

VideoXpert Servers

Admin Portal User Guide

Contents

Installation and Configuration Process Overview	4
Single Server Vs Clustered Installations	4
Installing VideoXpert Core	4
Installing an NTP Client Application	4
Logging In	5
Configuring your VideoXpert Site	5
Configuring a Cluster	6
Configuring Device Discovery for Clustered Environments	6
Configuring Media Gateway Communications	6
Installing the Media Gateway	6
Licensing Your System	7
Adding and Updating Entitlements	7
Migrating to VideoXpert	8
Migrating from Endura to VideoXpert	8
Migrating from Digital Sentry to VideoXpert	9
Configuring Storage	10
Using Digital Sentry Servers as VideoXpert Storage	10
Discovering and Commissioning Devices	11
Commissioning and Decommissioning Devices	11
Deleting Devices from the Registry	11
Editing Source Names and IDs	11
Changing Source Settings	12
Aggregating Systems	13
Tags	14
Creating Tags	14
Editing Tags	14
Deleting Tags	14
Assigning Tags to Sources	15
Managing Users	16
Adding Users	16
Duplicating Users	16
Renaming Users	17
Deleting Users	17
Deactivating and Activating Users	17
Resetting Passwords	17
Assigning Roles to Users	18
Managing Roles	19
Creating a Role	19
Renaming a Role	19
Duplicating a Role	19
Deleting a Role	20
Assigning Permissions to Roles	20

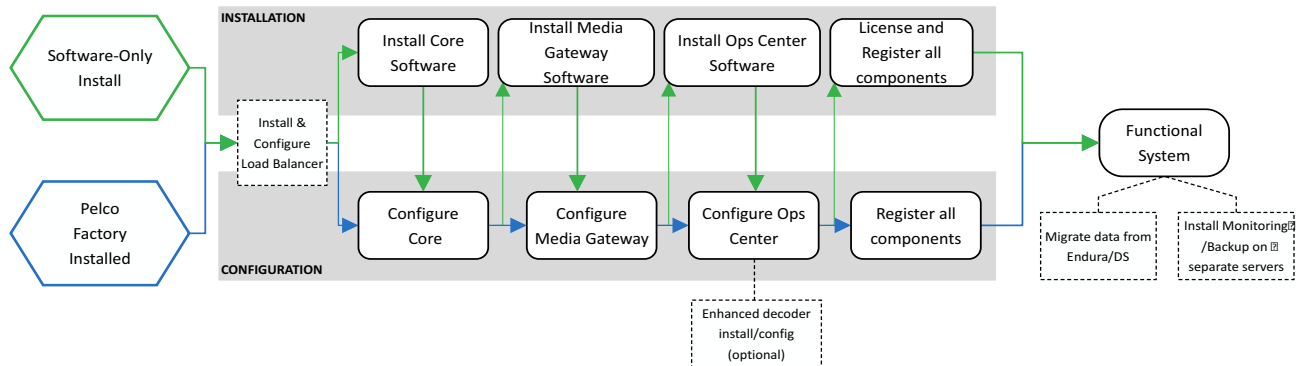
Restricting Resource Access for a Permission	20
Configuring and Managing Events	21
Using the Event Log	22
Responding to Events	22
Downloading Reports	23
Backing Up Your System	24
Running a One-Time Backup	24
Canceling a Backup In Progress	24
Checking Backup Status	24
Scheduling Backups	24
Canceling or Changing the Backup Schedule	25
Changing the Server or Password for Backups	25
Restoring the Database	25
Watching Live Video	27
Viewing Settings and Behaviors	27
Installing the Pelco Media Plugin	27
Video Overlay Controls	27
Using PTZ Controls	28
Engaging Presets and Patterns	28
Updating Core Servers	29
Updating Software (Uninstall/Reinstall Method)	29

Installation and Configuration Process Overview

The order in which you install and configure VideoXpert servers is determined by the number of servers your system contains and whether you are installing VideoXpert applications on existing hardware or purchased purpose-built hardware from Pelco.

The diagram below represents the recommended installation process for both Pelco factory-installed products, or for software-only installations on recommended hardware. It is strongly recommended that you follow the process outlined below to install and configure your VideoXpert system.

Figure 1: Recommended Installation Process Diagram



Single Server Vs Clustered Installations

Single-Server Installations You can host both the Core and Media Gateway server applications on the same physical server or on separate servers. You cannot have more than one of each server active on the network unless the servers are clustered behind a load balancer.

For Clustered Installations, complete each operation in the installation diagram for each server in the cluster before moving to the next operation.

Installing VideoXpert Core

Before installing VideoXpert, ensure that all network interfaces besides the primary NIC are disabled. Additional network interfaces may prevent the system from discovering devices. While you can cluster Core servers through a load balancer to increase the capacity of your VideoXpert network, you cannot have separate, individual Cores operating on the same network.

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

1. Run the MSI installer. If prompted, elect to run the installer as an administrator. Follow the on-screen instructions to complete the installation. As a part of the installation process, you will:
 - a. Accept the license agreement, and then click Next. Declining the license agreement will quit the installer.
 - b. Set your installation, data, and event directories, and then click Next.
2. Click Finish when the installation process is complete.

Installing an NTP Client 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. It is recommended that your NTP server be independent of your VideoXpert servers.

As a part of the setup process, you must install an NTP application separate from VideoXpert. VideoXpert has been tested with Meinberg NTP client software, versions 2.4.6 and later. The software is available at https://www.meinberg-global.com/english/sw/ntp.htm#ntp_stable.

1. Run the Meinberg installer as an administrator.
2. Follow the installation process.
3. When requested, select **Create an initial configuration file with the following settings** and specify the address of your NTP server and then click **Next**. You may add or edit servers later directly from the NTP.conf file.
4. When setting up NTP services, it is recommended that you select **Create and use a special NTP account**, and then click **Next**. This account is used only for NTP services.
5. Specify the name and password for the Windows user account that will run NTP services.
6. Finish the installation process.

Logging In

Log in to the Admin Portal to configure the system or watch video without the Ops Center application. The default user name and password for the Admin Portal are both admin. It is recommended that you change the password for the admin user after logging into the system for the first time.

1. Open a browser.
2. Enter the IP address or host name of your VideoXpert Core in the navigation bar.
3. Enter your credentials at the login page.
4. Click Log In.

Configuring your VideoXpert Site

Before you configure your system and bring VideoXpert online, you should install an NTP client and point all potential members of the system to the same NTP server.

When you login to the system for the first time, the system will prompt you for basic configuration information. You may return to the **Config** page after setting up the system to edit the system configuration.

1. Provide your **company name**. The company name is a field you will enter during initial setup; you cannot change the company name after setting up the system.
2. Provide the **Site Name**; the site name identifies the particular instance of VideoXpert. If you aggregate the VideoXpert environments, the site name will identify the various environments belonging to the aggregation server.
3. Provide an IP address for the Core.
 - a. If configuring a cluster of Core servers, select **Multiple Cores**.
 - b. Provide a Virtual IP address for your Core Servers. This is the address by which users will access the system.
 - c. Click **Add** and addresses for additional Core servers.
4. Provide the address of your Media Gateway server. If you have multiple Media Gateway servers, provide the virtual IP address of your Media Gateway cluster.

Configuring a Cluster

When configuring a cluster, you should install the WinPCAP driver from <http://www.winpcap.org> on all systems belonging to the cluster.

Reduce the TCP/IP TIME-WAIT interval by creating a DWORD value named “TcpTimeWaitDelay” with a value of “30” (representing seconds) under *HKLM\CurrentControlSet\Services\Tcpip\Parameters*.

A clustered environment requires an odd number of Vx Cores, no fewer than three. As a part of the clustering process, the system may configure additional services. For more information about clustering an environment, refer to the system design guide.

Configuring Device Discovery for Clustered Environments

When configuring your cluster, you must manually edit device discovery settings to optimize device discovery and subscriptions for your Core servers.

1. Open *Program Files\Pelco\Core\config\deviceDiscovery.yml* using Notepad or another plain text editor.
2. Set *useMulticastSourceSpoof* to 1 if using the *loadBalancerIP* and Port settings. This spoofs the device discovery virtual IP address as the discovery callback IP address, preventing each Core server in the cluster from sending and receiving device discovery messages individually; this reduces discovery times and load on the Cores in the cluster.
3. Set *loadBalancerIP* to the Device Discovery IP Address that you set on the load balancer governing your cluster; this is the IP address over which your cluster will receive device subscriptions.
4. Set *port* to the port your load balancer uses for Device Discovery.
5. Save and close the file.

Configuring Media Gateway Communications

Your Media Gateway is capable of trans-casting to suit your 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. Your network topology and need for users to access sources simultaneously should inform your choice.

1. Go to the *Config* page.
2. Select the communication method that best supports your needs.
3. Click *Save Configuration*.

Installing the Media Gateway

It is recommended that you install and configure your Core server before installing the Media Gateway application.

The VideoXpert Media Gateway serves video to users connected to your VideoXpert system. You can install the Media Gateway software on the same physical server as VideoXpert Core or on a separate server.

As a part of the Media Gateway installation process, you will provide the IP address of your Core server, even if hosting both applications on the same physical server. You will configure your Media Gateway through the Admin Portal, hosted by your Core server.

1. Run the MSI installer.
2. Accept or reject the End User License Agreement. Rejecting the EULA will cause the installer to quit.
3. When prompted, provide the IP address of your VideoXpert Core server or the virtual IP address of a cluster of VideoXpert Core servers and press Enter.
4. Follow the instructions provided by the installer to complete the installation process.

Licensing Your System

You must license your VideoXpert software to continue using the system after the initial grace period. The licenses you install determine the features to which your system is entitled and the number of sources your system can support.

You will need your activation ID and access to the Entitlement Fulfillment Server at <http://licensing.tac.com> to install a license. If you cannot connect to the Entitlement Fulfillment Server directly, you will need to transfer your Entitlement Request File to a computer with Internet access during the activation process.

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. Login to the Admin Portal and go to the *Licensing* page.
2. Click **Add**.
3. Enter your activation ID in the Activation ID box, and then click **Enter**. A Entitlement Request File, named request.bin, will be downloaded to your computer.
4. Open a new browser window or tab and go to the Entitlement Fulfillment Server at <http://licensing.tac.com>.
5. Log on to the Entitlement Fulfillment Server. You can use your user name and password or your Activation ID.
6. Click **Generate License**.
7. Click **Choose File**, select your Entitlement Request File, and then click **OK**.
8. Click **Generate License**. The Entitlement File, named response.bin, will be downloaded to your computer.
9. Return to the Aggregation Page.
10. Click **Choose file** under Upload Entitlement File.
11. Select your Entitlement File, and then click **OK**.
12. Click **Upload**.
13. Click **Save**.

RESULT:

When the process is complete, the Web portal will display the installed license, and, if applicable, its expiration date.

Adding and Updating Entitlements

The *Licensing* page contains options to update or add entitlements to VideoXpert. The page shows your current entitlements and the licenses used on the system.

- Click **Add** to add a new license. Follow the on-screen instructions to
- Place your cursor over an existing entitlement to reveal additional options; you may delete existing entitlements as necessary.

Migrating to VideoXpert

You can migrate your database from Endura or Digital Sentry to VideoXpert using the appropriate migration utility. You can migrate from your previous system permanently, or you can run your VideoXpert system in tandem with another video management system. If running systems in tandem, you can run the migration process periodically to capture the change from your Endura or Digital Sentry system and “catch up” the VideoXpert system.

Migrating from Endura to VideoXpert

It is highly recommended that you perform an SM backup from Endura Utilities before migrating to VideoXpert.

If your Endura environment contains an SM5200 operating on version 1.5 or later, you can migrate your entire Endura database from Endura to VideoXpert to ensure a relatively seamless transition between video management systems. However, due to the differences between the Endura and VideoXpert databases, the migration process translates some aspects of your Endura database for use with VideoXpert.

The migration process transfers user names, roles, permissions and the associations for all three items. Passwords for accounts in VideoXpert must be 8 characters or more; if an Endura user’s password was less than 8 characters, their password will be appended with 1s until it reaches 8 characters. For example, a password of “ABC” would become ABC11111. Users with a password appended in this way will have to change their passwords upon logging into VideoXpert.

The migration process transfers all camera names, numbers, groups, and locations to VideoXpert. Locations and Groups are converted to VideoXpert tags during the migration process. For example, a camera that was assigned to the “PTZ Cameras” group in the “Casino Floor” location in your Endura environment becomes a camera that is assigned “PTZ Cameras” and “Casino Floor” tags in your VideoXpert environment.

1. Run the *sm_export* utility.
2. Provide the address of your primary system manager, in the format *sm_export -s 192.168.0.1*.
 - By default, the backup utility will attempt to use the default administrative account to export the database. If necessary, you can specify another user account using the *-user* and *-password* arguments in the format: *sm_export -s 192.168.0.1 -user username -password password*.
 - The utility outputs a SQL file in the format *export_192.168.0.1.sql* and a JSON file in the format *migrate_192.168.0.1.json*. You can change the name of the JSON file with the *-o* argument in the format: *sm_export -s 192.168.0.1 -o outputFileName.json*
3. Run the *ve_import* utility providing the IP address of the system to which you want to import a database, the credentials of an administrative user, and the name of the file exported in previous steps. Use the format: *ve_import 192.168.0.2 user password migration_192.168.0.1.json*.

Migrating from Digital Sentry to VideoXpert

Before migrating your Digital Sentry database, you should perform a complete system backup.

The Digital Sentry export process captures users, roles, permissions, friendly names of cameras, and groups. User passwords will not migrate; upon logging into VideoXpert for the first time, a users migrated from Digital Sentry must provide a new password.

VideoXpert does not have a direct analog for Digital Sentry's groups. When migrating from Digital Sentry to VideoXpert, groups become tags, maintaining the same associations as in the Digital Sentry database.

1. Run the `ds_export` utility.
2. Provide the IP address of the server from which you want to export the database in the format: `ds_export -s 192.168.0.1`
 - The utility attempts to use the `dsserviceuser` account with the default password. If this account has changed, you can specify new credentials with the `-user` and `-password` parameters. in the format `ds_export -s 192.168.0.1 -user username -password password`
 - The utility outputs filenames in the format *migrate_192.168.0.1.json*. You can change the filename with the `-o` parameter in the format: `ds_export -s 192.168.0.1 -o outputName`
3. Run the `ve_import` utility providing the IP address of the system to which you want to import a database, the credentials of an administrative user, and the name of the file exported in previous steps. Use the format: `ve_import 192.168.0.2 user password migration_192.168.0.1.json`.

Configuring Storage

From within VideoXpert, you can add cameras to or remove cameras from recording pools. For more advanced recording controls, connect to your storage devices directly.

It is recommended that you assign cameras through the VideoXpert Admin Portal and not through the storage manager's interface. Camera assignments made through the storage manager's interface may not be reflected in the Admin Portal, resulting in inaccurate reports and camera searches or filters based on recording status and recording assignments. The VideoXpert Admin Portal will not reflect any cameras unassigned through the storage manager's interface.

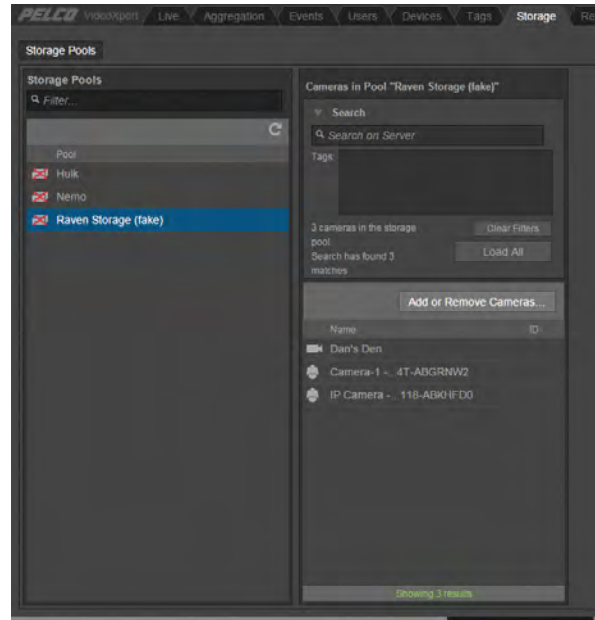


Figure 1: The Storage Page

1. Go to the Storage page.
2. Select the recording device or pool to which you want to add or remove cameras, and then click **Add or Remove Cameras**.
3. Select the cameras you want to add or remove from the pool. You can sort the list of available cameras using the tags or search box above


Using Digital Sentry Servers as VideoXpert Storage


Digital Sentry servers operating on version 7.9 or later can be used as VideoXpert storage servers. Your Digital Sentry server must have the FrameServer service, Pelco API, and NSM REST services installed to support VideoXpert.

Digital Sentry servers should not be pooled.

Discovering and Commissioning Devices


Your system continually searches the network to discover devices relevant to VideoXpert. Discovered devices are not available to users within the system until they have been commissioned to operate within the system. The Devices page contains a registry showing devices that the system has discovered and an interface for commissioning or decommissioning discovered devices.

Devices displaying a  in the list require a license to be commissioned. Upon discovery, Media Gateway and Storage Devices immediately begin a 7-day grace period. During the grace period, you may commission and use the device, but it will become unavailable if the grace period lapses and you have not applied a license applicable to the device. When you install a license for devices currently operating within their grace period, the license is automatically applied.

Devices that do not display a  in the list do not require a license to be commissioned and, by default, are automatically commissioned upon discovery.

NOTE: Any video source connected through Digital Sentry servers operating as VideoXpert storage appear twice in the Devices list. VideoXpert discovers the source individually, and then again as a member of the Digital Sentry server through which it is recording. The Digital Sentry-discovered device displays the IP address of the DS server through which it is discovered, rather than the source IP address.

Commissioning and Decommissioning Devices

Devices containing a  consume a license seat when you commission them. The number of seats for each particular license is listed in the *License Summary* section of the page. You can reclaim seats by decommissioning devices, or add additional seats by installing licenses.

NOTE: If operating on a grace period, it may take up to 30 minutes to commission storage managers. If you receive an error when commissioning a storage manager, log out and back in, and then try commissioning the storage manager again.

1. Go to the Devices page.
2. Select the devices you want to commission or decommission.
3. Click *Commission* to make the device available within VideoXpert or *Decommission* to render devices unavailable.

Deleting Devices from the Registry

Once discovered, a device will persist in the system's device registry until deleted, even if the device no longer exists on the network.

1. Go to the Devices page.
2. Select the device you want to delete.
3. Click *Remove*.

Editing Source Names and IDs

Users with appropriate rights can edit the name and ID of a video source. IDs are not assigned by default, enabling users to number sources as they please. Both source names and IDs can be used to filter sources.

The ability to edit source names and IDs is governed by permissions.

1. Go to the Live page.
2. Right-click the source you want to edit, and click Edit.
3. Edit the name and ID of the source.
4. Click OK.

Changing Source Settings

From the *Live* page, you can right click a source and opt to go directly to the web interface for the source (where applicable), and change settings directly for the camera or source device. For devices connected through a Digital Sentry server acting as VideoXpert storage, you cannot access the camera settings page in this way as the camera will attempt to send you to the address of the DS server rather than to the direct IP address of the camera.


Changing certain settings may interrupt video streaming or recording for a source within the VideoXpert system. For example, changes made to video compression settings for a particular source may not register with the Media Gateway for up to 15 minutes; during this time, users will be unable to stream video from the source.

Aggregating Systems

VideoXpert Ultimate Core systems support an aggregation server, providing centralized access to a series of member systems. Through aggregation, you can maintain a distributed network within a single VideoXpert instance.

Systems belonging to the aggregation server are referred to as “member systems”; all devices and video for the member system are 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 may have access the member system directly to change settings,

When adding a member system to the aggregation server, you will use the **aggregator** account. This user account is visible only to VideoXpert system administrators. and authorizes connections between the aggregation server, the member system you are aggregating, and other member systems. The system administrator can change the password for the **aggregator** user, but the account cannot be otherwise modified or deleted.

1. Go to the Aggregation page.
2. Click Add System, or click  to edit a system.
3. Provide the IP address of the system you want to aggregate in the Server Address field. If aggregating a clustered system, enter the IP address of the load balancer governing the cluster of systems you want to aggregate.
4. Enter the port number the system uses for HTTP/HTTPS communications in the Port field.
5. Enter the password for the **aggregator** user.
6. Click **Add System** or **Save**.

Tags

Tags are custom attributes that users with sufficient rights can create and assign to cameras and devices, helping organize resources within your VideoXpert environment. Tags can help users find items in searches where normal search fields (name, number, etc.) may not reveal all the right results. In search fields, tags populate as tokens, ensuring that users cannot search for a tag that does not exist.

The ability to assign tags is determined by permissions. Likewise, a search for a particular tag will only reveal components a user has permission to view.

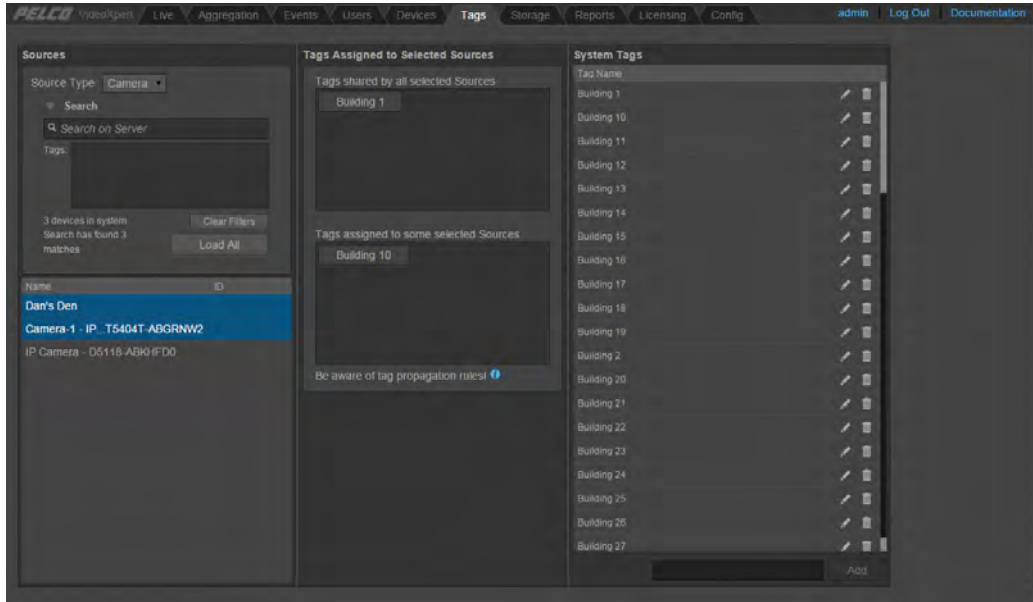




Figure 1: The Tags Page

Creating Tags


1. Go to the Tags page.
2. Enter the name of the tag you want to create in the field under System Tags.
3. Click Add.

Editing Tags

Editing a tag does not affect tag assignments; any resources to which the original tag was assigned will reflect the edited tag title.

1. Go to the Tags page.
2. Click  next to the tag you want to edit.
3. Click .

Deleting Tags

On the Tags page, click  next to any tag you want to delete.

Assigning Tags to Sources

1. Go to the Tags page.
2. Search for the source or sources to which you want to assign tags.
3. Select the source or sources to which you want to assign tags.
4. In the *Tags shared by all selected sources* box, type the name of the tags you want to assign.

Managing Users

Aside from *superadmin*, users do not exist at the aggregation level; when users log in, their credentials are authenticated directly against aggregated systems. A user must be authenticated by a system to view video from the system, and must possess the appropriate role to view restricted cameras on the system. As *superadmin*, you can use the Manage Users page to add or remove users from member systems; you can also assign roles to users, determining the level of access they have to video for each system.

You must be logged in as *superadmin* to access the Manage Users page. When adding users to Endura systems that authenticate users through an Active Directory (using LDAP), you should create the users within the Active Directory before you add them through the Web portal.

Aggregated systems must be running SM5200 version 1.5 or later to allow user management.

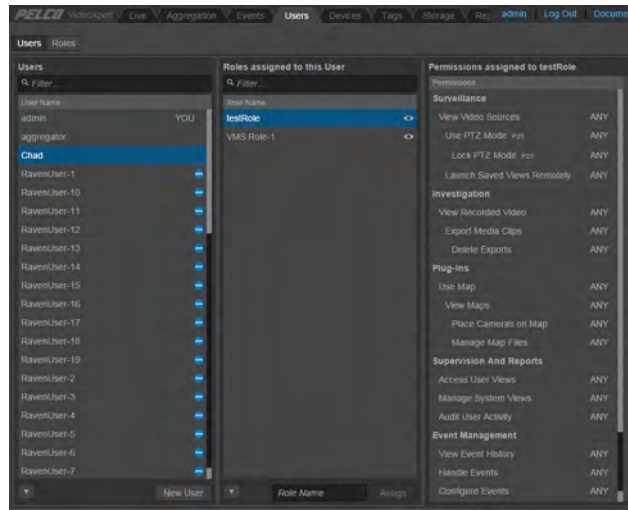


Figure 1: The Users Page and Tab

Adding Users

When adding users to the system, you give them a temporary password. Upon logging in for the first time, the system will require users to change their passwords.

1. Go to the Users tab on the Users page.
2. Click New User.
3. Enter a user name and password.
4. Click Save.

Duplicating Users

Duplicating a user creates a new user with the same name as another user, but does not grant the new user the same permissions as the original. You must assign permissions after duplicating a user.

1. Go to the Users tab on the Users page.
2. Click ▼ and select Duplicate.
3. Enter a password for the user. You can also change the user's name.
4. Click Save.

Renaming Users

1. Go to the Users tab on the Users page.
2. Select the user you want to rename.
3. Click ▼ and select Rename.
4. Enter a new user name.
5. Click Save.

Deleting Users

1. Go to the Users tab on the Users page.
2. Select the user you want to remove.
3. Click ▼ and select Delete.
4. Confirm your selection.

Deactivating and Activating Users

You can prevent a user from accessing the system for a period of time without deleting the user from the system by deactivating the user. You can then re-activate the user at a later time.

Deactivated user accounts still appear in the list of users, but are struck through.

1. Go to the Users tab on the Users page.
2. Select the user you want to activate or deactivate.
3. Click ▼ and select Activate or Deactivate.

Resetting Passwords

By default, users must change their passwords every 60 days. Users with appropriate permissions can either reset users' passwords or force users to change their passwords early.

Resetting a user's password will allow you to grant the user a temporary password. Upon logging in, the system will require the user to change his or her 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 he or she is locked out of the system due to failed login attempts or let the password change timer lapse.

1. Go to the Users tab on the Users page.
2. Select the user whose password you want to affect.
3. Click ▼ and select **Reset Password** or **Force User to Reset Password** depending on your application.
4. If you selected **Reset Password**, provide a new password for the user, and click Save.

Assigning Roles to Users

1. Go to the Manage Users page.
2. Select the user for whom you want to assign or remove roles.
3. Click the checkboxes corresponding to the roles you want to add or remove from the user. You can filter roles using the box under Assigned Roles. Selecting a system provides the user with all roles within the aggregated system.

Managing 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.

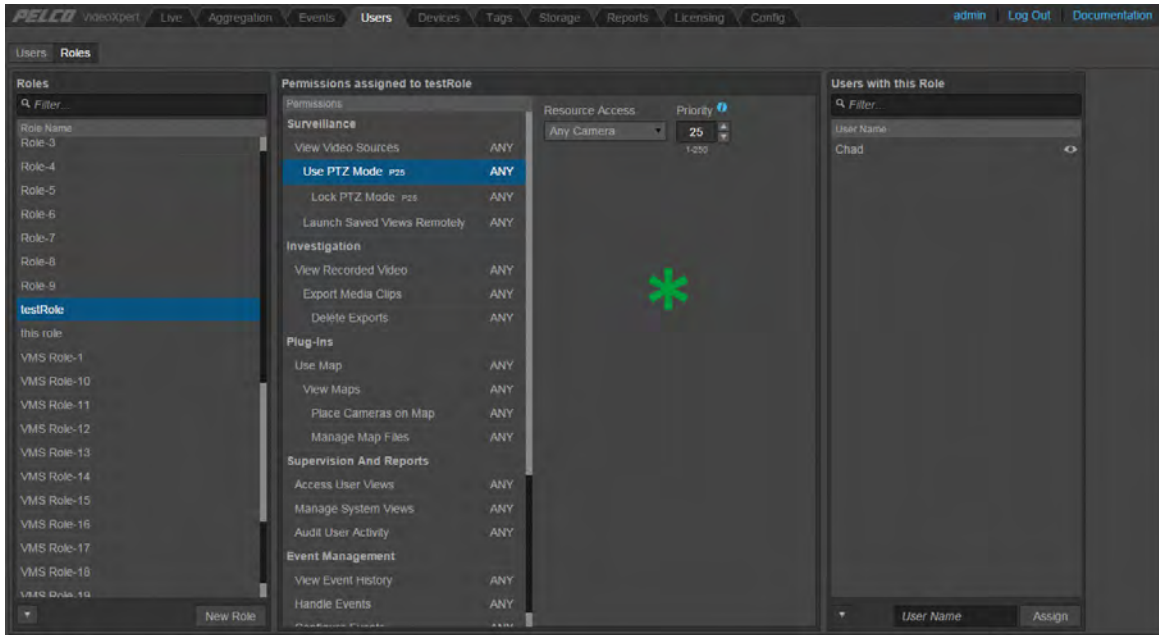


Figure 1: The Roles Tab on the Users Page

Creating a Role

1. Go to the Roles tab on the Users page.
2. Click New.
3. Provide a name for the new Role
4. Click **OK**.

Renaming a Role

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

1. Go to the Roles tab on the Users page.
2. Click ▼ and select Rename.
3. Provide a new name for the role. Click **OK**.

Duplicating a Role

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

1. Go to the Roles tab on the Users page.
2. Click ▼ and select Rename.
3. Provide a name for the duplicated role, and click OK. Deselect *edit permissions now* if you want to leave the duplicate roles with identical permissions.

Deleting a Role

1. Go to the Roles tab on the Users page.
2. Click ▼ and select **Rename**.
3. Click **Delete**, and confirm your selection.

Assigning Permissions to Roles

By default, a new role contains no permissions. When assigning permissions to a role, you can determine resource restrictions, if any, for the permission.

Permissions assigned to a user display the resource restrictions associated with the permission.

1. Go to the Users page and select the Roles tab.
2. Select the role for which you want edit permissions.
3. Select the permission you want to assign or edit.
4. Select the Resources the user can access.
 - **Any Camera** indicates that the permission is not restricted for the role; the permission applies to all cameras.
 - **Restricted Resources, Selected Cameras, etc** allows you to restrict the permission to a particular set of resources. (Do restricted cameras start out with all permissions?)

Restricting Resource Access for a Permission

Changing a permission's **Resource Access** setting to **Selected Cameras** disables all cameras for the permission. You must then assign cameras to the permission, making them available to users possessing that permission.

Use the Search Cameras field to quickly determine whether or not the permission allows access to a camera.

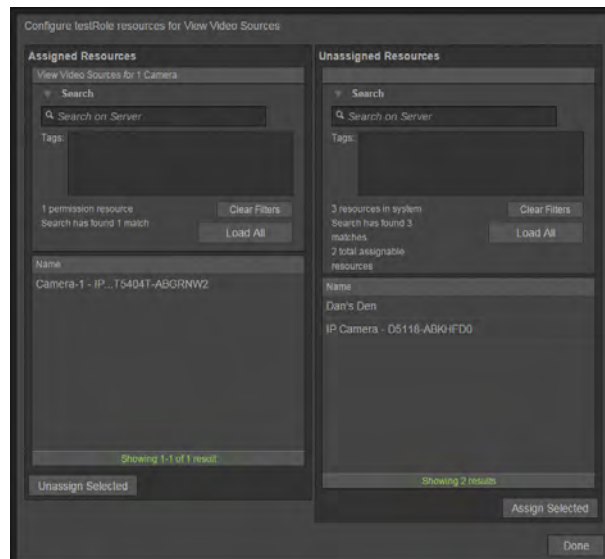


Figure 2: Selecting the Resources Available to a Permission

1. When Resource Access is set to Selected Cameras, click Configure Resources.
2. Use the search fields to locate cameras you want to assign or unassign. Assigned cameras are available to users possessing the permission; unassigned cameras are not.
3. Click **Done** when you have finished assigning resources to the permission.

Configuring and Managing Events

On the Manage Event Types page, you can configure the way in which the system will report each event and the users who will receive notifications for each event type.

1. Go to the Events page, and select the *Manage Event Types* tab.
2. Select the event you want to configure.
3. Determine whether or not the event will be recorded in the event log.
4. Set the severity of the event, 1 indicating a low severity and 10 indicating high severity.
5. Determine whether or not the event is reported in a banner; enabling a banner will cause the system to send notifications through both the Admin Portal and the Ops Center. If you enable a banner:
 - a. Determine whether or not to allow the snooze function for the event, and set the number of minutes for which users can snooze the event.
 - b. Select the roles for users who will receive event notifications.
 - c. Set camera associations for the event. When the event occurs, the notification banner will include a link to associated cameras.
6. Click **Save**.

Using the Event Log

By default, the Event Log contains a list of events that have occurred in the last 30 days, initially sorted between events that require attention, and events that have either been acknowledged or do not require acknowledgment. Use the Filter functions to find specific events in the log. Select events in the log to reveal more information and options to respond to the event.

Responding to Events

Users with appropriate permissions can respond to events that trigger notifications. Users' responses to events are logged with the system, indicating whether or not the event has been acknowledged and by whom.

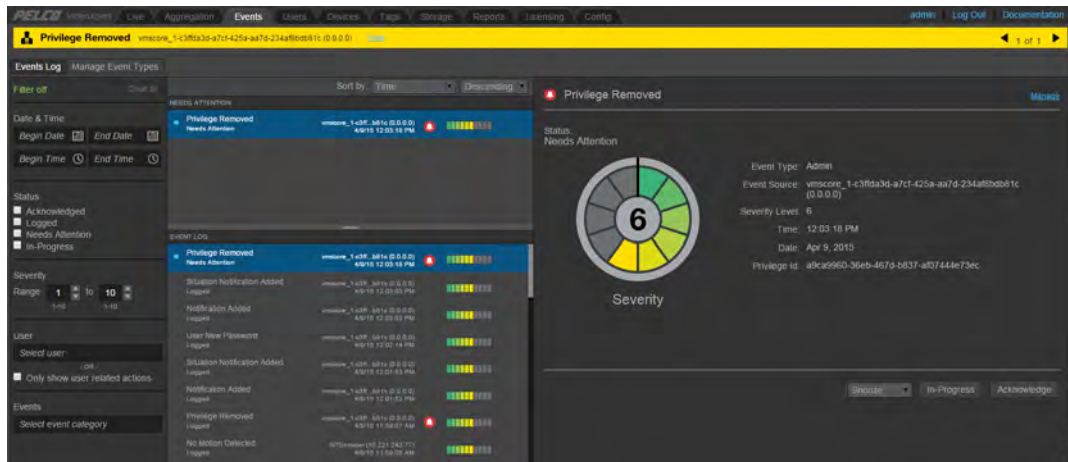


Figure 1: The Event Log

1. Go to the Events page. If an event triggers a notification banner, you can click the banner to go to the Events page.
2. Select the event requiring your attention.
3. Select an action.
 - **Acknowledge** indicates that you have alleviated the condition causing the event.
 - **In Progress** indicates that a user is in the process of correcting an event condition or performing work on the system that may result in additional events.
 - **Snooze** Hides an event notification for up to 60 minutes. The snooze function only affects notifications locally; it does not hide event notifications from other users.

Downloading Reports

From the Reports page, you can download reports from the system. Reports are exported in CSV format contained within a ZIP archive.

NOTE: In all reports, devices discovered through Digital Sentry servers display the IP address of the DS server through which they are connected rather than their direct IP address.

1. Select the reports you want to download.
2. Set start and end dates for the report you want to download. Reports based on events logged by the system must be captured within the event-retention time period; by default, the system stores events for 30 days.
3. Click Export Reports.

Backing Up Your System

It is recommended 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.

You can use the `backupInteractive` script to perform one-time backups or to schedule daily backups. If your system contains a single core, you may back up to a local or network drive; if your system contains a cluster of Cores, you must backup to a network drive. If your cluster contains more than one replica set, you must use Mongo Management Services or another application to back up your system.

A system backup will contain the system database, including the previous 30 days' events. Backups will not capture exported video or any settings that you may have changed outside the Admin Portal application (for example, changes made to configuration scripts directly).

NOTE: As a part of the backup process, you must provide administrative credentials to the backup application. Your credentials enable the backup application to access your Core servers, but do not protect backup data or the settings for the backup application.

Running a One-Time Backup

Before you run the application, you will need to know the IP address of a Core server in your VideoXpert system; if your environment contains multiple Cores, any Core will do. You must also know the directory to which you want to back up files, network or local.

While running a backup, it is important that you do not stop Core or MongoDB services running on the server. Doing so will cause the backup process to fail.

1. Run the `backupInteractive.exe` file as an administrative user.
2. Enter the IP address of a Core server in your VideoXpert system.
3. Provide the password for your system's **admin** user. Only the **admin** user can perform backups.
4. Press 2 to start a backup.
5. Provide the path of the folder that will receive and store the backup.
6. When prompted, provide the domain and user name of a user with credentials to the network save in the format `domain\username`.

Canceling a Backup In Progress

Press 3 to cancel a backup in progress. When you cancel a backup, the incomplete backup files will remain in the destination folder.

Checking Backup Status

Press 4 to check the status of a backup that is currently in progress.

Scheduling Backups

The `backupInteractive` application allows you to perform daily backups at a time you specify. You can specify the total number of backups to store. When the application reaches the limit, it will overwrite the oldest daily backup.

1. Run the `backupInteractive` application as an administrative user.
2. Enter the IP address of a Core server in your VideoXpert system.
3. Provide the password for your system's **admin** user. Only the **admin** user can perform backups.
4. Press 4 to schedule a periodic backups.
5. Provide the path of the folder that will receive and store the backup. If required, enter the user name and password required to access the network folder specified for the backup.

6. Provide the hour (in 24-hour daily format) during which the system will perform the backup.
7. Provide the minute during which the backup will begin.

Canceling or Changing the Backup Schedule

After you have scheduled backups, you cannot change the schedule for backups; you must cancel the backup, and then schedule periodic backups again.

Canceling a backup schedule while a backup is in progress will cancel the current backup, leaving an incomplete backup file.

Press 6 to display the current configuration of periodic backups.

Press 5 to cancel periodic backups.

Changing the Server or Password for Backups

The application stores the address of the server for which from which it takes backups, and the password of the *admin* user for that server.

Within the application, press 7 to change the password for the *admin* user against which you authenticate backups, or to change the address of the server from which you pull backups.

Restoring the Database

Before you attempt to restore a database, ensure that VideoXpert Core is installed, but not configured, on all servers to which you are restoring the database. You cannot restore a database backup on a system that has already been configured.

You can restore a backup to servers utilizing the same configuration as the server setup from which the backup was taken, or a different configuration. However, just as the VideoXpert backup utility only supports backups for single replica-set clusters, you can only restore a backup to a system containing a single replica set.

All filepaths specified assume that you have installed the Core server application to the default directory, *C:\Program Files\Pelco\Core*. When running commands or opening a command prompt as a part of this process, you must execute commands as an administrator.

1. Copy the *configuration.txt* file from your backup to all of your Core servers. The location of the configuration file doesn't matter.
2. On each Core server, open a command prompt and run the following command, providing the path to the *configuration.txt* file you copied to the system:

```
C:\Program Files\Pelco\Core\tools\restoreSystemId <path to configuration.txt>
```

3. Open the Admin Portal and configure your server.

4. On any one of the Core servers, run:

```
C:\Program Files\Pelco\Core\tools\dumpClusterConfig
```

5. On all servers, run *services.msc* and stop the Core service.
6. Run *C:\Program Files\Pelco\Core\tools\stopMongoon* all Core servers.

7. On each Core server, replace the following directories with corresponding folders from your backup file:
 - *C:\ProgramData\Pelco\Core\db\data\mongod\admin*
 - *C:\ProgramData\Pelco\Core\db\data\mongod\aspenDb*
 - *C:\ProgramData\Pelco\Core\db\data\mongod\eventsDb*
 - *C:\ProgramData\Pelco\Core\db\data\mongod\situationsDb*
8. On each server containing a *C:\ProgramData\Pelco\Core\db\data\configsvr<X>* directory, where <X> equals 1, 2, or 3, replace the directory with the applicable folder from the backup.
9. On each server, run *C:\Program Files\Pelco\Core\tools\startMongo*.
10. On any one of the Core servers, run *C:\Program Files\Pelco\Core\tools\dropExports*.
11. On the server against which you ran the “dumpClusterConfig” script in previous steps, run:
C:\Program Files\Pelco\Core\tools\restoreClusterConfig
12. On each Core server, run *services.msc* and restart the Core service.

Watching Live Video

The Live page provides access to live video. Live video is subject to the network bandwidth restrictions set by your administrator and the transcoding limitations of aggregated systems. Surpassing either limitation will prevent you from watching additional video streams.

1. Go to the Live page.
2. Click one of the layout icons to arrange cells in your workspace
3. Locate the camera or cameras you want to view in the sidebar. You can sort cameras by location or group; you can also search for cameras by name or number.
4. Add the camera to the page. You can double-click the camera to add it to the next video cell, or you can click and drag the camera to the video cell of your choice.

Viewing Settings and Behaviors

Click Viewing Settings to reveal settings determining the behavior of video playback. Viewing settings are available on the Live or Search pages, but affect video playback on any page of the interface.

Display camera names on videos: Select whether or not camera names appear over your video cells.

Video Quality Preference: Choose whether video performance aims for better picture quality or higher frame rates.

Connection Speed: Set your connection speed to match the connection speed of the client you are using to access the Web portal. Your connection speed setting determines the quality of video streamed through the Web portal; setting your connection speed too high or too low (by comparison with your client's actual connection speed) can impact video performance. The client-side Connection Speed setting is subject to bandwidth restrictions set by the administrator.

Sidebar: Choose whether the sidebar, containing cameras, viewing settings, and server information, appears on the left or right side of the interface.

View Video Using: Choose whether you want to view video using the Pelco Media Plugin (PMP) or your browser's native motion JPEG viewer. The PMP displays H.264 video, resulting in better picture quality, a higher framerate, and potentially lower resource usage, but it is only available in certain network configurations (typically LAN). It is recommended that you stream video using the PMP when available.

Installing the Pelco Media Plugin





The Pelco Media Plugin (PMP) enables you to view H.264 video through your Web browser. To view video using the PMP, you must be able to receive UDP traffic directly from the system containing the camera you want to view; the port over which you receive the UDP traffic is auto-negotiated when you access a PMP video stream. This typically means that you should be able to use the PMP when you have access to systems over LAN, but you will likely be limited to motion JPEG viewing when accessing systems over WAN.

It is recommended that you update your graphics driver before installing the Pelco Media Plugin.


1. Click the link in the web interface. If you have Internet access, the Web portal will attempt to direct you to the Pelco Media Plugin page on www.Pelco.com. If you do not have Internet access, you will download the version of the PMP stored directly on the Vx server through which you're accessing the Web portal.
2. Run the PMP installer.
3. Restart your Web browser.




Video Overlay Controls

Place your mouse cursor over a video cell to reveal additional controls.

	Opens one or more video cells in a new browser window. Click over an individual cell to expand the cell in a separate browser window; click the icon in the sidebar to expand your entire workspace in a separate browser window.
	Closes a video cell; open video cells consume the resources of the system from which the video stream originates. Closing a stream makes those resources available to other users.
	Enables and disables PTZ control. Click when the icon is gray to enable PTZ; click when the icon is blue to disable PTZ. PTZ controls are only available to PTZ cameras in Live view, and are subject to user roles and prioritization rules.
	Plays back video; playback controls are available when previewing recorded video.


Using PTZ Controls

When watching live video, you can issue PTZ controls to cameras identified by the dome icon . PTZ controls are subject to user permissions (determined by roles) and prioritization rules. If your user account does not have the appropriate role or permissions to issue PTZ controls to a camera, or a user with a higher priority is already controlling the camera, you will be unable to control the camera.

- Click the PTZ icon  to enable PTZ controls.
 - Pan and Tilt: Click within the video to center the camera's field of view on your cursor. You can double-click to center the camera's field of view and zoom in on a particular point.
 - Zoom: Use the slider or the scroll wheel on your mouse to zoom in or zoom out.
 - Lock: Click the lock icon  to prevent lower priority users from controlling the camera. Priority is determined by user roles defined within each aggregated system. The camera will automatically unlock after 15 minutes or when the user who has locked the camera closes the video stream.
- Click the PTZ icon  again when you have finished positioning the camera to disable PTZ controls.

Engaging Presets and Patterns

When PTZ controls are engaged for a camera, you can execute PTZ presets and patterns. A preset is a set PTZ position; calling the preset will move the camera to the preset location. A pattern is a series of presets, causing the camera to move at a particular interval. Presets and patterns are set and stored on the camera; you must go to the camera's interface to set or change presets and patterns.

- Click the PTZ icon  to enable PTZ controls.
- Right click within the cell containing the PTZ-enabled camera, and select whether you want to engage a pattern or preset.
- Select the pattern or preset you want to engage.

Updating Core Servers

It is recommended that you update your Core server by running an updated installer; the upgrade process preserves your configuration and database. During the update process, the Core will fall offline and the system will restart. Ensure that you are prepared for the Core to go offline, either by failover or by scheduling maintenance at an appropriate time before attempting to update the Core.

Updating Software (Uninstall/Reinstall Method)

The uninstall process does not delete your data and events folders. If you must uninstall the Core software before installing a newer version of the software, you may recover your data and events manually.

When reinstalling the Core software, install in the same directory as your previous installation. A prompt will appear, indicating that you have previous data, and asking whether or not you want to incorporate that data. Affirm that you want the data, and your installation will be restored.

Declining to restore the data will cause it to be deleted permanently.



by **Schneider** Electric

Pelco by Schneider Electric

3500 Pelco Way Clovis, California 93612 USA

(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 2015, Pelco, Inc.
All rights reserved.