording method allows you to initiate recording on selected cameras when an event occurs. An event can be the triggering of an alarm, a network disconnection, a particular user account that connects to the Command Recording Software or a custom event you create.

To configure on-event recording

1 Configure a programmed recording and customize the recording options for individual cameras.

For more information, see “Configuring Programmed Recording” on page 207 and “Customizing Camera Recording Options” on page 206.

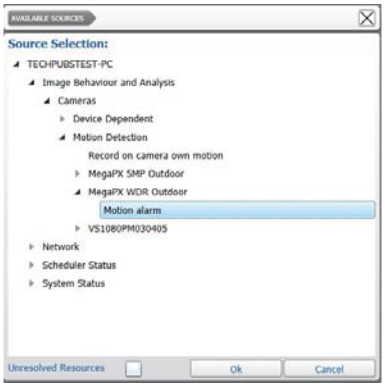
2 In the **Settings** panel, in the **Recorder condition** section, click the + button to add the condition that triggers the recording.



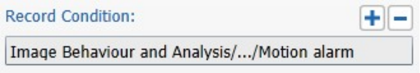
Record Condition:

None

The **Available Sources** dialog box appears.



3 Select a condition from the **Source Selection** list and click **Ok**.



Record Condition:

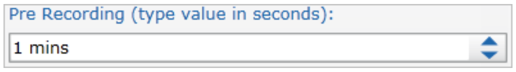
Image Behaviour and Analysis/.../Motion alarm

Note: You can include unresolved resources to the tree by selecting the **Unresolved Resources** check box. Unresolved resources are conditions based on sources that are added to the Command Recording Software, but currently not available. For example, the motion detection feature of a camera currently disconnected.

The condition is added to the scheduler.
Tip: Repeat step 2 to step 3 to change the condition, or select the condition and click the − button to remove the condition.

4 Configure the **Pre Recording** time interval to create a video buffer that Command uses to start the recording before the event.

For example: If you configure a **Pre Recording** time interval of one minute, Command will constantly buffer a minute of video recording. When the event happens, Command starts recording live video and automatically adds the one minute video buffer to the video evidence.

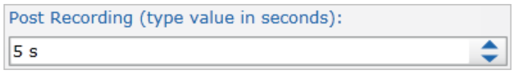


Pre Recording (type value in seconds):

1 mins

5 Configure the **Post Recording** time interval to force Command to continue recording after the event has happened.

For example: if you configure an alarm as the event and a **Post Recording** time interval of five seconds, Command will continue recording for five seconds after the alarm is turned off.

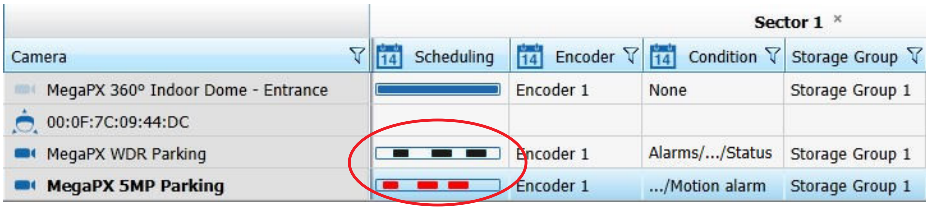


Post Recording (type value in seconds):

5 s

6 Click the 💾 button to save and apply the changes.

The schedule appears in the **Camera/Sector** table. Schedules for post-event recording are represented as red timelines for recording on motion detection, or as black timelines for generic post-event recording as in the following image.



	Sector 1			
Camera	Scheduling	Encoder	Condition	Storage Group
MegaPX 360° Indoor Dome - Entrance	▬	Encoder 1	None	Storage Group 1
00:0F:7C:09:44:DC				
MegaPX WDR Parking	■ ■ ■	Encoder 1	Alarms/.../Status	Storage Group 1
MegaPX 5MP Parking	🟥 🟥 🟥	Encoder 1	.../Motion alarm	Storage Group 1

Recording Indicator

The recording indicator allows you to check if Command is currently recording a camera.

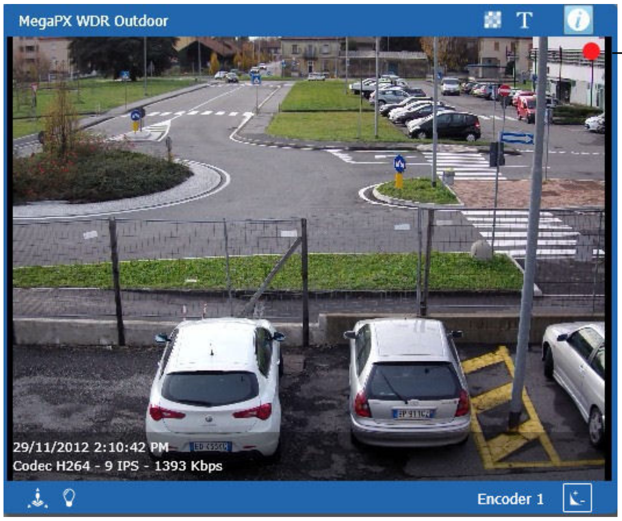
To check if Command is recording a camera

1 On the Command Config main page, under **Device Management**, click **Cameras**.

The **Camera Configuration** page appears.

2 Select a camera in the **Camera List** panel.

3 Check the Video Preview window. The Recording Indicator means that Command is recording the camera's video stream.



29/11/2012 2:10:42 PM
Codec H264 - 9 IPS - 1393 Kbps

Recording Indicator

Chapter 12

Creating and Customizing Alarms

You can create and customize alarms on a Command Recording Software on the **Alarm Configuration** page. You can also select which cameras are triggered after an event, launch PTZ actions, and automatically send alarm notifications.

Note: You can acknowledge alarms using Command Client or SiteManager. For more information, see the *Command Client User Guide* and the *SiteManager User Guide*, available on the Software DVD or from the March Networks Partner Portal and official websites.

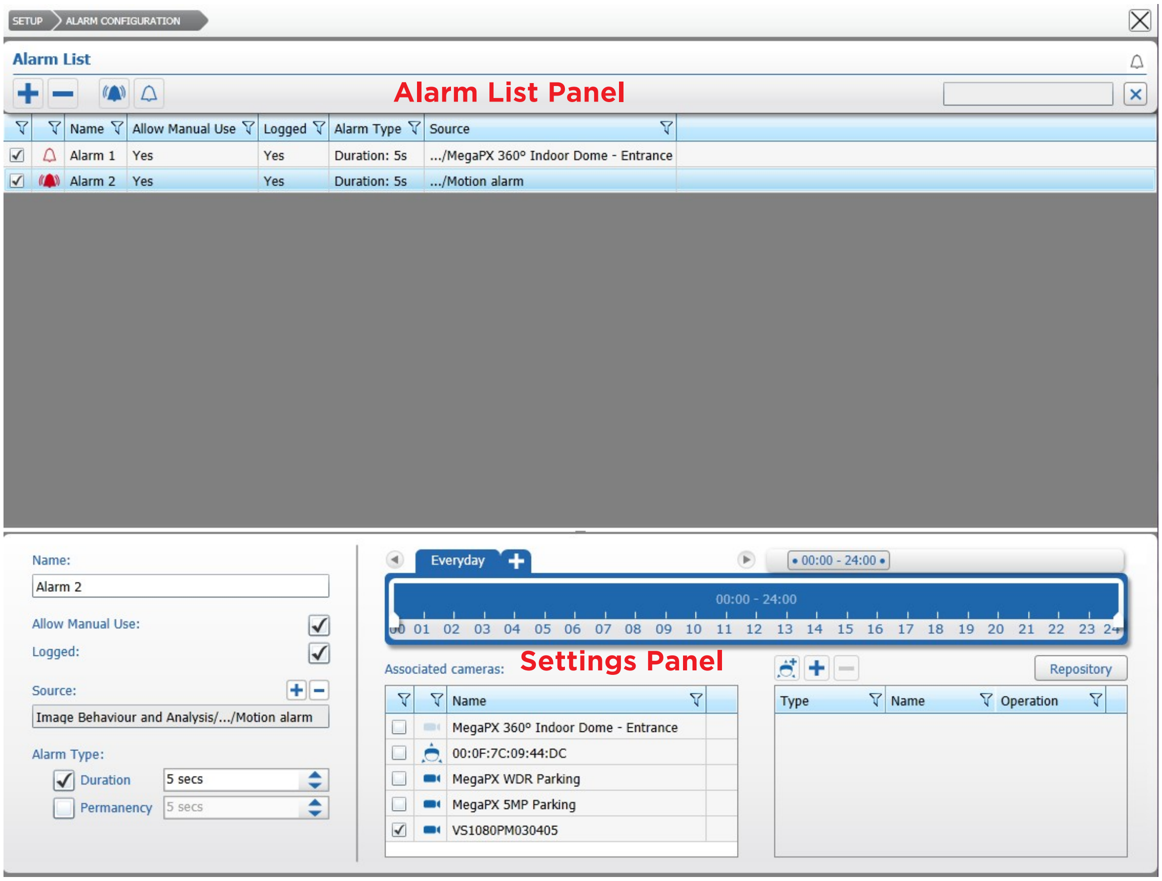
This chapter contains the following sections:

Overview

The **Alarm Configuration** page allows you to create and customize alarms. You can create alarms based on any condition in the condition tree.

To access the page, on the Command Config main page, under **Device Management**, click **Alarms**.

The following illustration shows the **Alarm Configuration** user interface.



Alarm List Panel

		Name	Allow Manual Use	Logged	Alarm Type	Source
☑		Alarm 1	Yes	Yes	Duration: 5s	.../MegaPX 360º Indoor Dome - Entrance
☑		Alarm 2	Yes	Yes	Duration: 5s	.../Motion alarm

Name: Alarm 2

Allow Manual Use: ☑

Logged: ☑

Source: Image Behaviour and Analysis/.../Motion alarm

Alarm Type:

☑ Duration 5 secs

□ Permanency 5 secs

Associated cameras:

Settings Panel

		Name
□		MegaPX 360º Indoor Dome - Entrance
□		00:0F:7C:09:44:DC
□		MegaPX WDR Parking
□		MegaPX 5MP Parking
☑		VS1080PM030405

Type	Name	Operation

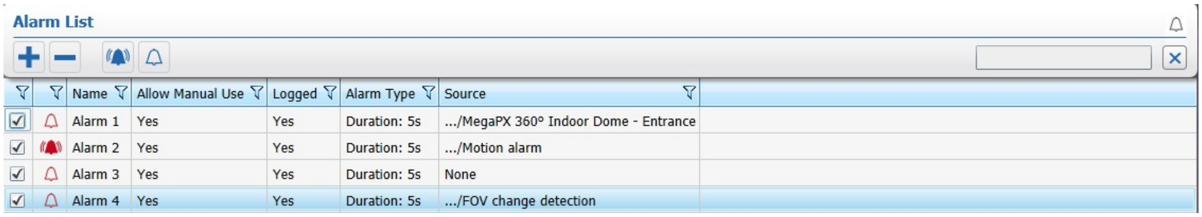
The **Alarm Configuration** page is divided into two main areas.

1 **Alarm List** panel — Located at the top of the screen, it allows you to create, filter, select and turn on/off the available alarms.

2 **Settings** panel — Located at the bottom of the screen, it allows you to manage and configure the alarms.

Alarm List Panel

The **Alarm List** panel is located at the top of the screen. You can create, filter, select, and turn on/off alarms using the **Alarm List** panel.



Alarm List

		Name	Allow Manual Use	Logged	Alarm Type	Source
☑	🔔	Alarm 1	Yes	Yes	Duration: 5s	.../MegaPX 360° Indoor Dome - Entrance
☑	🔔	Alarm 2	Yes	Yes	Duration: 5s	.../Motion alarm
☑	🔔	Alarm 3	Yes	Yes	Duration: 5s	None
☑	🔔	Alarm 4	Yes	Yes	Duration: 5s	.../FOV change detection

The following table provides a description of the panel buttons.

Button	Action
+	Creates a new alarm.
−	Deletes the selected alarm.
🔔	Turns the selected alarm on.
🔔	Turns the selected alarm off.
▭ ☒	Filters the alarm list by entering text criteria.
▽	Filters data in a column.
☑	Enables/disables the selected alarm.

Alarm Status Icons

The following status icons appear in the **Alarm List** panel:

Icon	Description
🔔	Alarm turned off
🔔	Alarm turned on
🔔	Alarm disabled
🔔	Alarm created, but not configured

Filtering in the Alarm List Panel

You can sort and filter the alarms by text or by column. See the following sections for more details:

- “Filtering by Text” on page 216
- “Sorting in Columns” on page 216
- “Filtering in Columns” on page 217

Filtering by Text

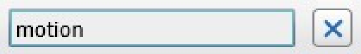
In the **Alarm List** panel, you can filter for a text string. The filter applies to all columns in the **Alarm List** panel.

When the text box field is empty, there is no active search and all resources appear.

As you enter letters, characters, or numbers in the text box, the **Alarm List** panel automatically refreshes with the selected criteria.

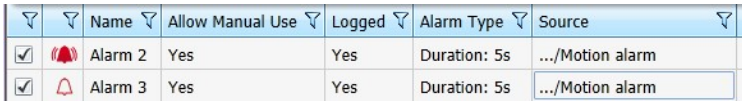
To filter by text in the Alarm List panel

1 On the **Alarm List** panel, enter the filter criteria in the text box.



motion ☒

The panel refresh to display only those alarms that correspond to the filter criteria.



		Name	Allow Manual Use	Logged	Alarm Type	Source
☑	🔔	Alarm 2	Yes	Yes	Duration: 5s	.../Motion alarm
☑	🔔	Alarm 3	Yes	Yes	Duration: 5s	.../Motion alarm

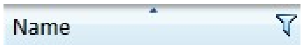
2 To remove the filter, click the ☒ button.

Sorting in Columns

You can alphabetically or numerically sort a column list (depending on the content of the list).

To sort in a column

1 Click on a column header to show the **Sort** ▲ icon.



Name

2 Click the **Sort** icon to automatically sort the elements in the column list in ascending or descending alphabetical or numerical order.

Note: Click on the **Sort** icon again to change the order from ascending to descending or from descending to ascending.

Filtering in Columns

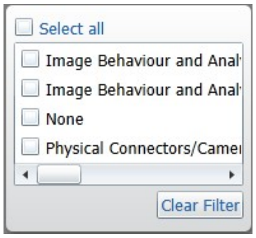
You can filter data in a column list to show only specified list values.

To filter in a column

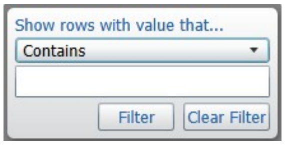
1 Select a column header and click the **Filter** icon.

The **Filter** dialog box appears. According to the selected column, you can apply filters by type or by text.

Filter by Type


□ Select all
□ Image Behaviour and Anal
□ Image Behaviour and Anal
□ None
□ Physical Connectors/Camer
Clear Filter

Filter by Text



2 For columns filtered by type, do one of the following:

- Select one or more check boxes.
- Click the **Select all** box to select all column elements.

As you select a check box, the column list displays only those alarms details that match the specified filter criteria.

3 For columns filtered by text, do the following:

a Click the **Show rows with value that** drop-down list and select a filter expression.

Options include **Contains** and **Does not contain**.

b Enter a filter criteria in the text box.

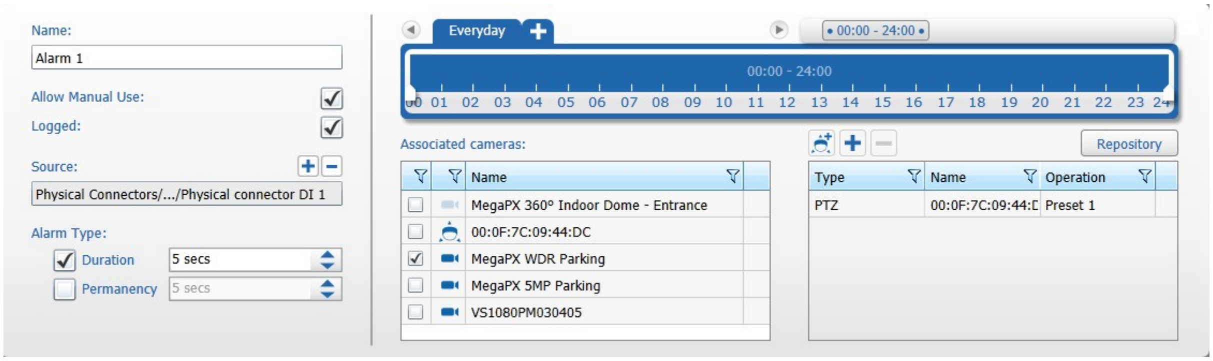
c Click **Filter** to apply the filter to the list.

The column list displays only those alarms details that match the specified filter criteria.

Tip: To remove the filter, click the **Filter** icon in the column, and then click **Clear Filter**.

Settings Panel

The **Settings Panel** is located at the bottom of the screen. You can manage and configure the available alarms and their schedules using the **Settings Panel**.



Name: Alarm 1

Allow Manual Use: ☑

Logged: ☑

Source: Physical Connectors/.../Physical connector DI 1

Alarm Type:

☑ Duration 5 secs

□ Permanency 5 secs

Everyday • 00:00 - 24:00 •

Associated cameras:

	Name
□	MegaPX 360º Indoor Dome - Entrance
□	00:0F:7C:09:44:DC
☑	MegaPX WDR Parking
□	MegaPX 5MP Parking
□	VS1080PM030405

Type	Name	Operation
PTZ	00:0F:7C:09:44:D	Preset 1

Creating Alarms

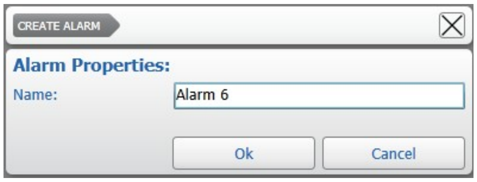
You can create and customize alarms on Command using system events, camera-related events, or custom events.

Note: You can create custom events on the **Custom Conditions** page. For more information, see "Creating Custom Conditions" on page 252.

To create an alarm

1 On the **Alarm Configuration** page, click the ✚ button.

The **Create Alarm** dialog box appears.



CREATE ALARM

Alarm Properties:

Name: Alarm 6

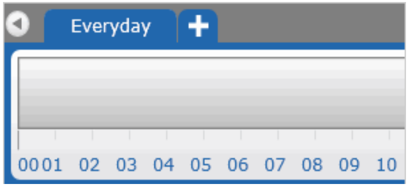
2 Enter a name for the alarm and click **Ok**.

The alarm is added to the **Alarm List** panel.

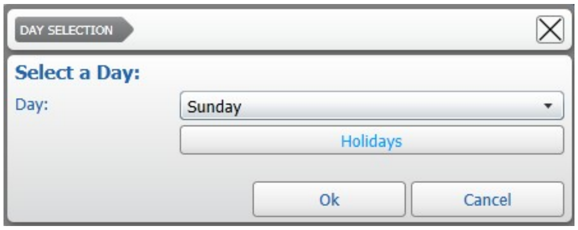
Note: You can rename the alarm by holding the mouse button on the alarm name or using the **Settings** panel. After typing the new name, press **ENTER** to confirm.

3 In the **Settings panel**, in the **Scheduler** section, do one of the following:

- To configure the alarm activity for every day, use the default **Everyday** tab.
- To configure the alarm activity for a specific day of the week/month, click the plus tab ✚ to create a new tab for a specific day.



The **Day Selection** dialog box appears.



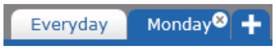
DAY SELECTION

Select a Day:

Day: Sunday

Select a day from the list and click **Ok**.

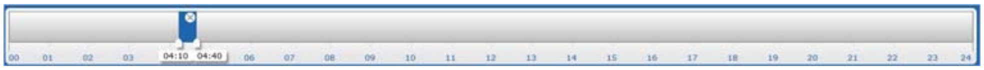
The tab for the selected day is added to the list.



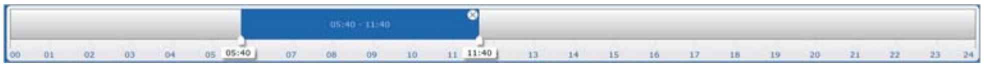
Note: When schedules conflict (for example, the **Everyday** tab is configured from 10 A.M., while the **Monday** tab is configured from 8 A.M.), Command follows an internal priority list. The priority, starting from top to bottom, is: Holiday, 1st/10th/15th day of the month, Single day of the week, Everyday.

4 To select a time interval for that day using the timeline, do the following:

- Click and hold the left mouse button down at the desired start time.

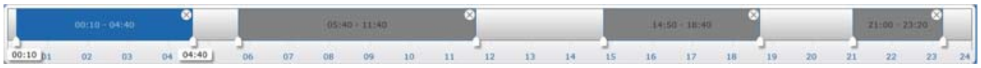


- Click and drag to define the length of the time interval.

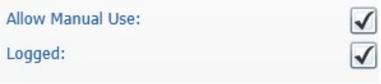


Tip: To resize a time interval, click and drag the white tab at the beginning of at the ending of the interval. To move a time interval, click and drag inside the interval.

- You can set multiple time intervals for the same day. Every time interval on the time line has its own schedule. Click a time interval to select it or hold down the **SHIFT** key to select multiple intervals.



5 Select the **Allow Manual Use** check box to allow users to modify the alarm status to test the alarm effectiveness.



Allow Manual Use: ☑

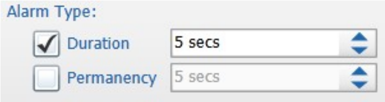
Logged: ☑

Tip: To modify the alarm status, click the 🔔 (alarm triggered) or 🔔 (alarm not triggered) buttons on the **Alarm List** panel toolbar.

6 Select the **Logged** check box to save the alarm activity information in the system log.

7 In the **Alarm Type** section, select one of the following alarm management modes:

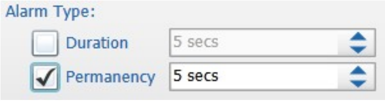
- **Duration** — The alarm is turned on for the entire duration of the event and turned off after the specified period of time following the end of the event.



Alarm Type:
☑ Duration 5 secs
□ Permanency 5 secs

For example, if you select a time period of 5 seconds for **Duration**, and the event that triggers the alarm lasts 20 seconds, the alarm will be on for 25 seconds.

- **Permanency** — The alarm is turned off after the specified period of time following the beginning of the alarm.

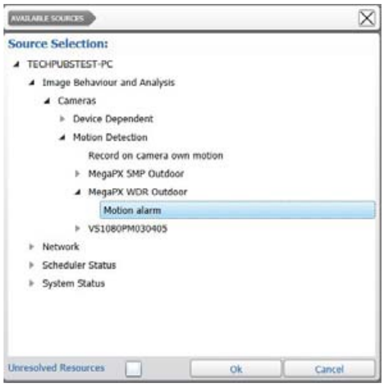


Alarm Type:
□ Duration 5 secs
☑ Permanency 5 secs

For example, if you select a time period of 5 seconds for **Permanency**, and the event that triggers the alarm lasts 20 seconds, the alarm will only be on for 5 seconds.

8 In the **Source** section, click the + button to add the source condition that triggers the alarm.

The **Available Sources** dialog box appears.



AVAILABLE SOURCES

Source Selection:

```
TECHPUBSTEST-PC
  Image Behaviour and Analysis
    Cameras
      Device Dependent
      Motion Detection
        Record on camera own motion
        MegaPX SMP Outdoor
        MegaPX WDR Outdoor
          Motion alarm
        VS1080PM030405
  Network
  Scheduler Status
  System Status
```

Unresolved Resources □ Ok Cancel

9 Select a condition from the **Source Selection** list and click **Ok**.

Note: You can include unresolved resources to the tree by selecting the **Unresolved Resources** check box. Unresolved resources are conditions based on sources that are added to the Command Recording Software, but currently not available. For example, the motion detection feature of a camera currently disconnected.

The condition is added to the **Source** field.

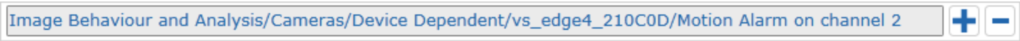
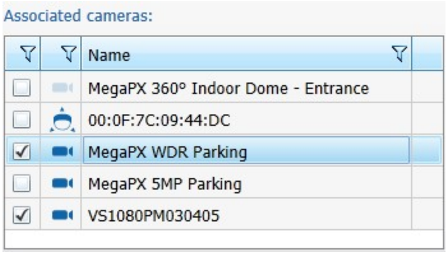


Image Behaviour and Analysis/Cameras/Device Dependent/vs_edge4_210C0D/Motion Alarm on channel 2

Tip: Click the − button to remove the condition.

10 To associate the alarm to one or more cameras, select the check boxes corresponding to the cameras you want to associate in the **Associated Cameras** section.

Tip: You can select multiple cameras by holding down the **CTRL** or **SHIFT** key.



Associated cameras:

		Name
□		MegaPX 360° Indoor Dome - Entrance
□		00:0F:7C:09:44:DC
☑		MegaPX WDR Parking
□		MegaPX 5MP Parking
☑		VS1080PM030405

11 Repeat step 1 to step 10 to create additional alarms.

12 Click the 💾 button to save and apply the changes.

Managing Alarms

After creating an alarm, you can automatically configure post-event PTZ actions and set Command to send automatic notifications after an alarm.

Select your configuration:

- “Configuring Post-Event PTZ Actions” on page 221
- “Setting Automatic Alarm Notifications” on page 222

Configuring Post-Event PTZ Actions

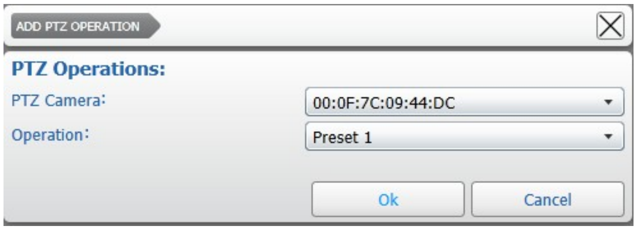
The **Alarm Configuration** page allows you to configure a PTZ action that a PTZ camera is forced to perform after an alarm is triggered.

To configure a post-event PTZ action

1 On the **Alarm Configuration** page, select an alarm in the **Alarm List** panel.

2 In the **Settings** panel, in the **Actions** panel under the scheduler, click the button.

The **PTZ Operations** dialog box appears.



ADD PTZ OPERATION

PTZ Operations:

PTZ Camera: 00:0F:7C:09:44:DC

Operation: Preset 1

3 Select an enabled **PTZ Camera** from the list.

4 Select a configured PTZ action (tour, preset view, or preset tour) from the **Operation** list.

Notes:

- You can also select PTZ cameras not currently associated to the alarm.
- You must select a valid preset or tour. You can configure these actions on the **Camera Configuration** page. For more information, see “Saving Preset Views and Tours” on page 188.
- Post-event PTZ actions have the priority over “standard” scheduled PTZ actions. For more information, about standard PTZ actions, see “Saving Preset Views and Tours” on page 188.

5 Repeat step 2 to step 4 to configure additional actions on different PTZ cameras.

6 Click the 💾 button to save and apply the changes.

Setting Automatic Alarm Notifications

You can send e-mails to the specified addresses, set automatic alarm notifications to a computer running SiteManager, or to a server running the Benbria Blazecast software using the **Alarm Configuration** page.

Important: Before you create e-mail and Benbria notification actions, you must configure the **Email Profile** and **BENBRIA Profile** options in the **System Configuration** page. For more information, see “Configuring Services” on page 115.

Select your configuration:

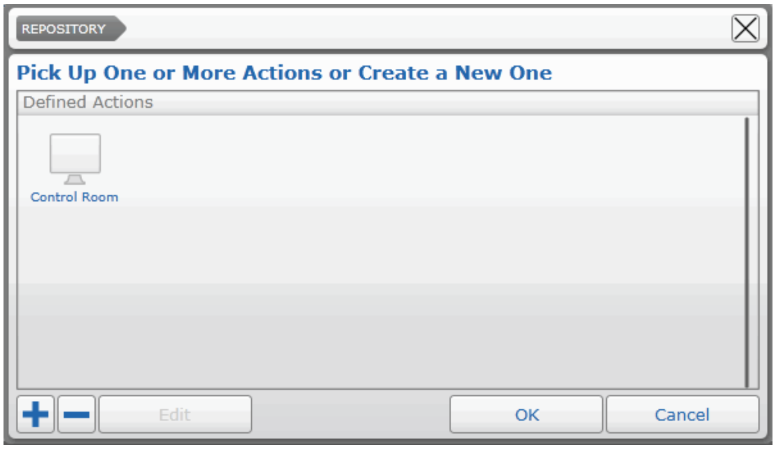
- “To set automatic e-mail notifications” on page 222
- “To set automatic notifications to SiteManager” on page 224
- “To set automatic notifications to Benbria Blazecast servers” on page 226

To set automatic e-mail notifications

1 On the **Alarm Configuration** page, select an alarm in the **Alarm List** panel.

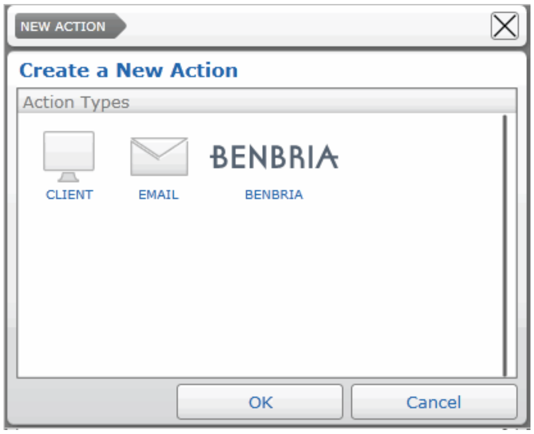
2 In the **Settings** panel, in the **Actions** panel under the scheduler, click the ✚ button.

The **Repository** dialog box appears.



3 Click the + button to create the notification action.

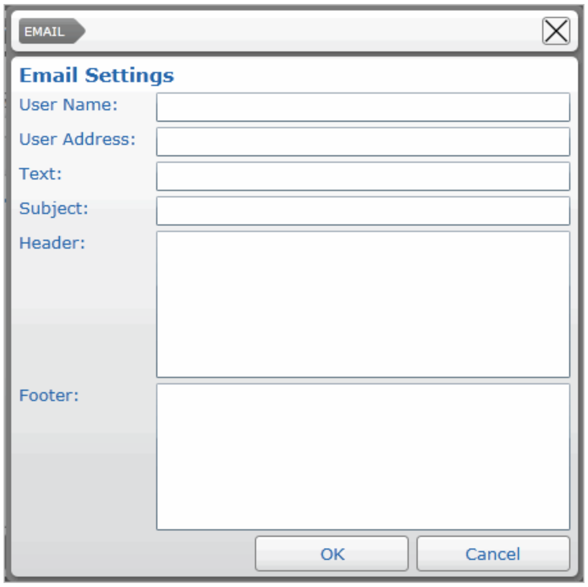
The **New Action** dialog box appears.



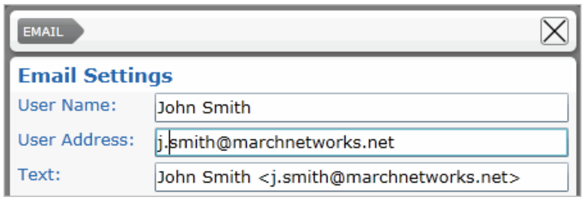
Tip: Alternatively, you can select an action configured for a different alarm and click **Edit**.

4 Select the **EMAIL** icon and click **Ok**.

The **Email** dialog box appears.



5 Enter the recipient **Name** and **Address**.



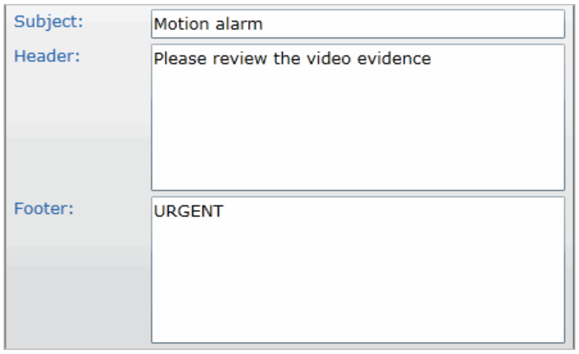
User Name: John Smith

User Address: j.smith@marchnetworks.net

Text: John Smith <j.smith@marchnetworks.net>

Tip: You can optionally modify the **Text** for the *To* field of the e-mail.

6 Enter the e-mail **Subject**, the e-mail body (**Header**), and the e-mail **Footer**.



Subject: Motion alarm

Header: Please review the video evidence

Footer: URGENT

7 Click **Ok**. The notification action appears in the **Repository** dialog box. Click **Ok**.

The notification action is added to the alarm.

Tip: To modify an automatic notification action:

a Click the **Repository** button.

The **Repository** dialog box appears.

b Select the notification icon and click **Edit**. Alternatively, you can delete the notification by clicking the − button.

8 Click the 💾 button to save and apply the changes.

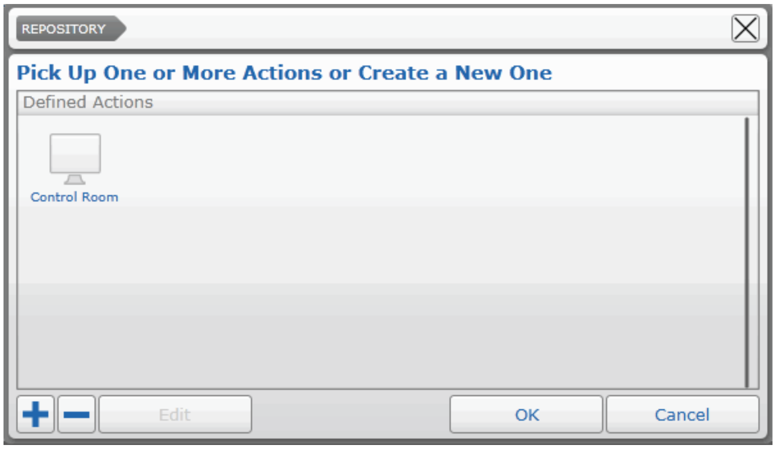
Command automatically notifies the alarm by sending an e-mail to the specified address, using the SMTP server specified in the **System Configuration** page. For more information, see “Configuring Services” on page 115.

To set automatic notifications to SiteManager

1 On the **Alarm Configuration** page, select an alarm in the **Alarm List** panel.

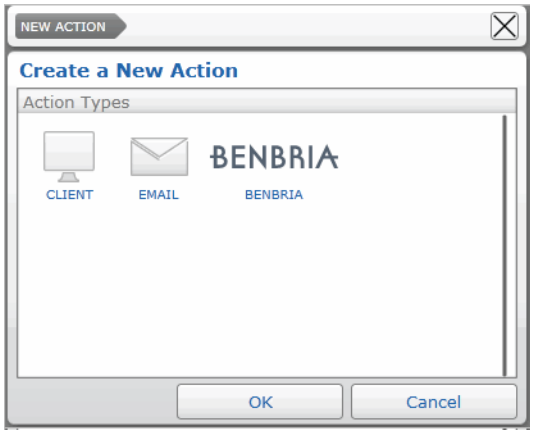
2 In the **Settings** panel, in the **Actions** panel under the scheduler, click the + button.

The **Repository** dialog box appears.



Pick Up One or More Actions or Create a New One

3 Click the + button to create the notification action.

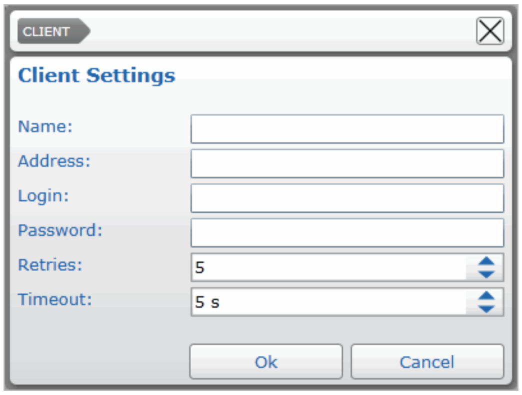


The **New Action** dialog box appears.

Tip: Alternatively, you can select an action configured for a different alarm and click **Edit**.

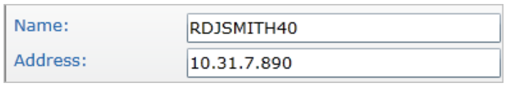
4 Select the **CLIENT** button and click **Ok**.

The **Client** dialog box appears.



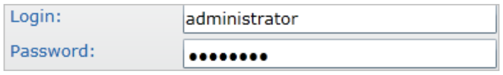
Name:
Address:
Login:
Password:
Retries: 5
Timeout: 5 s

5 Enter the computer **Name** and its IP **Address**.



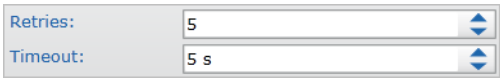
Name: RDJSMITH40
Address: 10.31.7.890

6 Enter the credentials (**Login** and **Password)** that are used to log on to SiteManager.



Login: administrator
Password: ••••••••

7 Select the maximum number of **Retries**, and the **Timeout** for the connection to the computer running SiteManager.



Retries: 5
Timeout: 5 s

8 Click **Ok**. The notification action appears in the **Repository** dialog box. Click **Ok**.

The notification action is added to the alarm.

Tip: To modify an automatic notification action:

a Click the **Repository** button.

The **Repository** dialog box appears.

b Select the notification icon and click **Edit**. Alternatively, you can delete the notification by clicking the − button.

9 Click the 💾 button to save and apply the changes.

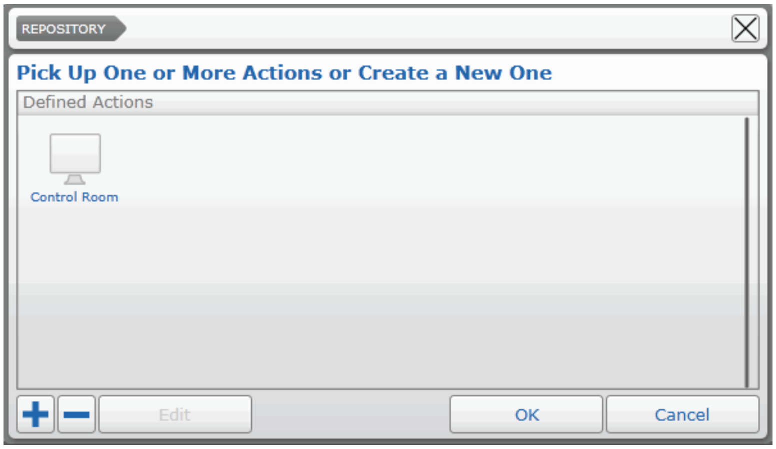
Command automatically notifies the alarm to the SiteManager application installed on the specified computer. For more information about the SiteManager application, see the *SiteManager User Guide*, available for download from the March Networks Partner Portal and official websites.

To set automatic notifications to Benbria Blazecast servers

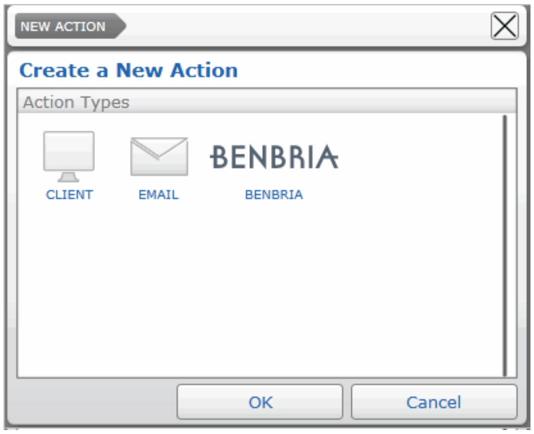
1 On the **Alarm Configuration** page, select an alarm in the **Alarm List** panel.

2 In the **Settings** panel, in the **Actions** panel under the scheduler, click the + button.

The **Repository** dialog box appears.



3 Click the + button to create the notification action.

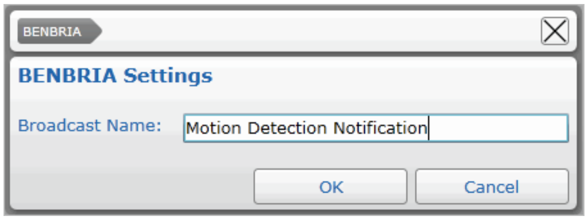


The **New Action** dialog box appears.

Tip: Alternatively, you can select an action configured for a different alarm and click **Edit**.

4 Select the **BENBRIA** button and click **Ok**.

The **Benbria** dialog box appears.



BENBRIA Settings

Broadcast Name: Motion Detection Notification

5 Enter a custom title for the notification in the **Broadcast Name** text box.

6 Click **Ok**. The notification action appears in the **Repository** dialog box. Click **Ok**.

The notification action is added to the alarm.

Tip: To modify an automatic notification action:

a Click the **Repository** button.

The **Repository** dialog box appears.

b Select the notification icon and click **Edit**. Alternatively, you can delete the notification by clicking the − button.

7 Click the 💾 button to save and apply the changes.

Command automatically notifies the alarm to the Benbria Blazecast server specified in the **System Configuration** page. For more information, see “Configuring Services” on page 115.

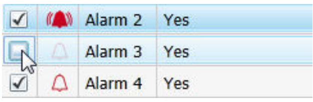
Disabling an Alarm

You can temporarily disable an alarm in Command.

To disable an alarm

1 On the **Alarm Configuration** page, select the alarm you want to disable in the **Alarm List** panel.

2 Clear the check box corresponding to the alarm in the **Alarm List** panel.



☑	🔔	Alarm 2	Yes
□	🔔	Alarm 3	Yes
☑	🔔	Alarm 4	Yes

3 Click the 💾 button to save and apply the changes.

Note: You can enable the alarm again by selecting alarm’s check box.

Deleting Alarms

If you no longer need an alarm, you can delete it from the alarm list.

To delete an alarm

1. On the **Alarm Configuration** page, select the alarm you want to delete in the **Alarm List** panel.
2. Click the − button to delete the alarm.

   A confirmation dialog box appears.
3. Click **Yes** to confirm the alarm deletion.
4. Click the 💾 button to save and apply the changes.

Chapter 13

Managing Switches

Command automatically detects the auxiliary channels (*switches*) of March Networks and selected IP cameras or a Command Recording Software through the Input/Output Extension Board. You can easily manage and activate auxiliary devices after an alarm or an event on the **Switch Configuration** page.

This chapter contains the following sections:

Notes:

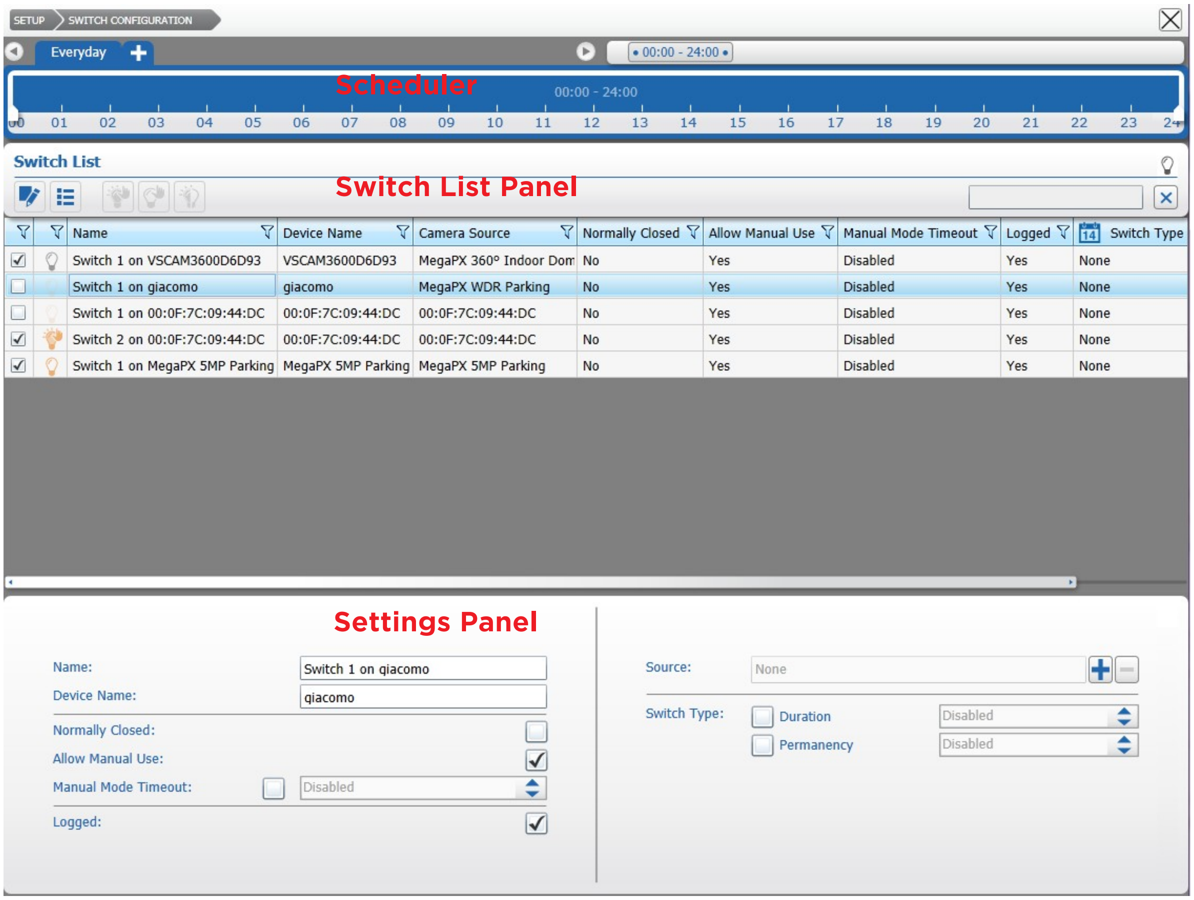
- The switches that the Command Recording Software automatically detects on the added devices are disabled by default.
- When upgrading the Command Recording Software from a version lower than 1.6, the switches names are also updated from *Aux #* to *Switch #*. To confirm the changes, access the new **Switch Configuration** page and click the 💾 button.
- When upgrading the Command Recording Software from a version lower than 1.6, the switches belonging to devices added to the Command Recording Software are always enabled.
- When an Edge 4 encoder is added to the Command Recording Software, the server duplicates the four switches for all of the channels, listing a total of 16 different switches. To avoid unexpected behavior, especially after an upgrade from a previous Command Recording Software version, it is recommended that you disable the duplicate switches.
- If the same camera is added to two or more Command Recording Softwares on the system, it is strongly recommended that you enable and configure the switches of the camera on a single Command Recording Software.

Overview

The **Switch Configuration** page allows you to add March Networks Extension Boards, and manage and configure the auxiliary channels of March Networks cameras.

To access the page, on the Command Config main page, under **Device Management**, click **Switches**.

The following illustration shows the **Switch Configuration** user interface.



		Name	Device Name	Camera Source	Normally Closed	Allow Manual Use	Manual Mode Timeout	Logged	Switch Type
☑		Switch 1 on VSCAM3600D6D93	VSCAM3600D6D93	MegaPX 360º Indoor Dom	No	Yes	Disabled	Yes	None
□		Switch 1 on giacomo	giacomo	MegaPX WDR Parking	No	Yes	Disabled	Yes	None
□		Switch 1 on 00:0F:7C:09:44:DC	00:0F:7C:09:44:DC	00:0F:7C:09:44:DC	No	Yes	Disabled	Yes	None
☑		Switch 2 on 00:0F:7C:09:44:DC	00:0F:7C:09:44:DC	00:0F:7C:09:44:DC	No	Yes	Disabled	Yes	None
☑		Switch 1 on MegaPX 5MP Parking	MegaPX 5MP Parking	MegaPX 5MP Parking	No	Yes	Disabled	Yes	None

Name: Switch 1 on giacomo

Device Name: giacomo

Normally Closed: □

Allow Manual Use: ☑

Manual Mode Timeout: □ Disabled

Logged: ☑

Source: None

Switch Type: □ Duration Disabled

□ Permanency Disabled

The **Switch Configuration** page is divided into three main areas.

1 **Scheduler** — Located at the top of the screen, it allows you to configure the switches activity for specific time and dates.

2 **Switch List** panel — Located at the middle of the screen, it allows you to filter, select and turn on/off the available switches. It also allows you to add March Networks Extension Boards.

3 **Settings** panel — Located at the bottom of the screen, it allows you to manage and configure the available switches.

Scheduler

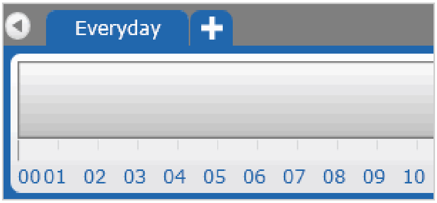
The **Scheduler** is located at the top of the screen. You can configure the switches activity for specific time and dates using the scheduler.

Note: Outside of the schedule the system automatically forces the switch to the *Auto off* 💡 status.

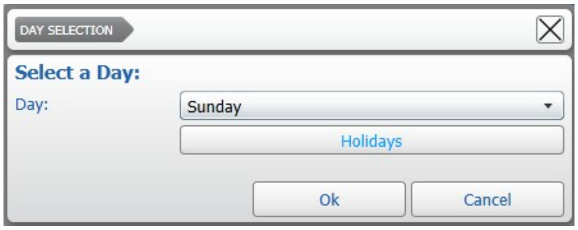
To create a schedule

1 In the **Switch Configuration** page, do one of the following:

- To configure the switch activity for every day, use the default **Everyday** tab.
- To configure the switch activity for a specific day of the week/month, click the plus tab + to create a new tab for a specific day.



The **Day Selection** dialog box appears.

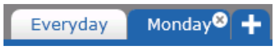

DAY SELECTION

Select a Day:

Day: Sunday

Select a day from the list and click **Ok**.

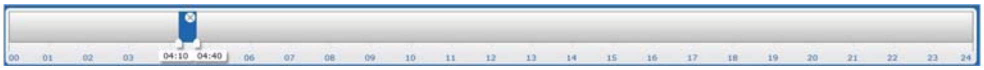
The tab for the selected day is added to the list.



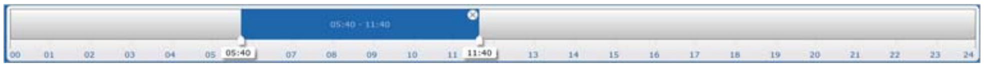
Note: When schedules conflict (for example, the **Everyday** tab is configured from 10 A.M., while the **Monday** tab is configured from 8 A.M.), Command follows an internal priority list. The priority, starting from top to bottom, is: Holiday, 1st/10th/15th day of the month, Single day of the week, Everyday.

2 To select a time interval for that day using the timeline, do the following:

- Click and hold the left mouse button down at the desired start time.

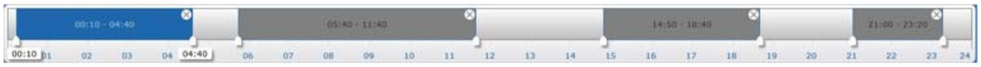


- Click and drag to define the length of the time interval.



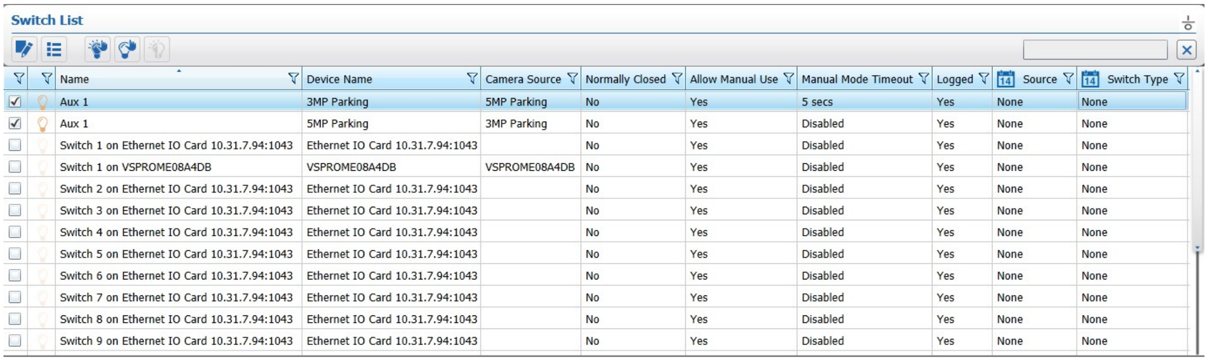
Tip: To resize a time interval, click and drag the white tab at the beginning of at the ending of the interval. To move a time interval, click and drag inside the interval.

- You can set multiple time intervals for the same day. Every time interval on the time line has its own schedule. Click a time interval to select it or hold down the **SHIFT** key to select multiple intervals.



Switch List Panel

The **Switch List** panel is located at the middle of the screen. You can filter, select and turn on/off the available switches using the **Switch List** panel. You can also search for March Networks Extension Boards on the network and add them to the switch list.



Switch List

		Name	Device Name	Camera Source	Normally Closed	Allow Manual Use	Manual Mode Timeout	Logged	Source	Switch Type
☑		Aux 1	3MP Parking	5MP Parking	No	Yes	5 secs	Yes	None	None
☑		Aux 1	5MP Parking	3MP Parking	No	Yes	Disabled	Yes	None	None
□		Switch 1 on Ethernet IO Card 10.31.7.94:1043	Ethernet IO Card 10.31.7.94:1043		No	Yes	Disabled	Yes	None	None
□		Switch 1 on VSPROME08A4DB	VSPROME08A4DB	VSPROME08A4DB	No	Yes	Disabled	Yes	None	None
□		Switch 2 on Ethernet IO Card 10.31.7.94:1043	Ethernet IO Card 10.31.7.94:1043		No	Yes	Disabled	Yes	None	None
□		Switch 3 on Ethernet IO Card 10.31.7.94:1043	Ethernet IO Card 10.31.7.94:1043		No	Yes	Disabled	Yes	None	None
□		Switch 4 on Ethernet IO Card 10.31.7.94:1043	Ethernet IO Card 10.31.7.94:1043		No	Yes	Disabled	Yes	None	None
□		Switch 5 on Ethernet IO Card 10.31.7.94:1043	Ethernet IO Card 10.31.7.94:1043		No	Yes	Disabled	Yes	None	None
□		Switch 6 on Ethernet IO Card 10.31.7.94:1043	Ethernet IO Card 10.31.7.94:1043		No	Yes	Disabled	Yes	None	None
□		Switch 7 on Ethernet IO Card 10.31.7.94:1043	Ethernet IO Card 10.31.7.94:1043		No	Yes	Disabled	Yes	None	None
□		Switch 8 on Ethernet IO Card 10.31.7.94:1043	Ethernet IO Card 10.31.7.94:1043		No	Yes	Disabled	Yes	None	None
□		Switch 9 on Ethernet IO Card 10.31.7.94:1043	Ethernet IO Card 10.31.7.94:1043		No	Yes	Disabled	Yes	None	None

The following table provides a description of the panel buttons.

Button	Action
✎	Opens the **Device Configuration** dialog box, which allows you to search for March Networks Extension Boards and add them to the switch list.
☰	Groups the switches by device.
✋	Turns the selected switch on (*Manual Mode*).

Button	Action
💡	Turns the selected switch off (*Manual Mode*).
💡	Activates the automatic management mode for the selected switch.
☒	Filters the switch list by entering text criteria.
▽	Filters data in a column.
☑	Enables/disables the selected switch.

Switch Status Icons

The following status icons appear in the **Switch List** panel:

Icon	Description
💡	Switch turned off (*Automatic Mode*)
💡	Switch turned on (*Automatic Mode*)
💡	Switch turned off (*Manual Mode*)
💡	Switch turned on (*Manual Mode*)
💡	Switch disabled
💡	Switch source (edge device or Extension Board) disabled
💡	Switch source (edge device or Extension Board) disconnected

Filtering in the Switch List Panel

You can sort and filter the switches by text or by column. See the following sections for more details:

- “Filtering by Text” on page 235
- “Sorting in Columns” on page 235
- “Filtering in Columns” on page 236

Filtering by Text

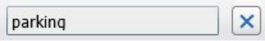
In the **Switch List** panel, you can filter for a text string. The filter applies to all columns in the **Switch List** panel.

When the text box field is empty, there is no active search and all resources appear.

As you enter letters, characters, or numbers in the text box, the **Switch List** panel automatically refreshes with the selected criteria.

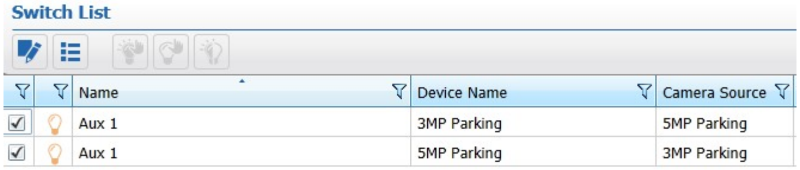
To filter by text in the Switch List panel

1 On the **Switch List** panel, enter the filter criteria in the text box.



parking ☒

The panel refresh to display only those switches that correspond to the filter criteria.



Switch List

		Name	Device Name	Camera Source
☑		Aux 1	3MP Parking	5MP Parking
☑		Aux 1	5MP Parking	3MP Parking

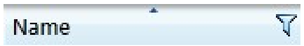
2 To remove the filter, click the ☒ button.

Sorting in Columns

You can alphabetically or numerically sort a column list (depending on the content of the list).

To sort in a column

1 Click on a column header to show the **Sort** ▲ icon.



Name

2 Click the **Sort** icon to automatically sort the elements in the column list in ascending or descending alphabetical or numerical order.

Note: Click on the **Sort** icon again to change the order from ascending to descending or from descending to ascending.

Filtering in Columns

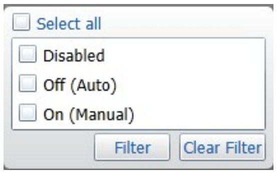
You can filter data in a column list to show only specified list values.

To filter in a column

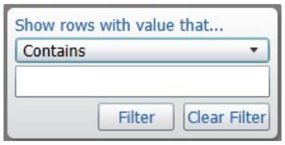
1 Select a column header and click the **Filter** icon.

The **Filter** dialog box appears. According to the selected column, you can apply filters by type or by text.

Filter by Type



Filter by Text



2 For columns filtered by type, do one of the following:

- Select one or more check boxes.
- Click the **Select all** box to select all column elements.

As you select a check box, the column list displays only those switches details that match the specified filter criteria.

3 For columns filtered by text, do the following:

a Click the **Show rows with value that** drop-down list and select a filter expression.

Options include **Contains** and **Does not contain**.

b Enter a filter criteria in the text box.

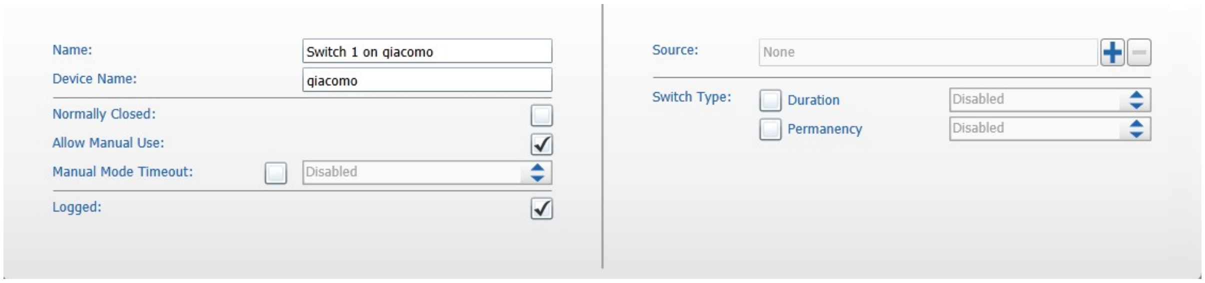
c Click **Filter** to apply the filter to the list.

The column list displays only those switches details that match the specified filter criteria.

Tip: To remove the filter, click the **Filter** icon in the column, and then click **Clear Filter**.

Settings Panel

The **Settings Panel** is located at the bottom of the screen. You can manage and configure the available switches using the **Settings Panel**.



Name: Switch 1 on giacomo
Device Name: giacomo
Normally Closed: □
Allow Manual Use: ☑
Manual Mode Timeout: □ Disabled
Logged: ☑

Source: None
Switch Type: □ Duration Disabled
□ Permanency Disabled

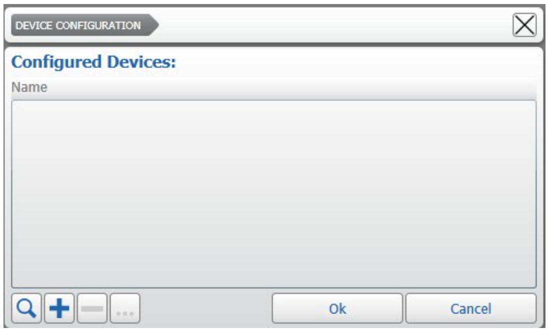
Adding Network Extension Boards

In addition to the switches automatically detected by Command, you can add switches from a Input Output Extension Board. The Extension Board is a is a peripheral that allows adding 16 alarm inputs and 16 switch outputs to Command. The Board can be powered and locally connected to a Command Recording Software through the USB port, and automatically detected by Command. The device also features a network and Power over Ethernet port, working as a standalone device integrated with March Networks Command. For more information about the Extension Board, contact your March Networks Sales representative.

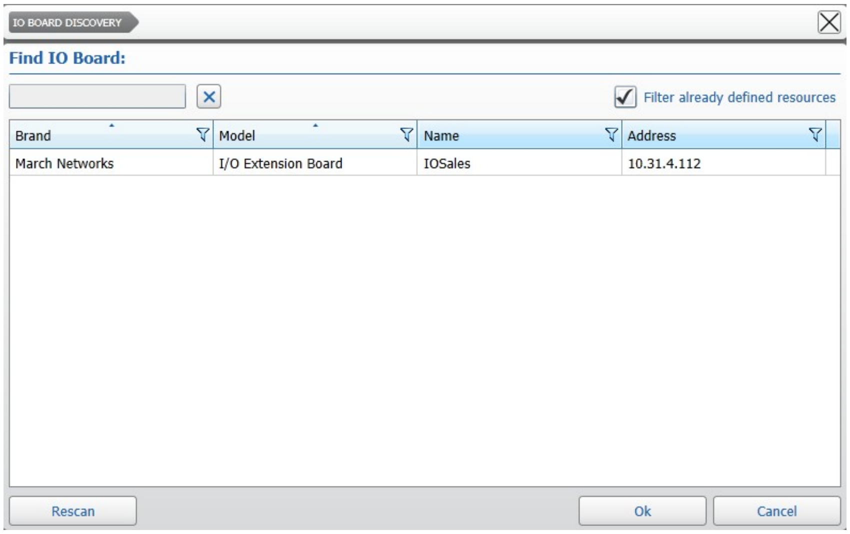
To add a network extension board

1 In the **Switch Configuration** page, click the ✎ button on the **Switch List** panel.

The **Device Configuration** dialog box appears.



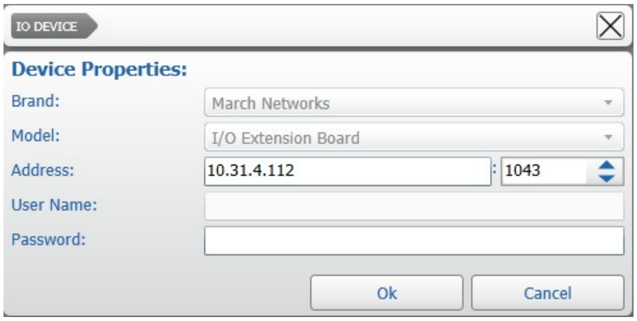
2 Click the 🔍 button to search for March Networks extension boards on the network.
The scan results appear in the **IO Board Discovery** dialog box.



Brand	Model	Name	Address
March Networks	I/O Extension Board	IOSales	10.31.4.112

Tip: Click **Rescan** to refresh the results.

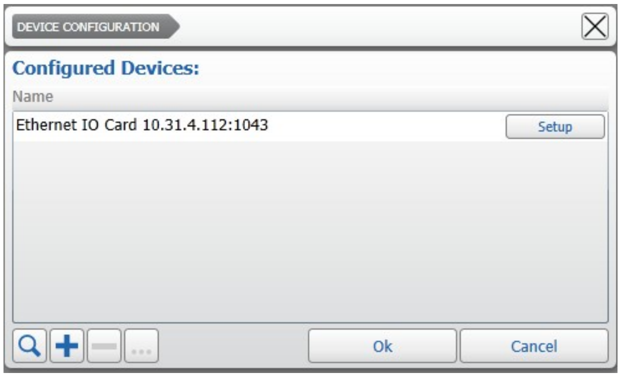
3 Select an available Extension Board and click **Ok**.
The **IO Device** dialog box appears.



Brand:	March Networks
Model:	I/O Extension Board
Address:	10.31.4.112 : 1043
User Name:	
Password:	

4 Check the board network settings and enter the **Password**.

5 Click **Ok**.
The board is added to the **Device Configuration** dialog box.



Name	
Ethernet IO Card 10.31.4.112:1043	Setup

6 Click the **Setup** button near the board to access the Web Setup interface, as required.

Tip: You can modify a board by selecting it in the **Device Configuration** dialog box and clicking the ⋯ button. You can also delete a board by clicking the − button or manually adding a new one by clicking the + button.

7 Click **Ok**.

The Extension Board is added to the list.

8 Click the 💾 button to save and apply the changes.

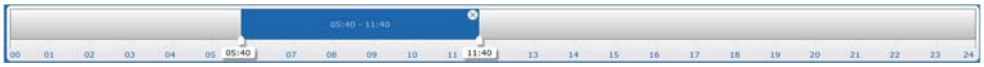
Configuring Switches

You can configure switches to be manually activated (*Manual Mode*), or to be activated a in response to a specific event (*Automatic Mode*). For example, you can activate a siren after an alarm. You can also configure a timeout to automatically switch from *Manual Mode* to *Automatic Mode*.

Note: It is recommended that you disable the switches you do not intend to manage using the Command Recording Software.

To configure a switch

1 In the **Switch Configuration** page, create a schedule, as described in “To create a schedule” on page 232.

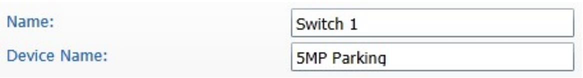


2 Select a switch in the **Switch List** panel.

Tip: You can rename a switch by double-clicking the **Name** field, or by pressing the **F2** key.

3 In the **Settings Panel**, enter a new custom name for the switch in the **Name** field.

4 (Optional) Enter a new custom name for the source device/board in the **Device Name** field.

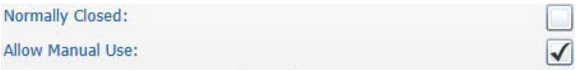


Name: Switch 1

Device Name: 5MP Parking

5 Select the **Normally Closed** check box if the default status of the auxiliary channel is a closed circuit.

6 Select the **Allow Manual Use** check box to enable *Manual Mode* and allow users to manually change the switch status.



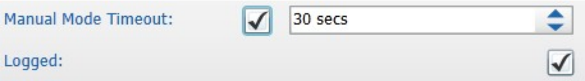
Normally Closed: □

Allow Manual Use: ☑

7 Select the **Manual Mode Timeout** check box to specify the time interval before Command reverts from *Manual Mode* to *Automatic Mode*.

Note: If the **Allow Manual Use** check box is selected and the **Manual Mode Timeout** check box is cleared, when the switch status is manually changed, *Manual Mode* is permanently triggered. As a result, the switch status can be changed only manually or by manually switching back to *Automatic Mode*.

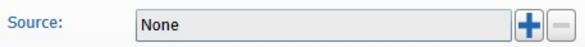
8 Select the **Logged** check box to save the switch activity information in the system log.



Manual Mode Timeout: ☑ 30 secs

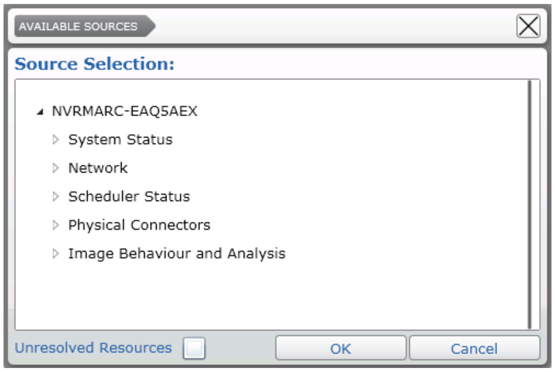
Logged: ☑

9 In the **Source** section, click the + button to add the condition that activates the switch.



Source: None

The **Available Sources** dialog box appears.



10 Select a condition from the **Source Selection** list and click **Ok**.

Note: You can include unresolved resources to the tree by selecting the **Unresolved Resources** check box. Unresolved resources are conditions based on sources that are added to the Command Recording Software, but currently not available. For example, the motion detection feature of a camera currently disconnected.

The condition is added to the auxiliary channel.

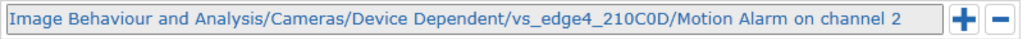
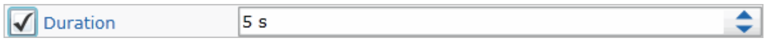


Image Behaviour and Analysis/Cameras/Device Dependent/vs_edge4_210C0D/Motion Alarm on channel 2

Tip: Click the − button to remove the condition.

11 In the **Switch Type** section, select one of the following switch management modes:

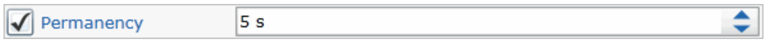
- **Duration** — The switch is activated for the entire duration of the event and turned off after the specified period of time following the end of the last event.

  ☑ Duration 5 s

  For example, if you select a time period of 5 seconds for **Duration**, and the event lasts 20 seconds, the switch will be activated for 25 seconds.

- **Permanency** — The switch is deactivated after the specified period of time following the beginning of the last event.

  ☑ Permanency 5 s

  For example, if you select a time period of 5 seconds for **Permanency**, and the event lasts 20 seconds, the switch will only be activated for 5 seconds.

12 Repeat step 2 to step 11 to configure additional switches.

13 Click the 💾 button to save and apply the changes.

Managing Switches

The **Switch List** panel allows you to manually change the status of a switch and to switch from *Manual Mode* to *Automatic Mode*.

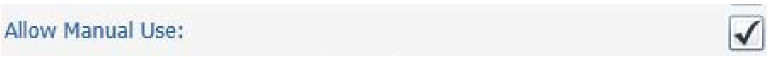
Important: You can manually manage a switch only if the **Allow Manual Use** check box is selected in the **Settings Panel**.

Tip: You can also manage switches using the Command Client interface and the SiteManager application.

To manage a switch

1 Select a switch in the **Switch List** panel.

2 Ensure that the **Allow Manual Use** check box is selected in the **Settings Panel**.



Allow Manual Use: ☑

3 In the **Switch List** panel, click the 💡 button to turn the switch on.

4 Click the 💡 button to turn the switch off.

5 Click the 💡 button to switch to *Automatic Mode*.

Chapter 14

Managing Audio Channels

You can record audio streams from microphones connected to cameras or from other network sources, associate them to cameras, and synchronize them to the video evidence using the **Audio Configuration** page. You can also configure the audio detection feature and set it as one of the conditions that trigger an event or an alarm. In addition, you can enable output audio channels, which allow you to stream audio to speakers connected to the cameras.

This chapter contains the following sections:

- “Creating and Deleting Audio Channels” on page 243
- “Configuring Mono or Stereo Audio Channels” on page 244
- “Activating Output Audio Channels” on page 246

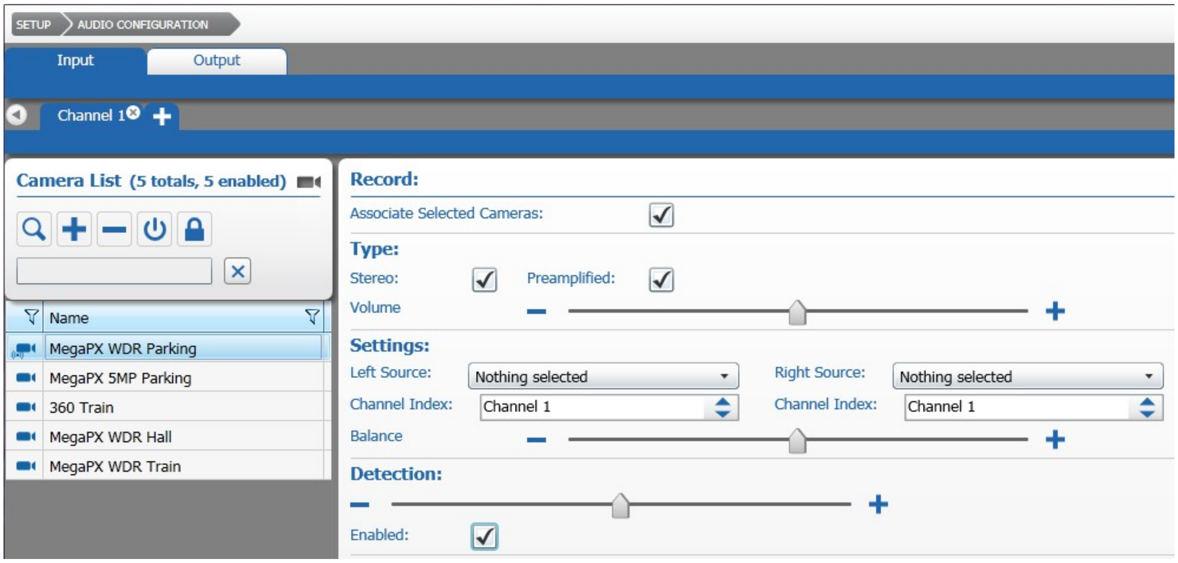
Creating and Deleting Audio Channels

You can associate audio stream to any configured camera and enable the audio detection feature as a source condition for alarms, on-event recording, and user account permissions on the **Audio Configuration** page.

To create audio channels

1 On the Command Config main page, under **Device Management**, click **Audio**.

The **Audio Configuration** page appears.



Camera List (5 totals, 5 enabled)

MegaPX WDR Parking
MegaPX 5MP Parking
360 Train
MegaPX WDR Hall
MegaPX WDR Train

Record:
Associate Selected Cameras: ☑

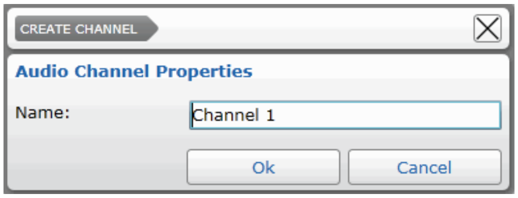
Type:
Stereo: ☑ Preamplified: ☑
Volume

Settings:
Left Source: Nothing selected Right Source: Nothing selected
Channel Index: Channel 1 Channel Index: Channel 1
Balance

Detection:
Enabled: ☑

2 Click the + tab to add an audio channel to Command.

The **Create Channel** dialog box appears.

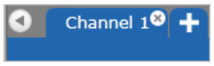


Audio Channel Properties

Name: Channel 1

3 Enter a name for the audio channel and click **Ok**.

The tab for the channel is added to the list.



Tip: You can rename an audio channel by double-clicking the **Name** field, or by pressing the **F2** key.

4 Repeat step 1 to step 3 to create additional audio channels.

5 Click the 💾 button to save and apply the changes.

Associating Audio Channels to Cameras

In order to enable an audio channel, you must associate it with one or more cameras.

To associate an audio channel to cameras

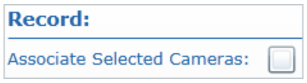
1 On the **Audio Configuration** page, click an audio channel tab to select it.

2 Select one or more cameras from the **Camera List** panel.

Note: For more information on using the **Camera List** panel, see “Camera List Panel” on page 147.

Tip: You can select multiple cameras by holding down the **CTRL** or the **SHIFT** key.

3 In the **Record** section, select the **Associate Selected Cameras** check box.



Record:

Associate Selected Cameras: □

The audio channel is now associated to the cameras.

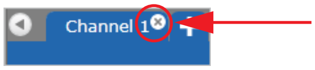
4 Click the 💾 button to save and apply the changes.

Deleting Audio Channels

You can delete audio channels that you have created. By deleting an audio channel, the audio stream will not be associated to cameras and will not be available for live viewing and recording.

To delete an audio channel

1 On the **Audio Configuration** page, click the (**X**) button that appears in the upper right corner of the audio channel tab.



A confirmation dialog box appears.

2 Click **Yes** to confirm the channel deletion.

3 Click the 💾 button to save and apply the changes.

Configuring Mono or Stereo Audio Channels

You can configure the settings for a mono or a stereo audio channel, according to the device specifications.

Select your configuration:

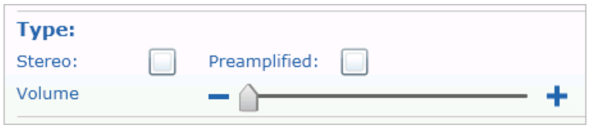
- “To configure a mono audio channel” on page 244
- “To configure a stereo audio channel” on page 245

To configure a mono audio channel

1 On the **Audio Configuration** page, click an audio channel tab.

2 In the **Type** section, ensure the **Stereo** check box is cleared.

3 Select the **Preamplified** check box if Command retrieves the audio signal from a device that amplifies it. Otherwise, Command amplifies the signal.



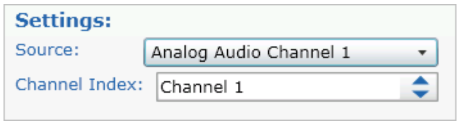
Type:

Stereo: □ Preamplified: □

Volume

4 Select the recording volume by moving the **Volume** slider.

5 In the **Settings** section, select the audio channel of a camera from the **Source** list.



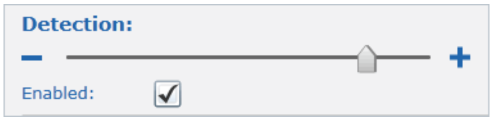
Settings:

Source: Analog Audio Channel 1

Channel Index: Channel 1

6 From the **Channel Index** list, select an identification number for the audio channel.

7 Optionally, you can activate the audio detection feature. This feature allows you to generate alarms when Command detects noises on the audio channel. In the **Detection** section, select the **Enabled** check box and set the detection threshold by moving the slider.



Detection:

Enabled: ☑

Note: When the feature is activated, it is available in the **Source Selection** list, and you can assign it to alarms, user accounts, and on-event recording schedules.

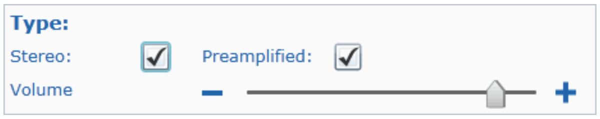
8 Click the 💾 button to save and apply the changes.

To configure a stereo audio channel

1 On the **Audio Configuration** page, click an audio channel tab.

2 In the **Type** section, select the **Stereo** check box.

3 Select the **Preamplified** check box if Command retrieves the audio signal from a device that amplifies it. Otherwise, Command amplifies the signal.



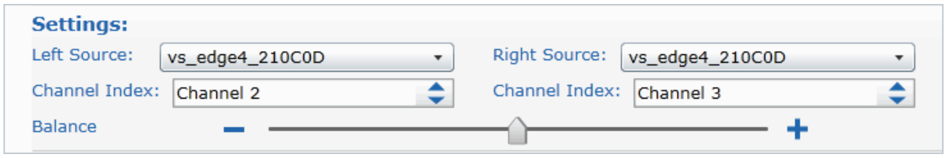
Type:

Stereo: ☑ Preamplified: ☑

Volume

4 Select the recording volume by moving the **Volume** slider.

5 In the **Settings** section, select the audio stream source on the network for the left and right audio channels from the **Left Source** and **Right Source** lists.



Settings:

Left Source: vs_edge4_210C0D Right Source: vs_edge4_210C0D

Channel Index: Channel 2 Channel Index: Channel 3

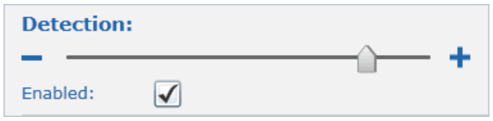
Balance

Note: You can select two different sources for the left and right channels.

6 From the left and right **Channel Index** lists, select an identification number for the left and right audio channels.

7 Set the balance between the left and right channels by moving the **Balance** slider.

8 Optionally, you can activate the audio detection feature. This feature allows you to generate alarms when Command detects noises on the audio channel. In the **Detection** section, select the **Enabled** check box and set the detection threshold by moving the slider.



Detection:

Enabled: ☑

Note: When the feature is activated, it is available in the **Source Selection** list, and you can assign it to alarms, user accounts, and on-event recording schedules.

9 Click the 💾 button to save and apply the changes.

Activating Output Audio Channels

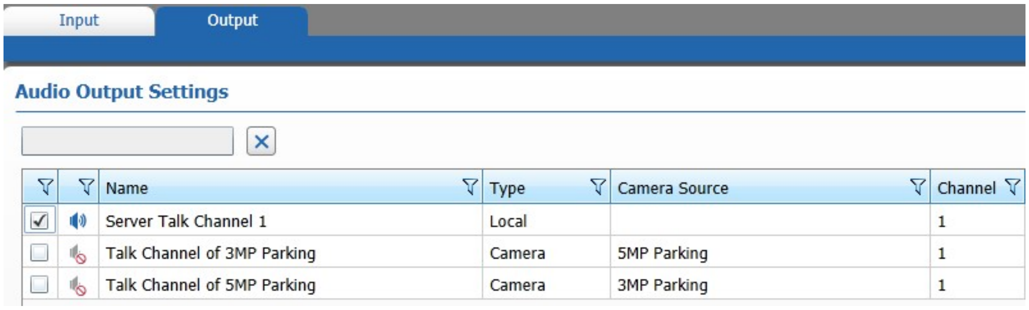
Command supports output audio channels (*Talk Channels*), allowing you to stream audio to speakers connected to the supported cameras.

Note: For more information about the cameras that support the Talk channel functionality, consult the *Supported Devices List* available on the March Networks Website (www.marchnetworks.com) in the Command Professional section.

To activate an output audio channel

1 On the **Audio Configuration** page, click the **Output** tab.

The **Audio Output Settings** page appears. The server's output channel is enabled by default, while the cameras' output channels are disabled by default.



Audio Output Settings

		Name	Type	Camera Source	Channel
☑	🔊	Server Talk Channel 1	Local		1
☐	🔇	Talk Channel of 3MP Parking	Camera	5MP Parking	1
☐	🔇	Talk Channel of 5MP Parking	Camera	3MP Parking	1

Tip: You can use the text box or the **Filter** ▽ icons to filter the talk channels list.

2 Clear the **Enabled** check box for the **Server Talk Channel** to disable the server's output audio channel.

3 Select the **Enabled** check box for the **Talk Channel of X** to enable the camera's output audio channel.

4 Click the 💾 button to save and apply the changes.

Chapter 15

Creating Custom Conditions

You can create custom conditions using the integrated editor. A custom condition is an expression that connects two or more different existing source conditions, created using the integrated editor. This allows you to set up more efficient alarms, and more specific conditions for on-event recording.

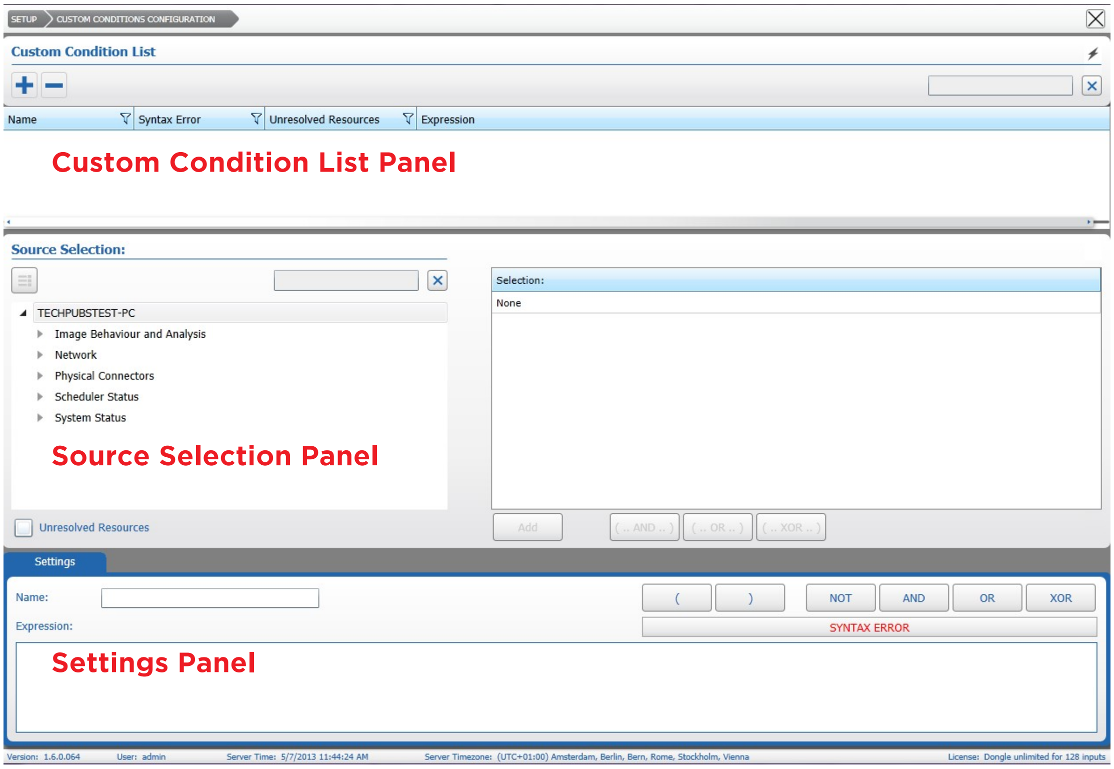
This chapter contains the following sections:

Overview

The **Custom Conditions Configuration** page allows you to create custom events that build on existing conditions. The existing conditions are based on alarms created on the IP cameras, text insertion filters, or on Command related events, such as the connection of a specific user.

To access the page, on the Command Config main page, under **Miscellaneous**, click **Custom Conditions.**

The following illustration shows the **Custom Condition** user interface.



Custom Condition List Panel

Source Selection Panel

Settings Panel

Version: 1.6.0.064 User: admin Server Time: 5/7/2013 11:44:24 AM Server Timezone: (UTC+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna License: Dongle unlimited for 128 inputs

The **Custom Conditions Configuration** page is divided into three main areas.

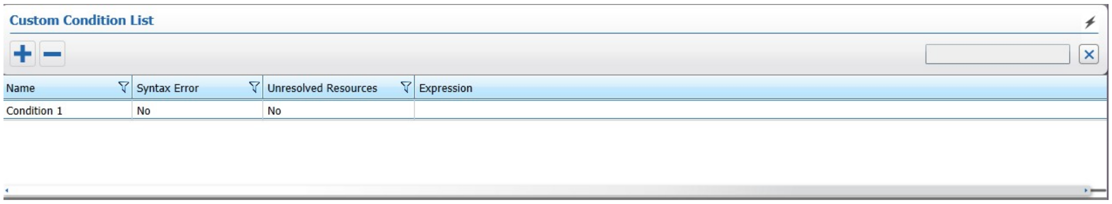
1 **Custom Condition List** panel — Located at the top of the screen, it allows you to create, edit and delete custom conditions.

2 **Source Selection** panel — Located at the middle of the screen, it allows you to filter, select and add the available conditions. You can add single conditions or group of conditions.

3 **Settings** panel — Located at the bottom of the screen, it allows you to create custom conditions using the integrated editor.

Custom Conditions List Panel

The **Custom Condition List** panel is located at the top of the screen. You can create, edit and delete custom conditions using the **Custom Condition List** panel.



Name	Syntax Error	Unresolved Resources	Expression
Condition 1	No	No	

Filtering in the Custom Conditions List Panel

You can sort and filter the conditions by text or by column. See the following sections for more details:

- “Filtering by Text” on page 249
- “Sorting in Columns” on page 250
- “Filtering in Columns” on page 250

Filtering by Text

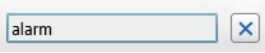
In the **Custom Condition List** panel, you can filter for a text string. The filter applies to all columns in the panel.

When the text box field is empty, there is no active search and all conditions appear.

As you enter letters, characters, or numbers in the text box, the **Custom Condition List** panel automatically refreshes with the selected criteria.

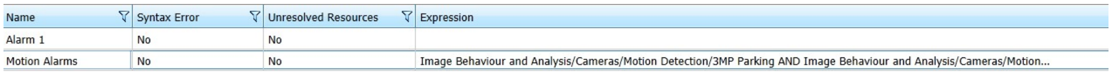
To filter by text in the Switch List panel

1 On the **Custom Condition List** panel, enter the filter criteria in the text box.



alarm

The panel refresh to display only those conditions that correspond to the filter criteria.



Name	Syntax Error	Unresolved Resources	Expression
Alarm 1	No	No	
Motion Alarms	No	No	Image Behaviour and Analysis/Cameras/Motion Detection/3MP Parking AND Image Behaviour and Analysis/Cameras/Motion...

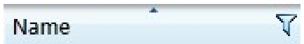
2 To remove the filter, click the ✕ button.

Sorting in Columns

You can alphabetically or numerically sort a column list (depending on the content of the list).

To sort in a column

1 Click on a column header to show the **Sort** ▲ icon.



2 Click the **Sort** icon to automatically sort the elements in the column list in ascending or descending alphabetical or numerical order.

Note: Click on the **Sort** icon again to change the order from ascending to descending or from descending to ascending.

Filtering in Columns

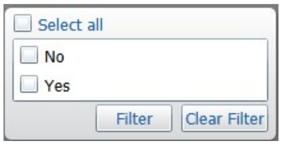
You can filter data in a column list to show only specified list values.

To filter in a column

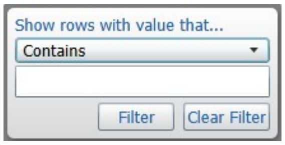
1 Select a column header and click the **Filter** ▽ icon.

The **Filter** dialog box appears. According to the selected column, you can apply filters by type or by text.

Filter by Type



Filter by Text



2 For columns filtered by type, do one of the following:

- Select one or more check boxes.
- Click the **Select all** box to select all column elements.

As you select a check box, the column list displays only those conditions details that match the specified filter criteria.

3 For columns filtered by text, do the following:

a Click the **Show rows with value that** drop-down list and select a filter expression.

Options include **Contains** and **Does not contain**.

b Enter a filter criteria in the text box.

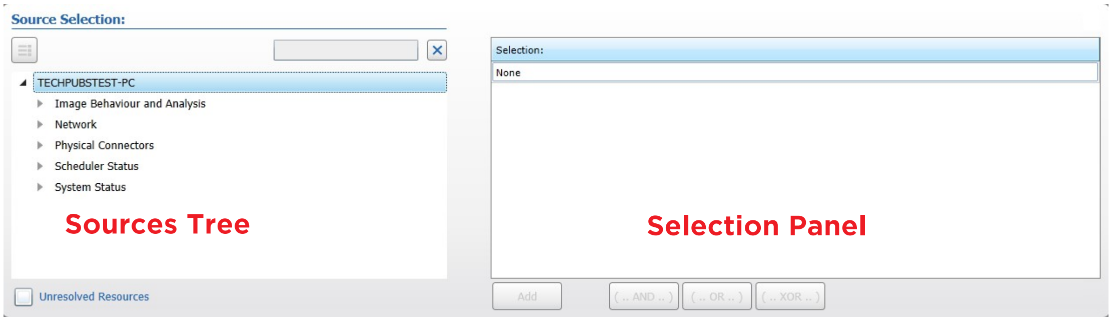
c Click **Filter** to apply the filter to the list.

The column list displays only those conditions details that match the specified filter criteria.

Tip: To remove the filter, click the **Filter** ▽ icon in the **Brand** column, and then click **Clear Filter**.

Source Selection Panel

The **Source Selection** panel is located at the middle of the screen. You can filter, select and add the available conditions using the **Source Selection** panel. You can add both single conditions or group of conditions to the expression. The **Source Selection** panel is divided into two areas, the **Sources** tree and the **Selection** panel.



Sources Tree

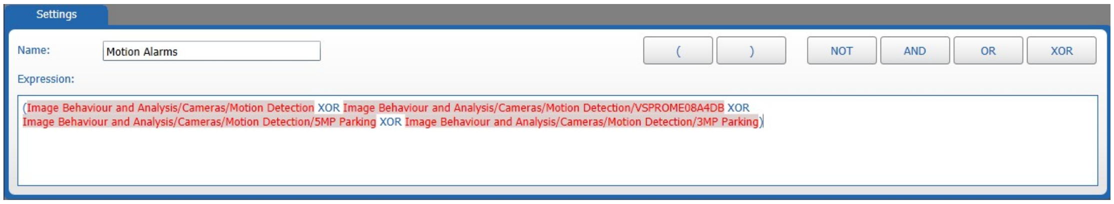
Selection Panel

The following table provides a description of the **Source Selection** panel buttons.

Button	Action
☰	Adds all of the conditions in the selected tree branch to the **Selection** panel.
□ ☒	Filters the **Sources Tree** by entering text criteria.
Add	Adds the selected condition to the **Settings** panel.
(...AND...)	Adds all of the selected conditions to the **Settings** panel using the boolean connector AND.
(...OR...)	Adds all of the selected conditions to the **Settings** panel using the boolean connector OR.
(...XOR...)	Adds all of the selected conditions to the **Settings** panel using the boolean connector XOR.

Settings Panel

The **Settings Panel** is located at the bottom of the screen. You can create custom conditions using the integrated editor.



Name: Motion Alarms

Expression:

(Image Behaviour and Analysis/Cameras/Motion Detection XOR Image Behaviour and Analysis/Cameras/Motion Detection/VSPROME08A4DB XOR Image Behaviour and Analysis/Cameras/Motion Detection/5MP Parking XOR Image Behaviour and Analysis/Cameras/Motion Detection/3MP Parking)

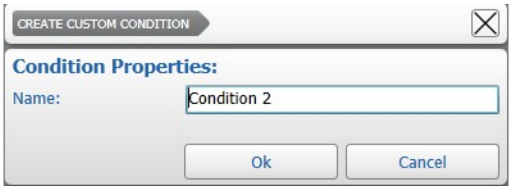
Creating Custom Conditions

The **Custom Condition List** panel allows you to create and remove custom conditions that build on existing conditions.

To create a custom condition

1 In the **Custom Conditions Configuration** page, click the ✚ button.

The **Create Custom Condition** dialog box appears.



Condition Properties:

Name: Condition 2

2 Enter a name for the custom condition and then click **Ok** to confirm the condition creation.

The custom condition is added to the list.

Tip: You can rename a custom condition by double-clicking the **Name** field, or by pressing the **F2** key.

3 Click the 💾 button to save and apply the changes.

Deleting Custom Conditions

You can delete a custom condition if you no longer need it. The custom condition is removed from the list of available source conditions.

To delete a custom condition

1 Select the custom condition you want to delete in the **Custom Condition List** panel.

2 Click the − button.

A confirmation dialog box appears.

3 Click **Yes** to confirm the deletion of the condition.

4 Click the 💾 button to save and apply the changes.

Editing Custom Conditions

The **Source Selection** and the **Settings** panels allow you to create custom conditions by selecting existing conditions from the **Sources** tree and grouping them in an expression using the integrated editor.

Custom conditions are expressions that are created by adding two or more existing conditions and connecting them with Boolean algebra connectors. The Boolean algebra connectors are described in the following table (in the table, the two existing conditions are labeled **A** and **B**).

Boolean Connector	Expression	Action
(	(A...	Opens a bracket where you can create a sub-expression.
)	...B)	Closes a previously created bracket.
AND	A AND B	Causes the custom condition to trigger only when conditions A and B occur simultaneously.
OR	A OR B	Causes the custom condition to trigger when either one of the conditions occurs, or both conditions occur simultaneously (A, B, or A and B simultaneously).
NOT	A <AND; OR; XOR> NOT B	Causes the custom condition to trigger only: • When condition A occurs and condition B does not occur (AND NOT). • When condition A occurs or condition B does not occur (OR NOT). • When condition A occurs and condition B does not occur or when condition A does not occur and condition B does occur (XOR NOT).
XOR	A XOR B	Causes the custom condition to trigger only when one condition occurs and the other does not occur. If both conditions occur or no condition occurs, the event does not trigger.

To edit a custom condition

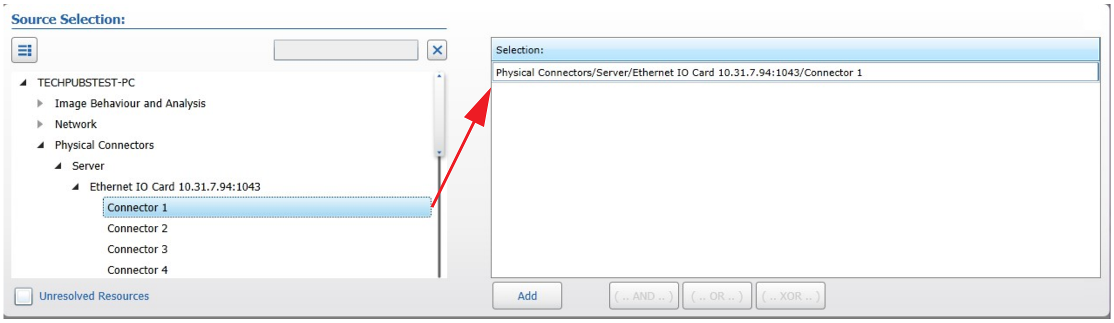
1 Select a custom condition in the **Custom Condition List** panel.

2 To add a single condition to the expression:

a Select a condition in the **Sources** tree.

Note: You can include unresolved resources to the tree by selecting the **Unresolved Resources** check box. Unresolved resources are conditions based on sources that are added to the Command Recording Software, but currently not available. For example, the motion detection feature of a camera currently disconnected.

The condition appears in the **Selection** panel.



Physical Connectors/Server/Ethernet IO Card 10.31.7.94:1043/Connector 1

Tip: You can filter the **Sources** tree using the text filter.

b Click the **Add** button to add the selected condition to the expression.

The condition is added to the **Settings** panel.

3 To add multiple conditions to the expression:

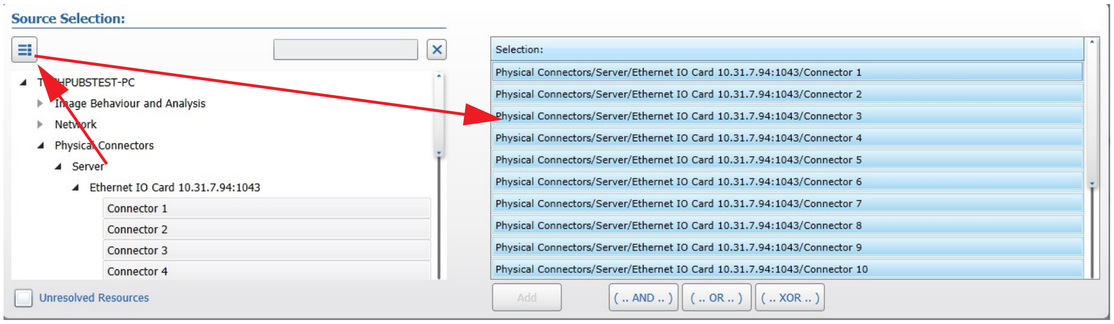
a Select a condition branch in the **Sources** tree.

Note: You can include unresolved resources to the tree by selecting the **Unresolved Resources** check box.

Tip: You can filter the conditions included in the branch using the text filter. You can also select multiple branches by pressing the **CTRL** or **SHIFT** keys.

b Click the ☰ to select the filtered conditions belonging to the branch(es).

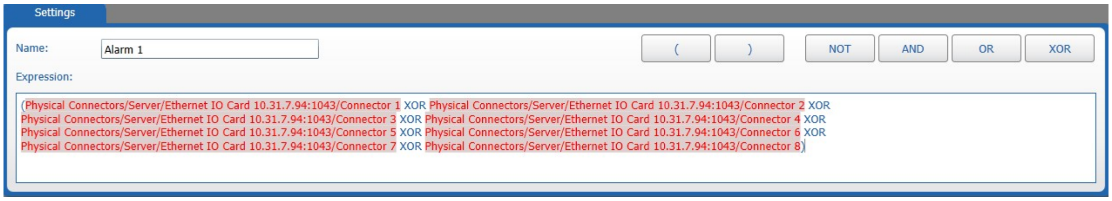
The conditions appear in the **Selection** panel.



Physical Connectors/Server/Ethernet IO Card 10.31.7.94:1043/Connector 1
Physical Connectors/Server/Ethernet IO Card 10.31.7.94:1043/Connector 2
Physical Connectors/Server/Ethernet IO Card 10.31.7.94:1043/Connector 3
Physical Connectors/Server/Ethernet IO Card 10.31.7.94:1043/Connector 4
Physical Connectors/Server/Ethernet IO Card 10.31.7.94:1043/Connector 5
Physical Connectors/Server/Ethernet IO Card 10.31.7.94:1043/Connector 6
Physical Connectors/Server/Ethernet IO Card 10.31.7.94:1043/Connector 7
Physical Connectors/Server/Ethernet IO Card 10.31.7.94:1043/Connector 8
Physical Connectors/Server/Ethernet IO Card 10.31.7.94:1043/Connector 9
Physical Connectors/Server/Ethernet IO Card 10.31.7.94:1043/Connector 10

c (Optional) Refine the selection using the **CTRL** or **SHIFT** key.

d Click the **(...AND/OR/XOR...)** button to add the selected conditions to the expression. The conditions are automatically added in brackets and with the selected Boolean connector.



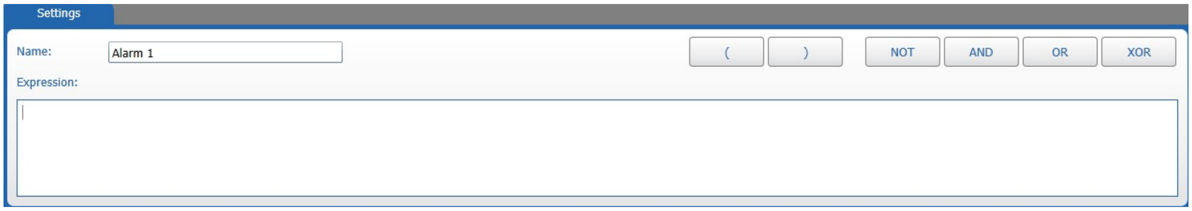
Name: Alarm 1

Expression:

(Physical Connectors/Server/Ethernet IO Card 10.31.7.94:1043/Connector 1 XOR Physical Connectors/Server/Ethernet IO Card 10.31.7.94:1043/Connector 2 XOR
Physical Connectors/Server/Ethernet IO Card 10.31.7.94:1043/Connector 3 XOR Physical Connectors/Server/Ethernet IO Card 10.31.7.94:1043/Connector 4 XOR
Physical Connectors/Server/Ethernet IO Card 10.31.7.94:1043/Connector 5 XOR Physical Connectors/Server/Ethernet IO Card 10.31.7.94:1043/Connector 6 XOR
Physical Connectors/Server/Ethernet IO Card 10.31.7.94:1043/Connector 7 XOR Physical Connectors/Server/Ethernet IO Card 10.31.7.94:1043/Connector 8)

4 Configure your custom condition using the editor in the **Settings** panel. To add a Boolean connector to the expression, click before or after a condition, and then click the button corresponding to the connector.

Note: The expression editor warns if there is a syntax error in the expression.



Name: Alarm 1

Expression:

Tip: You can delete an element of the expression by clicking at the end of the expression and pressing the **BACKSPACE** key.

5 After creating a valid expression, click the 🖫 button to save and apply the changes.

The custom condition is automatically added to the **Source Selection** list. You can use it to configure user accounts, set on-event recording schedules, create alarms, and configure switches.

Chapter 16

Configuring Text Insertion Filters

Command supports the insertion of text on the camera images. This text comes from external devices such as bar code readers, POS terminals, ATM, and teller workstations. You can configure text filters on the Command Recording Software as events to trigger an on-event recording or a custom alarm using the **Text Insertion Configuration** page. Both Command Client and SiteManager are compatible with text insertion.

Note: You cannot directly add text insertion devices to the Command Recording Software using Command Config, Command Client, or SiteManager, but you can use the *SerialToCRS* application, available on the March Networks Partner Portal. The application associates the text from a text insertion device to one or more IP cameras added to the Command Recording Software. Command, interacting with the application, is able to automatically record the images with the superimposed text.

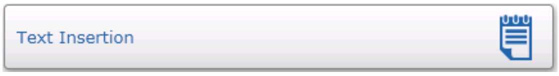
This chapter contains the following sections:

Configuring Text Insertion Filters

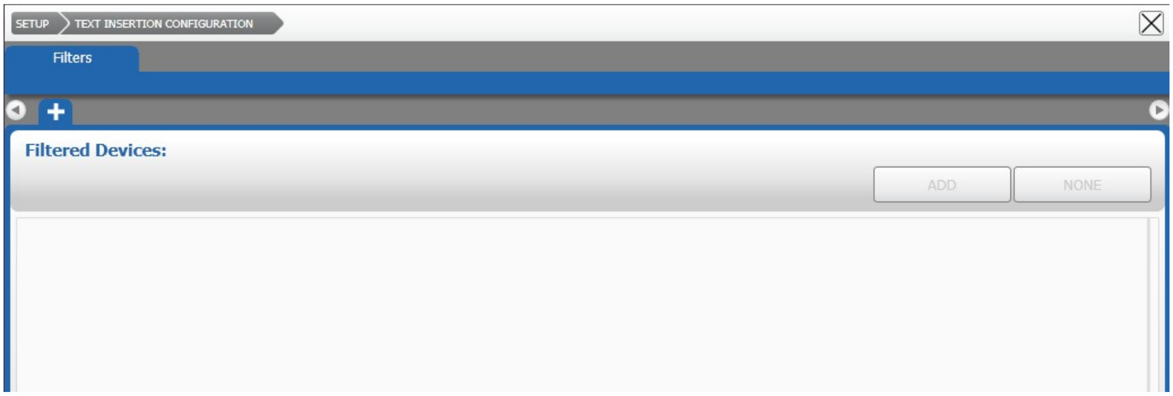
You can configure custom text filters as new events that trigger an on-event recording or a custom alarm using the **Text Insertion Configuration** page.

To configure a text insertion filter

1 On the Command Config main page, under **Miscellaneous**, click **Text Insertion**.



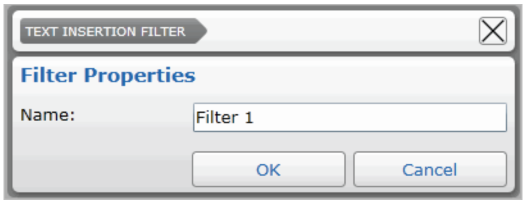
The **Text Insertion Configuration** page appears.



2 Click the **Filter** tab.

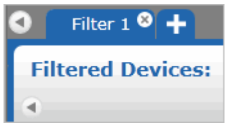
3 Click the + tab to create a new filter.

The **Filter Properties** dialog box appears.



Name: Filter 1

4 Enter a name for the filter and click **Ok**.

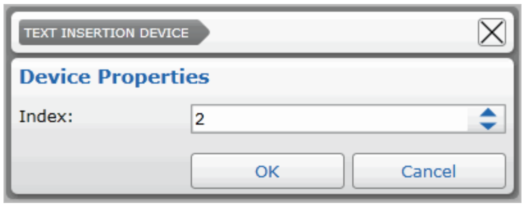


The tab for the filter is added to the list.

Note: You can rename the filter by holding the mouse button on the filter tab. After typing the new name, press **ENTER** to confirm.

5 Click **Add** to select the text insertion devices.

The **Text Insertion Device** dialog box appears.

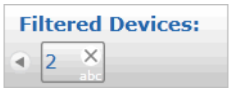


Device Properties

Index: 2

6 From the **Index** list, select the identification number corresponding to the text insertion device, and click **Ok**.

The device button appears in the **Filtered Devices** list.

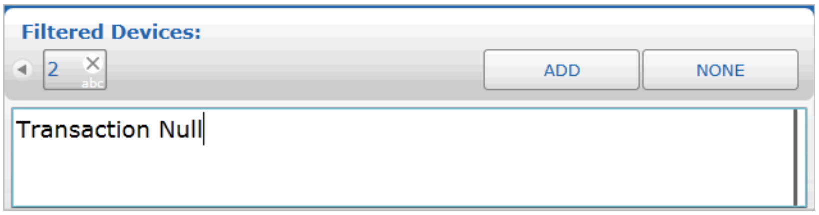


Filtered Devices:

7 Repeat step 5 to step 6 to add multiple text insertion devices to the filter.

Tip: You can remove a device by clicking the (**X**) symbol in the upper right corner of the button. You can also remove all the devices by clicking **None**.

8 Click under the **Filtered Devices** list to enter the text that triggers the event/alarm.

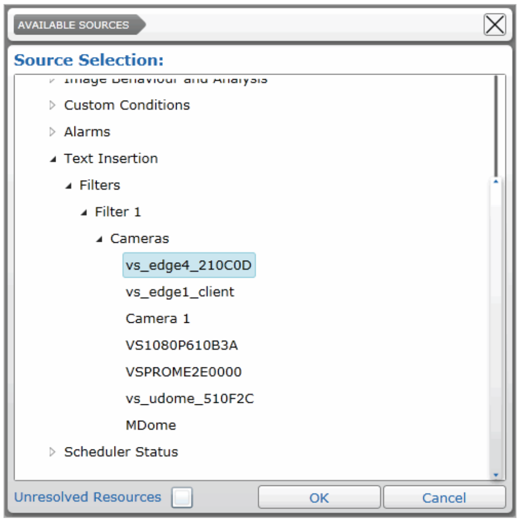


Filtered Devices:

Transaction Null

9 Click the 💾 button to save and apply the changes.

The filter is added to the **Source Selection** list and you can select it to trigger an on-event recording or a custom alarm. For more information see “Configuring On-Event Recording” on page 210 and “Creating Alarms” on page 218.

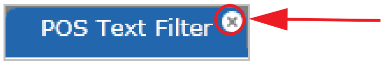


Deleting Text Insertion Filters

You can delete a text insertion filter if you no longer need it. The filter is removed from the list of available source conditions.

To delete a custom event

1. On the **Text Insertion Configuration** page, click the **Filter** tab.
2. Click the (**X**) button that appears on the upper right corner of the filter tab.

   A confirmation dialog box appears.
3. Click **Yes** to confirm the deletion of the filter.
4. Click the 💾 button to save and apply the changes.

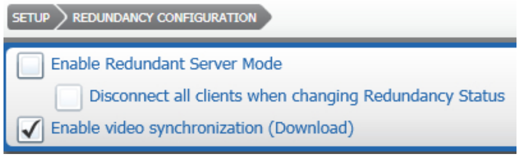
Chapter 17

Setting Redundant Machines

You can set up a Command Recording Software as a redundant machine for other Command Recording Softwares on the **Redundancy Configuration** page. A redundant machine automatically takes the place of a broken or disconnected Command Recording Software by applying its configuration, providing vital backup and creating a fault-tolerant system. It is also possible to activate the Shadow Archiving feature to automatically recover archived video evidence recorded by the redundant machine.

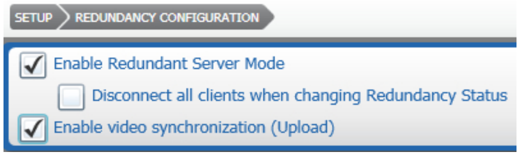
Important Notes:

- It is very important that you ONLY activate this feature on the Command Recording Software that you intend to use as a backup server. Activating this feature on other servers will cause the servers to lose their configuration settings.
- It is strongly recommended that you do not activate the Shadow Archiving feature if you have bandwidth constraints.
- To activate the Shadow Archiving feature, you must select the **Enable Video Synchronization** check boxes on the monitored Command Recording Software and on the redundant machine(s).



□ Enable Redundant Server Mode
□ Disconnect all clients when changing Redundancy Status
☑ Enable video synchronization (Download)

Monitored Command Recording Software



☑ Enable Redundant Server Mode
□ Disconnect all clients when changing Redundancy Status
☑ Enable video synchronization (Upload)

Redundant Machine

This chapter contains the following sections:

- “Adding an Additional Command Recording Software for Backup Support” on page 261
- “Setting Up Multiple Redundant Servers” on page 263

Adding an Additional Command Recording Software for Backup Support

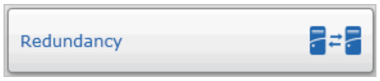
After configuring one or more Command Recording Softwares on your network, you can set up an additional server as a redundant machine. A redundant machine is capable of checking the status of the monitored Command Recording Softwares, periodically downloading configuration files from them, and automatically applying their configuration to substitute them.

Note: To set up a redundant machine, you must purchase another a license valid for the same number of channels as the monitored Command Recording Softwares.

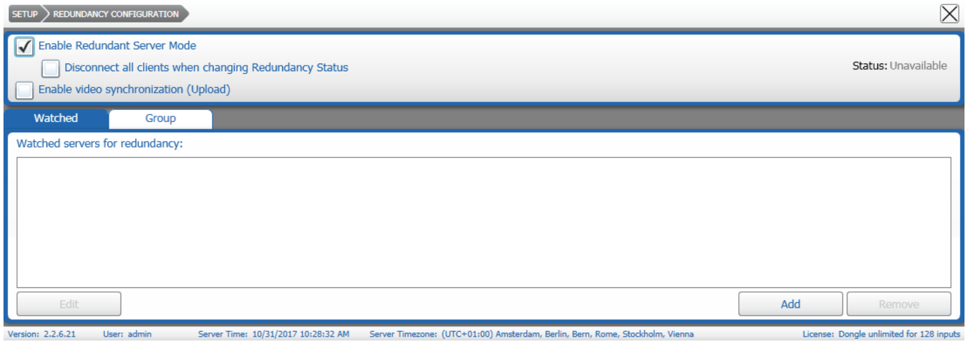
To add an additional Command Recording Software for backup support

1 Log on to the redundant machine.

2 On the Command Config main page, under **System Monitoring**, click **Redundancy**.



The **Redundancy Configuration** page appears.



☑ Enable Redundant Server Mode

☐ Disconnect all clients when changing Redundancy Status

☐ Enable video synchronization (Upload)

Status: Unavailable

Watched servers for redundancy:

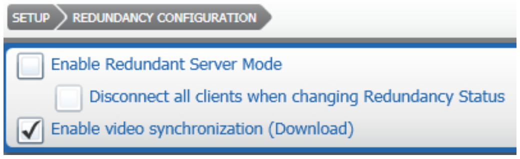
Version: 2.2.6.21 User: admin Server Time: 10/31/2017 10:28:32 AM Server Timezone: (UTC+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna License: Dongle unlimited for 128 inputs

3 Select the **Enable Redundant Server Mode** check box to transform the Command Recording Software into a redundant server.

4 (Optional) You can also select the **Disconnect all clients when changing Redundancy Status** check box to force a disconnection of all the profiles currently connected to the Command Recording Software before applying changes. We recommend that you enable this option if the monitored Command Recording Software and the redundant machine have been added to SiteManager.

5 Select the **Enable video synchronization (Upload)** check box to activate the Shadow Archiving on the redundant machine.

Note: Ensure that the **Enable video synchronization (Download)** check box is also selected on the monitored Command Recording Software. The Shadow Archiving feature is activated only if both check boxes are selected.



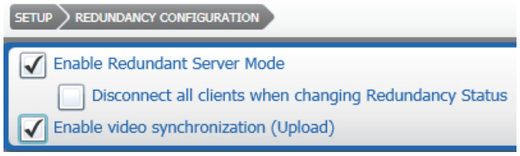
SETUP > REDUNDANCY CONFIGURATION

□ Enable Redundant Server Mode

□ Disconnect all clients when changing Redundancy Status

☑ Enable video synchronization (Download)

Monitored Command Recording Software



SETUP > REDUNDANCY CONFIGURATION

☑ Enable Redundant Server Mode

□ Disconnect all clients when changing Redundancy Status

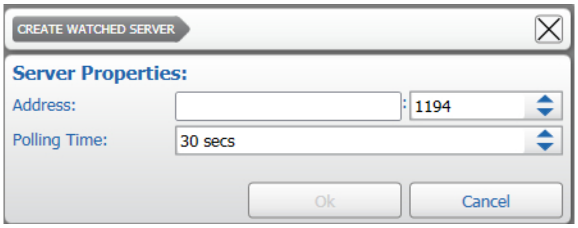
☑ Enable video synchronization (Upload)

Redundant Machine

6 Click the **Watched** tab.

7 Click **Add** to specify the Command Recording Software that the redundant machine will monitor.

The **Create Watched Server** dialog box appears.



CREATE WATCHED SERVER

Server Properties:

Address: : 1194

Polling Time: 30 secs

8 In the **Address** field, do the following:

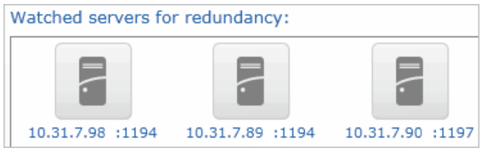
- Enter the server’s IP address.
- From the list next to the address, select the server’s communication port.

9 From the **Polling Time** list, select how often the redundant machine connects to the monitored Command Recording Software.

10 Click **Ok**.

An icon representing the server appears in the **Watched servers for redundancy** section.

11 Repeat step 7 to step 10 to add additional Command Recording Softwares.



Watched servers for redundancy:

10.31.7.98 :1194

10.31.7.89 :1194

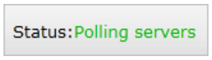
10.31.7.90 :1197

Tip: You can remove any of the monitored servers by selecting the server button and clicking **Remove**.

12 Click the 💾 button to save and apply the changes.

The Command Recording Software clears its current configuration and is switched to a redundant machine.

Tip: In the upper portion of the page, you can check the status of the redundant machine. If the status is green (**Polling servers**), redundancy is working correctly.



Status: Polling servers

For example:

The monitored Command Recording Software has an hardware fault and shuts down. The redundant machine detects that the monitored Command Recording Software is offline and automatically applies the latest configuration downloaded from the Command Recording Software. In this way the redundant machine takes the place of the faulty Command Recording Software. When the hardware fault is solved and the monitored Command Recording Software is back online, the redundant machine automatically applies its original configuration and returns to the monitoring status.

You can now view and export the video evidence recorded on the redundant machine while the monitored Command Recording Software was offline, by accessing it using Command Client or SiteManager. For more information, see the *Command Client User Guide* and the *SiteManager User Guide*, available on the Command Software DVD or from the March Networks Partner Portal and official websites.

Note: The monitored Command Recording Software can also recover part of the missing archive through the Shadow Archive feature, if enabled on the single cameras. For more information, see “Activate and Manage Shadow Archive” on page 163.

Setting Up Multiple Redundant Servers

The group functionality allows you to set up multiple redundant machines in your network which are monitoring the same Command Recording Softwares to provide backup for two or more different servers at the same time. When the monitored Command Recording Software had an hardware or a network failure, a redundant machine of the group takes the place of the faulty Command Recording Software. If also the redundant machine has a failure, one of the remaining redundant machines in the group is ready to take the place of the monitored Command Recording Software.

To set up multiple redundant servers

1 Set up two or more redundant machines in your network.

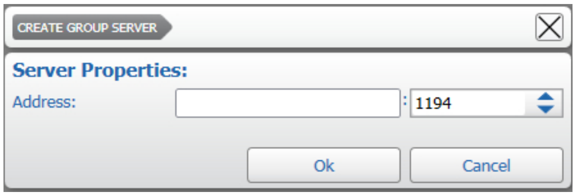
Important: The redundant machines must monitor the same Command Recording Softwares. For more information, see “Adding an Additional Command Recording Software for Backup Support” on page 261.

2 Log on to a redundant machine you want to add the redundancy group.

3 On the **Redundancy Configuration** page, click the **Group** tab.

4 Click **Add** to add the other redundant machines to the group.

The **Create Group Server** dialog box appears.



CREATE GROUP SERVER

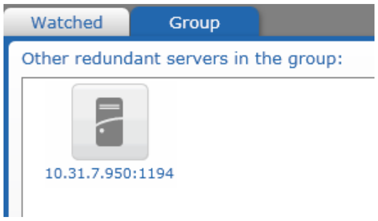
Server Properties:

Address: : 1194

5. Enter the **Address** of a redundant machine that you want to add to the group and select its communication **Port**.

   Important: You must not add the redundant machine you are logged on to the group.
6. Click **Ok**.

   An icon representing the server appears in the **Other redundant servers in the group** section.

7. Repeat step 4 to step 6 to add additional redundant machines to the group.

   Tip: You can delete a redundant machine from the group by selecting it in the page and clicking **Remove**.
8. Repeat step 2 to step 7 to configure the group on the other redundant machines.

   Important: You must configure the group on every redundant machine on the network that are monitoring the same Command Recording Softwares.
   For example: if you want to create a group for the redundant machines *A*, *B*, and *C*, you must log on to every redundant machine and add the other redundant machines to the group. So, when you configure the functionality on the redundant machine *A*, you will add machines *B* and *C* to the group, when you configure the functionality on the redundant machine *B*, you will add machines A and *C* to the group, and when you configure the functionality on the redundant machine *C*, you will add machines *A* and *B* to the group.
9. Click the 💾 button to save and apply the changes.

Company Overview

March Networks® helps organizations transform video into business intelligence through the integration of surveillance video, analytics, and data from business systems and IoT devices. Companies worldwide use our software solutions to improve efficiency and compliance, reduce losses and risk, enhance customer service and compete more successfully. With deep roots in video security and networking, March Networks is also recognized as the leader in scalable, enterprise-class video management and hosted services. We are proud to work with many of the world's largest financial institutions, retail brands, cannabis operators and transit authorities, and deliver our software and systems through an extensive distribution and partner network in more than 70 countries. Founded in 2000, March Networks is headquartered in Ottawa, Ontario, Canada. For more information, please visit *www.marchnetworks.com*.

Customer Support and Assistance

North America

Telephone – 1 613 591 1441
Toll Free (US & Canada) – 1 800 472 0116
Email – techsupport@marchnetworks.com

EMEA

Telephone – +39 0362 17935 extension 3 (CET)
Email – emeatechsupport@marchnetworks.com

APAC

Telephone – 1 613 591 1441
Email – techsupport@marchnetworks.com