PELCO
a Motorola Solutions Company

VideoXpert® Enterprise v 3.14
Installation Manual

Document number: C6609M-L

Publication date: 9/21

Table of Contents

Introduction

The VideoXpert® Enterprise System is a highly-customizable, distributed system comprised of hardware and software components that can include: VideoXpert Core and Media Gateway Servers, load balancers, VxOpsCenter, VxToolbox, VxStorage, and VxPortal.

Prerequisites

- If you have purchased a software-only solution and are installing VideoXpert on your own hardware, ensure that all aspects of the system meet the hardware and software specifications listed on www.Pelco.com.
- Every device running VideoXpert software must be configured with a unique static IP address. This includes, but is not limited to, the following VideoXpert devices:
  - VideoXpert Core (Static IP required)
  - VideoXpert Media Gateway (Static IP required)
  - VxStorage (Static IP required)
  - VxOpsCenter (Static IP recommended)
  - VxToolbox (Static IP recommended)

  Caution: Do not change the IP address of any VX component (VideoXpert Core, Media Gateway, etc.) after the system has been installed and configured. If the IP address is changed, the system will go offline and require a reboot. There is a potential risk of permanent disruption if proper steps are not followed.
- Ensure that the computer name is set on all equipment.
- Ensure that the time and timezone is set on all equipment.
- Ensure that you have administrative privileges on all workstations.
- Ensure that Microsoft Internet Information Services (IIS) is not installed on any of the Core or Media Gateway servers.
- Ensure that all network interfaces except the primary NIC are disabled. Additional network interfaces might prevent the system from discovering devices.
- Ensure that each computer on your system has an OS that meets one of the following minimum version requirements:
  - Windows 8.1
  - Windows 10 version 1607 (Anniversary Update)
  - Windows Server 2008 R2 SP1
- Ensure that the Microsoft OS on each computer on your system has the latest updates that address the most current known vulnerabilities. You can find this information at www.microsoft.com.
  On a continual basis:
  - Frequently update the OS to ensure newly discovered vulnerabilities are patched as soon as a patch is available.
  - Frequently update anti-virus libraries with the latest patches.

- Ensure that the browser on each computer on your system is one of the following supported browsers: Current version of Google Chrome, Mozilla Firefox, or Microsoft Edge.

Caution: To integrate the VX System with another system, contact Pelco Customer Support and use VX SDK. This is the only method that will work properly.

Installation and Configuration Order

The system must be installed and configured in the order presented below on either Pelco factory-installed systems or software-only installations on your own hardware.

1. Ensure that your system meets the prerequisites identified in the section titled *Prerequisites*.
2. If necessary, install and configure an NTP client application as instructed in the section titled *Installing an NTP Server Application*
3. Install and configure all instances of VideoXpert Core and Media Gateway as instructed in the section titled *Installing VideoXpert Core, Media Gateway, VxStorage, and VxToolbox*.

   If a Core and Media Gateway are installed on the same computer, it can be referred to as a CMG.

   Caution: Do not install a Core and/or Media Gateway on the same server as VxStorage. These must be installed on separate servers.
4. Install and configure VxStorage as instructed in the section titled *Configuring Advanced Storage Using VideoXpert Storage Portal*.
5. In VxToolbox, create a cluster using the Cores you installed previously. See the section titled *Configuring VideoXpert Core and Media Gateway Clusters*.
   - If you are *not* using VideoXpert Load Balancing, you cannot have more than one VideoXpert Core Media or Gateway server active on the network unless the servers are clustered behind a load balancer.
   - For clustered installations, complete each operation for each server in the cluster before moving on to the next operation.
6. (Optional) Enable FIPS 140-3 encryption. See the section titled *Enabling FIPS 140-3 Encryption (Optional)*.
7. If you have more than one VideoXpert Core and/or Media Gateway, set up load balancing.

   Caution: 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.
   - Load balancing is performed using VX load balancing, or third-party equipment and software.
   - If you are using third-party equipment and software, use the documentation from the vendor to perform this step. If necessary, contact Pelco Customer Support for assistance.
8. In VxToolbox, install the licenses as instructed in the section titled *Licensing Your System*. You must apply licensing to continue using VideoXpert past the 60-day grace period.
9. In VxToolbox, add devices to the system and perform other system setup activities. See the current version of the *VideoXpert® Toolbox Operations Manual*.
10. (Optional) Install the Access Control System Viewer (a VxOpsCenter plug-in). See the section titled *Installing and Configuring Components for Access Control System Viewer (Optional)*.

11. (Optional) Install other plugins, as described in the current version of the *VideoXpert® OpsCenter Operations Manual* chapter titled *Working With Plugins*. Plugins include:
    - BriefCam
    - Event Viewer
    - Image Viewer
    - Web Browser
    - Access Control System Viewer
    - VideoXpert Plates ALPR
    - Occupancy Counting
12. (Optional) Install add-ons, as described in the current version of the *VideoXpert® OpsCenter Operations Manual* chapter titled *Working With Add-ons*. Add-ons include:
    - ASCII Service
    - Event Monitor
    - VxConnect
    - VxSNMP

Installing an NTP Server Application

All servers in your VideoXpert system must reference a time server to ensure that all devices belonging to the system use the same time. Time disparities may result in errors when recording and recalling video.

- Pelco recommends that you use an official NTP server or purchase and use a network clock to keep your system synchronized.
- You can choose to use the VideoXpert Core cluster on your VideoXpert system as the NTP server, but doing so will allow the time of your system to drift significantly from the actual time if there is no time source.

Using an Official NTP Server as the NTP Server

If you have internet access, purchase and use an official NTP server. If you do not have internet access, purchase and use a network clock to keep your system synchronized. For either method, follow the instructions associated with that device.

Using a VideoXpert Core Server as the NTP Server

If you are using VideoXpert Cores as your NTP servers, select one Core to be the main Core for the NTP server, and select one or more failover Cores. If the main Core fails, another Core will become the NTP server.

1. Install the NTP server on all of the Cores. For each Core:
   a. Run the Meinberg installer as an administrator.
      Note: Download the installer from https://www.meinbergglobal.com/english/sw/ntp.htm#ntp_stable.
   b. Accept all defaults during the installation.
   c. Finish the installation process.
2. Starting with the primary Core server, update the configuration file.
   The configuration file contains almost everything required. You need only edit/add the stratum and server lines. You will use parts of this configuration file for the primary Core server as a starting point for the configuration file for all other cores.
   a. On the primary Core, open C:\Program Files (x86)\NTP\etc\ntp.conf.
      You will see a block that resembles the following:

      ```
      driftfile "C:\Program Files (x86)\NTP\etc\ntp.drift"
      server <IP>
      fudge <IP> stratum <Insert number as explained below>
      restrict -4 default kod nomodify notrap
      restrict -6 default kod nomodify notrap
      restrict 127.0.0.1
      restrict ::1
      ```

   b. Edit the existing fudge stratum to be 12 minus the potential number of Cores. For example: in a five node cluster, the fudge stratum value is 12 - 5 = 7.

Note: Pelco recommends that you start at 12 instead of 14 so that you can add up to 2 more Core servers later.

c. Copy the block from the server IP line to the restrict line.

d. Save the file.

3. On the secondary Core server:

   a. Open C:\Program Files (x86)\NTP\etc\ntp.conf.

   b. Locate the server block (shown in the previous step).

   c. Paste above this block the primary Core server information that you created and copied in the previous step.

   d. In the block for the secondary Core server (what was originally in this file), edit the fudge stratum value to be one number higher than that of the primary Core server. Continuing the example, the fudge stratum value is 8.

   e. Copy the block from the primary Core server IP line to the secondary Core server restrict line.

   f. Save the file.

4. On the tertiary Core server:

   a. Open C:\Program Files (x86)\NTP\etc\ntp.conf.

   b. Locate the server block.

   c. Paste above this block the primary and secondary Core server information that you created and copied in the previous step.

   d. In the block for the tertiary Core server (what was originally in this file), edit the fudge stratum value to be one number higher than that of the secondary Core server. Continuing the example, the fudge stratum value is 9.

   e. Copy the block from the primary Core server IP line to the tertiary Core server restrict line.

   f. Save the file.

5. On all other servers, follow the same pattern as above, ensuring that entries for all prior servers are included in the file (C:\Program Files (x86)\NTP\etc\ntp.conf).

6. Allow NTP through the firewall. To do so, on each Core on the system, sign on as Administrator and run C: ProgramData\Pelco\Core\bin\ntp-firewall-rules.bat.

7. Restart the NTP service on your system by one of the following methods:

   - Click Windows **Start**, click **Meinberg**, and then click **Restart NTP Service**.
   - In the Windows search field: type in services, click to open the *Services* dialog box, click **Services (local)**, click **Network Time Protocol Daemon**, and then click **Restart** the service.

Using DHCP With Windows Server

If you want to use VideoXpert to provide your DHCP service, you can use DHCP with Windows Server.

Note: This is a Microsoft Windows feature. The information provided here is a basic outline only. For specific information, see https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/hh831385(v=ws.11).

To set up DHCP with Windows Server:

1. Choose a Core server to be the DHCP server, or choose two core servers to be DHCP servers that will use either DHCP failover or DHCP load balancing.
2. Enable the DHCP role on the chosen servers. This will install the DHCP software.
3. Add the active user to the DHCP Administrators group.
4. If you are not using Active Directory, add the same user on each DHCP machine; use the same password for each user on each DHCP machine.
5. Finish the DHCP configuration.

Note: For detailed instructions, see the customer support article at https://support.pelco.com/s/article/VideoXpert-Setup-DHCP-on-Windows-Server-2012.

Installing VideoXpert Core, Media Gateway, VxStorage, and VxToolbox

After you have ensured that your hardware and network meet the prerequisites, install the VideoXpert Core, Media Gateway, VxStorage, and VxToolbox.

Caution: Do not run Microsoft Internet Information Services (IIS) on your Core server.

Pelco recommends that you install all instances of VideoXpert Core and Media Gateway server applications immediately, and then perform other installation and configuration tasks.

1. On each Core server, install VideoXpert Core. To do so, run the exe installer, and follow the prompts in the installation wizard.
   a. Click to select the checkbox to accept the terms of the End-User License Agreement, and then click **Begin Installation** or **Begin Upgrade**, whichever is present.
   b. If appropriate, select *Standard Installation* to install VideoXpert Core to the default path with default options, and then click **Install**.
   c. If appropriate, select *Advanced Installation* to select packages and change the default installation paths. Select installation directories for Core, data, database, and export locations, and then click **Next**.

      You can select a location other than the default to store exports to a network location off of the Core. This saves space and bandwidth on the Core server(s).

      In a clustered environment, exports are stored only on a single Core. Storing exports in an alternate location ensures that the loss of a Core will not prevent you from accessing any of your recordings.
   d. Click **Install**.
   e. Click **Restart Now** or **Restart Later**.
2. On each Media Gateway server, install Media Gateway software. To do so, run the exe installer and follow the prompts in the installation wizard.
   a. Click **Install** to begin.
   b. Click **Next**.
   c. Click to select the checkbox to accept the terms of the End-User License Agreement, and then click **Next**.
   d. (Optional) To select an the installation directory other than the default for Media Gateway:
      i. Click **Browse**.
      ii. Navigate to the appropriate directory, and then click **OK**.
   e. Click **Next**.
   f. Click **Install**.
   g. Click **Finish**.
   h. Click **Close**.

3. On each storage server, install VxStorage.

   Caution: Do not install VideoXpert Core or Media Gateway on the same server as VxStorage. These must be installed on separate servers.

   To install VxStorage, run the exe installer and follow the prompts in the installation wizard.

   a. Click **Install** to begin.
   b. Click **Next**.
   c. Click to select the checkbox to accept the terms of the End-User License Agreement, and then click **Next**.
   d. Click **Install**.
   e. Click **Finish**.
   f. Click **Close**.

4. On a client machine, install VxToolbox. To do so, run the exe installer and follow the prompts in the installation wizard.

   a. Click to select the checkbox to accept the terms of the End-User License Agreement.
   b. Click **Begin Installation**.
   c. If appropriate, select *Standard Installation* to install VideoXpert Toolbox to the default path with default options, and then click **Install**.
   d. If appropriate, select *Advanced Installation* to change the default installation paths, and then click **Next**, click **Browse**, browse to and select the appropriate VxToolbox Installation directory, and then click **OK**.
   e. Click **Install**.
   f. Click **Close**.

Enabling FIPS 140-3 Encryption (Optional)

VideoXpert supports FIPS 140-3 validated cryptographic modules. When VideoXpert detects that FIPS-mode is configured as part of the Microsoft Windows operating system, the application automatically employs FIPS validated cryptographic modules.

To enable FIPS 140-3 encryption:

1. Login to your system with administrative credentials.
2. In the windows *Search* field, type Local Group Policy Editor, and then click to open it.
3. In the *Local Group Policy Editor* window, navigate to **Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options**.
4. In the right panel, scroll to and double-click **System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing**.
5. Click to select the radio button for *Enabled*.
6. Click **OK** or **Apply** and then click **OK**.
7. Click the **X** at the upper right corner of the *Local Group Policy Editor* window to close it.
8. Restart your web server.

Upon reboot, VideoXpert will configure itself to use FIPS 140-3 cryptographic libraries.

- Bouncy Castle uses v 1.0.1 (https://csrc.nist.gov/Projects/cryptographic-module-validation-program/Certificate/3152).
- OpenSSL uses FIPS Object Module 2.0.16 (https://csrc.nist.gov/Projects/cryptographic-module-validation-program/Certificate/2398).

Note: NIST support for FIPS 140-2 will continue only until September 22, 2021. Pelco currently supports FIPS 140-2 and 140-3.

Installing and Configuring Components for Access Control System Viewer (Optional)

The Access Control System Viewer is a VxOpsCenter plugin that enables the communication and data exchange from various Access Control Systems to the VideoXpert system. A server component, called an Access Control Server, communicates directly to the Access Control System and relays information to the Access Control System Viewer while relaying events between the Access Control System and VideoXpert. While the Access Control System Server handles events, it also provides other information to the Access Control System Viewer, such as user images that the Access Control System Viewer might display in association with events injected by the Access Control System Server.

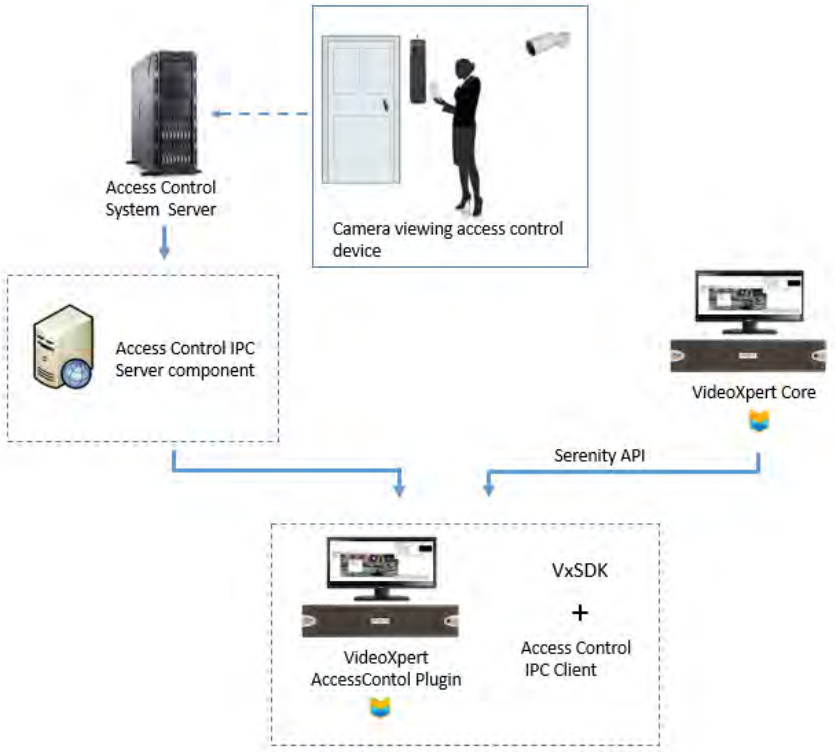

Figure 1: Access Control System overview

To use Access Control System, you must install AccessXpert VideoXpert Event Service, and then install the Access Control System Viewer.

Installing and Configuring AccessXpert VideoXpert Event Service

AccessXpert VideoXpert Event Service is an event bridge between AccessXpert and the VX System. Events that occur on one system can be viewed and acknowledged on the other. The service also acts as a server target for the Access Control System Viewer in VxOpsCenter.

To install AccessXpert VideoXpert Event Service:

1. Ensure that the target system meets the following prerequisites.
   - Microsoft .NET Framework 4.7.2 or later is installed.
   - Microsoft Visual C++ 2015 Redistributables (x86) is installed.

- VxOpsCenter Client is installed.

2. Run the exe installer, and follow the prompts in the installation wizard.
   a. Click **Next** to begin.
   b. Click **Install**.
   c. Click **Finish**.
3. (Optional) Start the Service manually.
   a. In the Windows search field, type in Services, and then click to open **Services Desktop app**.
   b. Click to highlight **AccessXpert Vx Event Service**.
   c. Click **Start** the service.
   d. Close the *Services* window, either by clicking **File** and then **Exit**, or by clicking the **X** in the upper right corner of the window.
4. Use the Administration Tool to configure AccessXpert Vx Event Service. Navigate to and select **AccessXpert VideoXpert Event Service Administration Tool** from Program files to open the *AccessControl Integration Administration* window.
5. Configure *Settings*.
   a. Click **Settings**.
   b. In the *AccessXpert Settings* area, type in the *IP Address/URL*, *Instance Name*, *User Name* and *Password*, and then click **Connect**. When the connection is established, the connection status icon will change from red to green.
   c. In the *VideoXpert Settings* area, type in the *IP Address*, *Port*, *User Name*, and *Password*, and then click **Connect**. When the connection is established, the connection status icon will change from red to green.
   d. In the *Access Control Server (MiddleWare PC) Settings* area, type in the *IP Address* and *Port*, and if appropriate click to select the checkbox for *use SSL*.
   e. Click **Apply**. If there are any errors, follow the prompts to correct them, and then try again.

      Caution: You must correctly configure the *Settings* page before configuring any other page in the *AccessControl Integration Administration* window.
6. Configure *CameraAssociations*.

   Each column in the *Camera Event Associations* table contains a drop-down list of available items. Each row specifies a camera, door device, and event associated with the door device. A camera can be mapped to multiple door events; multiple cameras can be mapped to the same door event.
   a. Click **CameraAssociations**.
   b. Select a *Camera Name* from the drop-down menu.
   c. Select a *Door* from the drop-down menu to correspond to the camera in the row.
   d. Select an *Event Name* from the drop-down menu to correspond to the camera in the row.
   e. To delete a row, right-click it, and then click **Delete Row [#]**.
   f. When you have finshed configuring the Camera Event Associations, click **Apply**.
7. Configure *Custom Situations*.

   From the *Custom Situations* page, you can define new Situations to inject into VideoXpert.

Note: After you create Custom Situations, you can associate them with VideoXpert Situations on the *EventMap* tab.

a. Click **Custom Situations**.
b. Type a string in the *Company Name (External Event Type)* field. Custom or external situations usually take the form of external/<company>/<event>; therefore, you must specify the company name.
c. In the first empty field in the *External Situation Type* column, type a string that describes the situation to inject, for example: "access_denied". This is the <event> for the Situation.
d. In the *Severity* column, enter a number from 1 (highest) to 10 (lowest) to indicate the severity of the Situation. Do this either by typing in the number or selecting it from the drop-down menu.
e. (Optional) Click to select the checkbox in the *Log* column to log the event in VideoXpert.
f. (Optional) Click to select the checkbox in the *Notify* column to notify operator of the Situation.
g. (Optional) Click to select the checkbox in the *Banner* column to display a banner to operators with the event occurs.
h. (Optional) Click to select the checkbox in the *Expand Banner* column to display an in-cell notification banner when the even occurs.
i. (Optional) Click to select the checkbox in the *Audible* column to produce an audible tone for the operators when the event occurs.
j. (Optional) Click to select the checkbox in the *Need Ack* column to require acknowedgement of the situation.
k. (Optional) In the *Auto Ack* field, type a value to indicate the number of seconds before the system will automatically acknowledge the alarm. Leave the field blank to disable automatic acknowledgment.
l. (Optional) In the *Snooze Intervals* field, type a value, in seconds, for the event. Leave the field blank to usethe default values of "60, 300, 600".
m. When you have finished configuring *Custom Situations*, click **Apply**.

8. Configure *Scripts*.
   a. Click **Scripts**.
   b. Type a value in the *Number* field. The value must be unique.
   c. Type a descriptive string in the *Name* field.
   d. In the *Actions* column, click **Edit**.
   e. Select an *Action* from the drop-down menu.
   f. If you selected the action **SetLayout**, select a *Layout* from the drop-down menu.
   g. If the *Monitor* field is active (white), type the monitor number in the field. This number is configured in the VX System.
   h. If the *Cameras* field is active, type the camera number in the field. This number is configured in the VX System.
   i. If the *Cell* field is active, type the cell number in the field. This number is configured in the VX System.

j. (Optional) If you selected the action **DisplayCamera**, in the *Previous Seconds* field, type a value that indicates the number of seconds in the past to display the camera video. For live streaming, leave this field blank.

k. If the *Preset* field is active, type the name of the preset in the field. The preset is configured on the camera or in the VX System.

l. If the *Pattern* field is active, type the name of the pattern the field. The pattern is confiugred on the camera.

m. If the *Description* field is active, type the text that will be shown with the bookmark.

n. When you have finished configuring settings in the *Actions for [script name]* window, click **OK**.

9. Configure *EventMap*.

   The *EventMap* page enables you to map an AccessXpert Event to a VideoXpert Situation, and to execute scripts when an event occurs or is acknowledged for the first time.

   a. Click **EventMap**.

   b. Select a *Direction* from the drop-down menu.

      - **To VideoExpert** is used for events that originate from AccessXpert and are injected into VideoXpert as a Situation. Any AccessXpert event can be mapped to a VideoXpert Situation; you can define Custom Situations for any event or situation that originates outside of VideoXpert. VideoXpert might reject situations that are not appropriate to originate from an external device.
      - **To AccessXpert** is used for Situations originating in VideoXpert that are being injected into AccessXpert as an event. All *To AccessXpert* events must have the *Access Control Event* type **VideoXpert Service/VideoXpert Event**. It will be selected automatically when you select *To AccessXpert*.

   c. Select a *VideoXpert Situation* from the drop-down menu. Custom Situations are listed here.

   d. Select an *Access Control Event* from the drop-down menu.

   e. (Optional) To execute one or more scripts when the event occurs, enter the script number(s) into the *Scripts* field using commas to separete them. (For example: to run scripts 1, 2 and 5 on an event, enter "1,2,5" in the *Scripts* field.)

   f. (Optional) To execute one or more scripts when the event is acknowledged for the first time, enter the script number(s) into the *Ack Scripts* field using commas to separete them.

   g. When you have finished configuring *EventMap*, click **Apply**.

10. When you have finished configuring *AccessControl Integration Administration*, click **OK**.

11. (Optional) Configure the service to start automatically.

    a. In the Windows search field, type in "Services", and then click to open **Services Desktop app**.

    b. Right-click **AccessXpert Vx Event Service**, and then click **Properties**.

    c. Click the *General* tab.

    d. In the Startup type field, use the drop-down menu to select **Automatic**.

    e. Click **Apply**.

    f. Click **OK**.

g. Close the *Services* window, either by clicking **File** and then **Exit**, or by clicking the **X** in the upper right corner of the window.

Configuring Advanced Storage Using VideoXpert Storage Portal

VideoXpert Storage Portal provides advanced settings and status that can help you fine-tune and monitor your VideoXpert Storage devices.

To use the VideoXpert Enterprise system, you must configure storage.

Accessing the VideoXpert Storage Portal on a VideoXpert Enterprise System

For each VxStorage module on the VideoXpert Enterprise system:

1. Login.
2. Click the desktop shortcut called **VideoXpert Storage Web Portal**.
3. Enter the *Username* and *Password*, and then click **Log In**. The default *Username* and *Password* are both “admin”.
4. If you are prompted to do so, reset the password.

   Note: For new VxStorage 3.7 or later installations, you will be required to set a new password for a storage device the first time you sign in.

Using Volumes and Volume Groups

You can organize your device video storage by creating and managing volumes and volume groups.

- A volume is a logical directory in which you want to store video.
- A volume group is a group of volumes to which cameras are assigned and distributed. You can use volume groups to:
  - Separate types of storage (like internal vs. external).
  - Set different retention parameters for different sets of drives.
  - Write video to more than one volume. When all volumes are full, the system will overwrite volume containing the oldest stored video.

  The system ships with a volume group called Default Volume Group. You can rename or delete this volume group.
- An archive volume group is a volume group to which the recorder will move the oldest video from the other volume groups, instead of deleting the oldest video. See the section titled *Using External NAS Storage (Archive Volume Group)* for more information about the archive volume group.

Using External NAS Storage (Archive Volume Group)

By connecting an external volume (network storage/NAS), you can extend your retention time for VideoXpert Storage recorders. When your VideoXpert Storage recorder achieves its maximum capacity and would normally begin to delete the oldest video, it will send video to the NAS instead. Video will still adhere to retention parameters, even when moved to external storage. The experience in accessing video is the same, whether a recording is served from a the VideoXpert Storage recorder or an external server.

Note: VideoXpert supports SMB1 NAS servers when using anonymous access. For systems that require a username/password for NAS access, you must use SMB2 or higher.

The external storage server must reside on the VideoXpert network. You can select whether to require login credentials. If the server requires and is provided login credentials, NAS Authentication is enabled.

As video transfers from a VideoXpert Storage recorder to an external storage server, bandwidth of your incoming cameras is equal to the bandwidth out to external storage. When using external storage, you should plan storage distribution to ensure bandwidth availability for incoming cameras, storage overflow, and user impact in viewing recorded video.

Note: While each VideoXpert Storage recorder can only have a single archive group, multiple VideoXpert Storage recorders can use the same NAS server. In this case, **each VideoXpert Storage recorder must point to a different path/folder on the NAS server**; pointing multiple VideoXpert Storage recorders to the same archive group network path will cause video to expire earlier than expected and without warning. You can individually select whether each path uses NAS Authentication.

Configuring the Recorder on a VideoXpert Enterprise System

For each VxStorage module on the VideoXpert Enterprise system:

1. Login.
2. Click the desktop shortcut called **VideoXpert Storage Web Portal**.
3. Log in to the server. The default *Username* and *Password* are both “admin”.
   See the current version of the *VideoXpert® Portal Operations Manual*, section titled *Configuring Advanced Storage Using VideoXpert Storage Portal* for instructions on using the interface.

Creating a New Volume Group

1. In VideoXpert Storage Portal, click the **Volumes** tab.
2. At the bottom-right of the *Volume Groups* panel, click the plus sign icon ( ).
3. In the *Create New Volume Group* dialog box:
   a. Enter a value in the *Name* field.
   b. Click to select or deselect the checkbox for *Designate this Volume Group as the Archive Volume Group*.
   c. Click **OK**.
4. If you selected this volume group to be the archive volume group, and there is already a designated archive volume group, the *Attention* dialog box will inform you of this, and instruct you to remove the current archive volume group. To proceed:
   a. Click **OK**
   b. Identify the current archive volume group by the *Archive Volume Group* icon ( ) to the left of the volume group name.
   c. Select the volume group that is the current archive volume group, click the pencil icon ( ), deselect the checkbox, and then click **Save**.
   d. Add the new volume group, and select the checkbox to set it as the *Archive Volume Group*.
   e. Click **Save**.

Creating a New Volume

1. In VideoXpert Storage Portal, click the **Volumes** tab.
2. In the *Volume Groups* panel, click to select a *Volume Group* to which the new Volume will be assigned.

3. At the bottom-right of the *Volumes* (center) panel, click the plus sign icon ( ).
4. In the *Create New Volume Group* dialog box:
   a. Enter a value in the *Path* field.
   b. Click to select or deselect the checkbox for *Requires credentials*. If you select this checkbox, enter values in the *Username*, *Password*, and *Domain* fields.
   c. Enter a value in the *Buffer Size* field.
   d. Click to select or deselect the checkbox for *Reserve bandwidth for this volume*.
   e. Click **OK**.

Configuring VideoXpert Core and Media Gateway Clusters

When you are configuring clusters, you will also configure Media Gateway Communications.

To configure clusters, the VX System must have two or more servers. You must configure the clusters and Media Gateway communications, and then manually edit device discovery settings, as explained in the following sections.

Adding a VX System to VxToolbox

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.

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 *Miscellaneous* area:

a. Click to select or deselect the checkbox for *Show previous camera names througout VX System*.
When selected, if you have changed the name of the camera within the last one year, the camera details window in VxOpsCenter will show the current name, a list of the previous names (up to 10), and the date that each name was changed.

b. (Optional) Click to select or deselect the checkbox for *Force encryption on all exports*.

c. (Optional) If you selected *Force encryption on all exports*, click to select the checkbox for *Use preset password for all encrypted exports*.

d. 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**.

Note: There are many other configuration settings available in VxToolbox. See the current version of the *VxToolbox Operations Manual* for instructions.

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 whether users must access sources simultaneously will inform your choice.

Use VxToolbox to configure clusters. See the current version of the *VideoXpert Toolbox Operations Manual* section titled *Adding Systems*.

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*.

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.

Using VideoXpert Enterprise

You can now use the VX system.

- Perform additional system configuration in VxToolbox using the current version of the *VideoXpert® Toolbox Operations Manual*.
- Begin monitoring the system in VxOpsCenter using the current version of the *VideoXpert ® OpsCenter Operations Manual*.

VideoXpert® Enterprise v 3.14 Installation Manual

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