VideoXpert Toolbox™ v 3.10

Operations Manual

VideoXpert™

Document number: C6602M-L

Publication date: 09/20

Table of Contents

Performing Initial VideoXpert Server™ Configuration Using VxToolbox™ 6

Logging Out 8

Changing the VxToolbox™ Password 9

Licensing Your System 10
- Viewing the License Summary 10
- Adding and Renewing Licenses 11
- Manually Activating Licenses 11
- Automatically Activating Licenses 12
- Installing Entitlements After Restoring Your System 13

Managing the System 14
- Adding a VX System™ 14
- Editing the System Validation 14
- Removing a System 15

Discovering Devices 16
- Finding Devices (Quick Discovery) 16
- Finding and Adding Devices (Quick Discovery and Add) 16
- Finding Devices (Advanced Discovery) 16
- Adding an RTSP Device 17
- Recognizing Device Credentials 17
- Adding Credentials for Devices that Require Authentication 18
- Creating a Default User on Cameras That Have No User 18
- Resetting the Password on a Storage Device 18
- Licensing and Configuring a Camera for the Pelco Advanced Analytics Suite™ 19
  - Licensing the Camera for the Pelco Advanced Analytics Suite™ 19
  - Configuring a Camera for the Pelco Advanced Analytics Suite™ 19
  - Understanding Counterflow zones 21

Managing Devices on a System 23
- Adding and Commissioning Devices 23
- Adding Devices Without Commissioning 24
- Commissioning Devices that were Added Previously 24
- Decommissioning Devices 24
- Replacing a Camera 24
- Removing Devices 25
- Adding Video Associations 25

Viewing Devices, Data Sources, Alarms & Relays, or Access Points 27
- Finding and Filtering Existing Sources 28
- Controlling the Columns Displayed in the Devices Window 28
- Viewing the License Summary 28

Viewing and Configuring Device Information 28
Disabling and Enabling Data Sources 32

Configuring the Rules Engine 33
Managing Rules 33
Creating a Rule 33
Duplicating a Rule 33
Editing an Existing Rule 33
Deleting a Rule 34
Managing Triggers 34
Adding a Trigger 34
Duplicating a Trigger 34
Editing a Trigger 35
Deleting a Trigger 35
Managing Schedules 36
Adding a Schedule 36
Creating a Copy of a Schedule 37
Editing a Schedule 37
Deleting a Schedule 38
Managing Responses 38
Adding a Response 39
Duplicating an Existing Response 39
Editing a Response 39
Deleting a Response 40
Configuring an SMS Messaging Response 40

Configuring Recording 42
Configuring a Recorder 42
Assigning Cameras to a Recorder 43
Adding a Recording Group to a Recorder 43
Creating a Recording Schedule for a Recording Group 44
Creating a Bump on Alarm Recording Schedule 45
Editing a Recording Group 46
Editing a Recording Schedule 46
Deleting a Recording Group 47
Deleting a Recording Schedule 47
Deleting a Recording Behavior (Trigger) 48

Managing Users and Roles 49
Understanding Internal and Restricted User Accounts 49
Creating a Role 49
Editing a Role 50
Duplicating a Role 51
Deleting a Role 51
Viewing Details of a Role 51

Adding Users ... 51
Editing Users ... 52
Searching for Users ... 52
Assigning Roles ... 53
Resetting Passwords ... 53
Setting the User Password Expiration Policy ... 53
Deleting Users ... 54

Configuring VideoXpert System™ Settings ... 55
Aggregating Systems (on VideoXpert Enterprise™ Systems Only) ... 55
Configuring General Settings for VideoXpert Enterprise™ Systems ... 56
Working with Clusters ... 58
Configuring Authentication ... 58
Enabling VideoXpert Authentication™ ... 58
Configuring LDAP Authentication: Simple Bind ... 58
Configuring LDAP Authentication: Two-Stage Bind Authentication ... 59
Configuring LDAP Authentication: Synchronizing Users and Roles From LDAP ... 60
Configuring LDAP Authentication: Using Single Sign-On ... 62
Configuring System Backups ... 63
Restoring Databases on VideoXpert Enterprise™ Systems ... 64
Replacing One or More Core or VxDatabase™ Nodes ... 64
Performing an Emergency Restoration of a Database Backup on VideoXpert Enterprise™ Systems 64
Manually Restoring a Database Backup on VideoXpert Enterprise™ Systems ... 65
Configuring the SMTP Server ... 65
Controlling Memory Usage ... 66

Configuring Monitor Walls ... 67
Creating a Monitor Wall ... 67
Editing a Monitor Wall ... 68
Deleting a Monitor Wall ... 68
Using Send Video Permissions ... 69

Using Reports ... 70
Creating a Report Template ... 70
Editing a Report Template ... 71
Deleting a Report Template ... 71
Generating a Report Manually ... 72
Exporting a Generated Report ... 72
Deleting a Generated Report ... 72

Managing Events ... 73
Setting Event Log Retention Periods ... 73
Finding and Filtering Events ... 73
Viewing and Configuring Event Details ... 74
Viewing and Configuring Event Notifications ... 74

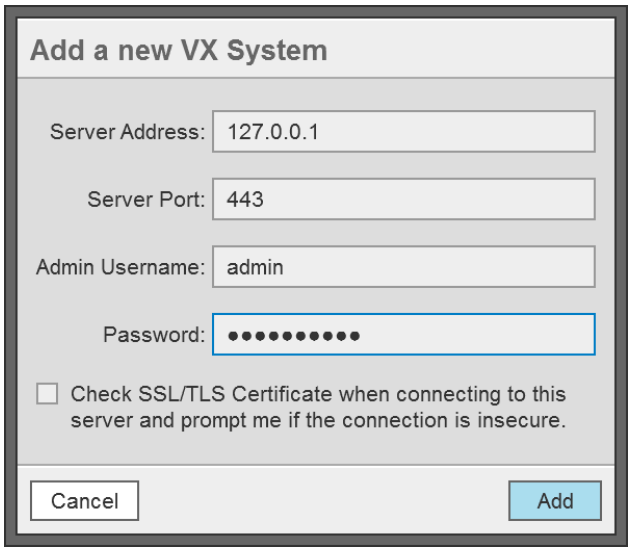
Using Maps™ 77
Preparing Your System for Maps 77
Creating a New Map 77
Viewing an Existing Map 78
Editing an Existing Map 78
Deleting an Existing Map 78
Managing Permissions for Maps 78
Appendix A: Working With Permissions 79
Understanding Permission Resource Restrictions 79
Using Surveillance Permissions 79
Using Investigation Permissions 80
Using Map Permissions 81
Using Supervision and Reports Permissions 81
Using Event Management Permissions 82
Using User Management Permissions 82
Using Device Management Permissions 82
Using System Management Permissions 83

Performing Initial VideoXpert Server™ Configuration Using VxToolbox™

VideoXpert Enterprise™ and VideoXpert Professional™ come with a time-limited trial license. During this trial, you have access to all VideoXpert features, and you can ignore the **Licensing** tab within VideoXpert.

To use VideoXpert beyond the trial, you must apply a license to the server. Licensing requires either an Internet connection on the VideoXpert server itself, or access to a separate computer with Internet access.

1. After installing VideoXpert, click *Configure* or run VxToolbox for the first time on your VideoXpert (VX) System™.
2. For VideoXpert Professional systems, in the *VideoXpert Basic System Setup* dialog box, type values in the *Company Name* and *Name Your System* fields, and then click **Save**.
3. Perform the steps in the section titled *Configuring General Settings for VideoXpert Enterprise™ Systems* or *Configuring General Settings for VideoXpert Professional Systems*.
4. Perform the steps in the section titled *Adding a VX System™*.
5. To set the VxToolbox password on VideoXpert Professional systems:
   a. Click the menu icon (☰), and then click **Set VxToolbox Password**.
   b. Type a value in the *Password* and *Reset Password* fields.
   c. Click **Save**.
6. To set the VxToolbox password and login requirements:
   a. Set the password for the *admin* user on your system.



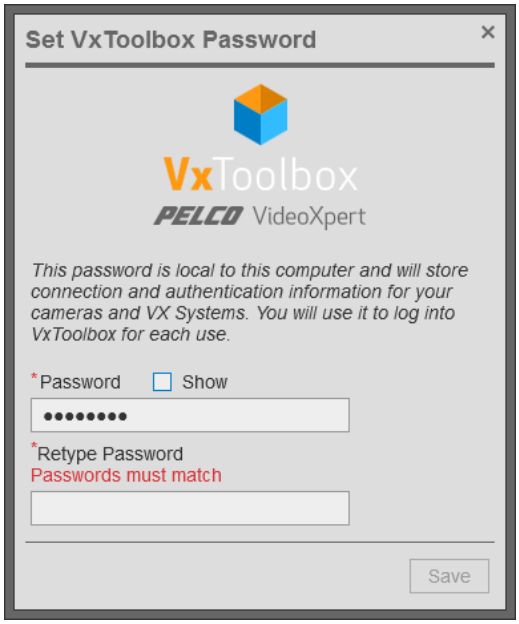
Note: The default user name is admin. You must set a new password.

   b. (Optional) Click to select the checkbox to ensure that the system checks the SSL/TLS Certificate when connecting to the server.
   Enable this feature if your organization uses signed HTTPS certificates and the certificate has already been loaded using VxToolBox.

c. Click **Add**.

d. In the *VxToolbox Password Confirmation Window*, click **Set Password** (recommended) or **No Thanks**.

e. If you clicked **Set Password**, in the *Set VxToolbox Password* dialog box, enter a password in the *Password* and *Retype Password* fields, and then click **Save**.

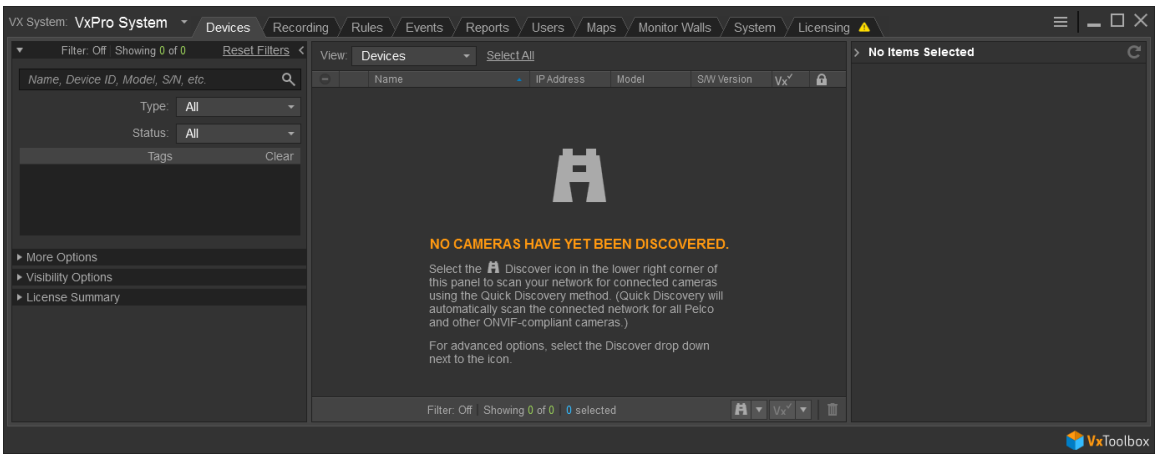


f. In the *Configure VxToolbox* dialog box, click **OK**.

g. If you enabled SSL/TLS Certificate checking, you might be required to interact with more dialog boxes. If so, follow the prompts.

h. In the *Configuration Required* dialog box, enter a *Company Name*. This is the name by which the Pelco licensing portal will recognize your VX server. The name cannot be changed later.

i. Click **Save & Continue**.
The VxToolbox application opens.



Logging Out

1. Click the menu icon (), and then click **Exit**.
2. In the *Exit* confirmation dialog box, click **Exit**.

Changing the VxToolbox™ Password

When starting VxToolbox, the application requests credentials. These credentials are local to the workstation and your VxToolbox installation; they do not log you in to any system or camera. Rather, your VxToolbox credentials protect your settings and the credentials for the individual cameras and systems you want to access from other users on the same workstation.

After logging in to VxToolbox, you can add systems with independent credentials, and pass credentials to cameras requiring them (closed authentication or third-party cameras).

Because your local VxToolbox environment may connect you to multiple systems and cameras, it is recommended that you protect your credentials and log out when you have finished using the application.

To change your VxToolbox password:

1. Click the menu icon (), and then select **Change VxToolbox Password**.
2. In the *Account Settings* dialog box, enter a new password in the *New Password* and *Confirm New Password* fields, and then click **Save Changes**.

Licensing Your System

VideoXpert is licensed for the system, for upgrades, and by channel—the video streams you view and record. It comes with one (1) license to start. The demo license provides unlimited channels that are active for a period of 60 days. These are active only the first time you install the software, or if the software was pre-installed, the first time you start up the system. In order for the system to function beyond the evaluation period, add the appropriate quantity of licenses to the system.

You can license the system automatically or manually.

- Manual licensing allows you to license a system that does not have an Internet connection. See the section titled *Manually Activating Licenses*
- Automatic licensing requires your VideoXpert system to be connected to the Internet and have access to the Pelco licensing server. See the section titled *Automatically Activating Licenses*.

If one or more licenses associated with the VideoXpert system are nearing or past the expiration date and require renewal, a warning dialog box will open. The dialog box lists the affected license(s) and the expiration date.

Note: You can also view your current licenses at any time. See section titled *Viewing the License Summary*.

For assistance, contact Pelco Product Support at 1-800-289-9100 (USA and Canada) or+1-559-292-1981 (international).

Viewing the License Summary

Entitlements are associated with licenses. A license might be a consolidation of several entitlements. To view licenses:

1. Open VxToolbox and click the **Licensing** tab.
2. In the *License Summary* table (bottom panel), view the list of licenses. For each license:
   - The license *Name* is listed. Unactivated *Entitlements* are listed as one license with the name *Pending*. The names in the *License Summary* table correspond to the names in the *Entitlements* table.
   - The *Total* column lists how many licenses and channels (sources) are included.
   - The *In Use* column identifies how many of the licenses and channels are in use.
   - The *Remaining* column identifies how many of the licenses and channels are not currently in use.
   - The *Expiration Date* column identifies when the licenses will expire.

If one or more licenses are nearing expiration, three warning icons appear in the *Licensing Summary* area of the *Licensing* page:

- On the right of the **Licensing** tab, itself
- In the left panel of the *License Summary* area, to the left of the license *Name*
- When the license is selected, in the top of the *Transaction History* (right) panel of the *License Summary* area

Hover over any of these warning icons to display relevant information.

Click **Details**, if present, to display *License Extension Details for [license name]*:

- View the current SUP expiration information, the number of channels on the VX System, and information about extending the SUP.
- If the SUP is expiring soon, instruct the system to use existing information to build an estimated price quote. If the necessary system variables cannot be retrieved, a default message is displayed instead of a quote.
- Click **OK** to close the dialog box.

For assistance, contact Pelco Product Support at 1-800-289-9100 (USA and Canada) or +1-559-292-1981 (international).

Adding and Renewing Licenses

When you are notified that one or more licenses are expiring or have expired, when you see the warnings in the *License Summary* area of the *Licensing* page, purchase a Software Update Plan (SUP).

- SUPs are purchased in units of "channel-years".
- One channel-year represents the use of one (1) licensed channel for one (1) year.
- Channel-years are usually purchased in such a way as to allow each channel on the system to be licensed for a period of several years.
  For example: a system with 40 channels will need to purchase 80 channel-years to extend the SUP by two (2) years.
- Integration licenses are combined to provide the longest time before expiration.
  For example: where appropriate, two one-year integration licenses will be recognized as a single license that expires in two (2) years.
- Adding channels to or removing channels from the system adjusts the expiration date of the licenses to reflect how long it will take the connected channels to use the remaining channel-years.
- If your licenses expired before you renew them, part of your SUP is used to backfill the period of time when the previous SUP/licenses had lapsed.

When licenses expire, all associated features are disabled until new licenses are installed or until the existing licenses are renewed. If the SUP has expired, you cannot upgrade the system until the SUP is purchased or renewed.

For assistance, contact Pelco Product Support at 1-800-289-9100 (USA and Canada) or +1-559-292-1981 (international).

Manually Activating Licenses

For manual licensing, you must have your activation ID and a separate computer with access to the licensing server at http://licensing.pelco.com. During the manual licensing process, you will need to transfer your Licensing Request File to a computer with Internet access during the activation process. If you received multiple activation IDs for VideoXpert products, you must complete the process below for each individual activation ID.

As a part of this process, you will download an Entitlement Request File and a Entitlement File; both files are specific to the product for which they were requested. It is recommended that you rename both files to reflect the system for which they are intended to prevent confusion during the licensing process.

1. Open VxToolbox and click the **Licensing** tab.
2. At the lower right corner of the *Entitlements* table (top panel), click the *Add License* icon (+).
3. Enter your activation ID in the *Activation ID* box.

4. If necessary, click to deselect the checkbox to *Automatically activate online*.
5. You will be prompted to save an activation request .bin file. Select a folder (optional) type in a file name, and then click **Save**.
   An Entitlement Request File (named either what you typed in or the same name as the *Activation ID*) with a .bin extension is downloaded to your computer.
6. Click **Enter**.
   - The *Entitlement Pending* status message appears at the top of the *Entitlements* table.
   - An entitlement named *Pending* will be listed in the table. At the far right of the *Pending* entitlement row will be two icons: *Download a new request (.bin) file* ( ) and *Remove this activation ID* ( ).
7. On a system connected to the Internet, open a new browser window or tab and go to the Pelco licensing server at http://licensing.pelco.com.
8. Under *Login*, click to select logging in **With User Name**, **With Entitlement Id**, or **With Activation Id**. You can also register as a **New User**.
9. Enter your credentials, and then click **Login** to access the Pelco licensing server.
10. Click the **Manage Devices** tab, and then click **Generate License**. Upload the request bin file to the licensing web site. The Entitlement File, named *response.bin*, will be downloaded to your computer.
11. Click the **Licensing** tab to return to the *Licensing* page within VxToolbox.
12. Click **Choose file** under the *Entitlements* section.
13. Select your Entitlement File (response.bin), and then click **Open**.
14. Click **Import License File**.

When the process is complete, VxToolbox will display the installed license(s) in the *Entitlements* table.

Automatically Activating Licenses

If your system has an active Internet connection with access to http://licensing.pelco.com, you can automatically activate licenses for your system.

1. Open VxToolbox and click the **Licensing** tab.
2. At the lower right corner of the *Entitlements* table (top panel), click the *Add License* icon ( ).
3. Enter your activation ID in the *Activation ID* box.
4. If necessary, click to select the checkbox to *Automatically activate online*.
5. Click **Enter**.
   The system logs in to the Pelco licensing server and performs several tasks. Do not navigate away from this page until you see the *Add License* dialog box.
6. Click **OK**.

VxToolbox will display the installed license(s) in the *Entitlements* table.

Installing Entitlements After Restoring Your System

Pelco highly recommends that you back up your system and save the response file used to apply your initial entitlement.

- If restoring your system after uninstalling VideoXpert, you can re-apply your initial entitlement or license.
- If you re-image your system, you cannot apply your previous entitlement. If you have re-imaged your system, contact Pelco Product Support at 1-800-289-9100 (USA and Canada) or+1-559-292-1981 (international) for assistance.

Managing the System

VxToolbox provides a single interface from which to manage and configure both cameras and your VideoXpert Systems. From VxToolbox, you can manage any system that you can access by IP address or hostname.

Selecting a system (by name) from the *VX System* menu allows you to configure that system; the settings you see are relevant to the system, and any discovery operations you perform are issued directly from that system.

Use the *VX System* menu to switch between various VideoXpert systems.

Adding a VX System™

VxToolbox allows you to administer systems remotely. To add a system to VxToolbox, you must have network access to the system and your user account must be assigned the administrative role.

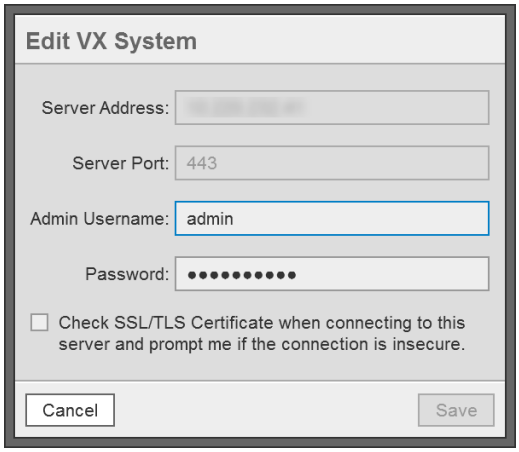
1. Access the *Add a new VX System* dialog box by one of these methods:
   - If the *Add a new VX System* dialog box opens automatically, and the *VxToolbox Password Confirmation Window* also opens automatically, click **Set Password**, enter the new password in the fields, and then click **Save**.
   - Click the menu icon ( ) at the upper right corner of the window, click **Manage VX System Connections**, and then click the *Add a new VX System* icon ( ).
   - At the upper left corner of the window, use the *VX System* drop-down menu to select *Add a VX system*.
2. Enter an IP address in the *Server Address* field.
3. Enter a value in the *Server Port* field, or use the default port.
4. Enter the *Admin Username* and *Password* for the system you are adding.
5. If an SSL/TLS certificate has been uploaded and configured, click to select the checkbox for *Check SSL/TLS Certificate...* to validate the certificate.
6. Click **Add**.
7. If necessary, click the at the top left of the *Manage VX System Connections* window to close it.

Editing the System Validation

You can change whether the SSL/TLS certificate is validated when connecting to a system from VxToolbox. Editing a system only affects your settings within your local VxToolbox installation.

1. Click the menu icon ( ) at the upper right corner of the window, and then click **Manage Vx System Connections**.
2. Select the system you want to edit.
3. In the right panel of the *Manage Vx System Connections* window, view the system connection information.
4. Click the *Edit VX System* icon ( ) to edit system settings.
   a. Enter the *Admin Username*.
   b. Enter the *Password*.

c. Click to select or deselect the checkbox for *Check SSL/TLS Certificate...*



5. Click **Save**.
6. In the *Update* dialog box, click **OK**.
7. Click the ✕ at the top left of the *Manage VX System Connections* window to close it.

Removing a System

You can remove a system from VxToolbox. It can be re-added at any time.

1. Click the menu icon (☰) at the upper right corner of the window, and then click **Manage Vx System Connections**.
2. Select the system you want to remove.
3. Click the *Delete* icon (🗑) to remove the system.
4. In the *Delete System* dialog box, click **OK** to confirm the deletion.
5. Click the ✕ at the top left of the *Manage VX System Connections* window to close it.

Discovering Devices

VxToolbox can search the local network or the network belonging to any particular VideoXpert system for devices, or you can add devices manually to the VxToolbox list. Through VxToolbox, you can manage device settings for all the devices on the network, without having to go to individual device interfaces.

VxToolbox can discover Pelco cameras or third-party cameras supporting ONVIF.

Note: You must be connected to a VideoXpert system to add devices to the system.

Finding Devices (Quick Discovery)

Use Quick Discovery to discover devices, but not add them. If you use Quick Discovery, you must add devices manually. Alternatively, use the *Quick Discovery and Add* option described in the section titled *Finding and Adding Devices (Quick Discovery and Add)*.

To use Quick Discovery, click **Devices**, and then do one of the following:

- Click the *Quick Discovery* icon ( ) to perform a quick search for devices.
- Click the *Advanced Discovery Options* icon ( ) to the right of the *Quick Discovery* icon, and then click **Quick Discovery**.
- Click the *Advanced Discovery Options* icon ( ) to the right of the *Quick Discovery* icon, and then click **Advanced Discovery**. In the *Discover Network Devices* dialog box, in the *Discovery Method* field, select **Discover by IP or Hostname** from the drop-down menu. Specify the *Host* address, and then click **Discover**.

Finding and Adding Devices (Quick Discovery and Add)

1. Click **Devices**, and then click the *Advanced Discovery Options* icon ( ) to the right of the *Quick Discovery* icon.
2. Click **Quick Discovery and Add**.
   All Devices and Data Sources that are discovered by VxToolbox are added to the VX System to which you are connected.
3. If the *Recorder Assignment* dialog box opens, assign the third-party devices to a recorder.
   a. Select an option from the *Select Recorder* drop-down menu.
   b. Click **Add**.
   c. If the devices cannot be added to the VX System, the *Operation Failure* dialog box opens. Make a note of the information in the box, click **OK**, and then try to add the devices to a different recorder. If necessary, contact Pelco Customer Support.

Finding Devices (Advanced Discovery)

Using Advanced Discovery, you can search for devices by protocol type or you can add individual devices by IP address. You may want to add devices that do not support ONVIF or Pelco discovery methods using the IP address.

1. Click **Devices**, and then click the *Advanced Discovery Options* icon ( ) to the right of the *Quick Discovery* icon.
2. Click **Advanced Discovery**.

3. To use Quick Discovery, but specify using either SSDP (Simple Service Discovery Protocol) or WS-Discovery (Web Services Dynamic Discovery):
   a. From the *Discovery Method* drop-down menu, select *Quick Discovery*.
   b. Click to select or deselect the checkbox for *SSDP*.
   c. Click to select or deselect the checkbox for *WS-Discovery*.
   d. (Optional) Click to select the checkbox for *Add discovered devices to the VX system*.
4. If you want to discover devices by IP address or hostname:
   a. From the *Discovery Method* drop-down menu, select *Discover by IP or Hostname*.
   b. Enter a value in the *Host* field.
   c. (Optional) Enter a value in the *HTTP Port* field.
   d. (Optional) Type values in the *Username* and *Password* fields.
   e. (Optional) Select a value from the *Driver* drop-down menu.
   f. (Optional) Click **Add Host Address**, and repeat the previous three steps.
   g. (Optional) Click to select the checkbox for *Add discovered devices to the VX system*.
5. Click **Discover**.

Note: While this feature adds devices to the system, it does not commission them. To commission the devices, add them, then select them, right-click a device that is selected, and then click **Commission**.

Adding an RTSP Device

To add a device that uses RTSP:

1. Click **Devices**, and then click the *Advanced Discovery Options* icon ( ) to the right of the *Quick Discovery* icon.
2. Click **Add RTSP Device**.
3. Type a value in the *Device Name* field.
4. (Optional) Click to select the checkbox for *Set Credentials*, and then enter values in the *Username* and *Password* fields.
5. Enter a value in the *URI* field.
6. (Optional) Click **Add Another URI to this Device**, and then enter a value in the *URI* field.
7. When you have added all URIs, click **Create**.

Recognizing Device Credentials

Some devices require credentials for you to access their video or change their settings. The *Authentication Status* column provides the status of each device.

Table 1: Icons in the Authentication Status column

Icon	Description
	Device requires authentication.
	Device does not require authentication.

Icon	Description
	VxToolbox has authenticated to this device.
	This device is authenticated in VxToolbox, but not on the system with which it is associated. Click the icon to attempt to authenticate the device with the system.
	This device is authenticated on a particular system with which it is associated, but not in VxToolbox. You must first authenticate to view and/or edit the device.
	The user must be created on the camera before accessing the camera

Adding Credentials for Devices that Require Authentication

To add credentials to a device:

1. Click **Devices**.
2. Select the device requiring credentials.
3. Enter credentials in the appropriate fields, and then click **Submit**.

Creating a Default User on Cameras That Have No User

For security purposes, cameras require a user to be created on the camera before the VideoXpert system can access the camera.

1. Add a camera using *Quick Discovery* or *Advanced Discovery*. See *Finding Devices (Quick Discovery)* or *Finding Devices (Advanced Discovery)*.
2. In the main panel of the *Devices* page, locate any cameras on the VideoXpert System that have a warning icon ( ) to the left of the camera *Name* and the locked camera icon ( ) in the *Authentication Status* column.
3. If necessary, refer to the camera instructions and add the user to the camera.
4. Select the camera for which a user must be created.
5. Enter credentials in the appropriate fields, and then click **Submit**.
6. Add and commission the camera. See *Adding and Commissioning Devices*.

Resetting the Password on a Storage Device

You must reset a password on a storage device before you can use it.

1. Add a storage device using *Quick Discovery* or *Advanced Discovery*. See *Finding Devices (Quick Discovery)* or *Finding Devices (Advanced Discovery)*.
2. In the list of devices, find a storage device with a locked server icon ( ) to the left of the device name and a warning icon ( ) in the *Authentication Status* column, and then click to select the device.
3. In the right panel, enter the credentials to reset the password, and then click **Reset Password**. A password must be at least eight characters long.

You can now add and commission the storage device. See *Adding and Commissioning Devices*.

Licensing and Configuring a Camera for the Pelco Advanced Analytics Suite™

When you discover a camera that supports advanced analytics, you must commission the device before you can apply a license and use advanced analytics.

Licensing the Camera for the Pelco Advanced Analytics Suite™

To license the camera:

1. Connect to a VX System.
2. Discover and commission the device. See the sections titled *Finding and Adding Devices (Quick Discovery and Add)* and *Commissioning Devices that were Added Previously*
3. Click the **Devices** tab.
4. In the center panel of the *Devices* page, select the camera for which you want to see analytics.
5. In the right panel, click to expand **Analytics**,and then under *ADVANCED ANALYTICS*, click *Apply a license*.
6. If the *No License Remaining* dialog box opens, click **OK**. If the dialog box does not open, skip to step 12.
7. Purchase a new license.
8. Click the **Licensing** tab, and follow the instructions in the section titled *Manually Activating Licenses* or *Automatically Activating Licenses* for adding a license for the camera.
9. Click the **Devices** tab.
10. In the center panel of the *Devices* page, select the camera for which you want to see analytics.
11. In the right panel, click to expand **Analytics**,and then under *ADVANCED ANALYTICS*, click *Apply a license*.
12. In the *Apply Analytics License* dialog box, click **Apply**.

Configuring a Camera for the Pelco Advanced Analytics Suite™

To configure the camera:

1. Click the **Devices** tab.
2. Click the Edit icon ( ) to the right of *ADVANCED ANALYTICS* in the right panel to open the *Configure Advanced Analytics for [device name]* dialog box.
3. (Optional) For a PTZ camera, in the left panel:
   a. Select a PTZ preset from the drop-down menu.
   b. (Optional) Set a *Confidence Threshold*, by either using the slider bar, or typing a value in the *%* field.
   A confidence threshold filters out object detections that have a confidence percentage lower than the threshold value. This is useful for filtering out detections that are not people or vehicles, or to help better detect objects at further distances. To filter objects out you can increase the threshold. To increase the distance of detections you can decrease the threshold.
4. In the *Configure Advanced Analytics for [device name]* dialog box, configure the zones or counters.
   a. To create a *New Zone*, in the *Analytic Rules* (left) panel, click the add icon ( ), and then select the type of zone or counter to add.
   Note: If you are configuring a Counterflow zone, see the section titled *Understanding Counterflow zones*.

b. To configure a Person in Zone or a Vehicle In Zone area, in the center panel:

- To reshape, expand, and/or move the zone (polygon with a blue or orange border—blue for person, and orange for vehicle), click and drag it or its points.
- To create a new point on the box, click the left mouse button. Drag the point to the appropriate location.
- To delete a point on the box, click the right mouse button on the point, and then click **Delete Point**.
- If there is a detection issue (for example: the analytics do not detect a person in the zone), change the size, shape, and position of the zone until detection is working as expected.

c. To configure a Person Counterflow or a Vehicle Counterflow area, in the center panel:

- To reshape, expand, and/or move the zone (polygon with a blue or orange border—blue for person, and orange for vehicle), click and drag it or its points.
- To create a new point on the box, click the left mouse button. Drag the point to the appropriate location.
- To delete a point on the box, click the right mouse button on the point, and then click **Delete Point**.
- If there is a detection issue (for example: the analytics do not detect a person in the zone), change the size, shape, and position of the zone until detection is working as expected.

d. To configure a Person Counter or a Vehicle Counter, in the center panel:

- Drag the counter line (blue or orange line—blue for person, and orange for vehicle) from the upper left corner of the center panel to the appropriate location.
- To shorten, lengthen, and or/move the line, click and drag it or its end points.
- If there is a detection issue, change the size, angle, and position of the line until detection is working as expected.

e. To name or rename a zone, click to select the zone name in the right panel, and then enter a new string in the *Zone Name* field in the left panel.

Note: Do not use quotation marks in the zone name.

f. In the right panel, enable or disable the zone by clicking to select or deselect the checkbox for *Zone is Enabled*.

g. (Optional) For zones, but not for counters, in the right panel, click to select the checkbox for *Override Default Severity*, and then set a new severity value, either by moving the slider bar or typing a number in the field.

h. For counterflow zones, select the *Counterflow Angle*, either by typing in a number or by selecting it using the slider bar.

i. For counter lines:

- Click to select the appropriate type of line from the *Counter Type* drop-down menu. This applies only to the line currently selected.
  - An **Uni-Directional Line** counts objects that cross the line in the configured direction. It has one or more white arrows on the line pointing in one direction.

  - A **Bi-Directional Line** maintains two separate counts—one for each direction that an object crosses the line. For example they can be used for a building entrance to differentiate between the number of people entering and exiting a building. It has one or more white arrows pointing in one direction; each is paired with a black arrow on the line pointing to the opposite direction.
  - An **Omni-Directional Line** counts when objects cross the line from any direction that is not parallel to the line. It has one or more white diamonds—two white arrows pointing in opposite directions from the line.

- (Optional) If you clicked **Bi-Directional Line**, you can either maintain the *Direction Labels* as they are, or you can type in new labels for each arrow type. This applies only to the line currently selected.

j. To save current settings before making more modifications or adding another zone, click **Apply Changes**.

k. To edit a zone or counter, click to select the zone or counter in the left panel; and then change any of the setting that are available in the right panel.

l. (Optional) To delete a zone, do one of the following:

- Click to select the zone name in the left panel, click the *Delete selected analytic zones* icon ( ), and then click **OK** in the *Delete Zones* confirmation dialog box.
- Right-click the zone border or the counter line, click **Delete Analytic Rule**, and then click **OK** in the *Delete Analytic Rules* dialog box.

m. Click **Save & Close**.

You can disconnect from a VX System and still configure the zones.

Understanding Counterflow zones

Counterflow alarms are triggered when the angle between an object's trajectory and the wrong direction is greater-than 110 degrees.

In *Figure 1: Counterflow at 90 degrees*, the Counterflow arrow is pointing at 90 degrees. Alarms trigger when the angle is between 20 and 160 degrees.

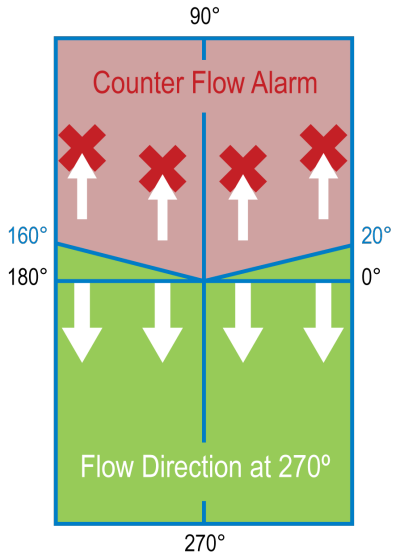


Figure 1: Counterflow at 90 degrees

In *Figure 2: Counterflow at 135 degrees*, the Counterflow arrow pointing at 135 degrees. Alarms trigger when the angle is between 155 and 245 degrees.

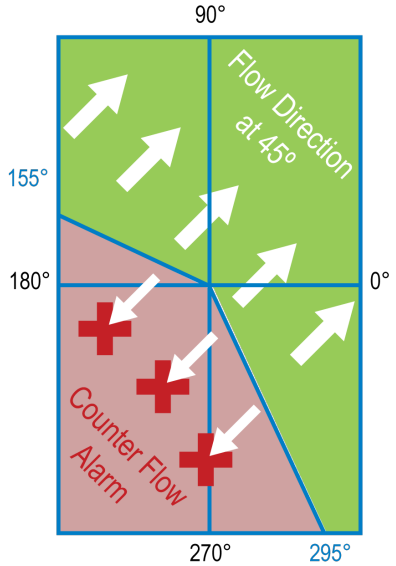


Figure 2: Counterflow at 135 degrees

Managing Devices on a System

You must add a device to VideoXpert to make it visible within the system and to manipulate device settings. VxToolbox enables you to add a device or change device settings.

You must commission a device to view its video or to use its video or resources within VideoXpert. VideoXpert typically commissions devices automatically when you add them to the system. In many cases, commissioning a device requires a license; the type of license required depends on the type of device you are commissioning.

Add or commission operations are available from the **Devices** tab for the selected system. Commissioning information is shown in the Added/Commissioned ( ) column; you can expose this column by selecting *Added/Commissioned* from *Show Data Columns* in the filtering panel.

Table 2: Icons in the Added/Commissioned column

Icon	Status
	NOT added to the system
	Added to the system, but not commissioned
	Added; commissioned

Adding and Commissioning Devices

VxToolbox will only provide adding and commissioning options applicable to the camera(s) you have selected. Add and Commission operations are relevant to the system you have selected from the *VX System* menu.

1. In the center panel of the *Devices* tab, select the devices you want to add and commission.
2. Perform one of the following steps:
   - Right-click the device, and then select **Add and Commission to [VX System name]**.
   - Click to select the device, and then click the *Add, Commission, and Assign Cameras to a recorder* icon ( ) at the lower right of the center panel.
   - Click to select the device, click the *Addition, Commission and Assignment options* icon ( ), and then click **Add and Commission to [VX System name]**.
3. If the *Authentication Notice* dialog box opens, follow the instructions in the dialog box.
4. If the *Recorder Assignment* dialog box opens, select a recorder from the drop-down menu, and then click **Add**.
   The icon for the device changes from *NOT added to the system* ( ) to *Added to the system and commissioned* ( ).

Adding Devices Without Commissioning

The Add operation is relevant to the system you have selected from the *VX System* menu.

1. In the center panel of the *Devices* tab, select the devices you want to add.
2. Perform one of the following steps:
   - Right-click the devices, and then select **Add to [VX System name]**.
   - Click the *Addition, Commission and Assignment options* icon (▼), and then click **Add to [VX System name]**.
3. If the *Recorder Assignment* dialog box opens, select a recorder from the drop-down menu, and then click **Add**.
   The icons for the devices change from *NOT added to the system* (🚫) to *Added to the system, but not commissioned* (Vx*).

Commissioning Devices that were Added Previously

VxToolbox will only provide commissioning options applicable to the camera(s) you have selected, and which were already added. Commission operations are relevant to the system you have selected from the *VX System* menu.

1. In the center panel of the *Devices* tab, select the devices you want to commission.
2. Perform one of the following steps:
   - Right-click the devices, and then select **Commission**.
   - Click the *Addition, Commission and Assignment options* icon (▼), and then click **Commission**.

   The icons for the devices change from *Added to the system, but not commissioned* (Vx*) to *Added to the system and commissioned* (Vx✓).

Decommissioning Devices

VxToolbox can decommission the camera(s) you have selected, on system you have selected from the *VX System* menu.

1. In the center panel of the *Devices* tab, select the devices you want to decommission.
2. Perform one of the following steps:
   - Right-click the devices, and then select **Decommission**.
   - Right-click the devices, click the *Addition, Commission and Assignment options* icon (▼), and then click **Decommission**.

   The icons for the devices change from *Added to the system and commissioned* (Vx✓) to *Added to the system, but not commissioned* (Vx*).

Replacing a Camera

If you are upgrading from an existing camera to a new one, or replacing a broken camera, VxToolbox enables you to select the existing and new cameras, and make the replacement. Replacing a camera allows you to transfer preconfigured settings (including camera name, tags, and recording schedules) from one camera to another.

1. If you have not already done so, ensure that the existing camera is offline (for example: turn off the camera).
2. If you have not already done so, add and commission the replacement camera. See the chapter titled *Discovering Devices*.
3. Click the **Devices** tab.
4. In the center panel of the *Devices* tab, select the camera that you will replace.
5. Right-click the camera, and then click **Replace Camera**.
6. In the *Select Replacement Camera for* dialog box, (optional) use the search field to help you locate the replacement camera, click to select the replacement camera, and then click **Replace**.
7. Read the information in the *Replace Camera* confirmation dialog box, and then click **OK**.

Removing Devices

After a device is discovered, it will persist in the system's device registry until it is removed, even if the device no longer exists on the network.

Removing a device will prevent you from retrieving any associated recordings through VideoXpert Storage™. To preserve access to recordings on VideoXpert Storage devices, decommission the devices until video for the device has expired or you are sure you will no longer need to access recordings for the device, then remove the device.

From VxToolbox, you can remove the device(s) you have selected, on the system you selected from the *VX System* menu.

1. Click the **Devices** tab.
2. In the center panel of the *Devices* tab, select the devices you want to remove.
3. Perform one of the following steps:
   - Right-click the devices, and then click **Remove**.
   - Right-click the devices, and then click the *Remove device(s) from VxToolbox and/or VX System* icon ( ) at the bottom right of the center panel.
   - Click the devices, click the *Addition, Commission and Assignment options* icon ( ), and then click **Remove**.
4. (Optional) In the *Remove Device(s)* confirmation dialog box opens, if the *Also remove from VxToolbox?* is present, click to select or deselect it.
5. In the *Remove Device(s)* confirmation dialog box, click **OK**.
   The devices are removed from the list. They can be discovered again at any time.

Adding Video Associations

You can associate an audio data source with a video data source on another device.

For example, if you have a microphone on a camera near a cash register, but you want that audio to be associated with a different camera that has a better view of that cash register, you can use **Add Video Associations** to make this configuration.

1. Click the **Devices** tab.
2. In the center panel of the *Devices* page, select the device with audio data source that you want to associate with a different video data source.
3. Right-click the device, and then click **Add Video Associations**.

In the *Associate Data Sources with Audio "[camera name] - Audio"* dialog box, the *All Data Sources* panel will list the name of the data sources already associated with the device.

4. (Optional) In the *Associate Data Sources with Audio "[camera name] - Audio"* dialog box, use the filter to narrow the list of available devices.
5. In the *Associate Data Sources with Audio "[camera name] - Audio"* dialog box, in the *Associated to* panel, click to select and deselect the checkboxes to indicate which of the available video data sources to associate with the audio data source.
6. Click **Save**.

Viewing Devices, Data Sources, Alarms & Relays, or Access Points

The audio and video sources produced by a device (for example, a camera) are referred to as data sources.

A device can have more than one data source. For example, a multi-channel encoder may have multiple cameras connected to it, each with its own data source; a camera may have a microphone, producing audio and video data sources.

A device can have one or more alarms and relays, depending on the device. For example: an encoder typically has one alarm and one relay per device channel; a camera might have only one alarm and one relay for the device. Alarms are configured and relays are enabled on the *Devices* page.

- To view all devices on the system, in the *View* field drop-down menu, at the top of the center panel, select **Devices**.
- If a device and its data sources are distinguishable, you can see the individual data sources, alarms, and relays. To see the data sources, alarms, and relays that are associated with a specific device:
  a. In the *View* field drop-down menu, select **Devices**.
  b. Click the expand icon (▶) to the left of the device.
     Data sources, alarms (if any), and relays (if enabled), are listed directly below the device.
- To view all data sources on the system, in the *View* field drop-down menu, at the top of the center panel, select **Data sources**.
- To toggle the view to show only the devices and not the data sources, alarms, and relays, right click anywhere in the device list, and then click **Collapse All**.
- To view the list of alarms and relays on the system, in the *View* field drop-down menu, at the top of the center panel, select **Alarms & Relays**.
  You can determine the status of an alarm or relay by the icons in the *State* column.

  Table 3: Icons in the State column

Icon	State
	Alarm is active
	Alarm is inactive
	Relay is active
	Relay is inactive

  You can determine whether an alarm or relay is enabled or disabled by the icons in the *Enabled* column.

  Table 4: Icons in the Enabled column

Icon	Enabled
	Yes
	No

- To view the list of access points on the system, in the *View* field drop-down menu, at the top of the center panel, select **Access Points**. If there are no devices with access points, the window will display the message *NO DEVICES HAVE YET BEEN DISCOVERED*.

Finding and Filtering Existing Sources

Use filtering options to show the devices and data sources relevant to you within the system or environment you have selected. Filters appear in the left-most panel of the *Devices* tab and in some other tabs. Click the **Devices** tab. Then use the filter, as appropriate:

- Enter a value in the filter field to filter by criteria including the device name, ID, model, IP address, serial number, vendor, or software version.
- Click to expand, and then click to select and deselect checkboxes in, the *Filter by Type* area.
- Click to expand, and then click to select and deselect checkboxes in, the *Filter by Status* area.
- Click to expand, and then type in or select a tag in the *Filter by Tags* field. Tags are set in VxOpsCenter™. See the *VxOpsCenter Operations Manual* for more information.
- Click the *Clear the current filter settings* icon ( ) to clear the filters.

Controlling the Columns Displayed in the Devices Window

1. Click the **Devices** tab.
2. Include columns in or exclude them from the display by one of the following methods:
   - In the left panel, below the filter areas, click to expand the *Show Data Columns* area, and then click to select and deselect checkboxes in the area.
   - Right-click the column header, and then click to select and deselect the column titles in the drop-down menu.

Viewing the License Summary

1. Click the **Devices** tab.
2. In the left panel, below *Show Data Columns*, click to expand **License Summary**. View the system license information.

Viewing and Configuring Device Information

If you have the proper credentials, from VxToolbox, you can view information for and configure some settings on a device that you have selected, on the system you selected from the *VX System* menu.

1. Click the **Devices** tab.
2. In the center panel of the *Devices* tab, select the device you want to configure. Information specific to the device is presented in the right panel. If the device has been authenticated in VxToolbox, you will see the current view from the device, and status information.
3. (Optional) Click the *Web View* icon ( ) to the right of the device name to view the device control panel in a web browser, and make changes there.

   Note: You must have permissions for the device in order to make any changes.

4. If necessary, to authenticate the device, enter correct values in the *Username* and *Password* fields, and then click **Submit**.

   Note: You must provide a valid username and password in order to update the device configuration using VxToolbox.

5. (Optional) To view and update Device Information in VxToolbox:
   a. Click to expand **Device Information**. All available device information is listed, and might include: name, hostname, IP address, port, MAC address, vendor, and model. Information varies based on the device type.
   b. If present, click the *Edit* icon ( ) to the right of *Device Information*.

      If the *Edit* icon ( ) is not present, you cannot update Device information. Continue to step 6.
   c. In the *Settings Editor* dialog box, enter correct values into the fields. For example: Type values into the *Name*, *Hostname*, *IP Address*, and *Port* fields (if available); and click to select or deselect the checkbox for *Apply name to Data Sources*.
   d. Click **Save Changes**.
6. (Optional) To view and update the Video Configuration, if present:
   a. Click to expand **Video Configuration**.
   b. Continue clicking to expand the items listed under *Video Configuration*, and then the primary stream, secondary stream, tertiary stream or smart compression settings to view. Depending on the device:
      - If there are primary, secondary, and tertiary streams, the stream information might include: device name, encoding, profile, GOP, resolution, maximum bitrate, frame rate, multicast address, and multicast port.
      - The smart compression information includes: the compression level, and weather each stream has dynamic GOP enabled.
   c. Click the *Edit* icon ( ) to the right of the primary, secondary, or tertiary stream or the smart compression listing.
   d. If you are updating the primary, secondary, or tertiary stream, in the *Settings Editor* dialog box, enter correct values into the fields. For example: Type in or select from the drop-down menus a stream *Name*, *Encoding*, *Profile*, *GOP*, *Resolution*, *Max Bitrate*, *Frame Rate*, *Multicast Address*, and *Multicast Port*.
   e. If you are updating the smart compression settings, in the *Settings Editor* dialog box:
      - Click to select or deselect the checkbox for *Smart Compression Enabled*.
      - Select the appropriate value from the drop-down menu in the *Level* field.
      - Click to select or deselect the *Primary Stream Dynamic GOP Enabled* checkbox. If you selected this checkbox, enter a value in the *Primary Stream Max GOP Length* field—either by typing-in a number or selecting one using the up and down arrows.
      - Click to select or deselect the *Secondary Stream Dynamic GOP Enabled* checkbox. If you selected this checkbox, enter a value in the *Secondary Stream Max GOP Length* field—either by typing-in a number or selecting one using the up and down arrows.
      - Click to select or deselect the *Tertiary Stream Dynamic GOP Enabled* checkbox. If you selected this checkbox, enter a value in the *Tertiary Stream Max GOP Length* field—either by typing-in a number or selecting one using the up and down arrows
   f. Click **Save Changes**.

7. (Optional) To view and update basic Analytics (motion detection, etc.), if present:
   a. Click to expand **Analytics**.
   b. Continue clicking to expand individual items listed under *Analytics*.
   c. If there is a setting to edit, click the *Edit* icon ( ) to the right of the information.
   d. In the *Edit [analytics name] Settings for [device name]* dialog box:
      – Select the appropriate radio buttons. If you chose *On Camera*, click **Edit camera settings in browser**, make the appropriate changes, exit the browser window, and then click **Done**.
      – If you chose *On Server*, use the slider bar to select a value for *Contrast Sensitivity*; use the icons under the device image to view information **Live**, *Jump Back 30 Seconds* ( ), *Jump to Specific Date/Time* ( ), or *Jump to Now* ( ).
      – If you chose *Off*, the analytics will be disabled.
      – When you are finished in this dialog box, click **Done**.
8. (Optional) To view and update the Pelco Advanced Analytics Suite, if present on the camera:
   a. Apply a license to the camera that uses the Pelco Advanced Analytics Suite. See the section titled: *Licensing and Configuring a Camera for the Pelco Advanced Analytics Suite™*.
   b. In the right panel, click to expand **Analytics**,and then to the right of *ADVANCED ANALYTICS*, click the *Edit* icon ( ).
   c. In the *Configure Advanced Analytics for [device name]* dialog box, configure the zones. See the instructions in the section titled *Licensing and Configuring a Camera for the Pelco Advanced Analytics Suite™* to update the configuration.
9. (Optional) To view and update Alarms, if present:
   a. Click to expand **Alarms**.
   b. Continue clicking to expand individual items listed under *Alarms*. All available alarm information is listed, and might include: state, name, description, ID, and type. Information varies based on the alarm type.
   c. Click the *Edit* icon ( ) to the right of the alarm item to update.
   d. In the *Settings Editor* dialog box, enter all appropriate values. For example: type values in the *Name* and *Description* fields, and then select a value from the drop-down menu in the *Type* field.
   e. Click **Save Changes**.
10. (Optional) To view and update Relays, if present:
    a. Click to expand **Relays**.
    b. Continue clicking to expand individual items listed under *Relays*. All available relay information is listed, and might include: status, state, name, description, and ID. Information varies based on the device type.
    c. To activate or deactivate the relay, click **Activate** or **Deactivate** under *STATE*.
    d. Click the *Edit* icon ( ) to the right of the relay item to update.

e. In the *Settings Editor* dialog box, enter all appropriate values. For example: select a value from the drop-down menu in the *Status* field, and then type values in the *Name* and *Description* fields. You cannot update the ID from this dialog box.

f. Click **Save Changes**.

11. (Optional) To view and update Recording and Retention, if present:

    a. Click to expand **Recording and Retention**.

    b. Continue clicking to expand individual items listed under *Recording and Retention*. All available recording and retention information is listed, and might include: full-framerate retention limit and the associated assigned recorders, and the standard retention limit and associated assigned recorders.

    c. Click the *Edit* icon ( ) to the right of *Recording and Retention*.

    d. In the *Recording Retention Limits* dialog box, click to select the radio button for the appropriate retention limit. If you select *Manual Retention Limit*, enter a value from the *Delete unlocked recordings after [#] days* field, either by typing-in a number or selecting one using the up and down arrows.

    e. Click **Save**.

12. (Optional) To view and update System information, if present:

    a. Click to expand **System**.

    b. Continue clicking to expand individual items listed under *System*. All available system information is displayed, and includes firmware version and time settings.

    c. To update the firmware: click to expand *FIRMWARE*; click **Update Firmware**; in the *Update Firmware* dialog box, navigate to and double-click the firmware file.

    d. To reboot the system: click to expand *MAINTENANCE*, click **Reboot**, and then click **OK**.

    e. To backup or restore the system: click to expand *BACKUP & RESTORE*, and then click either **Backup** or **Restore**.

13. (Optional) To view Tags, if present:

    a. Click to expand **Tags**.

    b. Continue clicking to expand individual items listed under *Tags*.

14. (Optional) To create a User, if the option is present:

    a. Click to expand **User**.

    b. Type values in the *Username*, *New Password*, and *Re-type Password* fields.

    c. Click **Save**.

15. (Optional) To view and update the device Driver, if present:

    a. Click to expand **Driver**.

    b. Click the *Edit* icon ( ) to the right of *Driver*.

    c. In the *Settings Editor* dialog box, select a value from the drop-down menu in the *System Driver* field.

    d. Click **Save Changes**.

Disabling and Enabling Data Sources

You can conserve license seats by disabling data sources that are not in use:

1. Click the **Devices** tab.
2. In the center panel of the *Devices* page, select the device with data sources that you want to disable.
3. Perform one of the following steps:
   - Right-click the devices, and then click **Disable/Enable Data Sources**.
   - Click the device, click the *Addition, Commission and Assignment options* icon (▼), and then click **Disable/Enable Data Sources**.
4. In the *Disable/Enable Data Sources* dialog box, click to deselect the data sources to disable.
5. Click **Save Changes**.

To enable the data sources, follow the steps above, but click to select the data sources to enable.

Configuring the Rules Engine

The *Rules* tab allows you to configure events generated by a source to trigger a response. Rules can have one or more triggers, zero or more schedules, and one or more responses. There can be multiple rules on the system.

Managing Rules

Use VxToolbox to create, duplicate, edit, or delete rules in the rules engine.

Creating a Rule

1. Click the **Rules** tab.
2. In the left panel, click the *Create a new Rule* icon ( ). The *Edit Mode* (right) panel is activated.
3. Enter a value in the *Name of Rule* field.
4. Click to select the radio button for *Active* or *Inactive*.
5. Add one or more triggers for the rule. See the section titled *Adding a Trigger*.
6. (Optional) Add one or more schedules to the rule. See the section titled *Adding a Schedule*.
7. Add one or more responses to the rule. See the section titled *Adding a Response*.
8. When you have finished configuring triggers, schedules, and responses, click **Save**.

Duplicating a Rule

To use an existing rule as a starting point to create a new rule:

1. Click the **Rules** tab.
2. (Optional) In the left panel, enter a value in the *Search Rules* field to filter the rules.
3. Click to select the rule to duplicate.
4. Click the *Duplicate the selected Rule* icon ( ). The *Edit Mode* (right) panel is activated.
5. Enter a value in the *Name of Rule* field.
6. Click to select the radio button for *Active* or *Inactive*.
7. (Optional) Add, duplicate, edit, or delete one or more triggers for the rule. See the sections titled *Adding a Trigger*, *Duplicating a Trigger*, *Editing a Trigger*, and *Deleting a Trigger*.
8. (Optional) Add, create a copy of, edit, or delete one or more schedules for the rule. See the sections titled *Adding a Schedule*, *Creating a Copy of a Schedule*, *Editing a Schedule*, and *Deleting a Schedule*.
9. (Optional) Add, duplicate, edit, or delete one or more responses for the rule. See the sections titled *Adding a Response*, *Duplicating an Existing Response*, *Editing a Response*, or *Deleting a Response*.
10. When you have finished configuring triggers, schedules, and responses, click **Save**.

Editing an Existing Rule

1. Click the **Rules** tab.
2. (Optional) In the left panel, enter a value in the *Search Rules* field to filter the rules.
3. Click to select the rule to edit.
4. Click the *Edit the selected Rule* icon ( ). The *Edit Mode* (right) panel is activated.

5. Click to select the radio button for *Active* or *Inactive*.
6. (Optional) Add, duplicate, edit, or delete one or more triggers for the rule. See the sections titled See the sections titled *Adding a Trigger*, *Duplicating a Trigger*, *Editing a Trigger*, and *Deleting a Trigger*.
7. (Optional) Add, create a copy of, edit, or delete one or more schedules for the rule. See the sections titled *Adding a Schedule*, *Creating a Copy of a Schedule*, *Editing a Schedule*, and *Deleting a Schedule*.
8. (Optional) Add, duplicate, edit, or delete one or more responses for the rule. See the sections titled *Adding a Response*, *Duplicating an Existing Response*, *Editing a Response*, or *Deleting a Response*.
9. When you have finished editing triggers, schedules, and responses, click **Save**.

Deleting a Rule

1. Click the **Rules** tab.
2. In the left panel (list of rules), click the rule to delete.
3. Click the *Delete the selected Rule* icon ( ).
4. In the confirmation dialog box, click **Delete**.

Managing Triggers

Add, duplicate, edit, or delete triggers from a rule to control the type of events that will trigger one or more responses.

Adding a Trigger

To add an entirely new trigger to a rule:

1. Click the **Rules** tab.
2. Click to select the rule to edit.
3. Click the *Edit the selected Rule* icon ( ). The *Edit Mode* (right) panel is activated.
4. In the *Triggers* panel, click the *Add New Rule Trigger* icon ( ).
5. (Optional) In the *Select an Event to trigger this Rule* dialog box, narrow the list of events. To do so, select a category from the *Show* drop-down menu, or type a value in the *Search* field.
6. In the *Select an Event to trigger this Rule* dialog box, click to select an event, and then click **Save**.
7. In the *Select Event Sources to limit this Trigger for Rule* dialog box, click to select the appropriate radio button. The options vary depending on the trigger you have chosen. If you are prompted to do so, make any other necessary selections, and then click **Save**.
8. When you have finished configuring the rule, click **Save**.

Duplicating a Trigger

To use an existing trigger as a starting point to create a new trigger:

1. Click the **Rules** tab.
2. Click to select the rule to edit.
3. Click the *Edit the selected Rule* icon ( ). The *Edit Mode* (right) panel is activated.
4. In the *Triggers* panel, click to select a trigger to duplicate.
5. Click the *Duplicate Rule Trigger* icon ( ).

6. (Optional) Edit the *When this event* settings, associated with the duplicate trigger:
   a. In the *When this event* column, click the edit icon ( ) in the appropriate trigger.
   b. (Optional) In the *Select an Event to trigger this Rule* dialog box, narrow the list of events. To do so, select a category from the *Show* drop-down menu, or type a value in the *Search* field.
   c. Click to select the event.
   d. Click **Save**.
7. (Optional) Edit the *is generated by* settings, associated with the duplicate trigger:
   a. In the *is generated by* column, click the edit icon ( ) in the appropriate trigger.
   b. In the *Select Event Sources to limit this Trigger for Rule* dialog box, click to select the appropriate radio button. The options vary depending on the trigger you have chosen. If you are prompted to do so, make any other necessary selections, and then click **Save**.
8. When you have finished configuring the rule, click **Save**.

Editing a Trigger

To edit an existing trigger:

1. Click the **Rules** tab.
2. Click to select the rule to edit.
3. Click the *Edit the selected Rule* icon ( ). The *Edit Mode* (right) panel is activated.
4. In the *Triggers* panel, click the trigger to edit.
5. (Optional) Edit the *When this event* settings:
   a. In the *When this event* column, click the edit icon ( ) in the appropriate trigger.
   b. (Optional) In the *Select an Event to trigger this Rule* dialog box, narrow the list of events. To do so, select a category from the *Show* drop-down menu, or type a value in the *Search* field.
   c. Click to select the event.
   d. Click **Save**.
6. (Optional) Edit the *is generated by* settings:
   a. In the *is generated by* column, click the edit icon ( ) in the appropriate trigger.
   b. In the *Select Event Sources to limit this Trigger for Rule* dialog box, click to select the appropriate radio button. The options vary depending on the trigger you have chosen. If you are prompted to do so, make any other necessary selections, and then click **Save**.
7. When you have finished configuring the rule, click **Save**.

Deleting a Trigger

If a trigger is no longer needed, delete it.

1. Click the **Rules** tab.
2. Click to select the rule to edit.
3. Click the *Edit the selected Rule* icon ( ). The *Edit Mode* (right) panel is activated.
4. In the *Edit Mode* panel, click to select the trigger to delete.

5. Do one of the following:
   - Click the ✕ at the right of the trigger entry.
   - Click the delete icon ( ).
6. When you have finished configuring the rule, click **Save**.

Managing Schedules

You can set one or more schedules to limit the times during which an event triggers a response; or you can leave the *Schedules* panel unpopulated to allow the trigger/response combination at all times.

Adding a Schedule

To create an entirely new schedule:

1. Click the **Rules** tab.
2. Click to select the rule to edit.
3. Click the *Edit the selected Rule* icon ( ). The *Edit Mode* (right) panel is activated.
4. At the bottom of the *Schedules* panel, click the *Edit Rule Schedules* icon ( ).
5. Click to select the *Add a new schedule* icon ( ).
6. In the *Create Schedule* dialog box, enter a value in the *Display Name* field.
7. Click to select the radio button for the appropriate increments of time (for example: *30 Minutes*).
8. Click to select or deselect the checkbox for *24-Hour Time*.
9. Indicate the times and days that the recording/rule is active by clicking to select boxes corresponding to a days and times. You can also click and drag to select a contiguous range of times and days. Click to deselect any days and times that you do not want the recording/rule to be active.

   Note: Schedules are shared between Recording Schedules and Rule Schedules. Any schedule that you create, modify, or delete in either location is reflected in both locations.
10. (Optional) Click the checkbox to select or deselect *Within limited date range*. If you select *Within limited date range*, enter dates in the *Start on* and *End after* fields, either by selecting the dates from the calendars or by typing in a date using the mm/dd/yy format. Deselect the checkbox to make the schedule unlimited by date.
11. Click **Add**.
12. In the *Select Schedules for Rule* dialog box, click to select the checkbox for the schedule to apply to the rule. If there is another schedule applied to the rule, you can deselect the checkbox to disable that schedule. If you select *No Time Restriction*, all other schedules are automatically deselected. Also, you cannot edit or copy the *No Time Restriction* schedule.
13. When you have finished configuring schedules, click **Save Changes**.
14. When you have finished configuring the rule, click **Save**.
15. (Optional) To quickly view the scheduled times, click to select the schedule, and then click the *View selected Rule Schedule* icon ( ). Click outside the calendar to close it.

Creating a Copy of a Schedule

To use an existing schedule as a starting point to create a new schedule:

1. Click the **Rules** tab.
2. Click to select the rule to edit.
3. Click the *Edit the selected Rule* icon ( ). The *Edit Mode* (right) panel is activated.
4. Click the *Edit Rule Schedules* icon ( ).
5. Click to select (highlight) the schedule to copy.
6. Click the *Create a copy of the selected Schedule* icon ( ).
7. In the *Duplicate Schedule* dialog box, enter a new value in the *Display Name* field. If you do not enter a new value, the schedule will be saved as *[Original name] - Copy*.
8. Click to select the radio button for the appropriate increments of time (for example: *30 Minutes*).
9. Click to select or deselect the checkbox for *24-Hour Time*.
10. Indicate the times and days that the recording/rule is active by clicking to select boxes corresponding to a days and times. You can also click and drag to select a contiguous range of times and days. Click to deselect any days and times that you do not want the recording/rule to be active.

    Note: Schedules are shared between Recording Schedules and Rule Schedules. Any schedule that you create, modify, or delete in either location is reflected in both locations.

11. (Optional) Click the checkbox to select or deselect *Within limited date range*. If you select *Within limited date range*, enter dates in the *Start on* and *End after* fields, either by selecting the dates from the calendars or by typing in a date using the mm/dd/yy format. Deselect the checkbox to make the schedule unlimited by date.
12. Click **Add**.
13. In the *Select Schedules for Rule* dialog box, click to select the checkbox for the schedule to apply to the rule. If there is another schedule applied to the rule, you can deselect the checkbox to disable that schedule. If you select *No Time Restriction*, all other schedules are automatically deselected. Also, you cannot edit or copy the *No Time Restriction* schedule.
14. When you have finished configuring schedules, click **Save Changes**.
15. When you have finished configuring the rule, click **Save**.
16. (Optional) To quickly view the scheduled times, click to select the schedule, and then click the *View selected Rule Schedule* icon ( ). Click outside the calendar to close it.

Editing a Schedule

To edit an existing schedule:

1. Click the **Rules** tab.
2. Click to select the rule to edit.
3. Click the *Edit the selected Rule* icon ( ). The *Edit Mode* (right) panel is activated.
4. Click to select (highlight) the schedule to edit.
5. At the bottom of the *Schedules* panel, click the *Edit Rule Schedules* icon ( ).
6. In the *Select Schedules for Rule* dialog box, click to select the checkbox for the schedule to apply to the rule. If there is another schedule applied to the rule, you can deselect the checkbox to disable

that schedule. If you select *No Time Restriction*, all other schedules are automatically deselected. Also, you cannot edit or copy the *No Time Restriction* schedule.

7. Click the *Edit the selected Schedule* icon ( ).
8. (Optional) In the *Edit the Schedule* dialog box, enter a new value in the *Display Name* field. If you do not enter a new value, the schedule will be saved with the original name.
9. Click to select the radio button for the appropriate increments of time (for example: *30 Minutes*).
10. Click to select or deselect the checkbox for *24-Hour Time*.
11. Indicate the times and days that the recording/rule is active by clicking to select boxes corresponding to a days and times. You can also click and drag to select a contiguous range of times and days. Click to deselect any days and times that you do not want the recording/rule to be active.

    Note: Schedules are shared between Recording Schedules and Rule Schedules. Any schedule that you create, modify, or delete in either location is reflected in both locations.

12. (Optional) Click the checkbox to select or deselect *Within limited date range*. If you select *Within limited date range*, enter dates in the *Start on* and *End after* fields, either by selecting the dates from the calendars or by typing in a date using the mm/dd/yy format. Deselect the checkbox to make the schedule unlimited by date.
13. Click **Save**.
14. In the *Select Schedules for Rule* dialog box, click to select the checkbox for the schedule to apply to the rule. If there is another schedule applied to the rule, you can deselect the checkbox to disable that schedule. If you select *No Time Restriction*, all other schedules are automatically deselected. Also, you cannot edit or copy the *No Time Restriction* schedule.
15. When you have finished configuring schedules, click **Save Changes**.
16. When you have finished configuring the rule, click **Save**.
17. (Optional) To quickly view the scheduled times, click to select the schedule, and then click the *View selected Rule Schedule* icon ( ). Click outside the calendar to close it.

Deleting a Schedule

1. Click the **Rules** tab.
2. Click to select the rule to delete.
3. Click the *Edit the selected Rule* icon ( ). The *Edit Mode* (right) panel is activated.
4. Click the *Edit the selected Schedule* icon ( ).
5. In the *Edit the Schedule* dialog box, click to select the schedule to delete.
6. Click the *Delete Schedule* icon ( ).
7. In the *Delete Schedule* confirmation dialog box, click **Delete Schedule**.
8. When you have finished configuring schedules, click **Save Changes**.
9. When you have finished configuring the rule, click **Save**.
10. (Optional) To quickly view the scheduled times, click to select the schedule, and then click the *View selected Rule Schedule* icon ( ). Click outside the calendar to close it.

Managing Responses

Set one or more responses to the events in the rule.

Adding a Response

To add a new response for a trigger:

1. Click the **Rules** tab.
2. Click to select the rule to edit.
3. Click the *Edit the selected Rule* icon ( ). The *Edit Mode* (right) panel is activated.
4. If necessary, click to select the appropriate trigger, and then click to select the appropriate schedule for which to add the response.
5. In the *Responses* panel, click the edit icon ( ) to the right of *then this will happen*. The *Edit the Responses triggered by Rule* dialog box opens.
6. Click the *Add a new Response* icon ( ).
7. Click to select an option from the *Response Category* drop-down menu.
8. Select or enter the appropriate options requested in the dialog box. These will vary depending on the *Response Category* chosen earlier.
9. (Optional) If you selected a response type that is not Custom Script, you can change it to a custom script. To do so, click **Convert to Custom Script**, and then click **Convert** in the confirmation dialog box. The name of the response is changed to *Custom Script*, and the code is displayed. In some cases, a response type *Notification - VX Internal* might not be converted to a Custom Script type.
10. When you have finished configuring responses, click **Save**.
11. When you have finished configuring the rule, click **Save**.

Duplicating an Existing Response

To use an existing response as a starting point to create a new response:

1. Click the **Rules** tab.
2. Click to select the rule to edit.
3. Click the *Edit the selected Rule* icon ( ). The *Edit Mode* (right) panel is activated.
4. In the *Responses* panel, click the edit icon ( ) to the right of *then this will happen*. The *Edit the Responses triggered by Rule* dialog box opens.
5. Click to select the response to duplicate.
6. Click the *Duplicate the selected Response* icon ( ).
7. With the duplicate highlighted, select the appropriate options requested in the dialog box. These will vary depending on the *Response Category* of the response you duplicated.
8. (Optional) If you selected a response type that is not Custom Script, you can change it to a custom script. To do so, click **Convert to Custom Script**, and then click **Convert** in the confirmation dialog box. The name of the response is changed to *Custom Script*, and the code is displayed. In some cases, a response type *Notification - VX Internal* might not be converted to a Custom Script type.
9. When you have finished configuring responses, click **Save**.
10. When you have finished configuring the rule, click **Save**.

Editing a Response

To edit an existing response:

1. Click the **Rules** tab.
2. Click to select the rule to edit.

3. Click the *Edit the selected Rule* icon ( ). The *Edit Mode* (right) panel is activated.
4. In the *Responses* panel, click the edit icon ( ) to the right of *then this will happen*. The *Edit the Responses triggered by Rule* dialog box opens.
5. Click to select the response to edit.
6. Select or enter the appropriate options requested in the dialog box. These will vary depending on the *Response Category* chosen earlier.
7. (Optional) If you selected a response type that is not Custom Script, you can change it to a custom script. To do so, click **Convert to Custom Script**, and then click **Convert** in the confirmation dialog box. The name of the response is changed to *Custom Script*, and the code is displayed. In some cases, a response type *Notification - VX Internal* might not be converted to a Custom Script type.
8. When you have finished configuring responses, click **Save**.
9. When you have finished configuring the rule, click **Save**.

Deleting a Response

To delete a response:

1. Click the **Rules** tab.
2. Click to select the rule to edit.
3. Click the *Edit the selected Rule* icon ( ). The *Edit Mode* (right) panel is activated.
4. In the *Responses* panel, click the edit icon ( ) to the right of *then this will happen*. The *Edit the Responses triggered by Rule* dialog box opens.
5. Click to select the response to delete.
6. Click the *Delete the selected Response* icon ( ).
7. In the confirmation dialog box, click **Delete**.
8. When you have finished configuring responses, click **Save**.
9. When you have finished configuring the rule, click **Save**.

Configuring an SMS Messaging Response

Administrators can configure a rule to send SMS notifications. To send SMS notifications, you must create a Twilio account for the system and then configure the notification in VxToolbox.

To configure the VideoXpert system to send SMS messages:

1. Log in to VxToolbox.
2. Click the **System** tab.
3. Click **SMS**.
4. Click to select the checkbox for *Enable SMS messaging via Twilio*.
5. Click **info**, follow the instructions in the *SMS Account Configuration* dialog box to set up a Twilio account, and then click **OK**.
6. Enter the values from the Twilio account in the *Phone Number to Send From*, *Twilio Account SID*, and *Twilio Auth Token* fields.
7. Click **Send Test Message**. If there is an error, check the values entered in the fields, and then try to send the test message again.
8. After the test message was successfully sent, click **Save Settings**.

To configure a rule to send an SMS message, follow the instructions in the sections titled *Creating a Rule* and *Adding a Response*. Use the response type **Notification - External**, select checkbox for *Send SMS*, and then add the appropriate information in each of the fields.

Configuring Recording

The *Recording* tab allows you to assign data sources (video and audio) to the recorder (VideoXpert Professional) or recorders (VideoXpert Enterprise) within the *VX System* you have selected.

You can assign devices to the recorder or recorders and create recording schedules through VxToolbox and VxStorage Portal; assigning data sources to a recorder without creating a schedule will prevent data sources from recording. You can perform advanced VxStorage configuration by connecting to the recorder using its IP address on port 9091.

Configuring a Recorder

1. Click the **Recording** tab.
2. At the top of the left panel, click **Recorders**.
3. Click to select the recorder to configure.
4. If available at the bottom of the left panel, click the *Edit selected recorder's configuration* icon ( ).

   Not every recorder has configurable settings. Update recorder configuration settings, depending on which are available for the recorder type.

   a. (Optional) To change the recorder name, enter a new value in the *Name* field.

   b. (Optional) To preserve recorder space, click to select the checkbox for, and then enter a number in the*Reduce framerate for video after [#] days* field, either by typing-in a number or selecting one using the up and down arrows
   When enabled, this option removes P-frames from all recordings older than the specified number of days, leaving only the I-frames. This cannot be set further back than the retention limit.

   c. (Optional) If available, under *Maximum Retention Limit*, click to select the checkbox for, and then enter a number in the *Discard video after [#] Days* field, either by typing-in a number or selecting one using the up and down arrows.

   d. If available, click to select the radio button for the *Transmission Method* field: *Multicast* or *Unicast*.

   e. If available, in the *Stream to Record* area, in the left-most field, select **Primary**, **Secondary**, or **Tertiary** from the drop-down menu; in the right-most field, select **None** or one of the other streams that are available from the drop-down menu.
   Specifically, if you selected Primary in the left-most field, Secondary and Tertiary will be available in the right-most field; if you selected Secondary, Primary and Tertiary will be available; if you selected Tertiary, Primary and Secondary will be available.

   f. (Optional) If available, for cameras that have local recordings, click to select the checkbox for *Auto-backfill recording gaps using on-camera storage*.
   When selected, if there is a gap in recording of a camera (an edge device), the recorder will query the camera for recordings, and automatically download video and audio (if present) to fill the gap.

   If you select this checkbox, you must also:

   - Type or select a number from the drop-down menu in the *Download data from up to [#] cameras at a time* field.
     Downloading from more cameras uses more bandwidth, which will slow the data transmission rate.

- Select a time-interval from the drop-down menu in the *Attempt to download every* field. If edge devices (cameras) and the recorder lose communication, the VX System will attempt to connect to the edge device again at the time-interval specified in this field.
- Type or select a value in the *Stop trying to download after [#] failed attempts* field.

g. (Optional) If available, click to expand **Advanced Options**, and then select the *Maximum Bitrate* from the drop-down menu.

h. Click **Save**.

Assigning Cameras to a Recorder

The recorders and cameras you see in the *Recording* tab are relevant to the *VX System* you have selected. VideoXpert Enterprise systems can have multiple recorders; VideoXpert Professional systems have only one.

You cannot assign cameras to every recorder. When assignment to a recorder is not available or allowed, the checkboxes in the steps below will be missing. Assignment to a recorder is not available or allowed for the following reasons:

- The user doesn't have permission to assign cameras to that recorder
- The recorder is a failover recorder
- The recorder is contained within a VxPro

To assign cameras to a recorder on a VideoXpert Enterprise System:

1. Click the **Recording** tab.
2. At the top of the left panel, click **Recorders**.
3. (Optional) Use filters to find the sources you want to add to the recorder.
4. Click to select the recorder to which you will add or remove data sources.
   The data sources already associated with the recorder are listed in the *Data Sources assigned to [recorder name]* column.
5. In the *All Data Sources* area of the right panel, click to select the checkboxes for the devices you want to add to the recorder; click to deselect the checkboxes for the devices you want to remove from the recorder.
   The update is immediately reflected in the *Data Sources assigned to [recorder name]* column.

Adding a Recording Group to a Recorder

1. Click the **Recording** tab.
2. At the top of the left panel, click **Schedules**.
3. In the *What to Record* (left) panel, click the *Create new Recording Group* icon (), or click to select a recording group similar to the one you will create, and then click the *Duplicate selected Recording Group* icon ().
4. Enter a value in the *Name of Recording Group* field of the *New Recording Group* or *Duplicate Recording Group* dialog box.
5. Click to select the radio button for *All Resources* or *Selected Resources*.
6. If you selected *Selected Resources*, in the *Add / Remove Cameras from Group* table, click to select the checkboxes for the sources to include in the recording group; click to deselect the checkboxes for the sources to exclude from the recording group.

(Optional) Use the filter to find the sources you want to add to the group. You can also sort on the *Name* and # columns in the *Add / Remove Cameras from Group* table.

7. Click **Save**.

Creating a Recording Schedule for a Recording Group

1. Click the **Recording** tab.
2. At the top of the left panel, click **Schedules**.
3. In the *What to Record* (left) panel, click to select the recording group for which create a recording schedule.
4. In the *When to Record* (center) panel, click the *Edit the Recording Schedules* icon ( ) to open the *Select Schedules for Recording Group* dialog box.
5. In the *Select Schedules for Recording Group* dialog box, click to select and deselect the checkboxes to build the schedule you want to apply to the recording group.
6. (Optional) To create and select a schedule that is not in the list:
   a. Click the *Add a new Schedule* icon ( ); or click the *Create a copy of the selected Schedule* icon ( ) to start with a schedule that is close to what you want.
   b. Enter a value in the *Display Name* field.
   c. Click to select the radio button for the appropriate increments of time (for example: *30 Minutes*).
   d. Click to select or deselect the checkbox for *24-Hour Time*. Deselecting the checkbox results in 12:00-11:59 AM and 12:00-11:59 PM recording timestamps.
   e. Indicate the times and days that the recording/rule is active by clicking to select boxes corresponding to a days and times. You can also click and drag to select a contiguous range of times and days. Click to deselect any days and times that you do not want the recording/rule to be active.

      Note: Schedules are shared between Recording Schedules and Rule Schedules. Any schedule that you create, modify, or delete in either location is reflected in both locations.

   f. (Optional) Click the checkbox to select or deselect *Within limited date range*. If you select *Within limited date range*, enter dates in the *Start on* and *End after* fields, either by selecting the dates from the calendars or by typing in a date using the mm/dd/yy format. Deselect the checkbox to make the schedule unlimited by date.
   g. Click **Add**.
   h. In the *Select Schedules for Recording Group* dialog box, click to select the checkbox for the schedule you just created.
   i. Click **Save Changes**.
7. (Optional) You can quickly view a recording schedule by selecting the schedule and then clicking the *View selected Recording Schedule* icon ( ) at the bottom left corner of the center panel. Click outside the calendar to close it.
8. Click to select one of the *Recording Schedules*.
9. In the *Recording Behaviors* (right) panel, click the *Create a new Recording Behavior* icon ( ).
10. Click to select the radio button for either *Continuous Recording* or *Event-Triggered Recording (Full Frame Rate)*.

11. If you selected *Continuous Recording*, click to select the radio button for either *Full Frame Rate* or *Reduced Frame Rate*.
12. If you selected *Event-Triggered Recording (Full Frame Rate)*:
    a. Select a value in the *Start recording* field, either by typing-in a number or selecting one using the up and down arrows.
    b. Click to select the event associated with the recording.
    c. In the *Stop recording* table, enter a value in the *seconds* field, either by typing-in a number or selecting one using the up and down arrows, and then click to select the radio button for *Event that triggers recording* or *Next opposite event*.
13. Click **Add & Create Another** or **Add**.
14. If you clicked **Add & Create Another**, repeat steps 9-13.
15. Repeat steps 7-14 for each recording schedule created.

Creating a Bump on Alarm Recording Schedule

A Bump on Alarm records continuous reduced frame rate (I-Frame only) video during normal situations, and records full frame rate video during an alarm or event. The video timeline for cameras set to record using a Bump on Alarm schedule shows a small green bar for continuous recording and a larger blue bar during event- or alarm-driven recording.

To configure a Bump on Alarm schedule:

1. Click the **Recording** tab.
2. At the top of the left panel, click **Schedules**.
3. In the *What to Record* (left) panel, click to select the recording group for which create a recording schedule.
4. In the *When to Record* (center) panel, click to highlight the schedule to which you will add the bump on alarm behavior.
5. Create a schedule for an alarm- or event-triggered recording:
    a. In the *Recording Behaviors* (right) panel, click the *Create a new Recording Behavior* icon ( ).
    The *Recording Mode and Trigger* will already be set to *Event-Triggered Recording (Full Frame Rate)*.
    b. Select a value in the *Start recording* field, either by typing-in a number or selecting one using the up and down arrows.
    c. Click to select the event associated with the recording.
    d. (Optional) If present, click to select or deselect the checkbox for *Record all cameras in the Recording Group*.
    e. In the *Stop recording* table, enter a value in the *seconds* field, either by typing-in a number or selecting one using the up and down arrows, and then click to select the radio button for *Event that triggers recording* or *Next opposite event*.
6. Click **Add & Create Another** or **Add**.
7. If you clicked **Add & Create Another**, repeat steps 5-6.
8. Repeat steps 3-7 for each recording schedule to create.

Editing a Recording Group

1. Click the **Recording** tab.
2. At the top of the left panel, click **Schedules**.
3. In the *What to Record* (left) panel, click to select the recording group to edit.
4. Click the *Edit selected Recording Group* icon ( ) to open the *Edit Recording Group* window.
   a. (Optional) Enter a new value in the *Name of Recording Group* field.
   b. Click to select the radio button for *All Resources* or *Selected Resources*.
   c. If you selected *Selected Resources*, in the *Add / Remove Cameras from Group* table, click to select the checkboxes for the sources to include in the recording group; click to deselect the checkboxes for the sources to exclude from the recording group.
   d. Click **Save**.

Editing a Recording Schedule

1. Click the **Recording** tab.
2. At the top of the left panel, click **Schedules**.
3. In the *What to Record* (left) panel, click to select the recording group for which to configure the schedule.
4. In the *When to Record* (center) panel, click to select the schedule to edit, and then click the *Edit the Recording Schedules* icon ( ).
5. In the *Select Schedules for Recording Group* dialog box, click to select and deselect the checkboxes for schedules to associate with the recording group.
6. Click **Save Changes**.
7. If you removed a schedule, the *Remove Schedule from Recording Group* dialog box opens. Click **Delete**.
8. (Optional) To create and select a schedule that is not in the list:
   a. In the *When to Record* (center) panel, click the *Edit the Recording Schedule* icon ( ).
   b. Click the *Add a new Schedule* icon (+); or click the *Create a copy of the selected Schedule* icon ( ) to start with a schedule that is close to what you want.
   c. Enter a value in the *Display Name* field.
   d. Click to select the radio button for the appropriate increments of time (for example: *30 Minutes*).
   e. Click to select or deselect the checkbox for *24-Hour Time*. Deselecting the checkbox results in 12:00-11:59 AM and 12:00-11:59 PM recording timestamps.
   f. Indicate the times and days that the recording/rule is active by clicking to select boxes corresponding to a days and times. You can also click and drag to select a contiguous range of times and days. Click to deselect any days and times that you do not want the recording/rule to be active.

      Note: Schedules are shared between Recording Schedules and Rule Schedules. Any schedule that you create, modify, or delete in either location is reflected in both locations.

   g. (Optional) Click the checkbox to select or deselect *Within limited date range*. If you select *Within limited date range*, enter dates in the *Start on* and *End after* fields, either by selecting

the dates from the calendars or by typing in a date using the mm/dd/yy format. Deselect the checkbox to make the schedule unlimited by date.

h. Click **Add**.

i. In the *Select Schedules for Recording Group* dialog box, click to select the checkbox for the schedule you just created.

j. Click **Save Changes**.

9. (Optional) To quickly view the scheduled times, click to select the schedule, and then click the *View selected Rule Schedule* icon ( ). Click outside the calendar to close it.
10. In the *Recording Behaviors* (right) panel, click to select an existing trigger.
11. Click the *Edit Selected Recording Behavior* icon ( ).
12. In the *Edit Recording Behavior for Recording Group [group name]* dialog box, click to select the radio button for the *Recording Mode and Triggers*: *Continuous Recording* or *Event-Triggered Recording (Full Frame Rate)*.
13. If you selected *Continuous Recording*, click to select the radio button for either *Full Frame Rate* or *Reduced Frame Rate*.
14. If you selected *Event-Triggered Recording (Full Frame Rate)*:

    a. Select a value in the *Start recording* field, either by typing-in a number or selecting one using the up and down arrows.

    b. Click to select the event associated with the recording.

    c. (Optional) If present, click to select or deselect the checkbox for *Record all cameras in the Recording Group*.

    d. In the *Stop recording* table, enter a value in the *seconds* field, either by typing-in a number or selecting one using the up and down arrows, and then click to select the radio button for *Event that triggers recording* or *Next opposite event*.

15. Click **Save & Create Another**, or click **Save**.

Deleting a Recording Group

Deleting a Recording Group will also delete the associated Recording Schedules and Recording Behaviors.

1. Click the **Recording** tab.
2. At the top of the left panel, click **Schedules**.
3. In the *What to Record* (left) panel, click to select the recording group to delete.
4. Click the *Delete selected Recording Group* icon ( ).
5. In the *Delete [recording group name]* dialog box, click **OK**.

Deleting a Recording Schedule

This will delete the selected *Recording Schedule*, and the associated *Recording Behaviors*.

1. Click the **Recording** tab.
2. At the top of the left panel, click **Schedules**.
3. In the *What to Record* (left) panel, click to select the recording group for which to delete the schedule.

4. In the *When to Record* (center) panel, click to select the schedule to delete.
5. At the bottom of the *When to Record* (center) panel, click the *Remove selected Recording Schedule* icon ( ).
6. In the *Remove Schedule from Recording Group* dialog box, click **Delete**.

Deleting a Recording Behavior (Trigger)

If you delete all *Recording Behaviors* for a *Recording Schedule*, the *Recording Schedule* is also deleted.

1. Click the **Recording** tab.
2. At the top of the left panel, click **Schedules**.
3. In the *What to Record* (left) panel, click to select the recording group for which to delete the trigger.
4. In the *When to Record* (center) panel, click to select the recording schedule for which to delete the trigger.
5. In the *Recording Behaviors* (right) panel, click to select the *Trigger* to delete.
6. At the bottom of the *Recording Behaviors* (right) panel, click the *Delete selected Recording Behavior* icon ( ).
7. In the *Delete [behavior name]* dialog box, click **OK**.

Managing Users and Roles

A role is a group of permissions defining abilities and responsibilities within a system. A user must be assigned at least one role to perform actions within the system.

If you are authenticating using LDAP, you are not required to manage users and roles, but you can in order to control settings that are not specified in LDAP.

Understanding Internal and Restricted User Accounts

VideoXpert contains some hard-coded user accounts that are integral to the system. You cannot edit, disable, or delete these accounts, nor can you change roles or permissions for these users. You can, however, change the password for these accounts in the case of the admin and aggregator accounts, it is recommended that you change the password from the default.

User	Description
admin	This is the basic administrative user for VideoXpert. This user account possesses the “administrator” role, so is granted all available permissions within the system.
internal	This role is used internally within the system to perform server-side tasks. It is not visible in the *Users* page, under the *Users* tab.
rule_engine	This role supports the rules engine.
snmp	This role is used to collect diagnostic information for the SNMP service that is available on the product.

Creating a Role

There are four default roles within VideoXpert:

- **Administrator** has full rights to the system.
- **Manager** has all Supervisor rights and the ability to configure recorders and devices within the system, including tags, recorder assignment, etc. Managers can also assign roles to users. (This role is available on VxPro Systems only.)
- **Supervisor** has advanced access to live and recorded video including investigations, PTZ control, and plug-ins. Supervisors can use plug-ins, configure events, and access workspaces configured by other users. (This role is available on VxPro Systems only.)
- **User** has basic rights to view live and recorded video. (This role is available on VxPro Systems only.)

Custom roles can also be created and assigned. To create a custom role:

1. Click the **Users** tab, and then click **Roles & Permissions** at the top left of the window.
2. Click the *Add a new role* icon (+).
3. In the *Create a new Role on the VX system* dialog box, enter a value in the *Role Name* field.
4. (Optional) Add one or more permissions individually for the role:
   a. In the *Enabled Permissions* section of the window, click **Add a Permissions Category**.
   b. Click to select a permissions category from the available categories.

c. Click to select the radio button to *Allow ALL [Category] Permissions* or *Allow Selected [category] Permissions*.

d. If you selected *Allow Selected [Category] Permissions*, click **Add a Permission**; click to select a permission from the drop-down list (including **Select All [Category] Permissions**); if a confirmation dialog box opens, click **OK**.

e. (Optional) To delete a permission from the category, click the *Delete* icon ( ) corresponding to the permission to delete.

f. (Optional) Click **Add Another Permission**, and repeat the process.

5. (Optional) Add all available permissions to the role:

Note: This is available only if you have not already added all available permissions to the role.

a. In the *Enabled Permissions* section of the window, click **Add a Permissions Category**.

b. Click to select **Add All Categories**.

c. Click to expand one of the categories, and then click the radio button to *Allow ALL [Category] Permissions* or *Allow Selected [Category] Permissions*.

d. If you selected *Allow Selected [Category] Permissions*, click **Add Another Permission**; click to select the permission (including **Select All [category] Permissions**).

e. (Optional) In the permissions table that is displayed beneath *Allow Selected [Category] Permissions* click the *Select Resource* icon ( ) to change the resource restrictions for the permission. In the *Manage Resource Restriction for* window, select **Match Parent Resources** (if present); **Allow All Resources**; **Allow Selected Resources**, and then select the resources to allow; or **Allow All Resources Except Selected**, and then select the resources to disallow.

The table provides the list of permission, resources allowed for each permission, and the number of devices that are allowed.

f. (Optional) To delete a permission from the category, click the *Delete* icon ( ).

g. (Optional) Repeat steps c through f for each of the categories.

6. To delete a category from the *Enabled Permissions* area, click the *Delete* icon ( ) in the category title.

7. Click **Save**.

Editing a Role

Renaming a role does not affect the users to whom the role is assigned.

1. Click the **Users** tab, and then click **Roles & Permissions** at the top left of the window.
2. Click to select the role to edit.
3. Click the *Edit the selected Role* icon ( ).
4. In the *Edit the Role* dialog box, change the role name and/or permissions as needed.
5. For detailed instructions, see the section titled *Creating a Role*.
6. Click **Save**.

Duplicating a Role

By default, a duplicate role retains the permissions of the original role. You can edit the permissions.

1. Click the **Users** tab, and then click **Roles & Permissions** at the top left of the window.
2. Click to select the role to duplicate.
3. Click the *Create a copy of the selected Role* icon ( ).
4. Enter a name for the duplicated role and edit the permissions as needed.
5. For detailed instructions, see the section titled *Creating a Role*.
6. Click **Save**.

Deleting a Role

1. Click the **Users** tab, and then click **Roles & Permissions** at the top left of the window.
2. Click to select the role to delete.
3. Click the *Delete Role* icon ( ).
4. In the confirmation dialog box, click **Delete**.

Viewing Details of a Role

To quickly view the permissions assigned to a specific role:

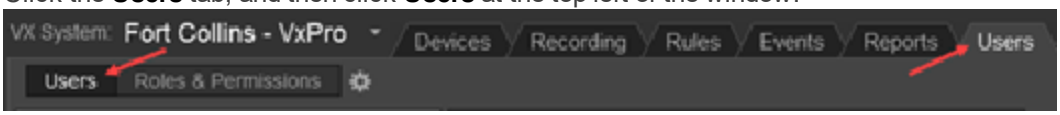
1. Click the **Users** tab, and then click **Roles & Permissions** at the top left of the window.
2. In the right panel, click to select the role to view.
3. In the *Permissions of Role: [Role]* (right) panel, view the permissions for each category.
   The information in the *Permission of Role: [Role]* panel is the same information displayed in the permission tables when you created or edited a role.
4. (Optional) To see the users who are assigned to the role, click the expand icon ( ) to the left of the role to display the list of users. To view the user's information in the *Users* page, hover over the user's name, and then click the change view icon ( ) to the right of the name.

Adding Users

When adding users to the system, you give them a temporary password.

You can also provide additional user information, to make it easier to associate user names with personnel; *Name* fields appear anywhere the system provides a user name.

1. Click the **Users** tab, and then click **Users** at the top left of the window.



2. Click the *Create a new User* icon ( ).
3. Enter a value in the *Username* field.
4. (Optional) Enter values in the *First Name* and *Last Name* fields.

5. If the *Password* field is enabled:
   a. Enter a value in the *Password* and *Confirm Password* fields.
   b. (Optional) To require a user to change the password the first time the user logs in, click to select the checkbox for *Must change password on first login with new password*.

   Note: The password can only be set if the system or the specific user is using VideoXpert authentication. To change the authentication method from Authenticate using LDAP/AD to Authenticate using VideoXpert, see the section titled *Setting the User Password Expiration Policy*

6. Choose a *Role* for the user from the drop-down menu.
7. (Optional) Click **Add another role**, and then choose a role for the user from the drop-down menu.
8. (Optional) To delete a role, click the *Remove this role from the selected user* icon ( ). This option is only available if more than one role is assigned to the user.
9. (Optional) Enter a value in the *User ID#*, Email Address, *Phone*, and *Notes* fields.
10. (Optional) Click to expand **Advanced Settings**.
    - Click to select or deselect the checkbox for *Allow this user to be used for Aggregation*.
    - Click to select or deselect the checkbox for *This user's password never expires*. This overrides the global user setting for password expiration.
11. Click **Add**.

Editing Users

To edit a user:

1. Click the **Users** tab, and then click **Users** at the top left of the window.
2. Click the *Edit the selected User* icon ( ).
3. (Optional) Enter new values in the *First Name* and *Last Name* fields.
4. (Optional) Click to select the radio button for *Active* or *Inactive*.
5. Update other settings as needed. For detailed instructions, see the section titled *Adding Users*.
6. Click **Save**.

Searching for Users

1. Click the **Users** tab, and then click **Users** at the top left of the window.
2. Enter a value in the *Search Users* field.

   The search applies to user name, first name, and last name values.

   The search begins as soon as you enter the first character; results are further refined as you enter more characters.
3. Add or delete characters to change the search results.
4. (Optional) To clear the search field, either delete all characters or click the *Clear* icon ( ) at the right of the *Search Users* field.

Assigning Roles

VideoXpert contains pre-defined roles that you can assign to users. You cannot change these roles but you can create new roles (see *Creating a Role*); each user must be assigned a role to use VideoXpert. Any locking features or competing actions performed by users are prioritized by user level.

To assign roles to an existing user:

1. Click the **Users** tab, and then click **Users** at the top left of the window.
2. Click to select the user to whom you are assigning a role, and then click the *Edit the selected User* icon ( ).
3. Click to select a *Role* from the drop-down menu.
4. (Optional) To add another role to the user, click **Add another role**, and then select a *Role* from the drop-down menu.
5. (Optional) If appropriate, edit additional user information from this dialog box. See sections titled *Editing a Role* and *Resetting Passwords*.
6. Click **Save**.

Resetting Passwords

Users with appropriate permissions can either reset users' passwords or force users to change their passwords.

Resetting a user's password will allow you to grant the user a temporary password. You may want to reset a user's password if a user does not remember his or her password, or the user is locked out of the system because of failed login attempts or because of letting the password change timer lapse.

Users with appropriate permissions can also reset other users' passwords and force users to change their passwords.

1. Click the **Users** tab, and then click **Users** at the top left of the window.
2. Select the user whose password you want to reset, and then click the *Edit the selected User* icon ( ).
3. Click **Change Password**
4. Enter a new value in the *New Password* and *Re-Enter New Password* fields.

   If you decide not to change the password, you must click **Do Not Change Password** in order to continue.
5. (Optional) If appropriate, edit additional user information from this dialog box. See sections titled *Editing a Role* and *Assigning Roles*.
6. Click **Save**.

Setting the User Password Expiration Policy

For users who are not using *Authenticate using LDAP/AD* single sign-on (SSO), you can set passwords to expire at specific intervals, or to never expire.

To set the global (all users) expiration policy:

1. Click the **Users** tab, and then click the *Global User Settings* icon ( ) above the left panel, to the right of the page tabs.
2. In the *Global User Settings* dialog box, click to select the radio button for *Passwords never expire* or *Passwords expire every [#] days*.

3. If you selected *Passwords expire every [#] days*, enter a value for the number of days, either by typing-in a number or selecting one using the up and down arrows.
4. Click **Done**.

For users who are using *Authenticate using LDAP/AD*, the password expiration does not apply. You can change the authentication method for a user from LDAP/AD to VideoXpert Authentication, so that you can set a password expiration policy for a specific user.

1. Click the **Users** tab, and then click **Users** at the top left of the window.
2. Click to select the user whose authentication method you will change.
3. Click the *Edit* icon ( ) at the bottom right of the left panel.
4. If the User was configured for *Authenticate using LDAP/AD* when the User was created, you must now provide password information for the User.
   a. Enter a value in the *Password* and *Confirm Password* fields.
   b. Click to select or deselect the checkbox for *Must change password on first login with new password*.
   c. Click to expand **Advanced Settings**.
   d. Click to select or deselect the checkbox for *The user's password never expires*.
5. Click **Save**.

Deleting Users

1. Click the **Users** tab, and then click **Users** at the top left of the window.
2. Click to select the user you want to remove.
3. Click the *Delete User* icon ( ).
4. In the confirmation dialog box, click **Delete**.

Configuring VideoXpert System™ Settings

From VxToolbox, you can configure most settings on the VX System to which you are connected. Setting types include General Settings, Aggregation, LDAP, Backup, and SMTP settings. These are described in the following sections.

The VX System settings also includes SMS settings, described in the section titled *Configuring an SMS Messaging Response*.

Aggregating Systems (on VideoXpert Enterprise™ Systems Only)

VideoXpert Enterprise systems support an aggregation server, providing centralized access to a series of member systems and cameras.

When you add a system to the VideoXpert Enterprise aggregation server, the video for the member system becomes available at the aggregation level. However, you may not be able to change settings for the member system and some components from the aggregation level; you might have to access the member system directly to change the settings.

As a prerequisite to adding an aggregated system to VxToolbox, the aggregation server must be configured. See the current *VideoXpert Enterprise™ Installation and Configuration Guide*.

1. Click the **System** tab.
2. Click **Aggregation**.
3. (Optional) To add or edit a system:
   a. Click **Add System**, or click the *Edit this aggregated member system* icon ( ) at the right of the appropriate server address row to edit an existing system.
   b. In the *Server Address* field, provide the IP address of the system you want to aggregate. If aggregating a clustered system, enter the IP address of the load balancer governing the cluster of systems you want to aggregate.
   c. In the *Port* field, enter the port number the system uses for HTTP/HTTPS communications.
   d. (Optional) In the *Streaming Configuration / Connection Type* area, click to select the checkbox for *Allow RTSP/RTP*. You can then click the checkbox to select *Allow UDP*. Further, you can click the checkbox to select *Allow Mutlicast*.
   If users begin to experience trouble streaming multiple cameras, deselect the checkbox for *Allow UDP* to try to resolve the issue.
   e. In the *Bandwidth* field, provide the connection speed between the aggregation server and the VideoXpert system you are aggregating. The higher the connection speed, the better aggregated devices will perform within VideoXpert. Selecting speeds lower than 100 Mbps will cause all cameras for the aggregated system to return MJPEG video.

      Note: The Media Gateway™ transcodes MJPEG video, and returns the full I-Frame rate requested by the camera. Cameras configured to deliver more than 2 I-frames per second will stress the performance of the Media Gateway and consume more bandwidth. It is recommended that cameras expected to return MJPEG video are configured to deliver no more than 2 I-frames per second to prevent cameras from taxing the Media Gateway.

   f. Enter a value in the *Aggregation Username* field.
   g. Enter a value in the *Password* field.

h. Click **Test Connection**. If the connection test fails, correct the information, and then click **Test Connection** again.

i. When the connection test passes, click **Add System** or **Save**.

4. To refresh an aggregated member system so that the aggregating and member systems are synchronized, click the *Refresh this aggregated member system.* icon ( ) at the right of the appropriate server address row.
5. To delete a system from aggregation, click the *Remove this member system.* icon ( ) at the right of the appropriate server address row.

Configuring General Settings for VideoXpert Enterprise™ Systems

1. Click the **System** tab.
2. Click **General Settings**.
3. Enter a value in the *VideoXpert System Name* field.
4. (Optional) Configure clusters:

   Note: Not all systems will have clusters. See *Working with Clusters* for more information.

   a. In the *Cluster Configuration* area, click to select or deselect the checkbox for *Multiple VideoXpert Cores*. This is selectable if there is only one VideoXpert Core™; otherwise, the checkbox is selected and cannot be deselected unless all but one VideoXpert Core is removed.

   b. Enter a value in the *VideoXpert Core Virtual IP Address* field.

   Caution: If you are using SSO, this value must be the FQN, and not the IP address.

   c. Enter a value in the *VideoXpert Core Address* field.

   d. If you selected *Multiple VideoXpert Cores* (or if it is automatically selected), click **Add Another VideoXpert Core**, and then enter another value in the new *VideoXpert Core Address* field. Do this as many times as is needed.

   e. Enter a value in the *VxMediaGatewayAddress* field.

   f. Click to select or deselect the checkbox for *Multiple VxMediaGateways*.

   g. If you selected *Multiple VxMediaGateways*, enter a value (associated with the initial VxMediaGateway Virtual IP Address), enter a value for another gateway in the new *VxMediaGateway Address* field. To add more VxMedia Gateways, click **Add Another VxMediaGateway**, and then enter a value for another gateway in the new *VxMediaGateway Address* field.

   h. Click to select the radio button for one of the following:

   - *Use VX load balancing*—The main Core is active, and up to two additional Cores are in standby mode. If the active Core fails, all traffic is redirected to another Core.
   - *Use external load balancer*—Select this option for a system with any number of cores.

   i. If you are configuring a VxDatabase that is installed separately from a VideoXpert Core:

      i. Click to expand **Advanced Database Configuration**.

      ii. Enter a value in the *VxDatabase Address* field.

      iii. Click **Add Another VxDatabase**.

iv. Enter a value in the new *VxDatabase Address* field.

v. To add another VxDatabase, repeat the previous steps.

5. Complete the System Configuration information:

   a. (Optional) Specify a *Transmission Method* by clicking to select the appropriate radio button(s) for the *Allow Multicast Communication to Camera*, *Allow Multicast Communication to Client*, and/or *Enable stream proxying through recorder*.

   Note: By default, VideoXpert is configured to stream using unicast communication mode. If users cannot access streams when they are being viewed by other users, consider selecting multicast communication mode. In addition to selecting multicast communication mode in VxToolbox, you must properly configure the system for multicast support.

   b. Click to select or deselect the checkbox for *Store exports in an alternate location*. If you select the checkbox, enter values in the *Network Storage Location*, *Username (if required)* and *Password (if required)* fields; click **Test Connection**; and then click **OK**.

   c. (Optional) Click to select or deselect the checkbox for *Prefer Hostnames*. When the feature is selected, the server will try to resolve the IP addresses into hostnames.

6. (Optional) In the *Exports* area:

   a. Click to select the checkbox for *Force encryption on all exports*.

   b. (Optional) Click to select the checkbox for *Use preset password for all encrypted exports*.

   c. If you will use a preset password, type a value in the field. Click the checkbox to select *Show* to see the password entered.

   When forced encryption is selected, all exports to the standard locations are encrypted by default and automatically use the same password. This does not apply to exports to alternate locations.

7. (Optional) In the *Bookmarks* area:

   a. Under *Automatically Delete Bookmarks*, click to select the radio button for *Never* or *After [###] days*. If you select *After [###] days*, select the number of days, either by typing-in a number or selecting one using the up and down arrows.

   b. Under *Automatically Unlock Clips*, click to select the radio button for *Never* or *After [###] days*. If you select *After [###] days*, select the number of days, either by typing-in a number or selecting one using the up and down arrows.

8. (Optional) In the *HTTPS Certificate* area:

   a. Click **Show current certificate details** to view information including *Issued to*, *Issued by*, and *Period of Validity*. To close this field, click **Hide current certification details**.

   b. (Optional) If present, click **Export current certificate to .pfx** to open the *Authenticate Certificate* dialog box, enter a *Password* in the field, and then click **OK**.

   c. (Optional) If present, click **Install New Certificate** to open the *Select SSL/TLS Certificate* dialog box, navigate to and select the certificate, and then click **Open**.

9. (Optional) To cancel any changes you have made before saving the settings, click **Revert** at the bottom of the panel.

10. Click **Save Settings**.

Working with Clusters

A clustered environment requires at least two VideoXpert Core, Media Gateway, or CMG servers.

- Cores and Media Gateways must be on the same VLAN. They must also have static IP addresses, and these IP addresses must be different from each other.
- Traffic will be managed by a single Core; if that Core fails, another Core will perform the management tasks. Other tasks, such as export processing, are shared among all Cores.
- A single Media Gateway will receive streaming requests, but will redirect streaming to other Media Gateways to balance the load.
- The Media Gateway trans-casts to suit the network topology and needs. While the system is configured to get multicast streams from sources and to issue multicast streams to clients, you can select the appropriate communication method both from sources to the Media Gateway and from the Media Gateway to clients. The network topology and need for users to access sources simultaneously will inform your choice.

For more information about clustering an environment, see the current version of the *VideoXpert™ System Design Guide*.

Configuring Authentication

You can select the authentication method and parameters used.

- VideoXpert Authentication—see the section titled *Enabling VideoXpert Authentication™*
- LDAP authentication using simple bind authentication—see the section titled *Configuring LDAP Authentication: Simple Bind*.
- LDAP authentication using two-stage binding—see the section titled and *Configuring LDAP Authentication: Two-Stage Bind Authentication*.
- If you select LDAP authentication, you can also (optional) use synchronize users and roles from LDAP—see the section titled and *Configuring LDAP Authentication: Synchronizing Users and Roles From LDAP*.
- If you select LDAP authentication, you can also (optional) use Single Sign-On—see the section titled *Configuring LDAP Authentication: Using Single Sign-On*.

Enabling VideoXpert Authentication™

VideoXpert Authentication uses the internal VX system authentication instead of LDAP.

1. Click the **System** tab.
2. Click **LDAP/AD**
3. Click to select the radio button for *VideoXpert Authentication*.
4. Click **Save Settings**.

Configuring LDAP Authentication: Simple Bind

LDAP authentication using simple bind authentication requires only the LDAP server name, port, Base DN, and search attributes.

1. Click the **System** tab, and then click **LDAP/AD**.
2. Click to select the radio button for *LDAP*.
3. If necessary, click to deselect the radio buttons for *Two-Stage Binding Authentication* and the checkbox for *Synchronize users and Roles From LDAP*.
4. Enter the host name or IP address of the LDAP server in the *LDAP Server* box.

5. (Optional) Click the *SSL/TLS* box if your LDAP server requires SSL/TLS authentication.
6. (Optional) Edit the server *Port* if the LDAP server is not on the default port (389, or 636 if you selected SSL/TLS).
7. Type a distinguished name (DN) in the *Base DN* box.
8. Type an attribute key name in the *Search Attributes* box. When inputting multiple entries in a box, separate entries with commas only (no spaces).
9. Click *Test Connection* to verify that your LDAP connection and search settings are correct.
10. Click **Save Settings**.

Here is an example of a simple bind request.

- In the *Base DN* box, the administrator has entered "CN=Users,DC=example,DC=com".
- In the *Search Attributes* box, the administrator has entered "CN".
- The user has signed on using "Joe" as the login name and "Pword" as the password.
- VideoXpert sends to LDAP a bind request with the specified parameters.

This is different from what happens in a two-stage bind. See *Configuring LDAP Authentication: Two-Stage Bind Authentication*.

Configuring LDAP Authentication: Two-Stage Bind Authentication

Two-stage bind authentication uses the parameters of simple bind, but adds a superuser distinguished name and password.

1. Click the **System** tab, and then click **LDAP/AD**.
2. Click to select the radio button for *LDAP*.
3. Click to select the radio button for *Two-Stage*
4. Enter the host name or IP address of the LDAP server in the *LDAP Server* box.
5. (Optional) Click the *SSL/TLS* box if your LDAP server requires SSL/TLS authentication.
6. (Optional) Edit the server *Port* if the LDAP server is not on the default port (389, or 636 if you selected SSL/TLS).
7. Type a distinguished name (DN) in the *Base DN* box.
8. Type an attribute key name in the *Search Attributes* box. When inputting multiple entries in a box, separate entries with commas only (no spaces).
9. Type a value in the *Superuser DN* field.
10. Type a value in the *Superuser DN Password* field.
11. Click *Test Connection* to verify that your LDAP connection and search settings are correct.
12. Click **Save Settings**.

Here is an example of a two-stage bind request.

- In the *Base DN* box, the administrator has entered "CN=Users,DC=example,DC=com".
- In the *Search Attributes* box, the administrator has entered "sAMAccountName,CN".
- The user has signed on using "Joe" as the login name and "Pword" as the password.
- VideoXpert first searches for an LDAP entry that has either sAMAccountName or CN set to "Joe".
- After finding the entry, VideoXpert sends to LDAP a bind request with the DN set to the DN of the entry that it found during the search, and that has the password set to "Pword".

Configuring LDAP Authentication: Synchronizing Users and Roles From LDAP

Synchronizing Users and Roles From LDAP uses the parameters of two-stage binding, but adds a root VX DN and a VX system DN. These enable your system to use the LDAP server to synchronize User and Role assignments.

To synchronize users and roles from an LDAP server, you must first configure users and roles on that server. For example, if you are using an Active Directory LDAP server:

1. Access the *Active Directory Users and Computers* window.
2. Create a folder structure that is appropriate to the planned permissions structure (for example: to mirror the geographic locations of systems).
3. Within that folder structure, create groups with names that match the names of roles in VideoXpert.
4. Add users or other groups to these groups.
5. Save the settings and close Active Directory.

To configure LDAP authentication in VxToolbox to synchronize users and roles from LDAP:

1. Click the **System** tab, and then click **LDAP/AD**.
2. Click to select the radio button for *LDAP*.
3. Click to select the radio button for *Two-Stage*.
4. Click to select the radio button for *Synchronize Users and Roles From LDAP*.
5. Enter the host name or IP address of the LDAP server in the *LDAP Server* box.
6. (Optional) Click the *SSL/TLS* box if your LDAP server requires SSL/TLS authentication.
7. (Optional) Edit the server *Port* if the LDAP server is not on the default port (389, or 636 if you selected SSL/TLS).
8. Type a distinguished name (DN) in the *Base DN* box.
9. Type an attribute key name in the *Search Attributes* box. When inputting multiple entries in a box, separate entries with commas only (no spaces).
10. Type a value in the *Superuser DN* field.
11. Type a value in the *Superuser DN Password* field.
12. (Optional) Type a value in the *Root VideoXpert DN* field.
    - If you are setting up only one VX System, you can leave this field blank.
    - If you are setting up multiple systems, this is the LDAP container under which all of the VX System information is stored for all of the systems. When determining which roles should be assigned to a user, the VX System will look for group entries within the VideoXpert System DN sub-container, and navigate up the LDAP tree until it reaches the Root VideoXpert DN container.
13. Type a value in the *VideoXpert System DN* field.

    This is the LDAP container for the VideoXpert System. It can be nested inside sub-containers in any configuration. When determining which roles should be assigned to a user, the VX System will look for group entries within the VideoXpert System DN sub-container and navigate up the LDAP tree until it reaches the Root VideoXpert DN container.
14. Click *Test Connection* to verify that your LDAP connection and search settings are correct.
15. Click **Save Settings**.

Note: Permissions for each role must still be configured in the *Roles and Permissions* tab of VxToolbox.

Here is an example of configuring LDAP authentication in VxToolbox to synchronize users and roles from LDAP.

The following users exist in your Active Directory system:

- Joe Jones (username=joe)
- Mary Smith (username=mary)—belongs to the AD group “Directors – West Region”

You have these four systems:

- Log Angeles
- San Francisco
- New York
- Boston

You want to ensure that:

- All Directors for the West Region can log in to systems in the West Region, with permission to view live and recorded video for all cameras
- Joe Jones can log in to the New York system ONLY, and add devices and users to that system

You create the following roles with the following permissions on their VX systems, using VxToolbox:

- Directors: “View Video Sources” and “View Recorded Video”
- SysAdmins: “Manage User Acocunts” and “Manage Cameras & Recorders”

You decide to store information about all of your VideoXpert systems under the following Root DN in AD:

- OU=VideoXpert,DC=example,DC=com

Under the root DN in AD,you create the following container entities:

- OU=New York,OU=East Region,OU=VideoXpert,DC=example,DC=com
- OU=Boston,OU=East Region,OU=VideoXpert,DC=example,DC=com
- OU=Los Angeles,OU=West Region,OU=VideoXpert,DC=example,DC=com
- OU=San Francisco,OU=West Region,OU=VideoXpert,DC=example,DC=com

Next, you create the following group entities:

- CN=Directors,OU=West Region,OU=VideoXpert,DC=example,DC=com
  - You add the existing AD group “Directors – West Region” to this group.
- CN=SysAdmins, OU=New York,OU=East Region,OU=VideoXpert,DC=example,DC=com
  - You add user “Joe Jones” to this group.

Finally, in VxToolbox, you:

- Enable “LDAP users and roles” on all 4 VX systems.
- Set the root DN to OU=VideoXpert,DC=example,DC=com on all 4 VX systems.
- Set the system DN to:
  - OU=New York, etc. on the New York system
  - OU=Boston, etc. on the Boston system
  - OU=Los Angeles, etc. on the Los Angeles system
  - OU=San Franscisco, etc. on the San Francisco system

With this configuration:

- Mary Smith can log in to both the Log Angeles and San Francisco systems, using “mary” as her username and her AD password as the password. When Mary logs in:
  - The VX system creates a user account with name “mary” in VX (if it doesn’t already exist).
  - The VX system adds user mary to the Directors role.
- Joe Jones can log in to the New York system only. When Joe logs in:
  - The VX system creates a user account with name “joe” in VX (if it doesn’t already exist).
  - The VX system adds user joe to the SysAdmins role.

Configuring LDAP Authentication: Using Single Sign-On

Single Sign-On (SSO) allows users to log in to multiple systems using a single set of login credentials. SSO can be used with either Single-Stage or Two-Stage binding, and can be used with the Synchronize Users and Roles From LDAP option.

Note: If VxOpsCenter is running on the same server as the VxPro or Core system, SSO will not be available. This is due to MS Windows limitations.

To configure authentication to use SSO:

1. Ensure that you have created a DNS entry for the cluster virtual IP address on the SSO domain. Include the Forward Lookup Zone and Reverse Lookup Zone entries. (Instructions for this operation are beyond the scope of this document.)
2. Click the **System** tab, and then click **LDAP/AD**.
3. Click to select the radio button for *LDAP*.
4. Click to select the radio button for *Two-Stage* and the checkbox for *Synchronize users and Roles From LDAP*.
5. Click to select the checkbox for *Use Single Sign-On*.
6. Enter the host name or FQN of the LDAP server in the *LDAP Server* box.
   - If the host name (IP address) is used, this points to a single Active Directory Domain Controller (DS). This creates a single point of failure; if the DC goes offline, authentication will break.
   - If the FQDN is used, any DC in the AD will respond to the authentication request. This provides fault tolerance for LDAP authentication.
7. (Optional) Edit the server *Port* if the LDAP server is not on the default port (636—SSL/TLS is required for SSO).
8. Type a distinguished name (DN) in the *Base DN* box.
9. Type an attribute key name in the *Search Attributes* box. When inputting multiple entries in a box, separate entries with commas only (no spaces).
10. Type a value in the *Superuser DN* field.
11. Type a value in the *Superuser DN Password* field.
12. (Optional) Type a value in the *Root VideoXpert DN* field.
    - If you are setting up only one VX System, you can leave this field blank.
    - If you are setting up multiple systems, this is the LDAP container under which all of the VX System information is stored for all of the systems. When determining which roles should be assigned to a user, the VX System will look for group entries within the VideoXpert System DN

sub-container, and navigate up the LDAP tree until it reaches the Root VideoXpert DN container.

13. Type a value in the *VideoXpert System DN* field.

    This is the LDAP container for the VideoXpert System. It can be nested inside sub-containers in any configuration. When determining which roles should be assigned to a user, the VX System will look for group entries within the VideoXpert System DN sub-container and navigate up the LDAP tree until it reaches the Root VideoXpert DN container.

14. Type a value in the *Active Directory Domain* field.
    This step does not test the SSO login; that was tested in an earlier step.
15. Click *Test Connection* to verify that your LDAP connection and search settings are correct.
16. Click **Save Settings**.

Note: Permissions for each role must still be configured in the *Roles and Permissions* tab of VxToolbox.

Note: If SSO is supported, VxPortal™ defaults to using it.

Note: If the VxPro or Core server is not part of the AD, or if you are using a core cluster, a service account will be created in your AD for the server. If the service account is not created, the value entered in the *LDAP Server* box (step 6) will be ignored.

For further assistance, contact Pelco Customer Support.

Configuring System Backups

Pelco recommends that you back up your system after initial setup, when you have configured a significant number of users and devices, and after significant changes to your system configuration.

A system backup contains the system database, including the previous 30 days' events. Backups do not capture exported video or any settings that you might have changed outside of VxToolbox (for example: changes made directly to configuration scripts). The speed of each backup depends on the size of the VideoXpert database, network bandwidth, and other variables.

To configure system backups:

1. Click **System**, and then click **Backup**.
2. In the *Location* area:
   a. Enter a value in the *Specify a Path* field.
   b. (Optional) Enter values in the *Username* and *Password* fields.
   c. Click **Test Connection**.
      - If the *Test Successful!* dialog box opens, click **OK**.
      - If the *Test Failed* dialog box opens, click **OK**, correct the information in the *Location* fields, and then click **Test Connection** again.
3. Enter a value in the *Retain (# of Backups)* field, either by typing-in a number or selecting one using the up and down arrows.
4. (Optional) To trigger backups automatically:

   Note: Ensure that you have correctly configured the backup location before you attempt to schedule backups.

a. Click to select the checkbox for *Backup Automatically*.
b. Enter a value in the *Time of Day* field, either by typing-in the time or selecting it using the clock icon ( ).
c. Enter a value in the *Expiration (Days)* field, either by typing-in a number or selecting one using the up and down arrows.

5. (Optional) To cancel the changes and return to the previously saved settings, click **Revert**.
6. Click **Save Settings**.
7. (Optional) After you have correctly configured backups, you can make a backup immediately. To do so, click **Backup Now**.
   a. At the top of the window, a caution triangle and "Backup is currently in progress…" message is displayed. When the backup is complete, a green checkmark and *Most recent backup at [date and time] SUCCESSFUL* is displayed. If the backup fails, an error message is displayed.
   b. To delete the backup, click the trash bin icon ( ) to the right of the backup message.

Restoring Databases on VideoXpert Enterprise™ Systems

Replacing One or More Core or VxDatabase™ Nodes

This procedure assumes that you have one or more functioning Cores from the original cluster, and that you need to replace one or more core nodes.

1. Install and/or update Core software on the replacement node(s) to the exact version on the remaining Cores of your existing cluster.
2. In VxToolbox, on the **Devices** tab, find the defunct Core and delete it. See the section titled *Removing Devices*.
3. In VxToolbox, on the **System** tab, add the new Core to your existing cluster. See the current version of the *VideoXpert Enterprise™ Installation Manual* section titled *Installing VideoXpert Core, Media Gateway, VxStorage, and VxToolbox*.

Performing an Emergency Restoration of a Database Backup on VideoXpert Enterprise™ Systems

This procedure assumes that none of the Cores from the original cluster are available. It also assumes that you have installed the same version of Core software on all the replacement Cores and that you have not configured the cluster.

1. Select one Core (node) replacement to be the primary.

   Note: If using separately installed VxDatabases, select one of them to be the primary as well.

2. On the primary node, open a command prompt (cmd) window as Administrator. In the cmd window:
   a. Navigate to the installation directory of VxDatabase, typically "C:\Program Files\Pelco\VxDatabase".
   b. Run the set command to set the full path to the database backup as a variable. For example: "set DbBackup=C:\Path\To\My\Backup\core-123124125.sql".
   c. Run the command "utils\manual_restore_db.bat %DbBackup% catastrophic".
   This is the restore script. It might take several minutes to complete.

3. Use VxToolbox to connect to the primary Core using the credentials admin/admin.
4. When you are prompted to change the admin password and to set the system and company name again, use the admin password that is contained in the backup.

   Note: Data from the backup, including the admin password, system name, and company name will be available to VideoXpert only *after* the next step is completed.

5. Use VxToolbox to configure a single-node cluster using the primary Core, and if applicable, the primary VxDatabase.
6. Use VxToolbox to configure any one VxMediaGateway.
7. Use VxToolbox to add all remaining Cores, VxDatabases, and VxMediaGateways to the cluster.

Manually Restoring a Database Backup on VideoXpert Enterprise™ Systems

This procedure assumes that you have a fully functioning VideoXpert Core cluster, and you need to restore to a previous backup because you have lost valuable data.

Caution: This procedure will cause you to lose all data that has been added after the backup was taken, so you must be sure that your old data is worth more than the newer data.

1. Select one node in the cluster to be the primary node.
2. Copy the appropriate database backup from your configured network storage location to the primary node.
3. Shut down the VideoXpert Core and VideoXpert Database services on everything except the primary node.
4. On the primary node, open a command prompt (cmd) window as Administrator. In the cmd window:
   a. Navigate to the installation directory VxDatabase (for example: "C:\Program Files\Pelco\VxDatabase").
   b. Run the set command to set the full path to the database backup as a variable. For example: “set DbBackup=C:\Path\To\My\Backup\database-123124125.sql”.
   c. Run the restore script using the command “utils\manual_restore_db.bat %DbBackup%”. The script might take several minutes to complete.
5. After the script has completed, start the VideoXpert Core service on all other nodes in the cluster.

Configuring the SMTP Server

You can configure the SMTP server to send email from the host to an email address. To do so:

1. In VxToolbox, click **System**, and then click **SMTP**.
2. If the *Mail From* field is not already populated with the correct value, enter a valid email address in the field.
3. Enter a value in the *SMTP Host* field.
4. Enter a number in the *SMTP Port* field.
5. (Optional) Click to select the checkbox for *Enable SMTPS*.
6. (Optional) Click to select the checkbox for *Enforce validation of the server’s certificate*.
7. Enter a value in the *Username* field.
8. Enter a value in the *Password* field.

9. Click **Send Test Email**, enter an email address in the *Send Test Email* dialog box, in the *Send to Email* field, and then click **Send Email**.
   - If the *Send Test Email* dialog box returns “Test email sent successfully!”, click **OK**.
   - If the *Send Test Email* dialog box returns “Test email failed...”, click **Try Again**, either correct the email address, and then click **Send Email**; or click **Cancel**, correct any errors in the SMTP configuration, and then try to send a test email again.
10. (Optional) To cancel the changes and return to the previously saved settings, click **Revert**.
11. Click **Save Settings**.

Controlling Memory Usage

VxToolbox memory usage defaults to 1 GB. To expand the amount of memory available to 4 GB:

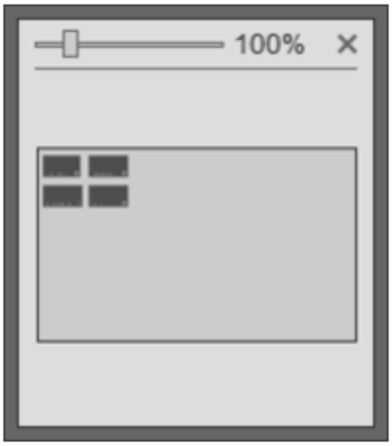
1. Create a file titled "user_runtime.txt".
2. In the file, type "-Xms4g".
3. Save the file to C:\ProgramData\Pelco\VxToolbox.
4. Restart the VxToolbox service so that the change will take effect.

Configuring Monitor Walls

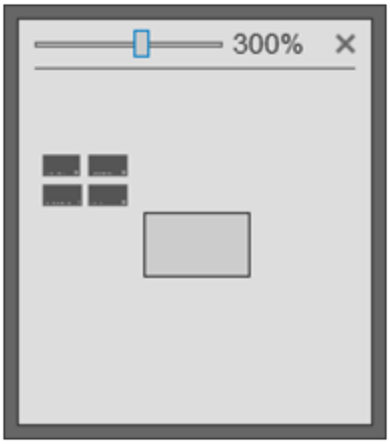
You can use existing monitors to configure several monitor walls.

Creating a Monitor Wall

1. Click the **Monitor Walls** tab.
2. At the bottom of the left panel, click the *Add a new Monitor Wall* icon ( ).
3. In the *Add a Monitor Wall* field at the upper left corner of the monitor wall window, enter a name for the monitor wall.
4. In the *Drag Monitors to assign* (right) panel, click and drag a monitor to the location you would like it to appear on the monitor wall. Repeat this step for each monitor that you want to add.
   - To refresh the list of monitors, in the upper right corner of the *Drag Monitors to assign* (right) panel, click the *Refresh* icon ( ).
   - To filter the list of monitors, in the *Drag Monitors to assign* (right) panel, enter a value in the *Search Monitors* field.
5. (Optional) To delete a monitor from the monitor wall, in the left panel, click the *Delete* icon ( ) in the monitor to delete.
6. (Optional) Scale the monitors:
   - To resize the monitors individually, click on a monitor and drag a corner to resize it.
   - To zoom in and out on all monitors by the same percentage, in the preview window, drag the selector bar to the appropriate magnification level. The images below show the monitor wall preview at 100% magnification and at 300% magnification. Notice that the monitors are no longer included in the frame.



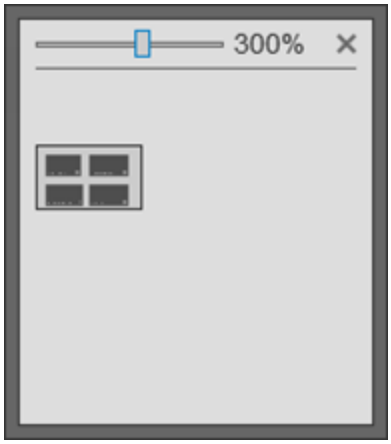
100% Magnification



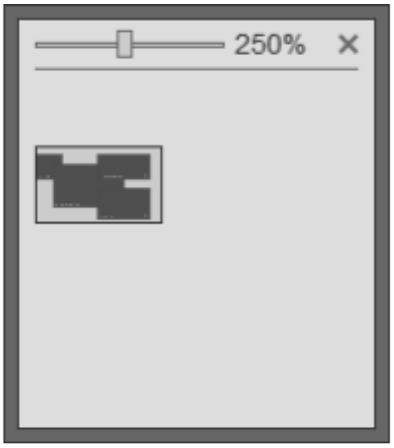
300% Magnification

7. (Optional) If necessary, move the monitors into the monitor wall frame:
   - Use the scroll bars at the bottom and right edges of the monitor wall window to bring the monitors into view.

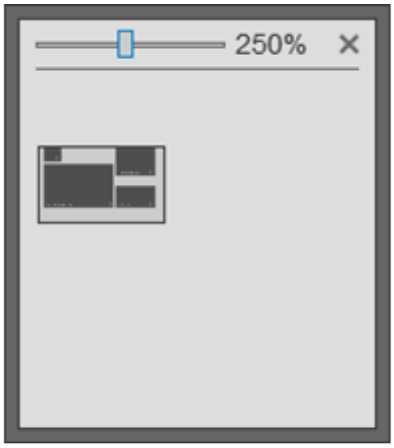
- In the preview window, drag the monitor wall frame so that the appropriate monitors are in the frame. The image below shows the monitors at 300% magnification, but they are now included in the monitor wall frame.



8. (Optional) Rearrange the monitors in any configuration by dragging them to the desired locations on the monitor wall. The image below shows the monitor wall with overlapping monitors and without overlapping monitors.



With Overlapping Monitors



Without Overlapping Monitors

9. When you are satisfied with the look of the monitor wall, click **Save**.

Editing a Monitor Wall

1. Click the **Monitor Walls** tab.
2. In the left panel, click to select the monitor wall to edit.
3. At the bottom of the left panel, click the *Edit the selected Monitor Wall* icon ( ).
4. Update the monitor wall as needed, using the steps in the section titled *Creating a Monitor Wall*.
5. When you are satisfied with the look of the monitor wall, click **Save**.

Deleting a Monitor Wall

1. Click the **Monitor Walls** tab.
2. In the left panel, click to select the monitor wall to delete.

3. At the bottom of the left panel, click the *Delete the selected Monitor Wall* icon ( ).
4. In the confirmation dialog box, click **Delete**.

Using Send Video Permissions

The *Send Video* permission enables a user to send video to a remote monitor wall based on the user's role and permissions.

Note: You can only send video to a monitor that has a number assigned to it.
See the *Configuring Monitors* section of the current version of the *VideoXpert OpsCenter™ Operations Manual* for Enterprise systems, or of this manual.

Using the instructions in the section titled *Creating a Role*, in the In the *Edit Role* window:

1. If *Surveillance* is not in the *Enabled Permission* area, click **Add a Permissions Category**, and then click **Surveillance**.
2. Click to expand **Surveillance**.
3. Click to select the checkbox for *Allow Select Surveillance Permissions*.
4. If the *Send Video* permission is not listed, click **Add a Permission**, and then click **Send Video**.
5. If necessary, in the *Allow Resources* column of the *Send Video* permission row, click the *Select Resource* icon ( ).
6. In the *Manage Resource Restriction for* window, use the drop-down menu to click one of the following:
   - **Allow All Resources**
   - **Allow Selected Resources**
   - **Allow All Resource Except Selected**
7. If you chose *Allow Selected Resources* or *Allow All Resources Except Selected*, in the list of resources in the right panel, click to select and deselect the checkboxes for the appropriate resource names.
8. Click **OK**.
9. Continue using the instructions for creating a role.

Using Reports

From the *Reports* page, you can create and generate reports, and export them from the system. Reports are exported in CSV format.

Report Templates preloaded to VxToolbox include:

- Default Camera Report
- Default Device Report
- Default Event Report
- Default Recording Gap Report
- Default Role Report
- Default Camera Role Access Report
- Default Storage Report
- Default User Report
- Default User Action Report
- Default System Status Report

You can edit an existing report template, or create a new one and edit the template details to include only the information needed.

Generating reports containing a large number of events might take some time. You can navigate away from the *Reports* page while the system generates your report. If your report parameters are too large, the request might time-out and the system might ask you to narrow your search.

Creating a Report Template

You can generate reports either manually or automatically from any of the templates in the *Report Templates* panel. To create a new template.

1. Click the **Reports** tab.
2. In the *Report Templates* list in the left panel, create a new report template using one of the following methods:
   - To make a copy of an existing template from the *Report Templates* panel, select the template in the *Report Templates* panel, and then click the *Create a copy of the selected Report Template* icon ( ). A new template (named the same as the original template - *Copy*) is added to the list.
   - To make a copy of an existing template from the *Template Details for [template name]* panel, select the template, and then click the **Save as New Template** button at the lower left of the *Template Details for [template name]* window (upper left panel). In the *Save New Template* dialog box, enter a value in the *Template Name* field, and then click **Save**.
   - To start with a blank template, click the *Create a new Report Template* icon ( ). A *New Unsaved Template* is added to the list.
3. Click to select the new report template.
4. If the *Report Type* drop-down menu is available, select from the report type.

   The report type can only be selected if you started with a blank template; if you copied an existing template, the copy is assigned the same report type as the original.

5. If the *Include [report type] (rows)* field is displayed:
   a. Click to select **All** or **Selected** from the drop-down menu.
   b. If you clicked *Selected*, click the *Select report filter sources* icon ( ) under the drop-down menu; in the *Select [report type]* window, click to select and deselect the appropriate options, and then click **OK**.
6. In the *Include Info (columns)* field, click to select and deselect the checkboxes for information to include in the report template.

   As you select and deselect this information, you can preview the report in the *Column Preview for [report template name]* panel in the (vertical) center of the window.
7. If the *Time Range* field is displayed, select an option from the drop-down menu. If you select *Custom*, set start and end dates and times in the *Date & Time* fields, either by typing-in values (mm/dd/yy and hh:mm AM or PM formats) or by using the selectors available by clicking the date icon ( ) or the time icon ( ).
8. (Optional) To generate a report for this template automatically:
   a. Click to select the checkbox for *Automatically Generate this Report*.
   b. From the drop-down menu below the option, select the day of the week on which the report will be generated.
   c. Type or click to select a time in the *at* field.
   d. (Optional) Click to select the checkbox for *Automatically Export to .csv*. If you select this, enter a *Network Storage Location*, *Username*, and *Password*. The user name and password are optional.
9. Depending on how you created the template and what you want to do, click **Save**, **Save template changes**, or **Save as new template**.
10. If the *Save New Template* dialog box is displayed, type a new name in the *Template Name* field, and then click **Save**.

Editing a Report Template

If appropriate, you can edit an existing template.

1. Click the **Reports** tab.
2. In the *Report Templates* list in the left panel, click to select the template to edit.
3. In the *Template Details for [template name]* (right) panel, make any changes needed to the template, except for the *Report Type*. The *Report Type* cannot be edited.
4. To save this over the existing template, click **Save template changes**.

   If you do not want to overwrite the existing template, you can click **Revert** to cancel the changes, or click **Save as new template** to save the settings as a new template.

Deleting a Report Template

If appropriate, delete a template.

1. Click the **Reports** tab.
2. In the *Report Templates* list in the left panel, click to select the template to delete.
3. Click the *Delete Template* icon ( ).
4. In the confirmation dialog box, click **OK**.

Generating a Report Manually

Even if a report is generated automatically, you can generate the report manually, as needed.

Note: You can run camera and device reports for locally discovered devices (*VX System* is **None**).

1. Click the **Reports** tab.
2. In the *Report Templates* list in the left panel, click to select the report to generate.
3. In the *Column Preview for [report template name]* panel (vertical center of the window), at the right of the panel:
   a. Type a value in the *Name your report* field, or keep the default report name.
   b. Click **Generate Report**.
   The report is listed in the *Generated Reports* table at the bottom of the window.

Exporting a Generated Report

To export a report from the *Generated Reports* table:

1. Click the **Reports** tab.
2. In the *Generated Reports* table at the bottom of the window, click to select the report to export.
3. Click **Export to .csv**.
4. Browse to a file location and, if appropriate, type a new value in the *File name* field.
5. Click **Save**.

Deleting a Generated Report

To delete a report from the *Generated Reports* table:

1. Click the **Reports** tab.
2. In the *Generated Reports* table at the bottom of the window, click to select the report to delete.
3. Click the *Remove report file* icon ( ).
4. In the confirmation dialog box, click **OK**.

Managing Events

From the *Events* tab, you can configure event details and notifications to ensure that the right users are notified when the system records a particular action or alarm.

Setting Event Log Retention Periods

Local events expire every 60 days on VideoXpert Professional systems. By default, on VideoXpert Enterprise systems, events expire every 30 days. However, you can you can set different expiration periods for both events local to the system and events from aggregated sites for up to 90 days.

Note: Event retention settings for aggregated events only affect the event log on the local system. The event log on the remote system has its own event log and may have different retention settings.

To change event retention settings:

1. Click the **Events** tab.
2. Click the *Event Configuration* icon ( ) at the upper left of the page.
3. In the Global Event Configuration dialog box:
   a. Set the retention periods for local events in the *Discard this system's events after* field, either by typing-in a number or selecting one using the up and down arrows.
   b. On VideoXpert Enterprise Systems, set the retention periods for local events and events coming from remote systems in the *Discard events coming from remote systems after* field, either by typing-in a number or selecting one using the up and down arrows.
   c. Set the *Maximum number of events to retain*, either by typing-in a number or selecting one using the up and down arrows
   d. If you reduce the number of days to retain event information, read the warning that is displayed in the *Global Event Configuration* dialog box and adjust the values accordingly, if appropriate.
4. Click **Save**.

Finding and Filtering Events

Use filtering options to show the events relevant to you. Filters appear in the left-most panel of the *Events* tab and in some other tabs.

1. Click the **Events** tab.
2. Click the expand the *Filter* panel, and then do one or more of the following.
   - Enter values in the *Situation Filter* field to filter by name, ID, model, IP address, serial number, vendor, or software version.
   - Select an event *Category* from the pull-down menu
   - Select an option from the *Requires Acknowledgment* pull-down menu.
   - Select an option from the *Pop-Up Banner* pull-down menu.
   - Select an option from the *Audio Alert* pull-down menu.
   - Enter a range in the *Severity* fields, either by typing-in a number or selecting one using the up and down arrows
   - Select the *Users* from the pull-down menu.

- Select the event *Roles* from the pull-down menu.
- Click the *Clear the current filter settings* icon ( ) to clear the filters.

The events matching the filter criteria are listed in the main panel.

Viewing and Configuring Event Details

1. Click the **Events** tab.
2. In the center panel, click to select the event you want to view or modify. You can use the filter, as described in the section titled *Finding and Filtering Events*.
3. Event details are shown in the right column. If necessary, click to expand **Event Details**.
4. To edit the event details settings, access the *Event Details for* dialog box by one of these methods:
   - In the right panel, click the edit icon ( ) to the right of *Event Details*.
   - Right-click the event name, and then click **Edit Event Details**.
5. In the *Event Details for* dialog box, change event settings as necessary.
   - Click to select or deselect the checkbox for *Enable logging and notification* to determine whether VideoXpert will report the event. If you select *Enable logging and notification*, VideoXpert will report the event.
   - Click to select or deselect the *Use Custom Display Name*.
   - If you selected *Use Custom Display Name*, enter a name in the corresponding field. The *Custom Display Name* is how VideoXpert will represent the event.
   - (Optional) If you selected *Enable logging and notification*, change the *Severity*, if necessary, either by moving the slider bar or typing a number in the field. The severity might help users determine whether or not they need to act on an event.
6. Click **Save**.

Viewing and Configuring Event Notifications

1. Click the **Events** tab.
2. In the center panel, click to select the event you want to view or modify. You can use the filter, as described in the section titled *Finding and Filtering Events*.
3. Event notification settings are shown in the right column. If necessary, click to expand **Notification Settings**, and view the notification information.
4. To edit the event notification settings, access the *Notification Settings* dialog box by one of these methods:
   - In the right panel, click the edit icon ( ) to the right of *Notification Settings*.
   - Right-click the event name, and then click **Edit Notification Settings**.
5. Click to select the checkbox for the appropriate *Notification Behavior*.

   Note: You can select more than one *Notification Behavior*. If you do, all settings in the *Notification Details* section of the dialog box will be configurable as described below.

6. If you selected *Generate a Pop-Up Banner*, configure these notification settings:
   a. In the *Roles and Users to Notify* section of the dialog box, and then:
      - Click in the *Roles* field, and then click to select one or more roles.
      - Click in the *Users* field, and then click to select one or more users.
   b. Scroll to the *Notification Details* section of the dialog box.
   c. Click to select or deselect the checkbox for *Auto-Acknowledge After*. If you select this option, also set a time interval, either by typing-in a number or selecting one using the up and down arrows in the first field, and then selecting the units (for example: **Minutes**) from the drop-down menu.
7. If you selected *Require Acknowledgment*, configure these notification settings:
   a. In the *Roles and Users to Notify* section of the dialog box, and then:
      - Click in the *Roles* field, and then click to select one or more roles.
      - Click in the *Users* field, and then click to select one or more users.
   b. Scroll to the *Notification Details* section of the dialog box.
   c. Click to select or deselect the checkbox for *Do Not Hide Cell Alerts*. Events associated with individual video sources provide alerts within VxOpsCenter cells; these alerts hide after three seconds. Select this option to prevent the alert from hiding.
   d. Click to select or deselect the checkbox for *Auto-Acknowledge After*. If you select this option, also set a time interval, either by typing-in a number or selecting one using the up and down arrows in the first field, and then selecting the units (for example: **Minutes**) from the drop-down menu.
   e. (Optional) Click to select the checkbox for *Allow Snooze (And Set Snooze Time)*, and then click the checkboxes to select and deselect the available intervals.
8. If you selected *Generate an Audio Alert*, configure these notification settings:
   a. In the *Roles and Users to Notify* section of the dialog box, and then:
      - Click in the *Roles* field, and then click to select one or more roles.
      - Click in the *Users* field, and then click to select one or more users.
   b. Scroll to the *Notification Details* section of the dialog box.
   c. Select the radio button for either *Standard Chime* or *Custom Sound*. If you select *Custom Sound*, browse to the *Audio File*, and then click **Open**.
   d. Type or select a value for the *Play Sound [#] times* field.
   e. Type or select a value in the *Delay Sound Playback For [#] seconds between iterations* field.
9. (Optional) To create a custom event:
   a. Click to select the checkbox for *Generate a Custom Event*.
   b. Type a value in the *Event Type Name* field.
   c. Set the *Severity* level, either by moving the slider bar or typing a number in the field.
   d. Click to select or deselect the checkbox for *Log this Event in the Event Log*.

10. When you have finished configuring responses, click **Save**.
11. When you have finished configuring the rule, click **Save**.

Using Maps™

The *Maps* tab in VxToolbox is used to import and use AutoCAD 2013 DWG files and raster maps (jpeg or png), and to use ESRI Street) maps, allowing customers to use their pre-existing building maps with Maps in VideoXpert.

- In VxToolbox, ensure that your system is set up for Maps. You can then create a new map, view or edit an existing map, manage permissions for maps, and remove an existing map.
- In VxOpsCenter, the operator can launch Maps, select a map file, add cameras to a map, manage available maps, set user preferences for mapping, and view an existing map. Refer to the current version of the *VideoXpert OpsCenter™ Operations Manual* for Enterprise systems, or the *VideoXpert OpsCenter* section of the current version of the *VideoXpert Professional™ Operations Manual*.

Preparing Your System for Maps

Maps requires the following prerequisites to function properly:

- Ensure that Visual C + + Redistributable for Visual Studio 2015 is installed. It can be found at https://www.microsoft.com/en-us/download/details.aspx?id=48145. This is installed by the VxToolbox or VxOpsCenter installer. If this was not installed, reinstall VxToolbox or VxOpsCenter.
- Install VideoXpert v 3.5 or later, and the latest version of VxToolbox.
- AutoCAD files must use the 2013 format.

Creating a New Map

1. If you have not already done so, start VxToolbox, and then click the **Maps** tab.
2. In the left panel, click the *Add a Map* icon (+), and then click to select one of the following:
   - For an outdoor map, select *Add a World Map (ESRI Street Map)*.
   - To use a jpeg or png file, select *Add a Raster Map (jpeg or png)*.
   - For an indoor map, select *Add a DWG Map*.
3. If you selected *Add a World Map (ESRI Street Map)*:
   a. Type a value in the *Name* field.
   b. Click **Save**.
4. If you selected *Add a Raster Map (jpeg or png)*:
   a. Type a value in the *Name* field.
   b. Click **Browse**, navigate to and select the file, and then click **Open**.
   c. Click **Save**.
5. If you selected *Add a DWG Map*:
   a. In the *Add a DWG Map* dialog box, type a value into the *Name* field.
   b. Under *Select a map file*, click **Browse**, select all files (including all xref dwg files), and then click **Open**.
   c. Click **Save**.

Viewing an Existing Map

1. If you have not already done so, start VxToolbox, and then click the **Maps** tab.

   Ensure that the user logging in is assigned the “administrator” role or has all of the maps permissions assigned.

2. From the list of maps in the left panel, click the map to preview.

   The selected map is displayed in the right panel.

Editing an Existing Map

1. If you have not already done so, start VxToolbox, and then click the **Maps** tab.
2. In the left panel) click to select the map to edit.
3. Click the *Edit map* icon ( ).
4. (Optional) To change the name of the map, type a new value in the name field to the right of *Edit Map*.
5. (Optional) To add cameras to the map, click the **Cameras** tab in the left panel, and from there, drag the camera name to the appropriate location on the current map.
6. (Optional) To add a link from the current map to another map, click the **Maps** tab in the left panel, and from there, drag a map name to the appropriate location on the current map.
7. (Optional) To add doors, alarms, and other devices, click the **Other** tab in the left panel, and from there, drag an item to the appropriate location on the map.
8. (Optional) To move a camera, linked map, or other item on the map, click the item to be moved, and drag it to the appropriate location.
9. To rotate a camera, right-click it, and then select a value in the *Set Rotation* window, either by using the slider bar or by typing a value in the field. Click anywhere in the map to close the window.
10. To remove a camera, drawing, or device from the map, right click it, and then click **Remove From Map**.
11. At the lower right of VxToolbox, click **Save**.

Deleting an Existing Map

1. If you have not already done so, start VxToolbox, and then click the **Maps** tab.
2. In the left panel, click to select the map to delete.
3. At the lower right corner of the left panel, click the *Delete map* icon ( ).
4. In the confirmation dialog box, click **Delete**.

Managing Permissions for Maps

After you have created maps, use VxToolbox to assign map permissions to different roles.

1. If you have not already done so, start VxToolbox, and then click the **Maps** tab.
2. Refer to the section titled *Managing Users and Roles* for instructions to add, edit, and assign roles.

Appendix A: Working With Permissions

Permissions define the actions a user can perform within the system. Where necessary, permissions are defined in a parent-child hierarchy; to assign a child permission, you must first define the parent permission.

Some features are not mapped to an obvious permission; in some cases, a feature might require compounding permissions. For example, users may have the “Place Cameras on Map” permission. However, users must also possess the “View Video Sources” permission for cameras they want to place in order to view video thumbnails and verify that they are placing cameras in the right locations on the map. Pay attention to compound or complex cases listed below to ensure that your users have the permissions they require to perform their surveillance roles within VideoXpert.

Understanding Permission Resource Restrictions

Permissions grant access to resources. Some permissions allow all-or-nothing access, using the **Allow All Resources** setting; some permissions allow you to select the resources to which a user has access using the **Allow Selected Resources** or **Allow All Resources Except Selected** settings. Some permissions can Match Parent Resources.

- If available and selected, **Match Parent Resources** assigns the same resource to the selected permission as is assigned to its parent.
- **Allow All Resources** indicates that all resources are accessible by the permission. If the permission does not support restrictions, but is an “on/off” permission, it is the only resource option. For example, selecting **Allow All Resources** for the *View Video Sources* permission grants a user access to view live video from all video sources within VideoXpert. If that same user was restricted to **Allow Selected Resources** for the *Use PTZ Mode* permission, then the user would be able to view video from all cameras but could only initiate PTZ controls for the cameras to which he or she had access.
- **Allow Selected Resources** indicates that the user can access all selected resources covered by that permission.
- **Allow All Resources Except Selected** indicates that the user can access all resources covered by that permission except those that are selected.

Using Surveillance Permissions

Surveillance permissions are common permissions required by operators in your VideoXpert environment. These permissions grant access to view live or recorded video and to control cameras.

Permission	Description
View Video Sources	Enables users to access live video or audio. Audio sources are tied to video sources; granting access to a video source automatically grants access to associated audio sources.
Use PTZ Mode	Provides the ability to pan, tilt, and zoom a camera. This permission includes a priority; priority determines who can control a camera in the event of competing users. If two or more users attempt to control a camera, the user with the highest priority will take command and lower priority users will be locked out.

Permission	Description
Lock PTZ Mode	Provides the ability to lock a camera into a particular PTZ position. PTZ locks may be overridden by users with higher priority than the user who set the lock.
Send Video	Allows a user to send video to a remote monitor, rather than all monitors, to monitor walls, and to shared displays.
Access Alarms	Allows a user to view system alarm devices.
Access Relays	Allows a user to view and activate system relay devices.

Using Investigation Permissions

Investigation permissions grant access to recorded video and the ability to export video from the system. Typical setups will want to assign the same access level to “view recorded video” permissions as to “view video sources”.

Permission	Description
View Recorded Video	Enables users to access live video or audio. Audio sources are presently tied to video sources; granting access to a video source automatically grants access to associated audio sources.
Create Exports	Allows a user to create exports.
Manage My Exports	Allows a user to edit or delete entries in the “Manage Exports” window.
Download My Exports	Allows users to download exports that they have created.
Stream My Exports	Allows users to stream exports that they have created.
Create Exports in Alternate Locations	Enables users to save exports to locations other than the default.
View All Exports	Allows a user to view all users' exports.
Manage All Exports	Allows a user to edit or delete all users' exports.
Download All Exports	Allows a user to download all users' exports.
Stream All Exports	Allows a user to stream all users' exports.
Create System Bookmarks	Allows a user to create system bookmarks
Lock System Bookmarks	Allows a user to lock system bookmarks.

Using Map Permissions

Map permissions provide access to maps and related features. Map operates in accordance with the *View Live Video* surveillance permission; even if a user has access to Map, the user might not be able to effectively use it without access to related cameras.

Permission	Description
Use Map	Allows users to access the mapping plug-in.
View Maps	Determines the maps to which a user has access. Maps only show cameras for which the user possesses the “View Video Sources” permission.
Place Cameras on map	Allows users to add and arrange cameras on the map; camera availability is limited by the “View Video Sources” permission.
Manage Map Files	Allows users to upload, delete, and select available map layers

Using Supervision and Reports Permissions

Supervision and Report permissions provide access to supervisors checking user activities auditing the system. These permissions are not hierarchical.

Permission	Description
Multiview	Enables a supervisor to see users that are viewing a camera in real time.
Define PTZ Presets	Allows for the creating of PTZ presets and pattens for cameras.
View Private & Public Views	View all private and public shared views/workspaces.
Manage Private & Public Views	Allows full access (create, update, and delete) to all private and public shared views/workspaces.
Audit User Activity	Allows users to export User Actions reports.

Using Event Management Permissions

Event management permissions enable users to view, act on, and configure event notifications. There is no hierarchy for these permissions, but in most cases, a user that can configure events should have access to the event log and be able to handle events.

Permission	Description
View Event History	Allows users to view the event history. **Note:** This permission does not include user audit events. The "Audit User Activity" permission is needed to view those events.
Handle Events	Allows a user to act on event notifications, marking them as “in progress” or acknowledging them. **Note:** This permission does not guarantee that a user will receive events, only that the users with this permission can act on event notifications the receive. Event notifications are defined within each event; the ability to modify events is granted by the “Configure Events” permission.
Configure Events	Provides the ability to configure events.

Using User Management Permissions

These permissions grant users the ability to manage user account settings.

Permission	Description
Manage User Accounts	Grants the ability to create, update, or delete user accounts.
Assign Roles to Users	Grants the ability to assign roles to users.
Reset User Passwords	Grants the ability to change the password for the user account.
Manage Roles	Grants the ability to create, delete, and assign permissions to roles.

Using Device Management Permissions

These permissions grant users the ability to edit devices on the devices page, or tags at the system level.

Permission	Description
Manage System Tags	Provides the ability to create, edit, delete, and assign System/Public tags. This permission does not apply to personal tags created or assigned through VxOpsCenter; personal tags only appear to the creating user and only the creating user can assign, modify, or delete his or her own personal tags.
Manage Device Licenses	Provides the ability to view, add, and update VX device licenses.
Manage I/O	Provides full access to add, remove, and update alarm and relay devices.

Permission	Description
Manage Cameras & Recorders	Provides full access to add, remove, and update camera and recorder devices.
Manage Display Devices	Provides full access to add, remove, and update monitor devices.
Configure Monitor Wall Decoders	Provides full access to add, remove, and update monitor walls on VideoXpert Enterprise systems.

Using System Management Permissions

System Management permissions should be reserved for administrators. Users with these permissions can modify system configuration settings; these changes should be carefully planned by administrators to ensure that they do not interfere with video recording or interrupt surveillance operations.

Permission	Description
Manage System Licenses	Provides the ability to view, add, and update VideoXpert system licenses.
Set System Locale Options	Allows configuration of the VideoXpert System time.
Configure Recording	Allows configuration of recording, including recording schedules, camera assignments, and retention periods; this permission does not affect access to the VXS Recorder interface.
View System Health	Allows the user to view VideoXpert system diagnostic information, including hardware and network status, temperatures, loads, and recording gaps.
Manage System Servers	Provides the ability to edit settings.
Manage Member Systems	Provides the ability to add, edit, and remove aggregated VideoXpert systems.

Pelco, Inc.
625 W. Alluvial Ave., Fresno, California 93711 United States
(800) 289-9100 Tel
(800) 289-9150 Fax
+1 (559) 292-1981 International Tel
+1 (559) 348-1120 International Fax
www.pelco.com

Pelco, the Pelco logo, and other trademarks associated with Pelco products referred to in this publication are trademarks of Pelco, Inc. or its affiliates. ONVIF and the ONVIF logo are trademarks of ONVIF Inc. All other product names and services are the property of their respective companies. Product specifications and availability are subject to change without notice.

© Copyright 2020, Pelco, Inc. All rights reserved.