COMPLETEVIEW

VERSION 7.6.0

Table of Contents

CompleteView Functional Overview

CompleteView lies at the heart of Salient Security Platform, which represents a family of interrelated software components, each specializing in providing a particular aspect of video and other types of security.

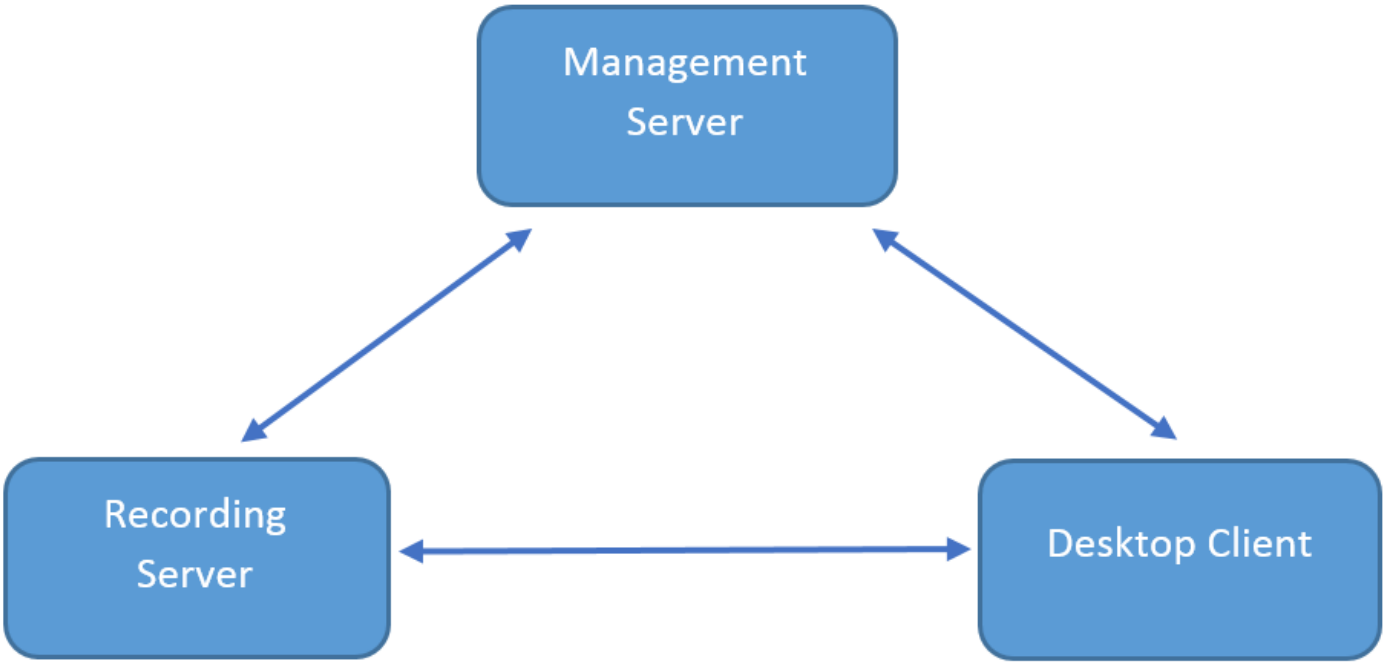
CompleteView is the engine of Salient Security Platform's VMS. In its simplest form, a Video Management System consists of Cameras, Video Servers and Video Clients.

Cameras generate video streams. Servers accept video streams as input, perform video stream processing, record video, and make live and recorded video available to video clients. Clients present live and recorded video from servers to end-users.

CompleteView implements these functions through three primary components.

Core Components

The core components of CV include the Management Server, Recording Server, and Desktop Client.



The above diagram illustrates these core components and their interactions. Components will be able to interact with one another through service calls and by listening to events. Management server will serve as central repository of all data related to the entire system. Recording server will be responsible for all VMS functionalities and services. Desktop client will be the user facing tool for both administering and monitoring the system. All other components, servers and clients will be built based on these core components.

Recommended System Specifications

At this time, CompleteView Recording Server, Management Server, and Desktop Client are certified to run on the following operating systems:

- Windows 10, 11
- Windows Server 2016, 2019, 2022

In addition, the Desktop Client may be run on Windows Server 2025.

No other operating systems are currently certified and the recommendations below reflect the minimum acceptable configuration for that component. CompleteView is only certified to run on x86-64 based platforms.

Desktop Client

Minimum recommended software configuration:

- Microsoft .NET v4.7.2
- VS 2019 C++ redistributable
- Microsoft DirectX
- Microsoft Direct3D

Minimum recommended hardware configuration:

- Intel Core i3 Processor
- 4 GB of system memory
- 10/100/1000 Ethernet Controller
- A graphics accelerator with 256MB of video memory
- 1920x1080 resolution

Recording Server

Minimum recommended software configuration:

- Microsoft .NET v4.7.2
- Microsoft DirectX

Minimum recommended hardware configuration:

- Intel Core i3 Processor
- 4 GB of system memory
- One PCI-e expansion slot per each Gen II video capture card*

*Gen I capture cards are not supported in CompleteView.

Management Server

Minimum recommended software configuration:

- SQL Server 2016, 2017, 2019, 2022*
- Microsoft .NET Runtime 8.0.4 x64
- Microsoft DirectX
- If using SQL Express, use ODBC Driver 18.0 (or newer, as appropriate) for SQL Server (available at **https://learn.microsoft.com/en-us/sql/connect/odbc/download-odbc-driver-for-sql-server?view=sql-server-ver16#download-for-windows**).

*The SQL Server does not have to be installed on the Management Server itself, but the Management Server does need access to wherever the SQL Server resides. In addition, CompleteView will work with more robust versions of SQL Server such as Enterprise, but SQL Express is the minimum version required for functionality.

Minimum recommended hardware configuration:

- Intel Core i3 Processor
- 8 Gigabytes (GB) of system memory
- 10/100/1000 Ethernet Controller

A Word About Databases

As part of the setup process, previous versions of CompleteView may have installed SQL Server Express as the default database. The current version of CompleteView continues to support SQL Server Express 2016, 2017, 2019, and 2022. If upgrading from a previous version of CompleteView using a supported version of SQL Express, no changes will be made to the existing database, but a new database will be created using the included migration utility. SQLite is not supported in versions 7.0.0 and newer. The SQLite database will need to be upgraded to SQL Server Express, either during Management Server installation via the integrated migration utility or as installed separately by an Administrator before CompleteView installation.

VMS System Network Communication

The CompleteView relies upon Microsoft Windows client/server network services to accomplish communications between system components. CompleteView servers use a set of well-known network ports and protocols to communicate with client systems and with other servers over the network. The ports and protocols servers use to communicate with IP cameras vary according to camera manufacturer and model. Nonetheless, most cameras adhere to one or more industry standard video compression and streaming protocols that provide streaming services on well-known ports or dynamic port ranges.

Firewall appliances, host-based firewalls, and Internet Protocol security (IPsec) filters are important components that must be implemented to secure a network. However, if these technologies are configured to block ports or application protocols used to provide a specific service such as video streaming, that service will no longer be available in response to client requests.

When planning a VMS network, it is imperative to ensure that network security requirements are harmonized with system functional requirements. Protocol and firewall requirements should be audited for each workstation and server in the system. IPsec filters and firewall exceptions should be carefully configured to ensure that all needed protocols and ports are available to every network member and, more importantly, that only needed protocols and ports are allowed.

Time Synchronization

For an optimal CompleteView experience, all components of a deployment (Management Server, Recording Servers, cameras, peripherals, clients, etc.) should be synchronized to the same system time.

Time synchronization is normally handled by network administrators using the Network Time Protocol (NTP) to synchronize all system clocks with a reference clock, usually via the Windows Time service (W32Time). Other methods may be employed that adhere to local security and other IT policies.

Microsoft Windows Integration

The CompleteView video management system fully integrates with Microsoft Windows operating systems and networking technologies.

CompleteView programs are Windows applications that run in the foreground, and incorporate a Graphical User Interface (GUI) to provide user interaction with the system.

CompleteView server programs are Windows system services that run in the background, do not incorporate a GUI, and whose primary purpose is to service requests from client and utility programs.

CompleteView Windows System Services

CompleteView server components run in the background as Windows System Services. Generally, services provide core operating system features, such as Web serving, event logging, file serving, help and support, printing, cryptography, and error reporting. Services do not incorporate a GUI, and load automatically as part of application or operating system startup processes.

During installation, CompleteView automatically configures server services to start automatically as part of the operating system startup process. Their primary purpose is to service requests received via the Windows TCP/IP service from CompleteView client and utility programs.

Services do not incorporate an application GUI, but they do have a set of properties that are configurable from the Services Snap-in in the Windows Computer Management Console.

CompleteView Port Information

Windows Firewall drops incoming network transport layer (UDP/TCP) traffic that does not correspond to pending requests (solicited traffic) or unsolicited traffic that has not been specified as a Firewall exception to be allowed. Windows Firewall can also be configured to block outgoing traffic. By default, Windows Firewall blocks all unsolicited traffic for server, peer, or listener applications and services. Therefore, Firewall exceptions must be configured in order for the CompleteView to function properly. The exact list of exceptions needed for an individual system will differ depending upon the system configuration, CompleteView options, cameras deployed, and third party extensions installed. Care must be taken to ensure that all needed Firewall exceptions are defined and more importantly, that only needed exceptions are defined.

If a system shipping with CompleteView was purchased from Salient, all firewall rules have been preconfigured.

Management Server Port Information

Management Server to Recording Server

Port	Type	Function
4502*	HTTP	Saving and retrieving configuration, operational state
4503	HTTPS	Saving and retrieving configuration, operational state
4242*	TCP	Operational info, real time status updates
4245*	TCP over TLS	Operational info, real time status updates

Recording Server Port Information

Recording Server to Cameras

Port	Type	Function
554	TCP	Camera RTSP
80	TCP	Camera API & RTSP

Recording Server General

Port	Type	Function
25	TCP	SMTP
389	TCP	Active Directory

Desktop Client Port Information

Desktop Client to Recording Server

Port	Type	Function
4502*	HTTP	Saving and retrieving configuration, operational data
4503	HTTPS	Saving and retrieving configuration, operational data
4242*	TCP	Video & audio data, operational info, real time status updates
4245*	TCP over TLS	Configuration and operational data
4255	TCP	Restarting the Recording Server service and pushing updates
8098	TCP	Video Wall

Desktop Client to Management Server

Port	Type	Function
8095*	HTTP	Configuration and operational data
8096	HTTPS	Configuration and operational data

Remote Applications Port Information

TouchView to Recording Server

Port	Type	Function
4502*	HTTP	Configuration and operational data
4503	HTTPS	Configuration and operational data

Web Client to Recording Server

Port	Type	Function
4502*	HTTP	Configuration and operational data
4503	HTTPS	Configuration and operational data

TouchView to Management Server

Port	Type	Function
8095*	HTTP	Configuration and operational data
8096	HTTPS	Configuration and operational data

Peripheral Port Information

Cameras to Recording Server

Port	Type	Function
6970-7226	UDP	UDP Video, audio, events over RTP
7775	TCP	ONVIF event handling
3702	UDP	Multicast device discovery

Mandatory Firewall Exceptions

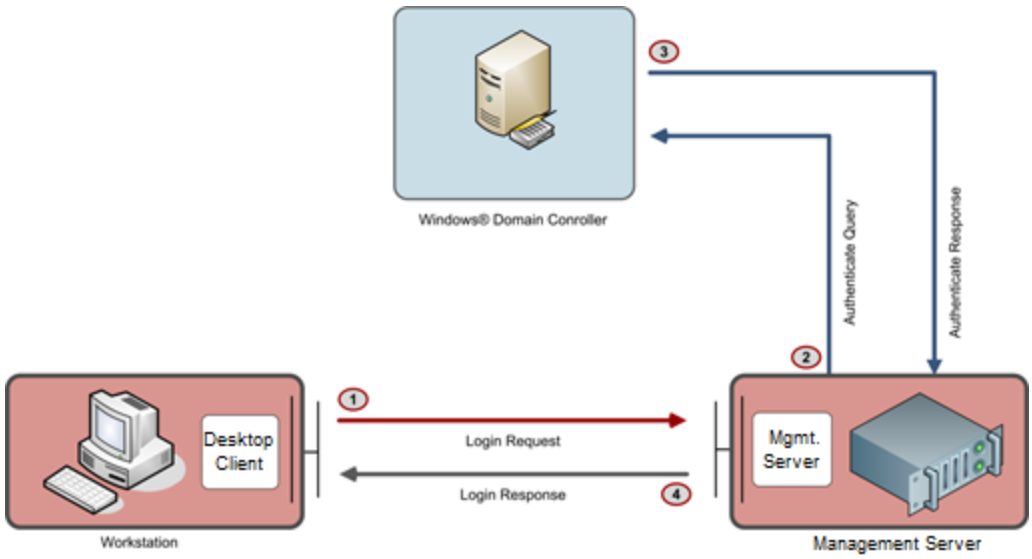
*Ports denoted with an asterisk above are required for CompleteView functionality.

Optional Firewall Exceptions

Depending upon system and component configuration, additional CV firewall exceptions may be required as noted above.

Active Directory Connector

CompleteView systems deployed on a Microsoft domain network can be integrated with the network Active Directory (AD) directory service in order to simplify user/group management, and to facilitate user authentication. Microsoft Active Directory is a distributed directory service that enables secure, centralized management of the entire network. AD is a central repository of information and integrated services that provide the means to manage network resources including users, services, and devices. AD is installed on a Windows network server that is configured for the Domain Controller (DC) role.



The CompleteView Active Directory Connector allows the System Administrator to define CompleteView users, groups, and permissions as part of the Windows domain controller Active Directory users/groups schema. In this way, Active Directory Connector eliminates the need to manually maintain identical user/group configurations across multiple CompleteView servers in a system. User/group configurations are maintained in a central location as part of the AD schema, and user authentication is performed by CompleteView servers against user credentials stored in the network Domain Controller Active Directory.

When implemented, an Active Directory Connector can only be deployed within a single domain.

When using Active Directory Connector, all CompleteView workstation and server computers must be members of the domain.

Active Directory integration is a feature of CompleteView Enterprise edition only.

For information on configuring CompleteView to work with Active Directory, see **Common Settings Services**.

CompleteView License Management

CompleteView systems are licensed on a per camera basis. Every Recording Server in a CompleteView must be provisioned with a License Key. The server License Key includes Feature Keys for IP Cameras recording to that server, as well as Feature Keys to enable system-wide functionality common to all Recording Servers in the system. **Note:** Systems with CompleteView pre-installed are pre-licensed. If upgrading from CompleteView 4.X and the new Feature Key has been applied, you may skip this step.

In a deployed system, the CompleteView licensing schema requires camera licenses to be allocated among CV Recording Servers.

- Each Recording Server is provisioned with a License Key.
- Every License Key incorporates a set of Feature Keys.
- The Feature Keys within a License Key enable the set of cameras allocated to that Recording Server.
- The Feature Keys within an individual server License Key also enable any other VMS capabilities or features allocated to that server.

Typically, all Recording Servers in a system incorporate a uniform set of capabilities and features, but each handles a different group of cameras

In a system that employs a single machine hosting the Recording and Management servers, all cameras and features are maintained in a single License Key located on the server.

In a system that employs multiple Recording Servers, the cameras and features included in the system are maintained in multiple license keys where one license key is allocated to each Recording Server.

For each Recording Server in this scenario, the set of cameras and features contained in its License Key agrees with its own configuration. In addition, client configurations must agree with the sum of server configurations.

In a multiple server system, all servers should incorporate the same set of VMS features, but each will manage a different set of cameras.

Obtaining and Applying a License Key

Note: If you purchased a PowerProtect server with CompleteView pre-installed, you may skip this section.

License keys are generated at the time of installation, are private, and cannot be transferred from one server to another.

Prior to server software installation, an email should be received from **licensing@salientsys.com** . Contact Salient at 512-617-4800, 1-844-725-4368, or the email address above for licensing assistance.

General Steps

1. All components of CompleteView must be installed first, per the instructions detailed in this manual.
2. Obtain the server Product ID (also referred to as a GUID), as shown below.
3. Reply to **licensing@salientsys.com** with the Product ID (GUID).
4. An email will be sent from **licensing@salientsys.com** with the "cvserver.lic" file attached.

5. When received, each unique license file should be saved or copied to the `C:\Program Files\Salient Security Platform\CompleteView\Recording Server\` directory for each Recording Server.

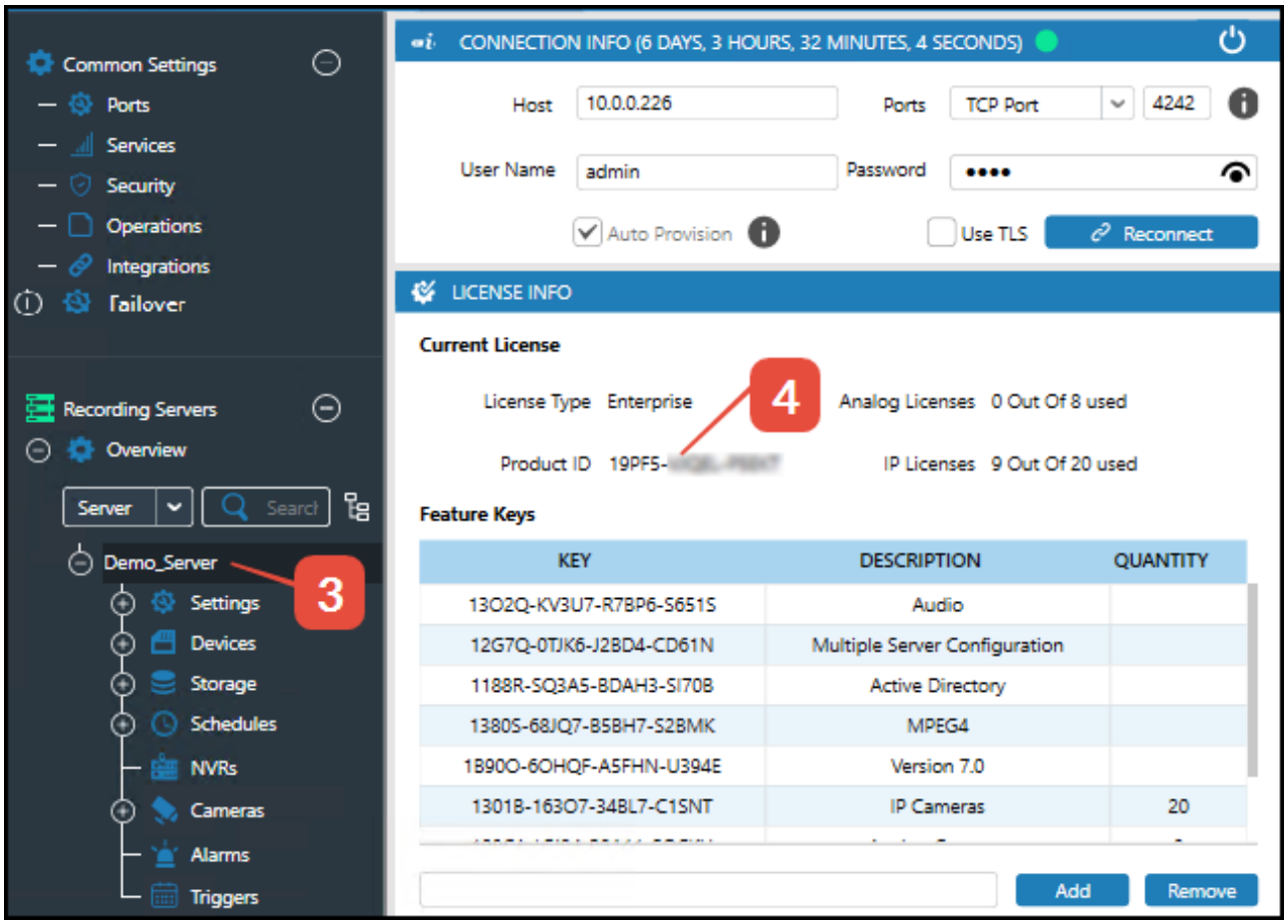
Each Recording Server is required to have a unique license file. Only one Management Server should be installed for a given deployment. The Desktop Client may be installed on as many machines as desired, but only one instance is required.

Obtaining the Product ID (GUID)

After all components of CompleteView have been installed:

1. Log into the Desktop Client.
2. Select the Configure module.
3. Select the desired Recording Server from the left pane.
4. Select and copy the Product ID.

For more information, see the Product ID and Feature Keys Job Aid video at:
https://support.salientsys.com/knowledgebase/training-resources/



5. Send the Product ID to licensing@salientsys.com.

Installation Introduction

If upgrading from any version of CompleteView previous to 7.0.X, please download and utilize the CompleteView **v7 Migration Guide** from the Knowledge Base section of the Salient website. The guide details all the steps required to update to 7.X.X from previous versions of CompleteView, including the use of the **License Distribution Utility**, its **documentation**, and includes information from the **Management Server Database Migration Utility's documentation**.

Installation Overview

CompleteView installs three main system components:

- Management Server (only one per deployment)
- Recording Server
- Desktop Client

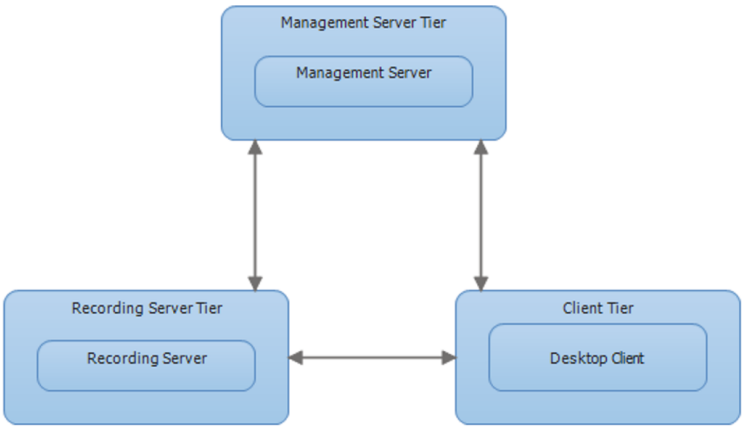
Deployment Patterns

CompleteView is comprised of **one** Management Server, along with one or more Recording Server(s), and Client(s). Consequently, CV may be deployed in a 1 to 4 tier configuration, illustrated below. Note that the SQL database is present in all patterns, but is only illustrated in the Four Tier installation, where it resides on its own dedicated server.

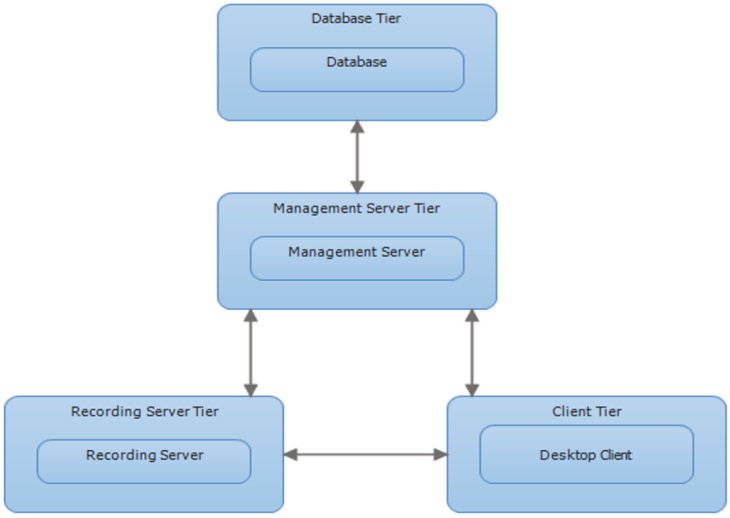
One Tier, the simplest pattern, where all components are installed on one machine. This guide will cover this type of installation. However, the steps covered herein are applicable to all installation paradigms. Simply run the appropriate installer on the appropriate machine as the desired topology dictates.

Two Tier, where components are divided between two machines, as illustrated.

Three Tier, where components are divided among three machines, as illustrated.

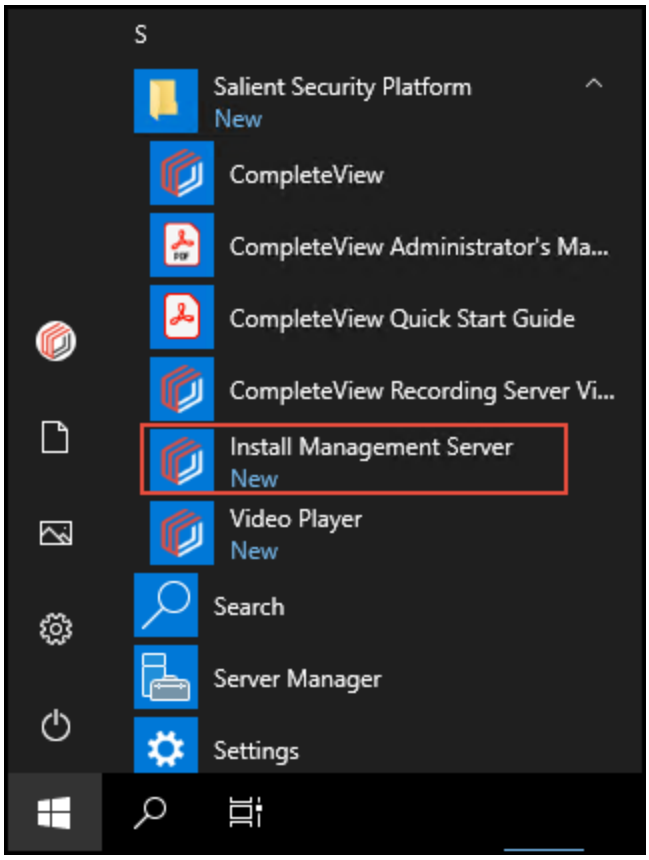


And, finally, **Four Tier**, where components are divided among four machines, as illustrated.



Management Server Installation

The Management Server coordinates communication between the various elements of CompleteView.
Note: Only one Management Server per deployment is permitted. If setting up a PowerProtect server for the first time, confirm the presence or absence of a Management Server in the site's deployment. If a Management Server is present, skip this section . If Management Server has not yet been installed, open the Start menu, browse to S, open Salient Security Platform, select Install Management Server, and proceed.

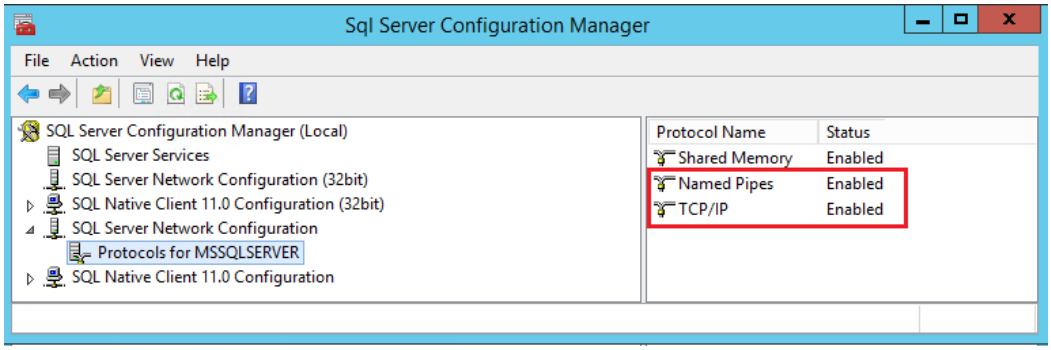


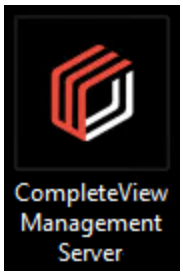
Prerequisite Installation and Configuration

Both Named Pipes and TCP/IP must be enabled within SQL Server Network Configuration **before** installing the Management Server. The following steps have already been applied to PowerProtect servers purchased from Salient.

Steps:

1. Launch SQL Server Configuration
2. Expand SQL Server Network Configuration
3. Select "Protocols for..." the appropriate SQL instance
4. Enable Named pipes and TCP/IP
5. Restart both SQL Server and SQL Server Browser Service from services.msc

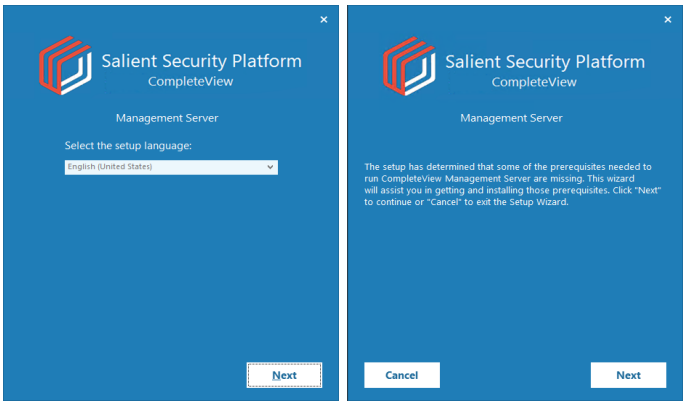




The installer will check the system for prerequisites.

Note: Various prerequisites may already be installed on a given system, and may not be mentioned during the installation process.

Note: If upgrading to a newer version of CompleteView and the previous version was utilizing SQL Server or an existing SQL Server will be used, you will be prompted to enter the database's credentials. CompleteView supports SQL Server 2016, 2017, 2019, and 2022 Express or better.



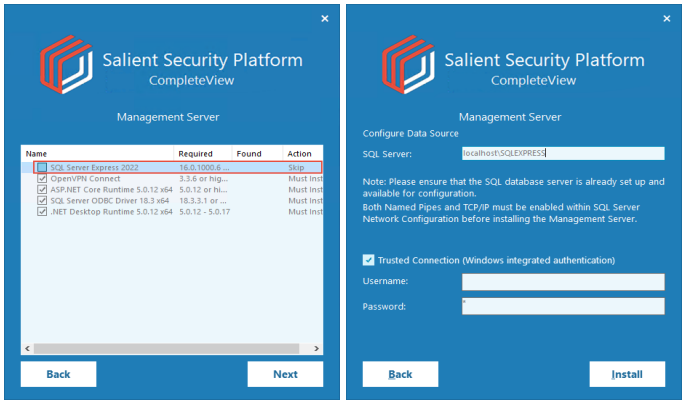
Database Selection

At this point in the installation, a choice of database configuration is required. If an existing local or remote SQL Express (or better) installation is to be used, de-select the option to install SQL Server Express 2022 and click Next. In the following screen, provide the path and sufficient credentials for the existing SQL server, and click Install. CompleteView supports SQL Server 2016, 2017, 2019, and 2022 Express or better.

SQL Users & Permissions Information

CompleteView utilizes two SQL users: one for initial database creation, and one for ongoing database access. Whether using an existing SQL deployment or downloading and installing SQL Express during installation, CompleteView will prompt for entry of credentials that will be used to create the CompleteView database and to create its own user for ongoing access. If Trusted Connection is selected,

the credentials of the currently logged in Windows user will be used to connect to the SQL Server and create the database. If Trusted Connection is not selected, an account with the dbcreator role or better (e.g., sa, a sysadmin, etc.) needs to be used. The credentials for this account will not be stored; the account will only be used to create the CompleteView database and associate CompleteView's SQL user, cvsqluser, with the database. It will not be accessed by CompleteView again. The second account, cvsqluser, will be created during the installation process. The cvsqluser account is created with db_owner permissions for only the CompleteView database, and must retain this level of permissions.

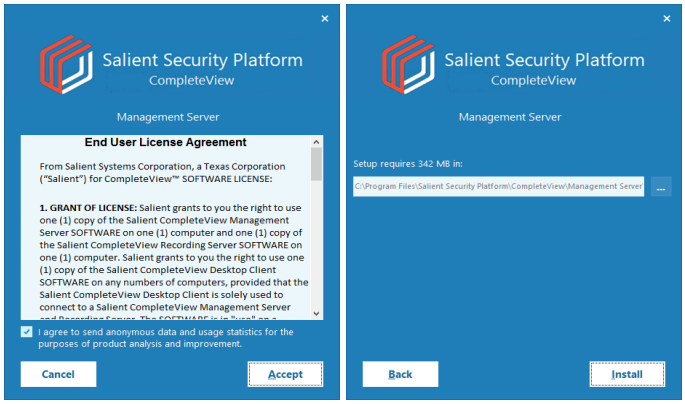


SQL Express Installation & Configuration

If no current SQL Express instance is available either locally or on the network, leave the SQL Server Express 2022 installation option checked and click Next.

Installation of the SQL server and other prerequisites may take some time, contingent upon network speed, etc. When completed, Accept the agreement, and either change the installation path or click Install.

Note: To improve future product development, CompleteView collects and sends anonymous analytic data such as geographic location, version information, OS, platform type, system memory, etc., to Salient. Users may opt out by deselecting the checkbox at the bottom of the installation screen.



After downloading and installing SQL Express and completing installation, CompleteView will prompt for entry of credentials that will be used to create the needed database in SQL Express. If Trusted Connection is selected, the credentials of the currently logged in Windows user will be used to connect and create the database in the SQL server. If Trusted Connection is not selected, an account with administrator (sa) permissions needs to be created or used for installation. This account will only be used for database creation.

Note: These credentials will not be stored, and are used to create the needed database and associate cvsqluser as db_owner.

The account that has the db_creator role just needs to have that role during database creation. That account is used only for database creation.

Cvsqluser is created with sa level permissions. The cvsqluser is required to be db_owner for the CompleteViewVms database, and is given the public and db_owner roles.

Enter a complex password which adheres to the specifications below for the SA password. It will be used for database creation and access. Click Install.

- The password must be at least eight characters long.
- The password contains characters from three of the following four categories:
    1. Latin uppercase letters (A through Z)
    2. Latin lowercase letters (a through z)
    3. Base 10 digits (0 through 9)
    4. Non-alphanumeric characters such as: exclamation point (!), dollar sign ($), number sign (#), or percent (%)
    5. Do not use the following special characters within the SQL Express password: & < > " '

- Passwords can be up to 128 characters long. You should use passwords that are as long and complex as possible.

For more information, see **Microsoft's SQL Password Policy.**

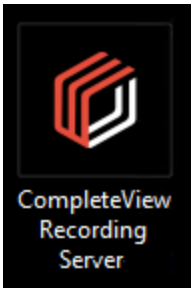
The Management Server is now installed. Proceed to the next section.

Recording Server Installation

This section describes the process of installing the CompleteView Recording Server. As with the other sections in this document, it presumes a One Tier installation. Recording Server comes pre-installed on PowerProtect servers.

Recording Server Installation

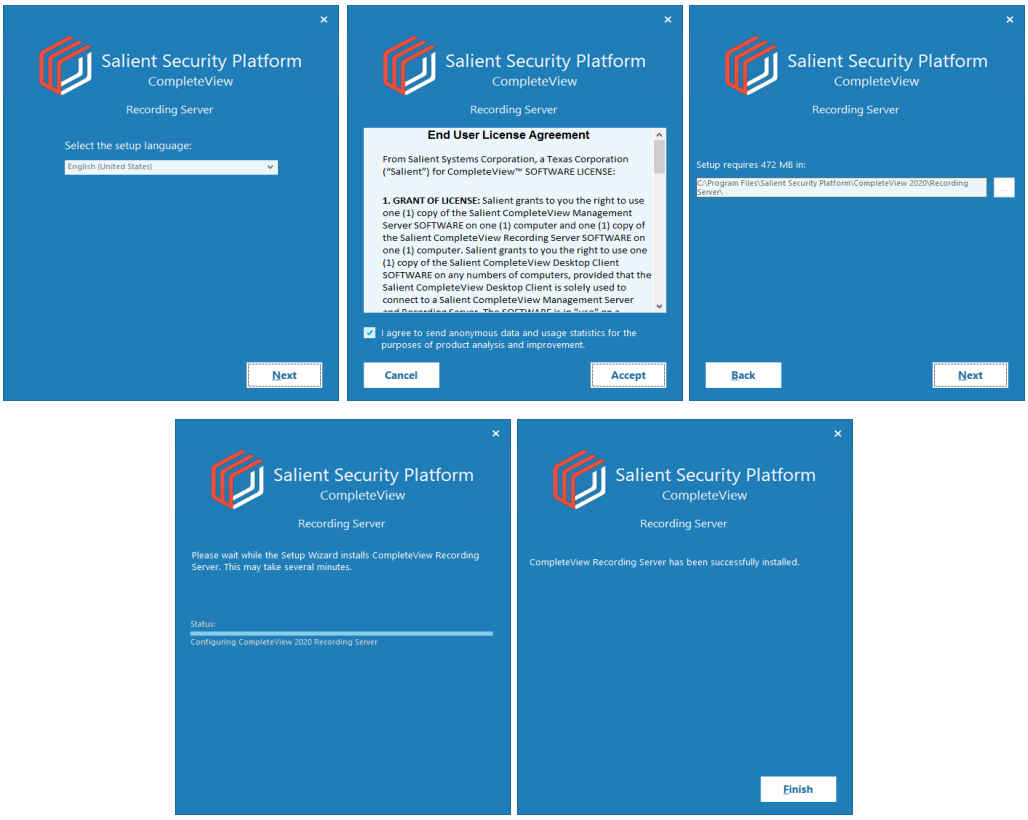
Double click the CompleteView Recording Server installer.



If upgrading from CompleteView 4.X, the Recording Server installer will prompt to uninstall the current version before installing the upgrade. Proceed through the uninstall.

Note: To improve future product development, CompleteView collects and sends anonymous analytic data such as geographic location, version information, OS, platform type, system memory, etc., to Salient. Users may opt out by deselecting the checkbox at the bottom of the installation screen.

Accept the licensing agreement, accept or specify the path to which the Recording Server should be installed, click Next, and wait for the installation to complete.



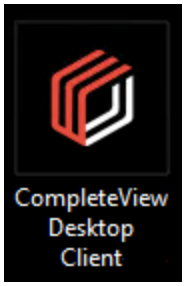
When completed, click Finish, and proceed to the next section.

Desktop Client Installation

This section describes the process of installing the CompleteView Desktop Client. As with the other sections in this document, it presumes a One Tier installation. Desktop Client comes pre-installed on PowerProtect servers.

Desktop Client Installation

Double click the CompleteView Desktop Client installer.

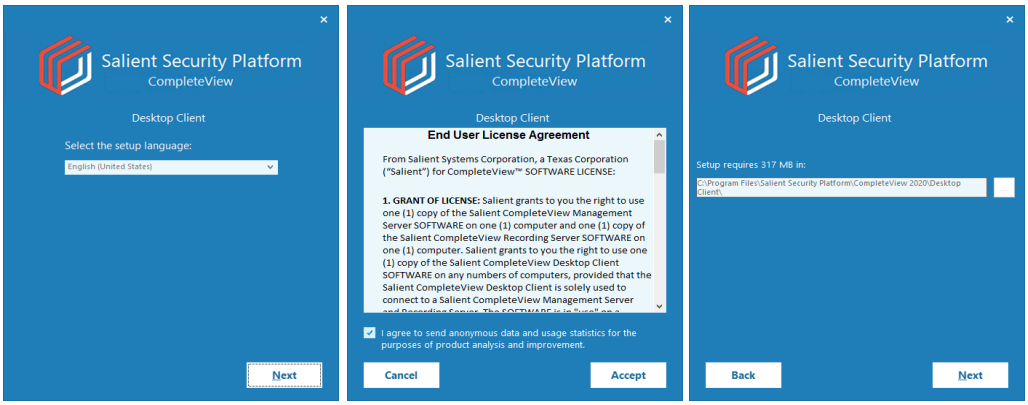


Note: To improve future product development, CompleteView collects and sends anonymous analytic data such as geographic location, version information, OS, platform type, system memory, etc., to Salient. Users may opt out by deselecting the checkbox at the bottom of the installation screen.

Optional Video Wall Agent Installation

During the Desktop Client installation process, an option to install the Video Wall Agent (VWA) is presented. The VWA allows a workstation to be configured to display full screen video, Views, and Maps across all attached monitors. The VWA is intended to be installed on client workstations meant for displaying data, and should not be installed on systems hosting the Management and/or Recording Server(s). For more information, see the Video Wall section of the main manual.

Accept the licensing agreement, accept or specify the path to which the Desktop Client should be installed, optionally select the Video Wall Agent, and click Install.



Wait for the installer to complete, and click Finish.

The Client has now been successfully installed. Proceed to the next section.

Desktop Client Initial Launch

The Desktop Client contains all of CompleteView's administrative and client functions. It enables both administrators and users to manage and use CompleteView from a single panel. Every VMS activity is configured from within the client, except legacy server configurations.

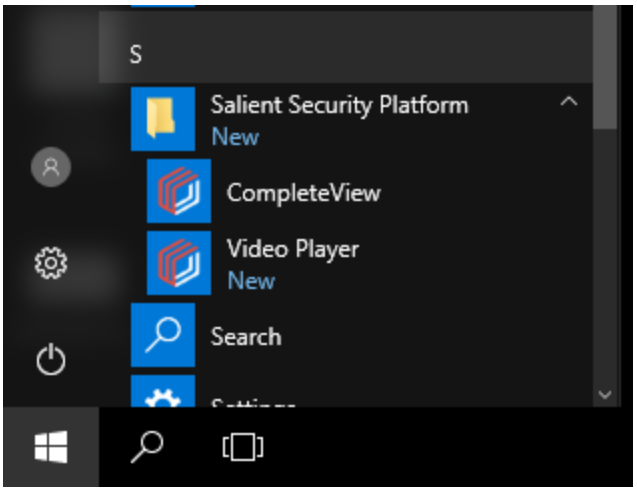
How to Launch the Desktop Client

Double click on the CompleteView icon on the Desktop, if present.

Alternately, follow the steps below.

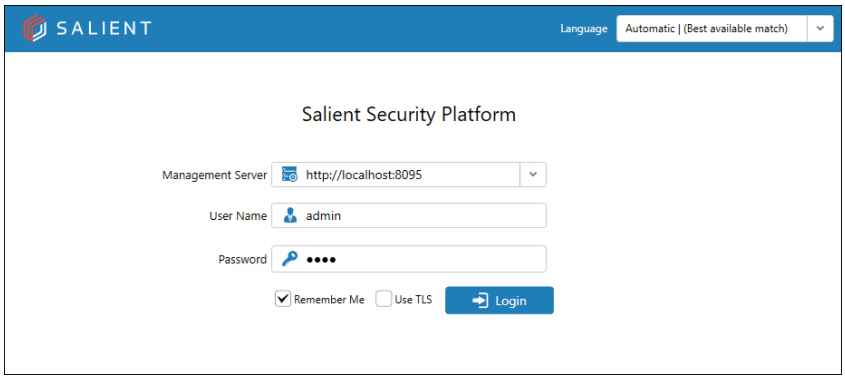
Steps:

1. Select the Start button
2. Scroll to the S entries
3. Select Salient Security Platform
4. Select CompleteView



Logging In

Steps:



1. Optionally, select a different language from the dropdown menu in the upper right corner of the window.
2. Ensure that the Management Server field is accurately populated.
3. Enter a valid CV username and password in the fields provided. The default ID is "admin," leaving the Password field blank.
4. Optionally, select Remember Me to store credentials for future use.
5. Select Login.

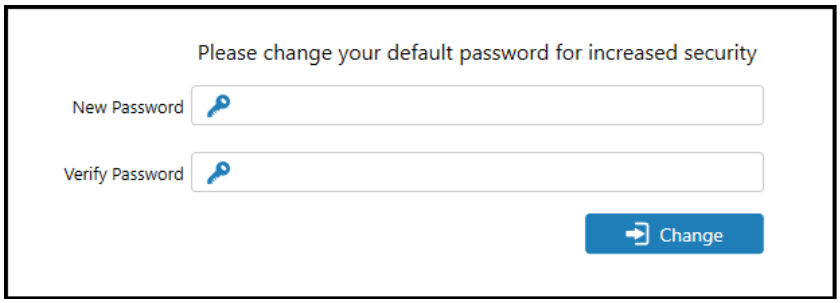
Note that multiple instances of the Desktop Client may be open at once. In addition, a history of previous Management Servers to which the Desktop Client has connected is stored in the Management Server field of the Desktop Client, and can be accessed by either clicking the down arrow or by typing the first few characters of the desired Management Server and selecting the appropriate result. Selecting or deselecting the Use TLS option will display secured versus non-secured Management Servers.

Network Auto-Detection

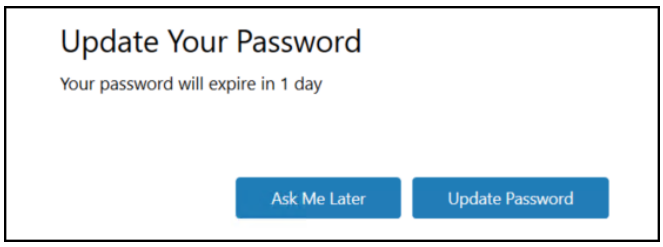
This feature enables CompleteView clients to determine the most efficient way to connect to the deployment. If using a Remote Access Cloud URL, the client will automatically detect if a route to the Management Server is available through the local network and use that instead.

Password Change

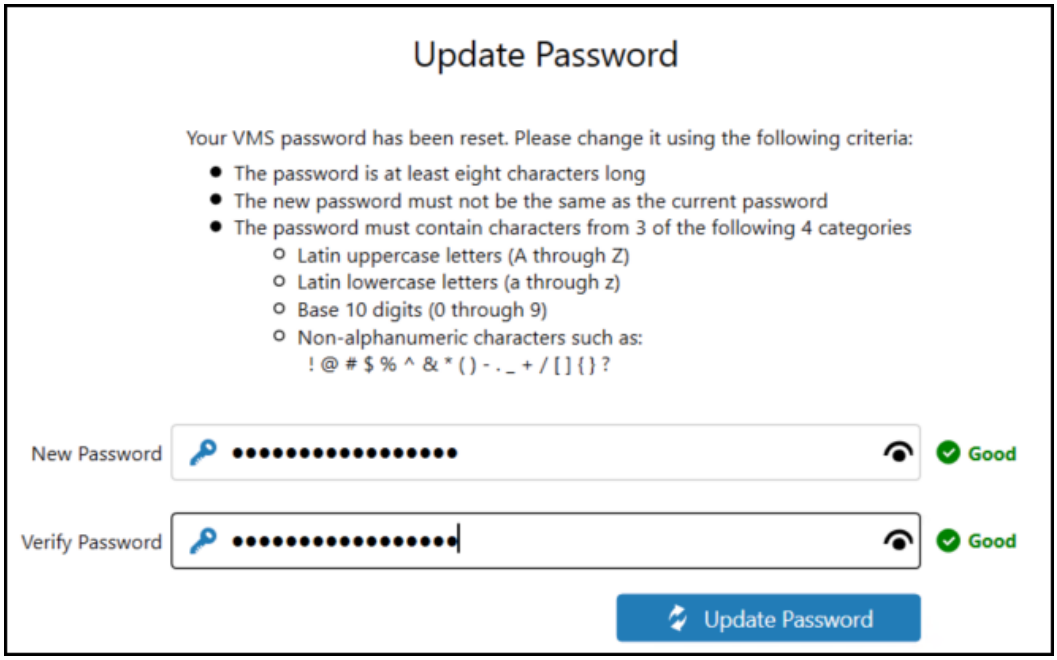
Upon initial login, CompleteView requires changing the default Admin password. Enter and verify the new password, and click Change.



If password policies are in effect, CompleteView will notify existing users when their password is about to expire. From the prompt, users may choose to delay changing their password or update it at that time. If they choose to update it then, they will be taken to an Update Password screen, similar to the one described below.



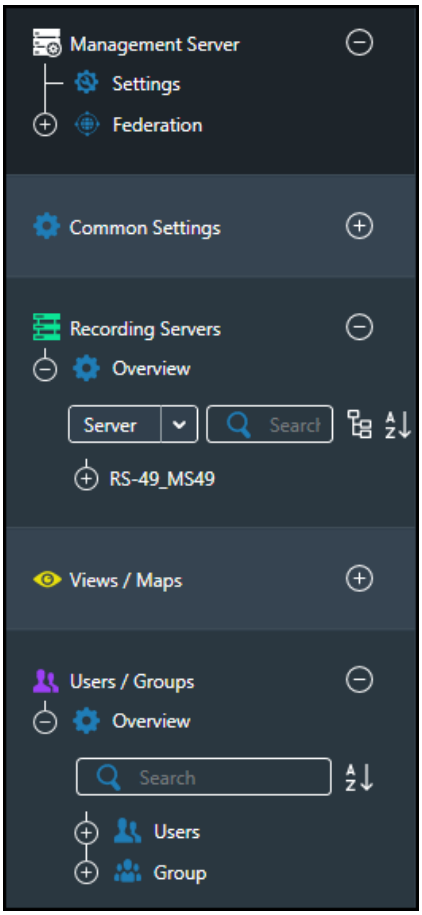
Upon log in, a new user, a user with an insufficiently complex password, or a user with an expired password will be presented with the following Update Password screen.



CompleteView will verify adequate password complexity before allowing the user to select Update Password.

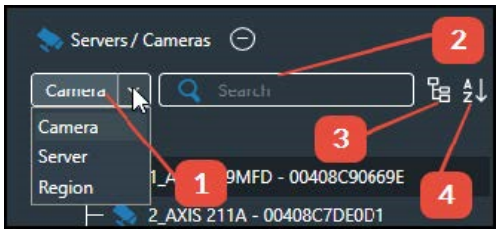
Desktop Client Navigation and Functionality

All modules except Alarm View and Search Video in Playback utilize the Navigation Panel, which is itself divided into various, contextual sub-panels. Many sub-panels are searchable and sortable. The following instructions describe the general steps involved in utilizing the search, sort, and filter features. Note that the options in the sub-panels are contextual, and that not all features will be available in all sub-panels.



Steps:

1. Select the element for which you'd like to search. This example utilizes the Servers/Cameras sub-panel, which contains Cameras, Servers, or Regions.
2. Enter part or all of the element's name or number, and press Enter. The result(s) will be displayed under the appropriate node.
3. Optionally, display the information in linear or region format.
4. Optionally, sort the results (or the whole tree) in ascending or descending order.



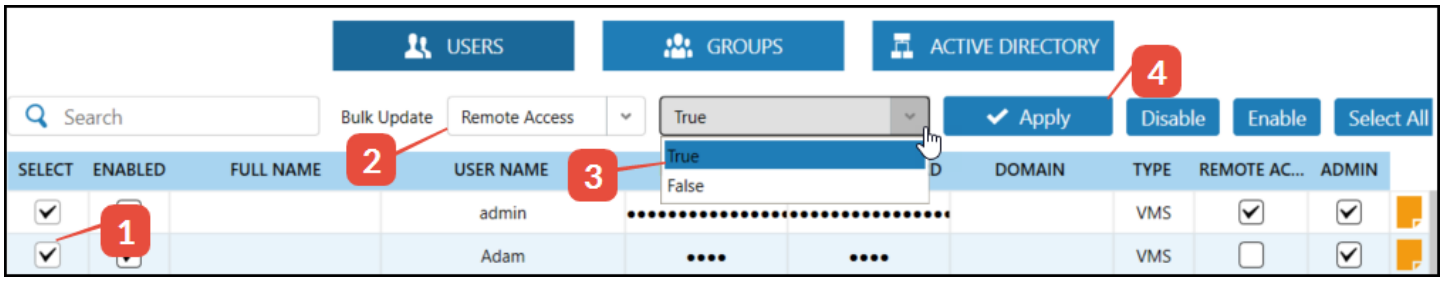
The Navigation Pane may be collapsed or expanded by clicking the double horizontal chevrons located in the bottom right corner.

The Navigation Pane within the Configure module may be locked to prevent changes. Click on the icon to lock and unlock the Navigation Pane.

Bulk Update

Bulk update provides administrators with the ability to change specified attributes for selected items en masse. Configurable attributes will change contextually.

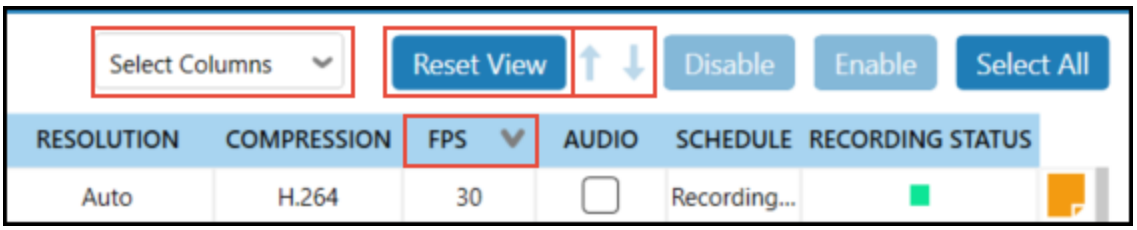
The example below illustrates the process of granting Remote Access to multiple Users.



1. Select the items to be modified (in this case, Users, but could be cameras, etc.)
2. Select which attribute is to be changed
3. Select the state of that attribute
4. Click Apply

Column Sorting and Selection

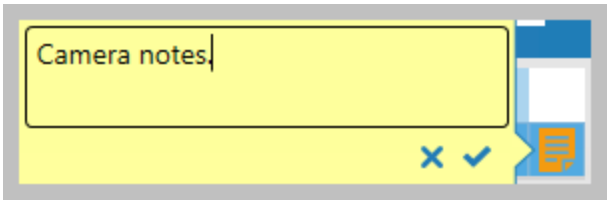
In some overview screens, columns may be selected for display or obscured for easier viewing and navigation. Clicking the Select Columns dropdown menu will display a list of the overview's columns. Check or uncheck the columns to be viewed as desired. Clicking Reset View will return the default columns to view. Clicking a column header will sort that column in either ascending to descending order or vice versa. Additionally, use the arrows to navigate to individual items in the list.



Notes

Anywhere within the CompleteView client where a notes icon is displayed allows for the addition and editing of comments. Click the notes icon to enter or edit text. Notes have a 256 character maximum. An icon with no lines indicates no notes have been added to that item. Icons with lines contain notes.

When finished, select the checkmark to save the edits to the note, or select the X to discard them. Click the module's Save button to ensure the note has been saved.

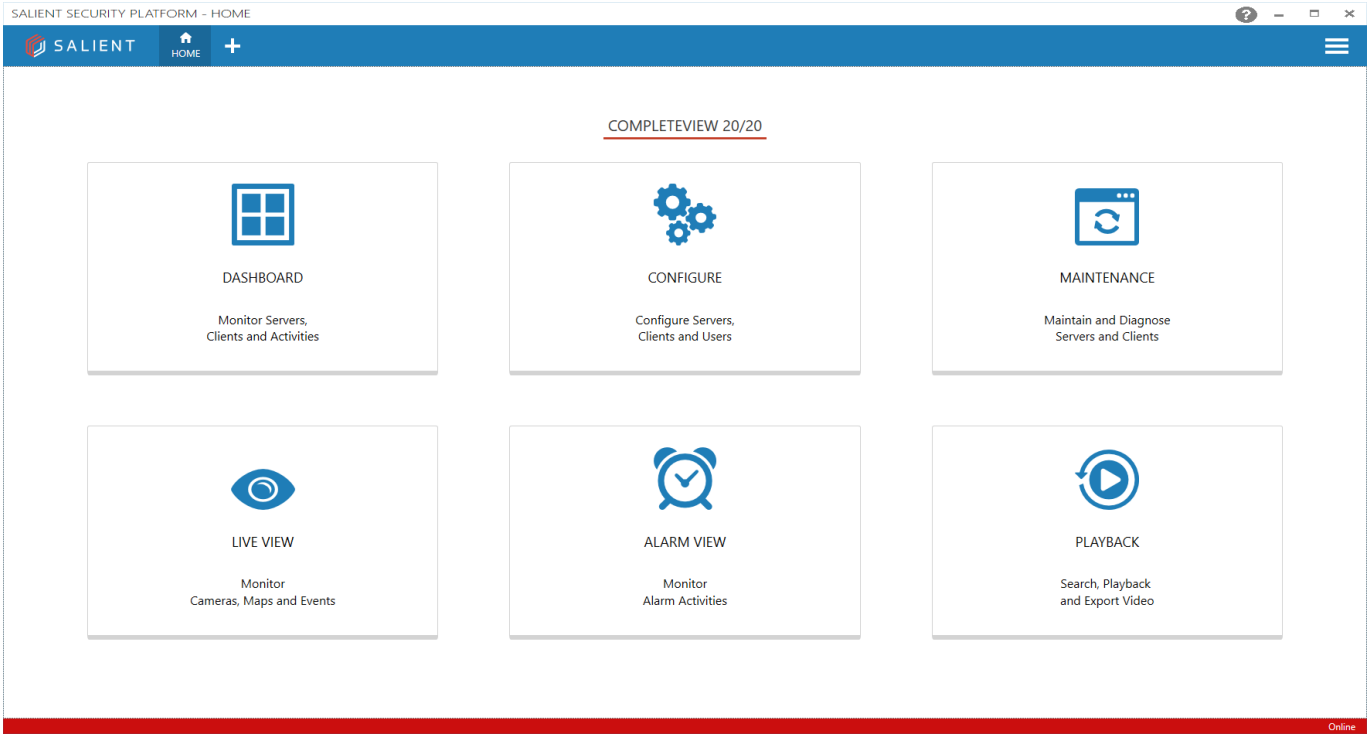


Notes follow the item to which they are attached, such as a camera. For example, if information has been added to a note for a camera in one screen, the information will be accessible in any other screen in which the camera is available and the notes icon is visible.

Security Platform Tasks

The client is divided into six selections. Each of the six buttons opens the given function's features and settings.

Each user's access is limited by permissions granted by an Administrator. Administrators have complete access to all functions. For more information about user permissions, Click Users & Groups Configuration.



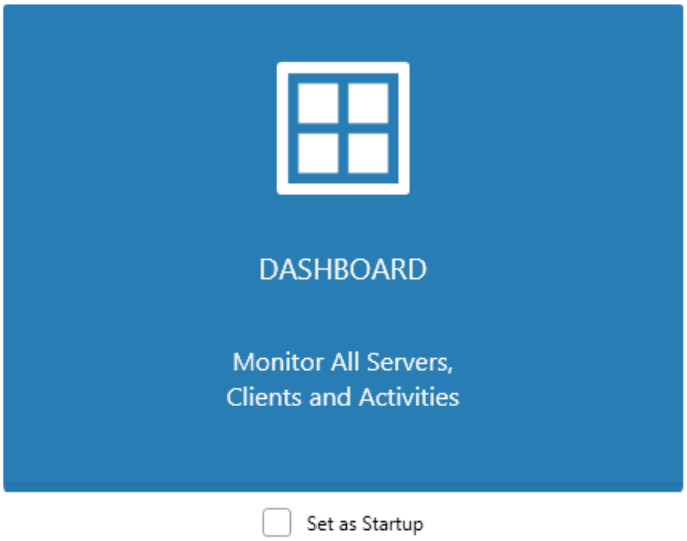
The functions are divided as follows:

1. **Dashboard** - Monitor all Servers, Clients, and Activities
2. **Configure** - Configure all servers and users
3. **Maintenance** - Manage and update software versions
4. **Live View** - View Camera live feeds
5. **Alarm View** - Monitor alarm activities
6. **Playback** - Playback recorded video

Default Task at Login

Setting a specific function to open at login can be a convenient way to display a specified function upon login. Only one function can be selected. If a second function is selected to open after login, the previous defaulted function will automatically deselected.

Steps:



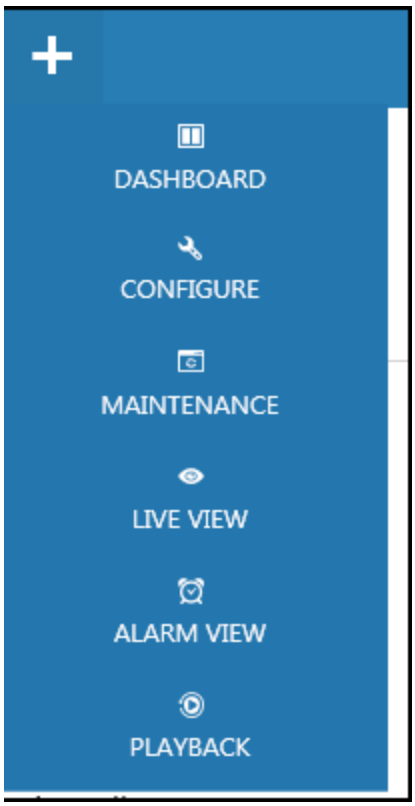
1. From the home screen, rollover your mouse onto a function.
2. Select the “Set as Startup” checkbox.

Client Toolbar

At the top of the home screen is a toolbar. The Home button is persistent, and cannot be removed. However, all of the remaining six functions may be shown or removed from the toolbar. If no single function is selected to open at client start up, the functions for which the user has permission will be displayed on the home screen for selection after login.

How to Display and Select Functions from the Toolbar

Steps:



1. Looking at the top and left of the area of the Home screen, select the plus symbol (+) on the toolbar to display the list of six functions.
2. From the list, select one or more of the function(s) to add it/them to the toolbar.

Secured Communication

CompleteView allows for secured communication via SSL/TLS certificates between the Desktop Client and the other core components of CV.

Requirements

To implement secured communication from the Desktop Client, security certificates need to be created and applied to both the Management and Recording servers with which the client will be communicating. In addition, the fully qualified domain name (FQDN) for the Recording Server must be entered for TLS to function. Unless both the Desktop Client and Management Server reside on the same physical machine, certificates must come from a Certificate Authority. Self-signed certificates will only work for systems where Management Server and Desktop Client are on the same system.

While communication between the Desktop Client and Recording and Management Servers is secured, that security does not extend to communication between CompleteView and devices such as cameras, NVRs, etc., at this time. In addition, CompleteView currently supports TLS versions up to and including 1.3.

Configuration of Secured Communication

Follow the steps below to implement secured communication between the Desktop Client and Management and Recording Servers. Note that if changing the default port settings for either or both the Recording and Management Servers, it should be done in their respective (Common) Settings > Ports menus, and not the Connection Info screen.

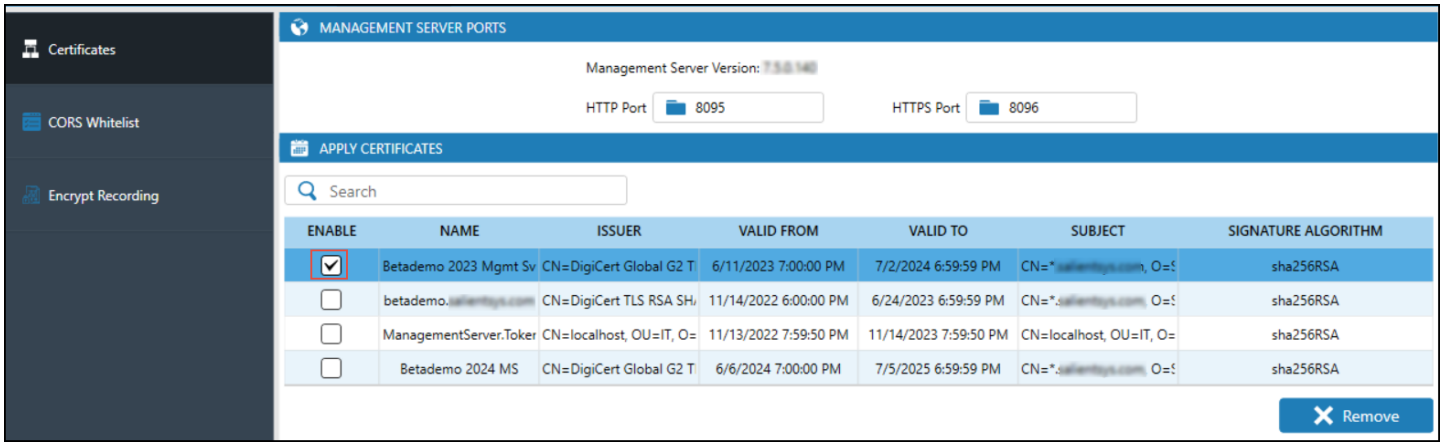
Create and Apply Certificates

Refer to procedures for certificate creation in **Common Settings Security** . The steps for creating and applying certificates for the Management Server (in Common Settings > Security) and a given Recording Server (Settings > Security) are the same. Apply the appropriate certificates to both the Management and Recording Server(s). Again, self-signed certificates will only work for systems where Management Server and Desktop Client reside on the same system, otherwise a certificate authority must be used.

Enable Management Server Certificate

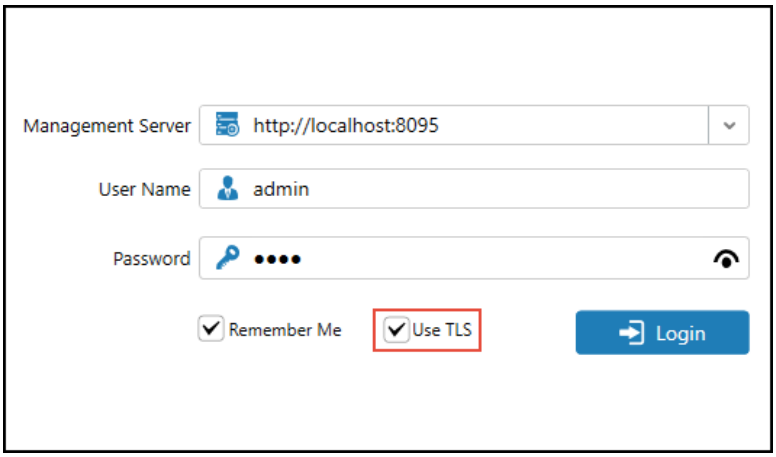
After applying appropriate certificates to both the Recording and Management Servers, save all configurations, log out, and log back into the Desktop Client.

After logging back in, launch the Configure Module and select Common Settings, Security. Enable the desired certificate, and save the configuration. Log out once more. If already enabled, skip to the next section.

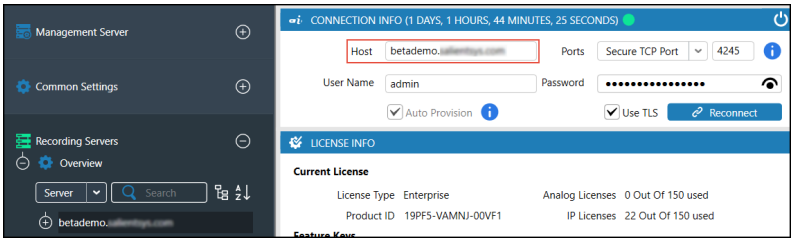


Enable Recording Server Certificate

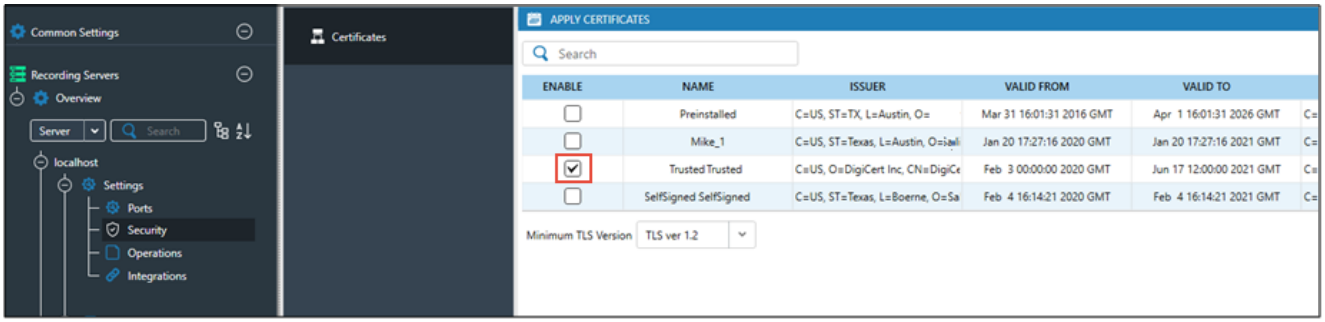
Log back into the Desktop Client, this time selecting the Use TLS option.



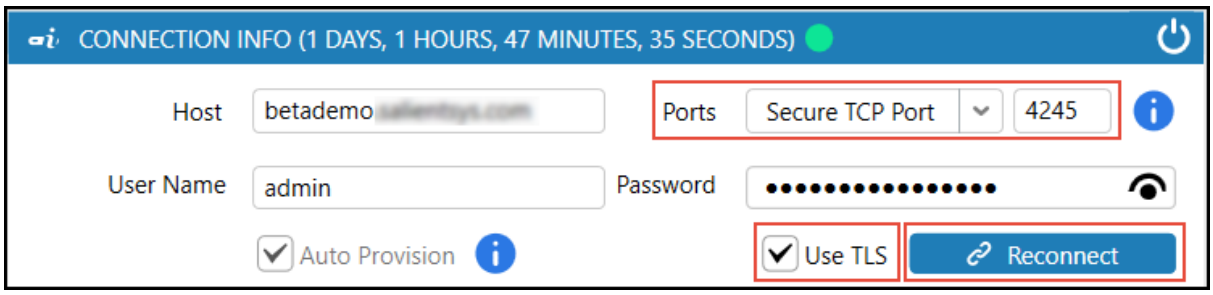
Select the Recording Server, and verify the FQDN is listed in the Host field. If not, enter it and Reconnect.



Select the Recording Server's Settings and Security and, as before, make sure the desired certificate is Enabled. Save the configuration.



Finally, select the Recording Server, select the Use TLS option, select the Secure TCP port option, and Reconnect.



Save the configuration, log out, and log back in to the Desktop Client. If SSL/TLS configuration was successful, the locked icon will be displayed next to the logged in username.

Web & Mobile Client Information

CompleteView web and mobile clients enable viewing, playback, investigation, video exportation and other functions associated with CompleteView. A supported web browser or mobile OS, internet connection, and a Management Server's address and valid credentials are required to use the clients.

Web Client Quick Start

Once a CompleteView deployment is operational, verify that the Embedded Webserver (HTTP/HTTPS) ports for both the Management Server and desired Recording Server(s) are enabled. See **Common Settings Ports** for more information.

Web Client System Requirements

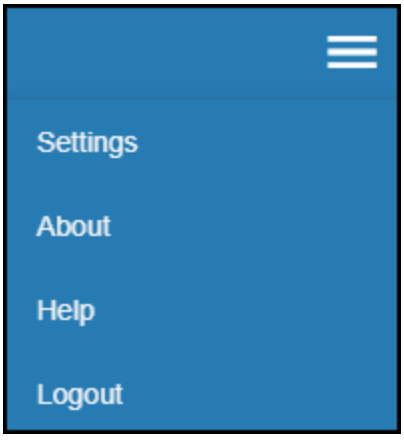
It is recommended to use the current versions of the listed browsers to run the CompleteView Web Client. In addition, it's recommended to have a minimum of 4GB of system memory and run current versions of MacOS or Windows.

- Firefox
- Chrome
- Edge
- Safari

Initial Browser Configuration

There are two methods to enable a supported browser to function as the Web Client. Using the supported browser, either proceed to **http://webclient.salientsys.com** or **https://webclient.salientsys.com** or browse to the deployment's Management Server's IP address or FQDN (fully qualified domain name), making sure to specify the secured or non secured port (e.g. https://FQDN:8096). Enter the address and credentials of the desired Management Server to log in. For more information about functionality and configuration, consult the online help included with the Web Client, located in the upper right corner.

Using a supported browser, navigate to the deployment's Management Server's IP address or FQDN (fully qualified domain name), making sure to specify the secured or non secured port (e.g. https://FQDN:8096). Enter the address and credentials of the desired Management Server to log in. For more information about functionality and configuration, consult the online help included with the Web Client, located in the upper right corner.



Mobile Client Quick Start

As above, verify that the Embedded Webserver (HTTP/HTTPS) ports for both the Management Server and desired Recording Server(s) are enabled. See **Common Settings Ports** for more information.

Mobile Client System Requirements

The mobile client may be run on iOS version 13 or newer, or Android version 24 or newer. The apps may be downloaded from the devices' respective app stores, or from the following links:

iOS: **https://apps.apple.com/us/app/completeview/id1637667124**

Android: **https://play.google.com/store/apps/details?id=com.salientsys.completeview&hl=en-US&pli=1**

As above, enter the deployment's Management Server's IP address or FQDN (fully qualified domain name), making sure to specify the secured or non secured port (8095 or 8096, typically), and enter appropriate credentials.

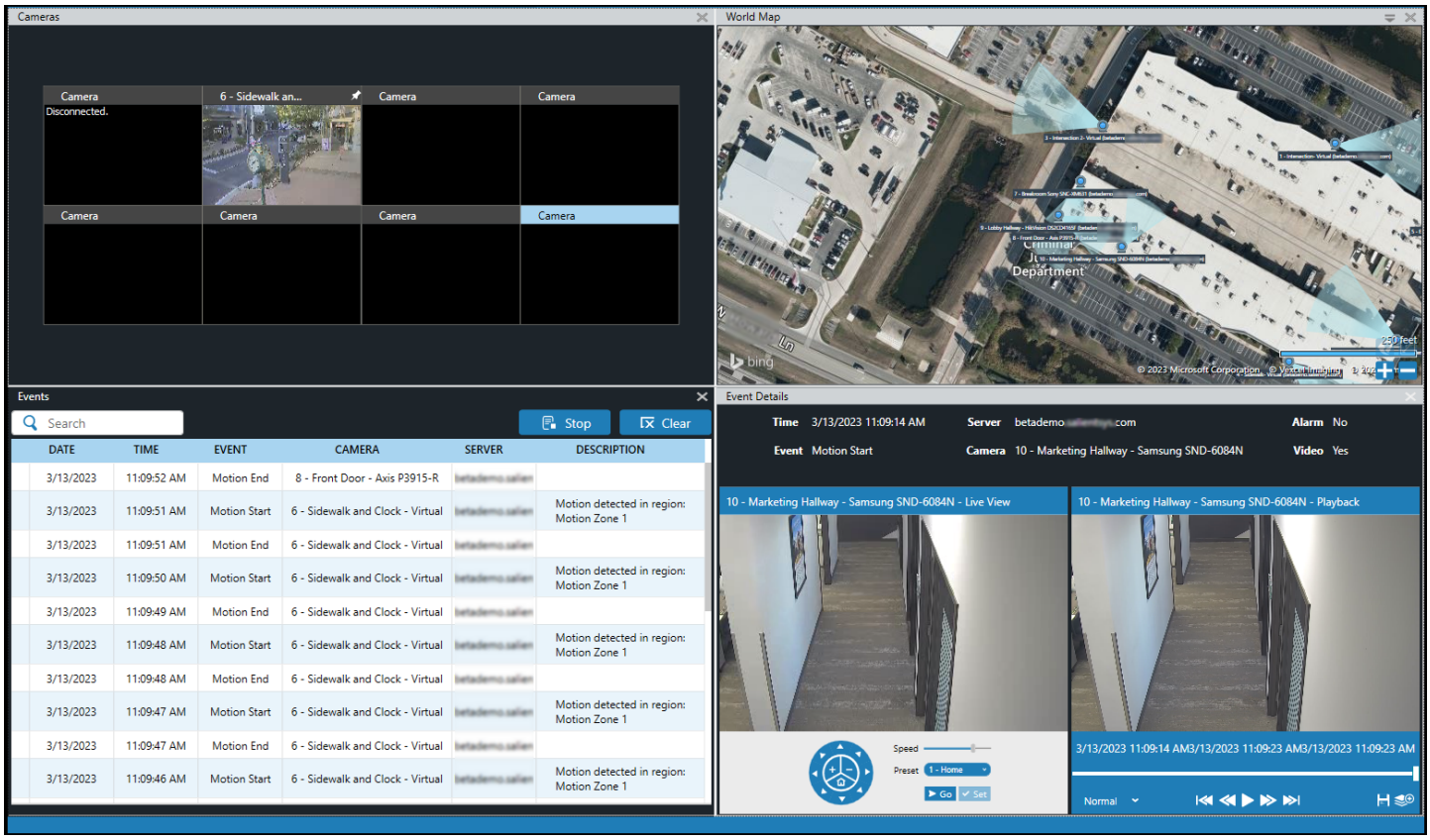
For more information, select Help from the Settings menu.

Alarm View Overview

Alarm View is composed of four panels designed to display video when either video motion or alarms are detected. Alarm View does not require Administrator permission to open or use. Configuration of Alarm View is typically an Administrator responsibility. Click Recording Servers Camera Events to learn more about configuration of alarms.

Alarm View Panels

The default Alarm Panel consists of four panels. Each of the panels and their features will be detailed in its own section.



Alarm View Menu

The Alarm View toolbar resides at the top right corner of Alarm View. The toolbar's icons, descriptions, and applications are described below.

Toggle Audio Notifications

When enabled, an audible notification will sound in Alarm View when either a motion or alarm event occurs. Motion and alarm events have distinct tones.

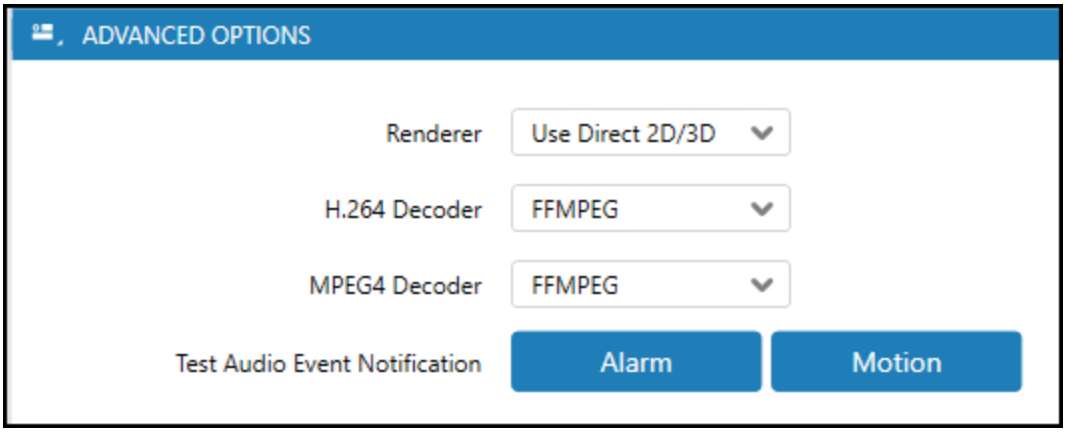
Export Queue

Navigates to the Export Queue

Menu  Launches the contextual menu

Alarm View Advanced Options

Clicking the Menu option described above produces a menu nearly identical to the **Live View menu**. The Advanced Options panel for Alarm View adds an option for testing audio event notifications.



Camera Panel

The Camera Panel provides both real-time video alerts as well as video associated with an alarm or motion event generated by the server or its associated alarm devices or cameras. Analog video associated with an alarm also displays in the panel.

Using the Layout Options menu and the Camera Layout submenu, users select from 4- 64 cameras to populate the Camera Panel. The panels in Alarm View may be floated.

Triggering Video Alerts

Alarm View camera tiles remain black, illustrated above, until either motion or an alarm are triggered. To generate video, the Administrator will properly configure motion recording and establish an Alarm and Motion Display schedule. Click Recording Servers Camera Motion Panel to learn more about configuring motion recording.

Alarm View camera tiles populate from the top left to the bottom right. To prevent video sensory overload, select those cameras that are of the highest importance to be included in the camera panel display schedule.

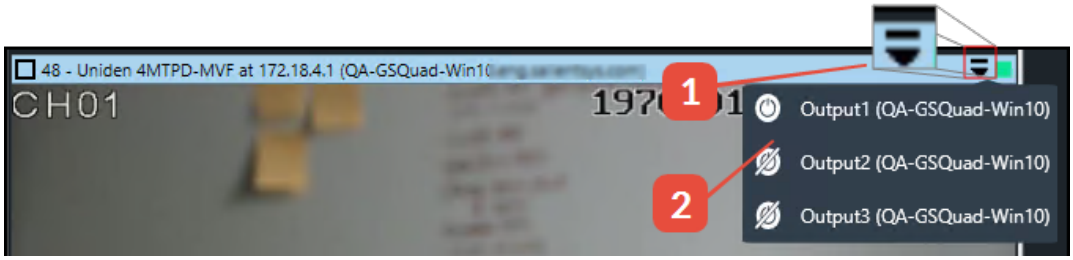
Both motion and alarms can be displayed from a CompleteView 4.X server that is integrated into CompleteView, along with any CompleteView cameras, simultaneously.

Alarm Device Output Trigger

Alarm Device outputs associated with alerted cameras may be triggered within Alarm View.

Steps:

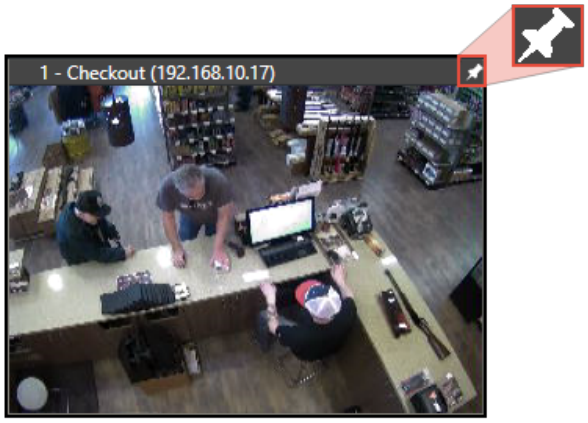
1. Select the Output Triggers icon in the upper right corner of the camera window.
2. Select the desired Output.



In addition, outputs may be manually triggered within Dashboard and Dashboard search, Live View, and anywhere the Output Triggers icon is displayed.

Pause Video Tile Change

When populated with video, each tile displays a thumbtack in the upper right corner. When pressed, the thumbtack pins the currently displayed video until the thumbtack is pressed a second time. The thumbtack enables the user to right click on the tile and call up the menu illustrated below.



Video Tile Menu

Right click on a video to produce the Video Tile Menu. The menu allows the user to take a snapshot or playback recorded video from the selected camera. The same menu can be called up from the Event Details panel when the video is presented in the Event Details tiles.

Tile Menu Options

Take Snapshot

When selected, a snapshot of the video in the tile is taken. The user can save the snapshot as a JPEG file to a CD, DVD, thumb drive or network location.

Playback Video: Review in Timeline

Review in Timeline returns a single video image with a timeline below the image. The timeline begins at midnight and stretches for twenty-four (24) hours.

Playback Video: Search by List

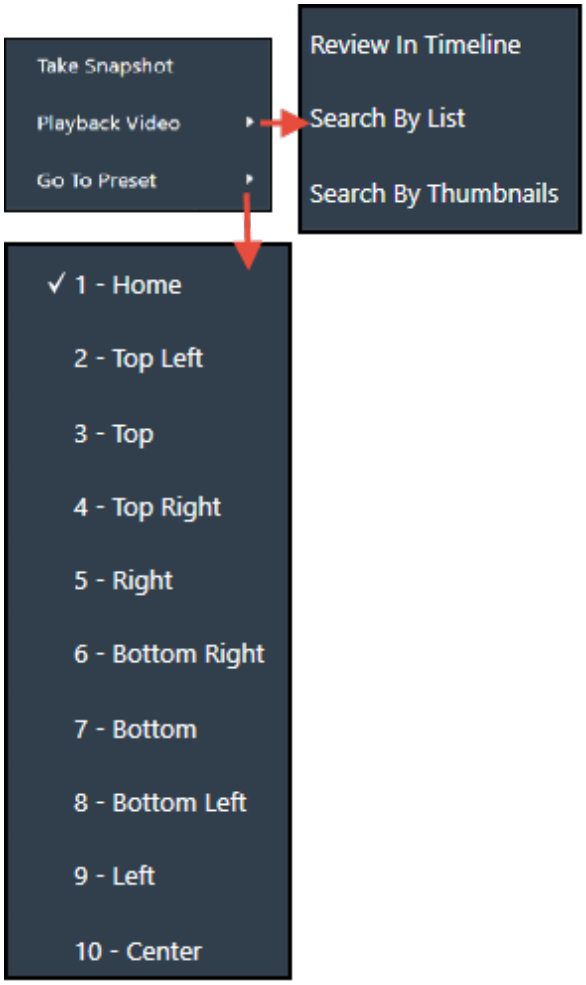
Search by List displays recorded video clips in a list. The top result in the list automatically begins when the playback screen appears. The list of results includes start and end time of the recorded video and a recording type indicator.

Playback Video: Search by Thumbnails

Selecting Search by Thumbnails transitions to Playback's Thumbnail search screen, and generates a thumbnail search using the default, twenty-four clips over twenty-four hours.

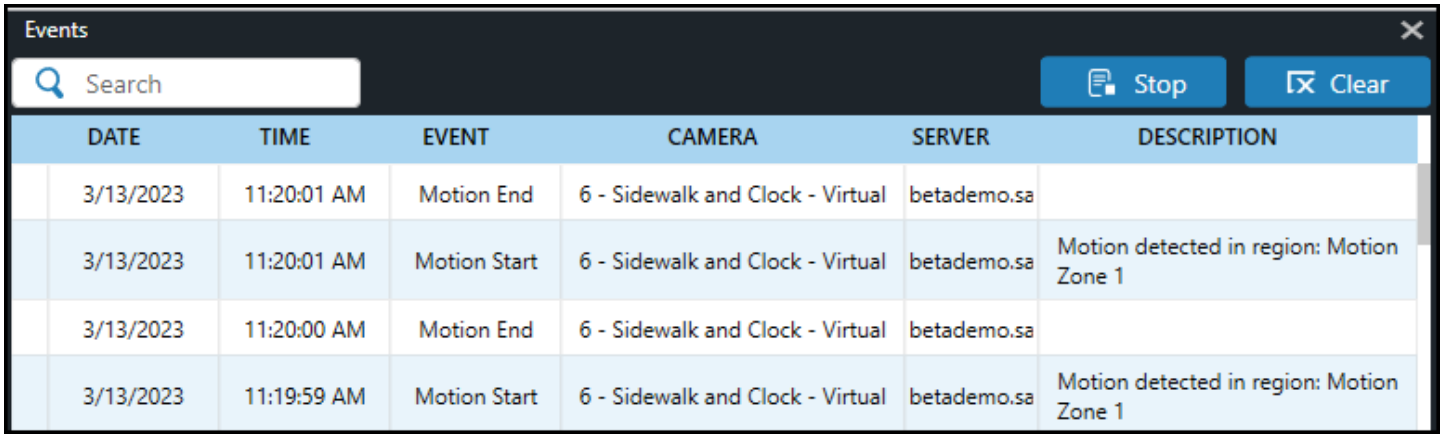
Go To Preset

Select the preset position that you wish to send the camera to.



Events Panel

The Events Panel displays a text description for each motion or alarm event, also providing the user with a date, time, camera name, and the camera's server information.

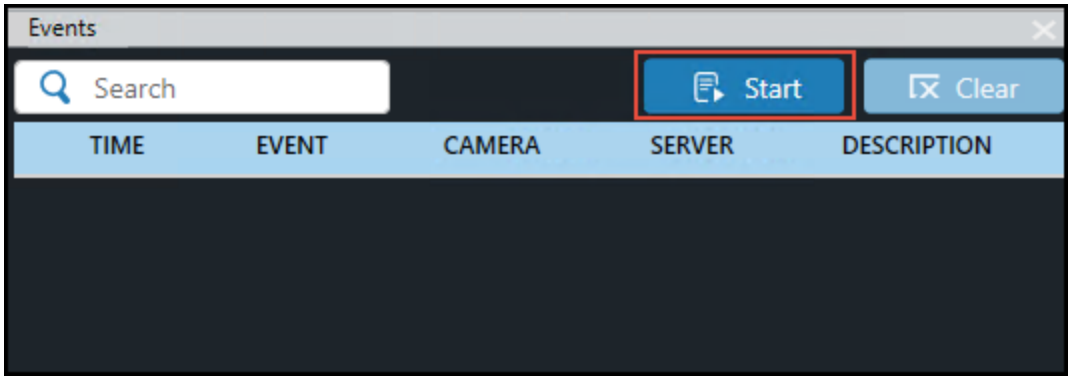


Search Event

Users may search for a particular event by name, event description, camera name, server name or time (hh:mm) by typing the criteria into the Search field in the upper left of the Event Panel and pressing Enter. Multiple values may be entered, separated by commas.

Stop/Start Function

In low bandwidth deployments, Recording Servers may be configured to report events only on demand. If events are not being displayed, events may be restarted by clicking the Start button in the Events panels of the relevant modules. See Bandwidth Control for more information.



Note: Live events will not update in the Events Panel with search criteria in the search box. Clear the search with the Clear button.

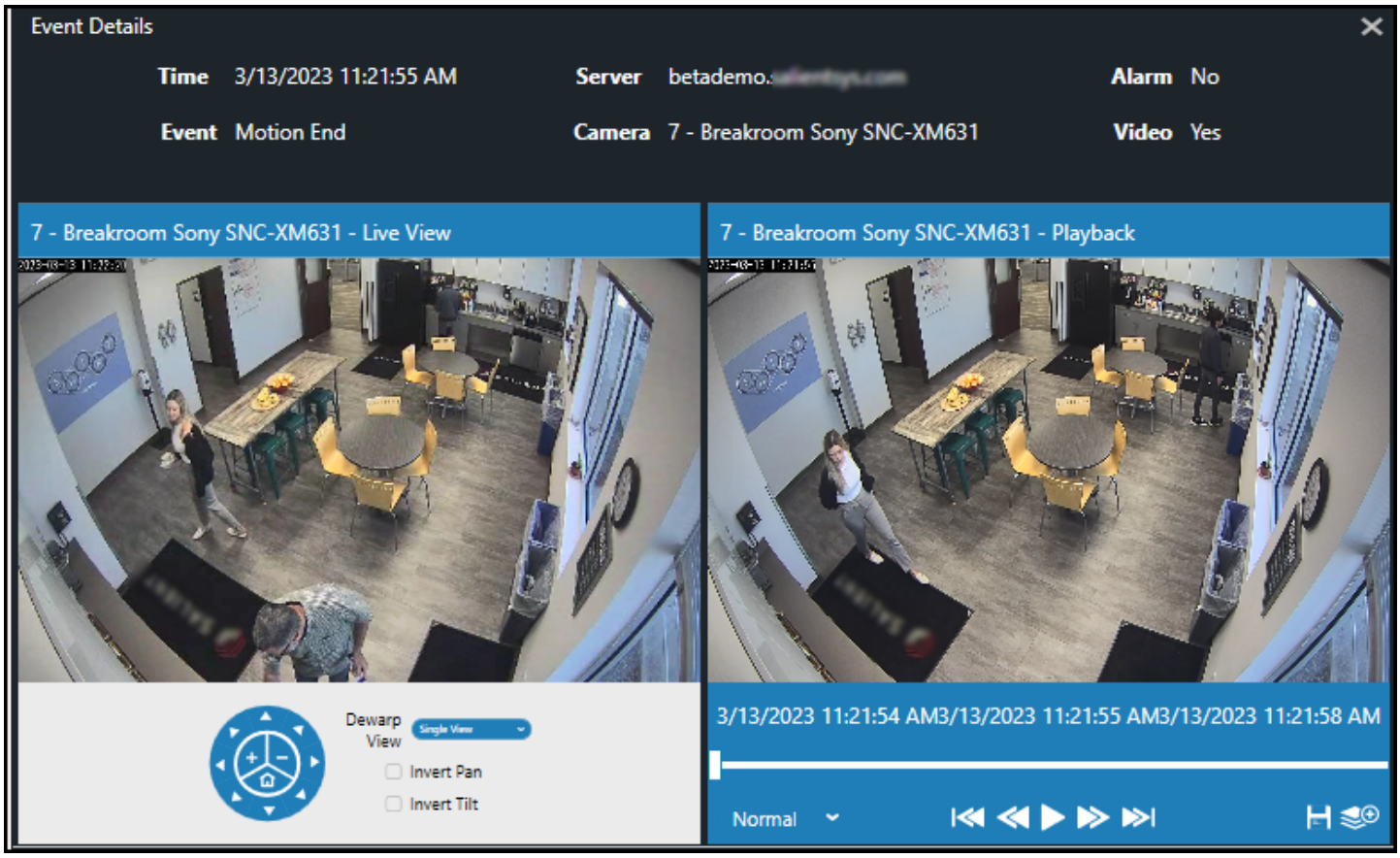
Displaying an Event's Video

Selecting an event from the Events panel will both show a live view of the associated camera and begin playback of the event in the Event Details panel, discussed in the next section.

Event Details Panel

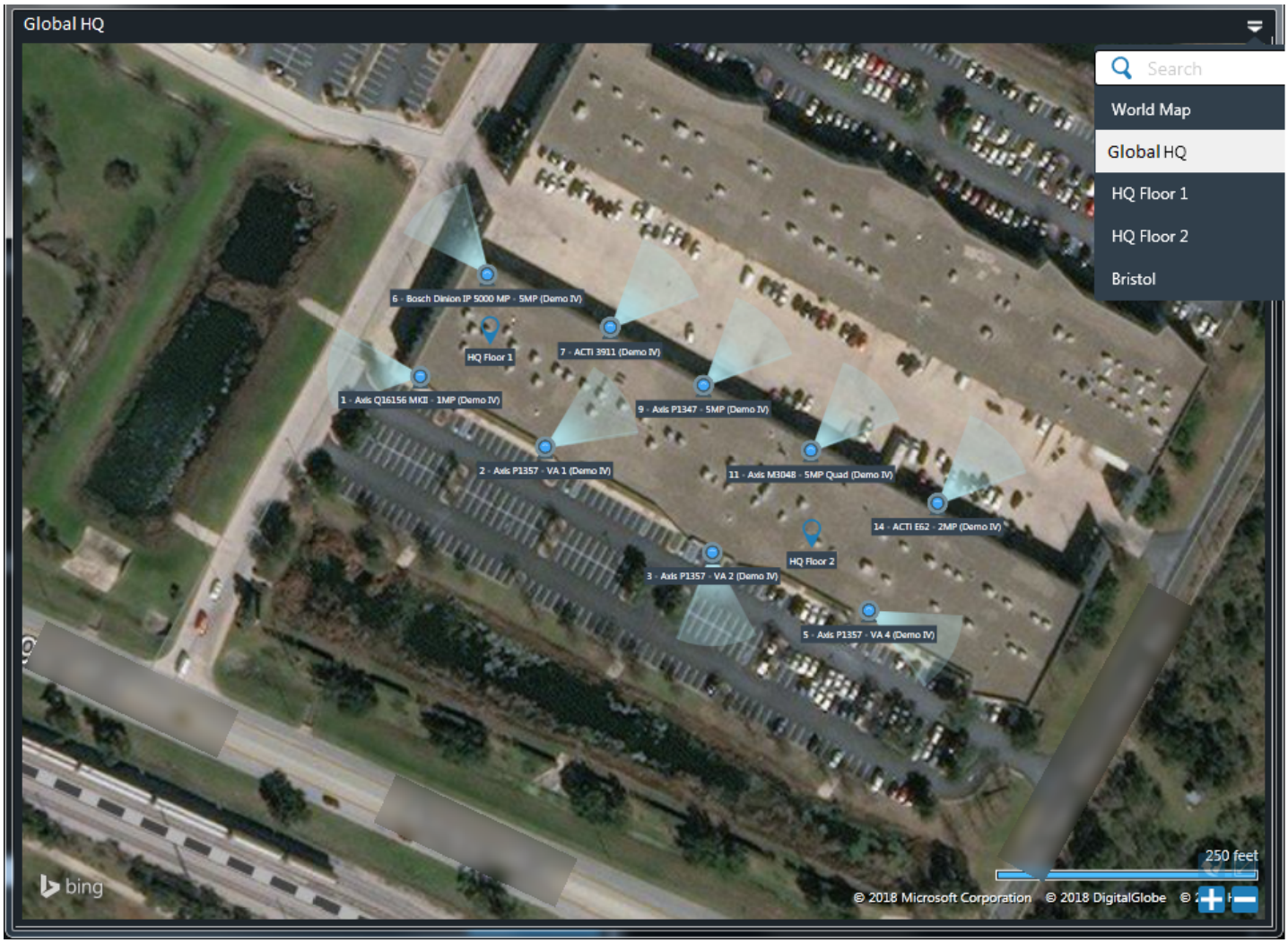
The Event Details panel displays recorded and live video in tandem from an event selected in the Events Panel.

In the video panels below, the left, Live View pane displays current video with PTZ controls, and the Playback pane displays the recorded video from the event that was selected in the Events Panel. The top of the Event Details panel displays the date and time of the video, the video server, the associated camera for the event, as well as alarm, video and event information. The clip associated with the event can be added to the Export Queue and a snapshot can be taken from the Playback pane.



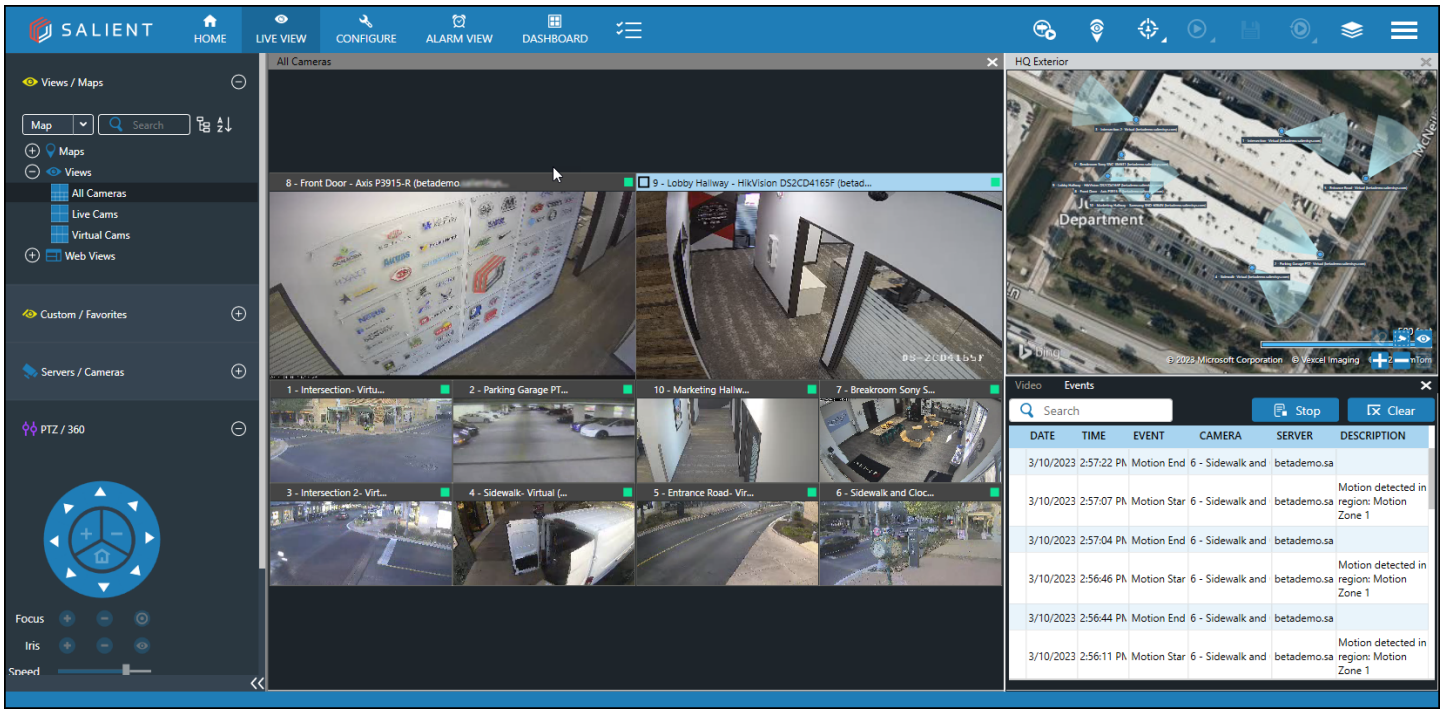
Maps Panel

The Maps Panel Maps displays video feeds that have been created by the Administrator. For more information on map creation and configuration, see Maps. The Maps Panel name is dynamic, adopting the name of the currently displayed map. A searchable list of predefined maps is available from the drop down menu in the upper right corner.



Live View Overview

CompleteView's Live View provides live access to video devices, predefined views, custom views, maps overlaid with video sources, and an Event panel. Most features within Live View require permissions, established by an Administrator by user or group when configuring the system. Predefined views are created by an Administrator. Click Views & Maps Creating Views and Templates to learn more about predefined views, and Click Users & Groups Introduction to learn more about permissions.



Live View Toolbar

The Live View toolbar resides at the top right corner of the Live View Panel. The toolbar's icons, descriptions, and applications are described below.

Tour Start/Stop

Starts and stops touring of created views.

Map View

Displays, in the Live View screen, all cameras positioned in the currently positioned on a map

QuickTrack On/Off

Toggles the QuickTrack virtual camera on or off for user selected video tiles*

Quick Review

Used to review a predefined amount of time for a specific camera

Steps:

1. Select a video stream (camera)

2. Select Quick Review
3. Select a time option

Save View

Live View permits users to create their own "custom views." The save button saves Custom Views after the views are created.

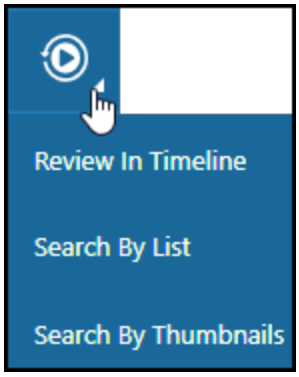
*For more information, see the Using QuickTrack Job Aid video at the link below. Note also that Quick-Track recordings do support audio.

https://support.salientsys.com/knowledgebase/training-resources/

Recorded Video

When selected, displays options for reviewing recorded video from the menu displayed below.

Recorded Video Menu



Option	Description
Review in Timeline	Returns a single video image with a timeline below the image. The timeline begins at midnight and encompasses twenty-four hours.
Search by List	Lists a set of recorded video clips. The top result in the list automatically plays when the playback screen appears. The list of results includes start and end times of the recorded video and a recording type indicator.
Search by Thumbnails	Transitions to Playback's Thumbnail search screen, and immediately proceeds to generate a thumbnail search using the default twenty-four clips over twenty-four hours, see Search Video for more information.

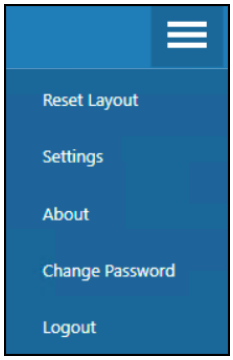
Export Queue

Export Queue redirects the user to Playback's video queue. To learn more, see Export Queue for more information.

Menu

Selecting the menu icon produces the options discussed below.

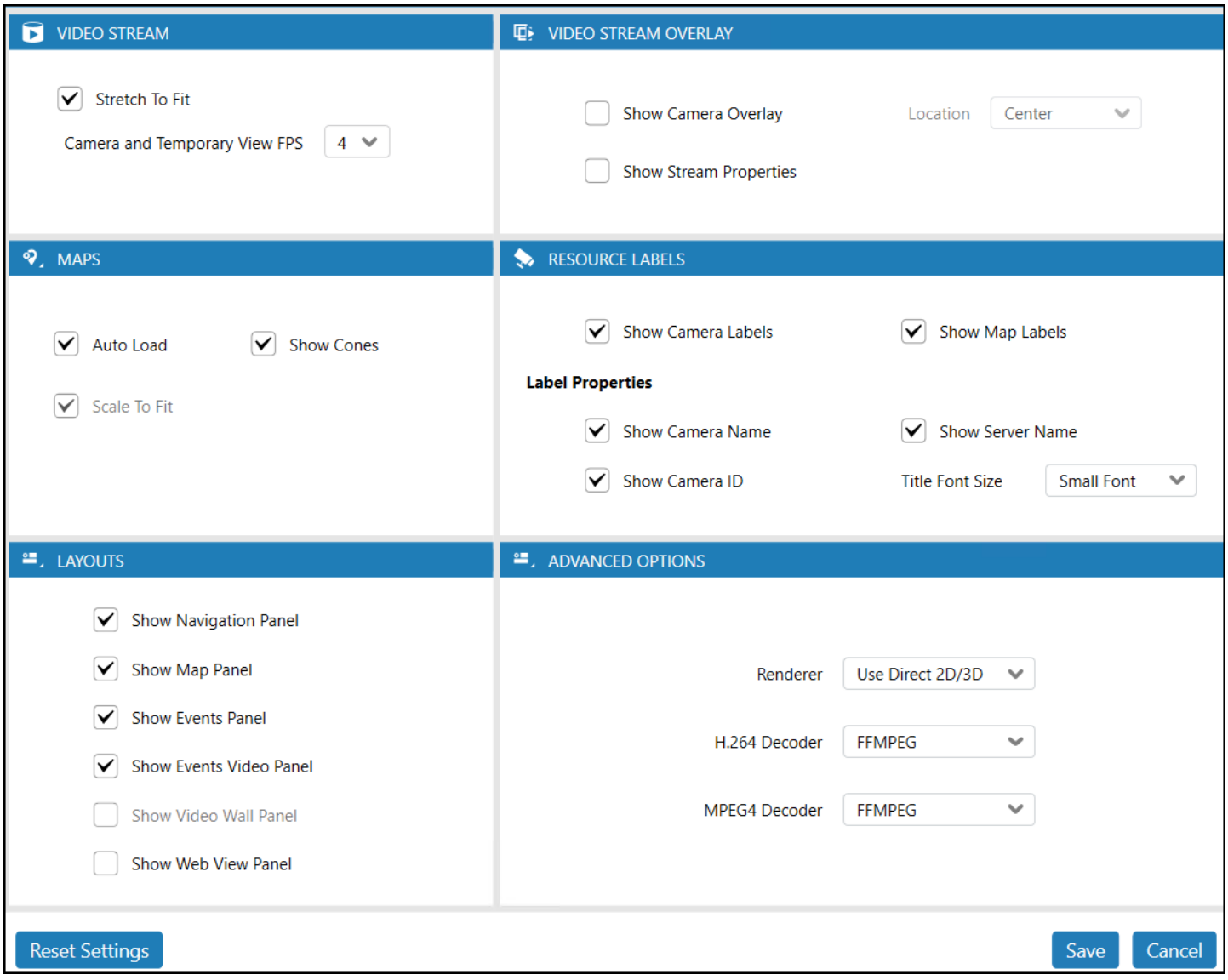
Menu Options



Option	Description
Reset Layout	Returns the Live View layout to its original state
Settings	Opens Live View Settings. See below.
About	Displays software version
Change Password	Allows user to change VMS password
Logout	Closes the CompleteView client

Live View Settings

When selected, a panel appears allowing configuration of Live View display options. Information on the pages to follow will break down each of the panels and what they control.



Video Stream

Stretch to Fit

When selected, Stretch to Fit expands images to fit within the video tile. Stretch to fit may help to clean up video tiles that have black banding around the displayed video.

FPS (Frames Per Second)

The dropdown allows selection of the desired frame rate for live viewing. Because live video streams from the Recording Server to the CompleteView client, live-view FPS will never exceed the Recording Server's configured frame rate. Example: if a camera is set to record at 15 FPS in the Recording Server, and the user selects 30 FPS, the live video feed will increase to 15 FPS but will not exceed 15 FPS.

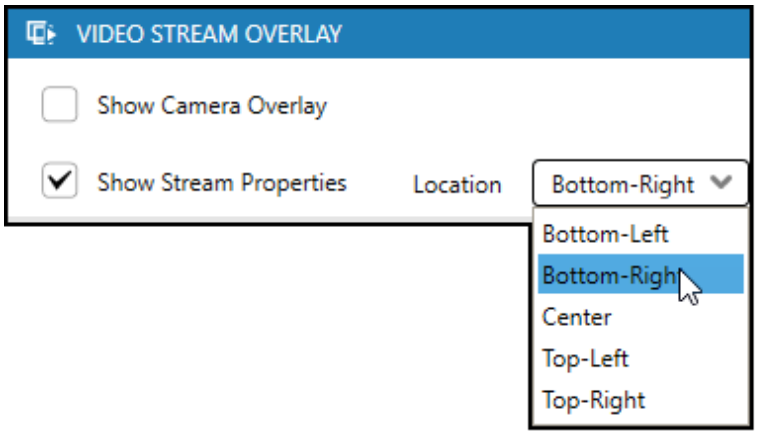
Video Stream Overlay

Camera Overlay

When selected, Camera Overlay places the camera name in a selected location on the screen.

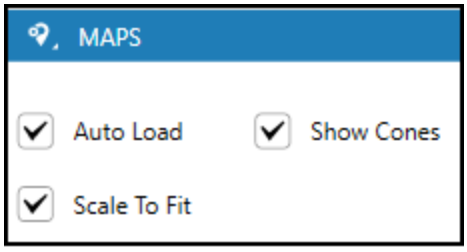
Show Stream Properties

Show Stream Properties displays Compression, Frames Per Second, Resolution, Bitrate, and Transcoder information from the Recording Server to Live View. Users may select the display location for the stream's properties.



Maps

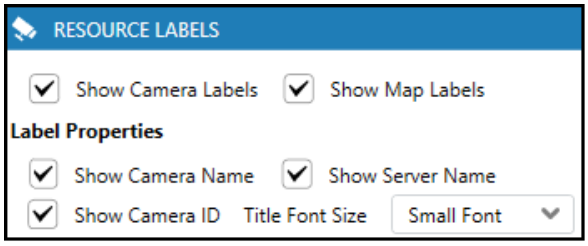
Auto Load Map	Maps that are associated with a view will automatically load in Live View.
Scale to Fit	Maps are automatically scaled by CompleteView to fit within the allotted map area.
Show Cones	Toggles the visibility of camera cone graphics within the map.



Resource Labels (Maps)

Map Resource Labels

Option	Description
Show Camera Labels	Displays camera labels on the map
Show Map Labels	Displays map's labels
Show Camera Name	Displays the camera name on the map
Show Server Name	Displays the server name on the map
Show Camera ID	Displays the camera ID on the map
Title Font Size	Allows font size selection

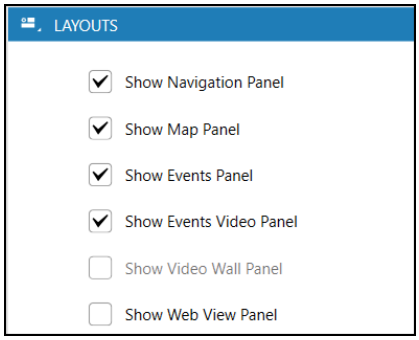


Layouts

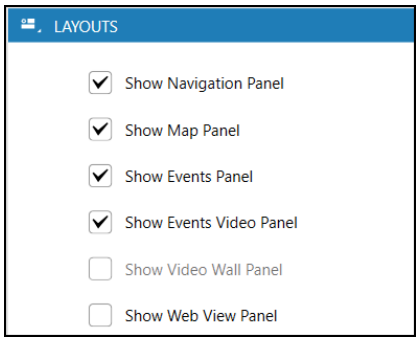
Layouts enables the user to determine what comprises the overall Live View experience. Boxes that are checked are displayed. If all boxes are unchecked and saved, video tiles will continue to display.

Layout Options Menu

Option	Description
Show Navigation Panel	Displays the Navigation Panel when checked
Show Map Panel	Displays the Map Panel when checked
Show Events Video Panel	Displays the Event Panel when checked
Show Video Panel	Displays the Video Panel when checked
Show Video Wall Panel	Displays the Video Wall Panel when

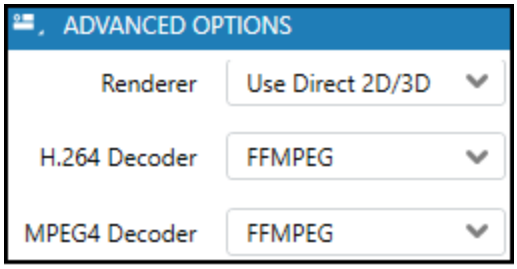


Option	Description
	checked
Show Web View Panel	Automatically displays Web Views in the Events Video Panel



Advanced Options

Advanced options specifies the renderer and decoder to be used when displaying video locally. By default, the Direct 2D/3D renderer is selected, along with FFMPEG for both H.264 and MPEG4 decoding. Unless specifically required, the default should be left in place. The Direct2D/3D renderer requires Direct3D to be present and enabled on the client workstation. If Direct3D is not present, this option will be grayed out, and GDI will be automatically selected.

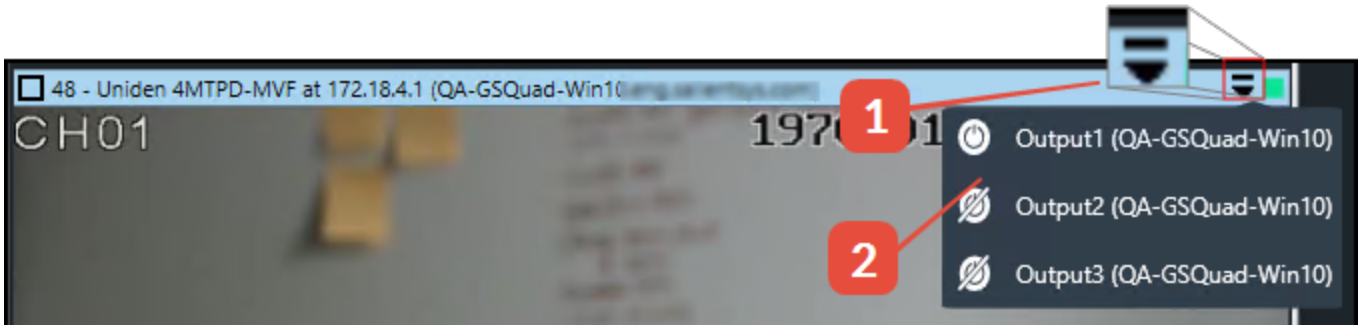


Alarm Device Output Trigger

Alarm Device outputs associated with either individual cameras or cameras located within a View may be manually triggered within Live View.

Steps:

1. Select the Output Triggers icon in the upper right corner of the camera window.
2. Select the desired Output.

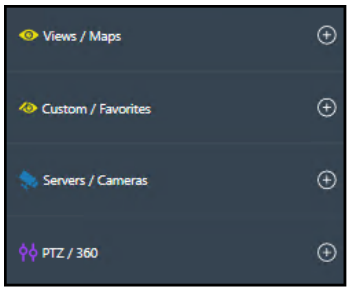


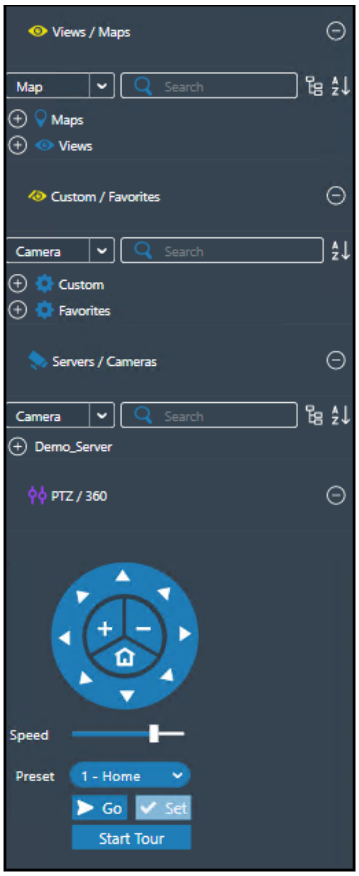
In addition, outputs may be manually triggered within Dashboard and Dashboard search, Alarm View, and anywhere the Output Triggers icon is displayed.

Navigation Panel

The Navigation Panel is subdivided into four sub-panels, providing access to Views/Maps, Custom/Favorites, Server/Cameras, and PTZ/360. The sub-panels have named containers that hold objects. See collapsed and expanded views to the right.

CompleteView allows end-user creation of sharable views, view templates, and maps from Live View's Navigation Panel, presuming the user has proper permissions. Administrator predefined views must be changed by the Administrator.

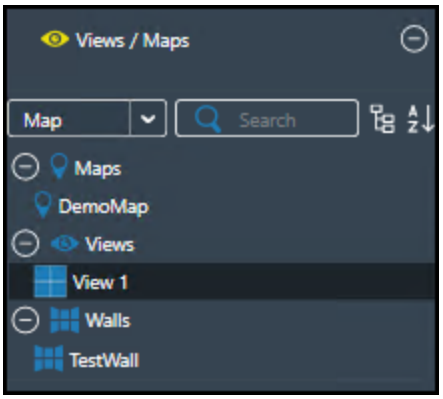




CompleteView allows end-user creation of sharable views, view templates, and maps from Live View's Navigation Panel, presuming the user has proper permissions. Administrator predefined views must be changed by the Administrator. For more information about predefined views, Click **Views / Maps Introduction**, for more about user permissions, Click **Users & Groups Introduction**.

Views / Maps & Walls

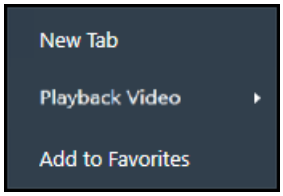
Selecting a View from the Navigation Pane displays the related camera video feeds in the display panel to its right. Use either the mouse or a keyboard's arrow keys to navigate the menus. Views and Maps are created by an Administrator.



Views Right Click Menu

Right clicking a View produces a dynamic submenu, the features of which are defined below.

New Tab	Creates a floating window and is present in all Client-Live View right click menus
Playback Video	Permits the user to select Review in Timeline. All cameras from the view will be selected for review.
Add to Favorites	Permits the user to add the selected view to their favorites, located in the navigation menu under Custom/Favorites.*



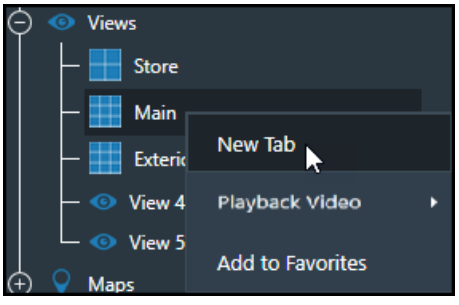
*Favorites are available on the local Desktop Client on which they were created. To create a Favorite, a user must be given specific access to the camera and/or view. Access to a camera or view through a group is not sufficient to add the camera or view to a Favorite.

New Tabs - Float Windows

CompleteView's New Tab feature enables the user to create and float additional Live View panels for view layouts, cameras, events, maps, and custom views. Floating panels may be freely moved to different areas of the client desktop. By default, all display type panels are docked.

Steps:

1. Select/ highlight in the navigation panel any listed view, map, specific camera, or video tile in the live view window.
2. Right-click and select New Tab
3. Click and hold the mouse pointer on the window
4. Drag the window to the desired position



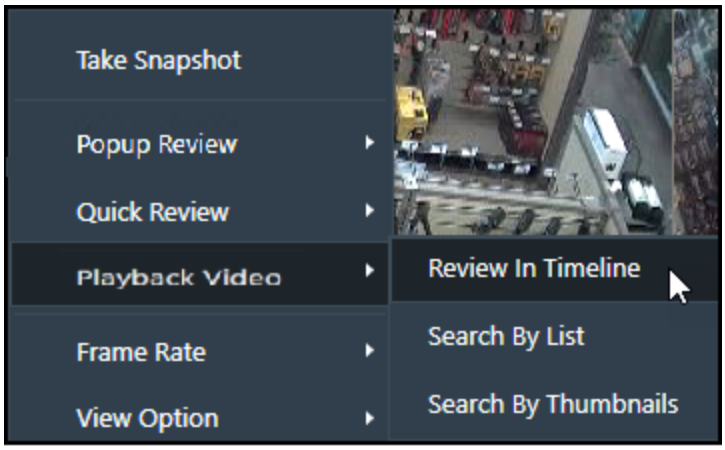
Note: Floated objects may be sized by grabbing the lower right corner of the screen, holding down the mouse button, and pulling to size.

View Recorded Video from Live View

Review recorded video for a specific camera from a view layout.

Steps:

1. From the Navigation Pane, right-click on any view.
2. Select Playback Video from the menu,
3. Then select Review in Timeline



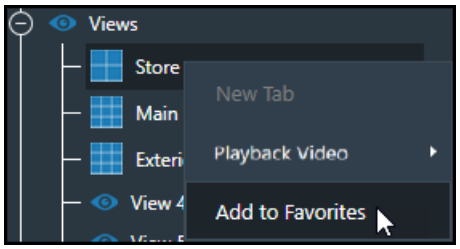
Playback will launch and display the selected video feed and its timeline from the originating live view. Selecting the checkboxes in the corners of multiple feeds will display those feeds and their respective timelines.

Add to Favorites

Views, maps, and individual cameras may be selected for addition to the Custom/Favorites container. As previously noted, Favorites are available on the local Desktop Client on which they were created. To create a Favorite, a user must be given specific access to the camera and/or view. Access to a camera or view through a group is not sufficient to add the camera or view to a Favorite.

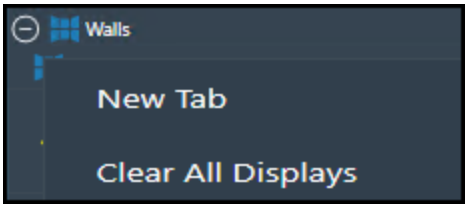
Steps:

1. Select the view/map from within its panel.
2. Right-click on the view/map to display the menu
3. Select Add to favorites



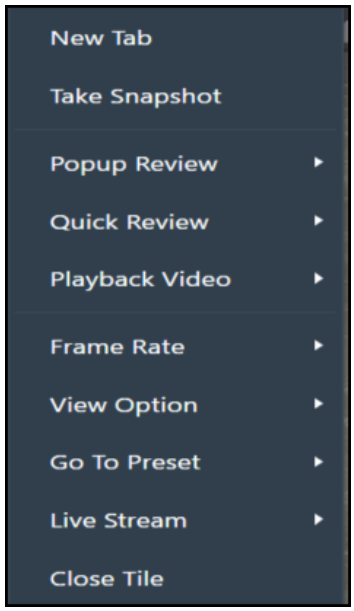
Walls Right Click Menu

Right clicking within Walls allows for a New Tab to be floated or to clear the current contents of populated displays.



Live View Right Click Menu

Option	Description
New Tab	Displays the selected camera's feed in its own new tab
Take Snapshot	Captures the current image and prompts for a location to save the snapshot
Popup Review	Opens a popup window and plays recorded video from the selected camera for playback in increments from 30 seconds to 10 minutes
Quick Review	Opens a new window and plays recorded video from the selected camera for playback in increments from 30 seconds to 10 minutes
Playback Video	Allows review of recorded video by three different means: a. Review in Timeline b. Search by List c. Search by Thumbnail
Frame Rate	Allows configuration of the frame rate for the current camera from 1 - 30 FPS. Because live video streams from the Recording Server to the CompleteView client, live-view FPS will never exceed the Recording Server's configured frame rate.
View Options	Sets whether the camera is displayed in its native aspect ratio or is stretched to fit the window
Go to Preset	Presents a list of PTZ presets for the selected camera, if available
Live Stream	Selects one of the three live viewing stream options: a. **Reconnect:** initiates a reconnection attempt between the Live View Client application and the Recording Server for the current camera. b. **Disconnect:** disconnects the video stream between the Live View Client and the Recording Server for the current camera. c. **Stream Properties:** determines if the video tile's stream properties should be displayed and sets the location of the information. d. **Resolution Scaling:** toggles functionalty of resolution scaling for that tile.
Close Tile	Closes the currently selected video tile. To close multiple tiles, select the checkboxes in the title bars of the desired tiles, right click, and select Close Tile. Closing a tile in a View will not eliminate that cam-

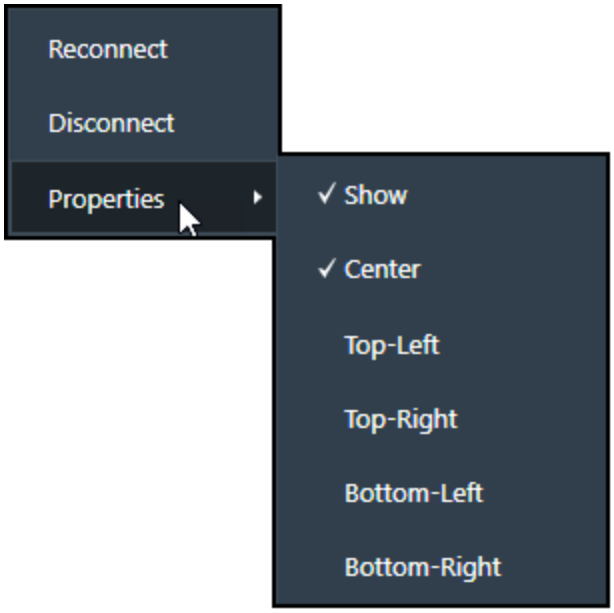


Option	Description
	era from the View, but only close it from that instance. Selecting a different View or camera then returing to the previous View will bring back the closed tile.

Display Stream Properties

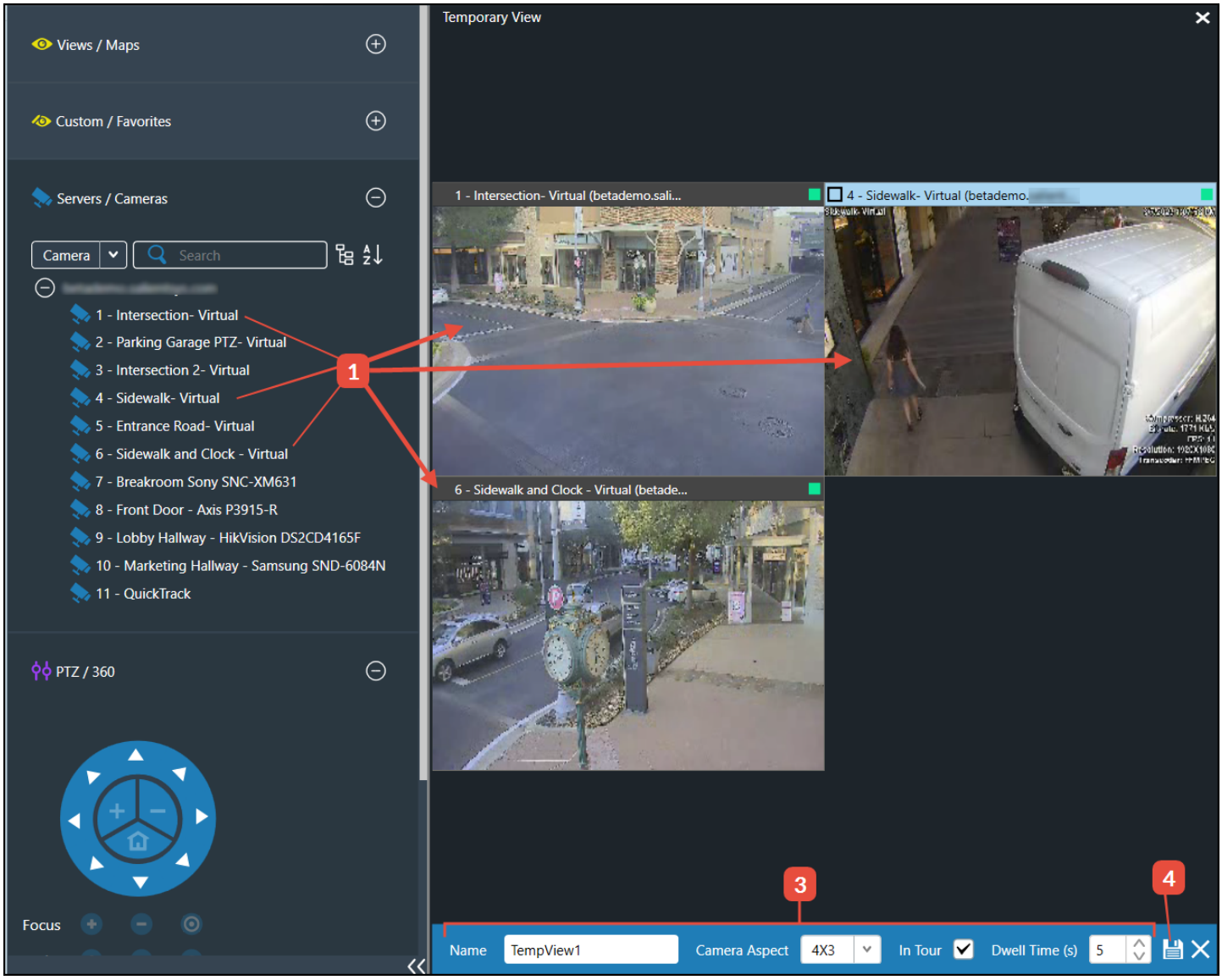
Steps:

1. Right-click on the video tile
2. Select Live Stream
3. Select Properties
4. Select Show to toggle-on Stream Properties
5. Select where Stream Properties should display
6. Deselect show to disable Stream Properties



Temporary Views

CompleteView allows for the creation of custom views within the Live View module. Temporary Views may be kept for as long as deemed necessary.



Creating a Temporary View

To create and save a Temporary View:

1. Drag the desired camera(s), Views, Maps, etc., from the left pane into the camera pane.
2. To save the view, first click the Save/Push button from the main toolbar menu.

3. Enter or select the pertinent information from the menu that appears at the bottom of the Temporary View pane.
4. Save the view.

The newly saved view will appear under Custom/Favorites, Views.

For more in-depth discussion of Views, see [Views / Maps Introduction](#).

GeoView

Similar to Temporary Views, GeoView allows for rapid creation of a view from cameras embedded in a map. This approach allows personnel to keep track of an unfolding situation in real time, such as following an individual moving across multiple cameras' fields of view.

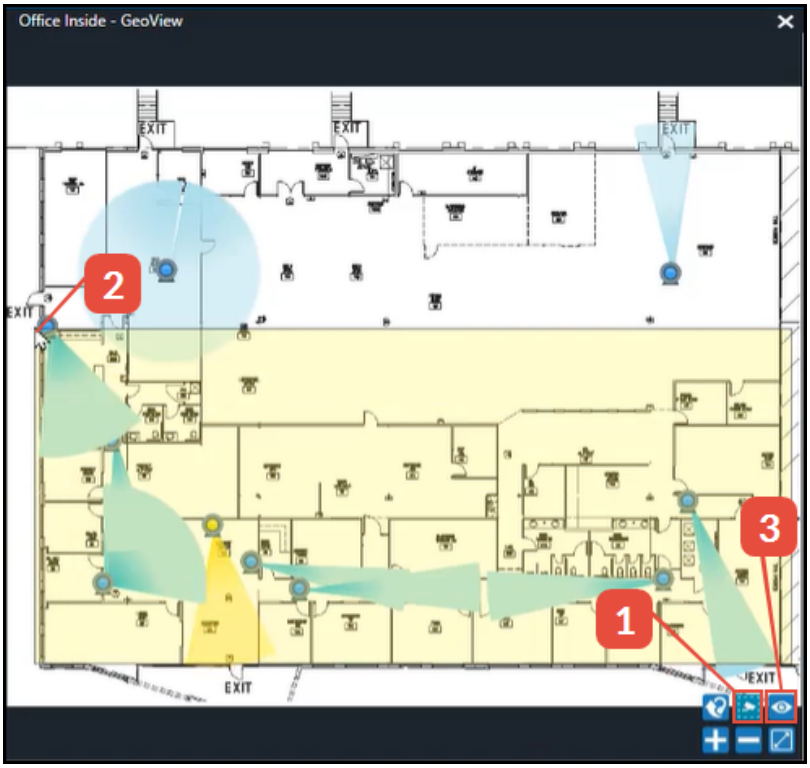
A typical scenario would begin with a person of interest triggering a motion event on a camera associated to a map. Security personnel could assess which cameras near the triggered one are the most relevant to the situation at hand, then create an ad hoc view of those cameras from the map to monitor the individual in question.

For more information, see the Maps and GeoView video in the Feature Demos section of the Salient website here: https://www.salientsys.com/about-salient/news/video-library/ .

Creating a GeoView

From within the Live View Maps pane:

1. Click the Select Camera icon
2. Drag a box around the desired nearby cameras
3. Click the View icon



After clicking the View icon, the selected cameras will populate in the camera pane.

Saving the GeoView

Saving the GeoView is identical to saving Temporary Views, described above.

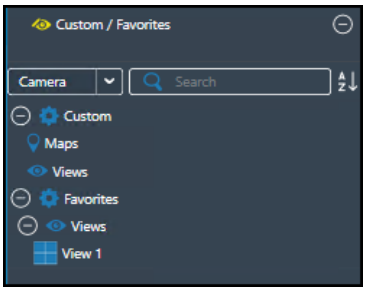
Custom / Favorites

Custom tools allows creation, modification, and deletion of Custom Views from the Recording Server's cameras. Custom Views are automatically assigned to the creator's credentials and will only appear in Live View when the originator's credentials are entered during CompleteView Client login. Note that Favorites are available on the local Desktop Client on which they were created. To create a Favorite, a user must be given specific access to the camera and/or view. Access to a camera or view through a group is not sufficient to add the camera or view to a Favorite.

For clarity, some UI elements may be omitted from the following information.

Custom Views

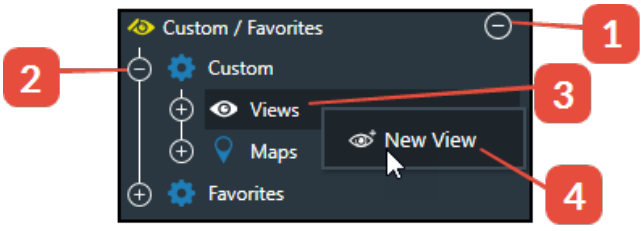
Custom Views are views created by the end user and saved on the user's desktop. Custom View creation is done from the Live View Panel. All live viewing options and right-click menu choices for Administrator created views are available for Custom Views.

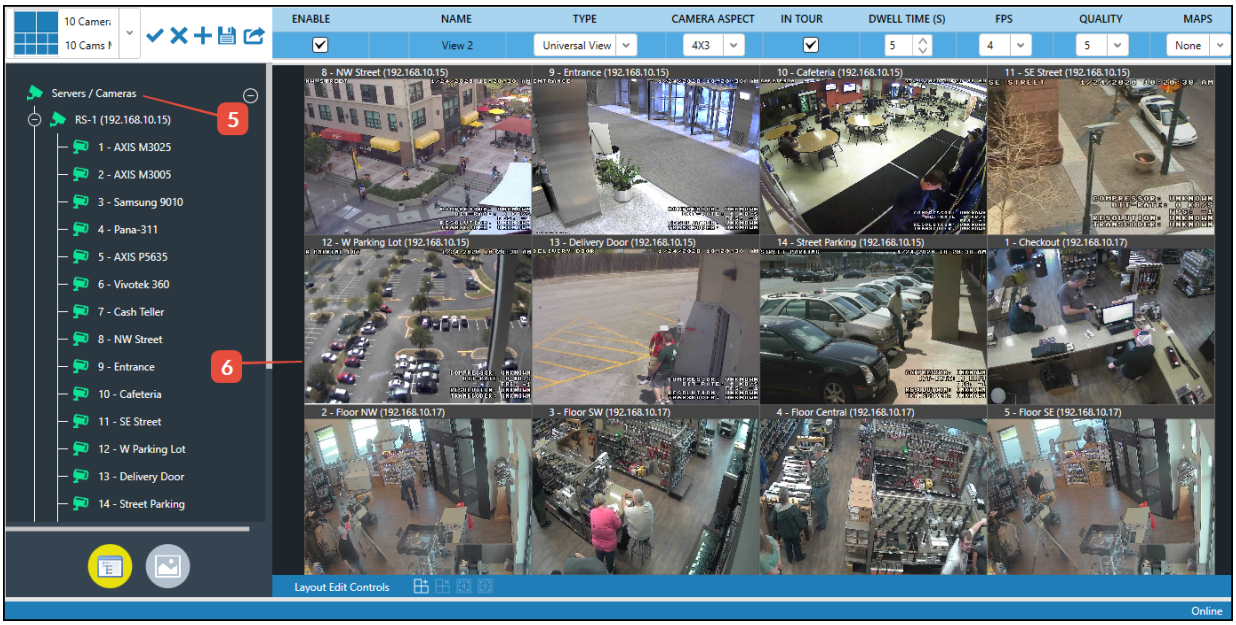


Create Custom Views

Steps:

1. Open Custom/Favorites Panel
2. Open Custom
3. Under Custom, right-click on Views
4. Select New View
5. Open the listed servers to select cameras
6. Drag and drop the cameras into the pane to the right of the list of servers and cameras





Additional Information

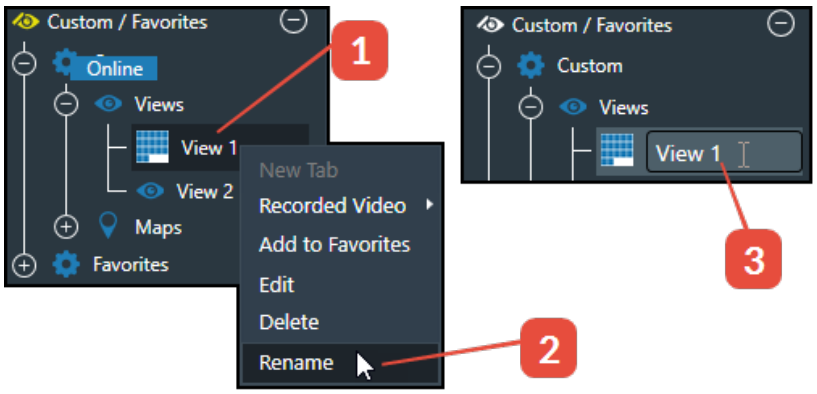
Cameras may be added as needed from different Recording Servers, and may be combined into the same Custom View. As cameras are added, the video tiles will scale automatically. Too many cameras within the same view will adversely affect legibility. The desired level of detail should determine how many cameras are added to a given view. Cameras may be dragged and dropped from a Server's list of cameras into an existing camera tile to replace an existing camera, if desired.

Name Change

Users may change Custom View names.

Steps:

1. Right click on the Custom View that needs a new name
2. Select Rename from the menu
3. When the View name is highlighted, type the new name over the existing name



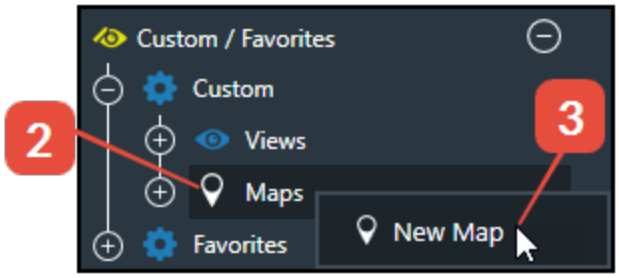
Views/Maps - Custom Maps

CompleteView allows creation of custom maps with icons of video feeds in the Live View panel. PNG, JPG, GIF, and BMP images may be imported into CompleteView for use with systems that are not connected to the Internet. For connected systems, satellite images from Bing© Maps may be predefined by the Administrator, and will display in Views/Maps in the Live View Navigation Panel. End users may create their own custom maps, which will display within Custom and Favorites in the Live View Navigation Panel.

Create a Map in Custom/Favorites

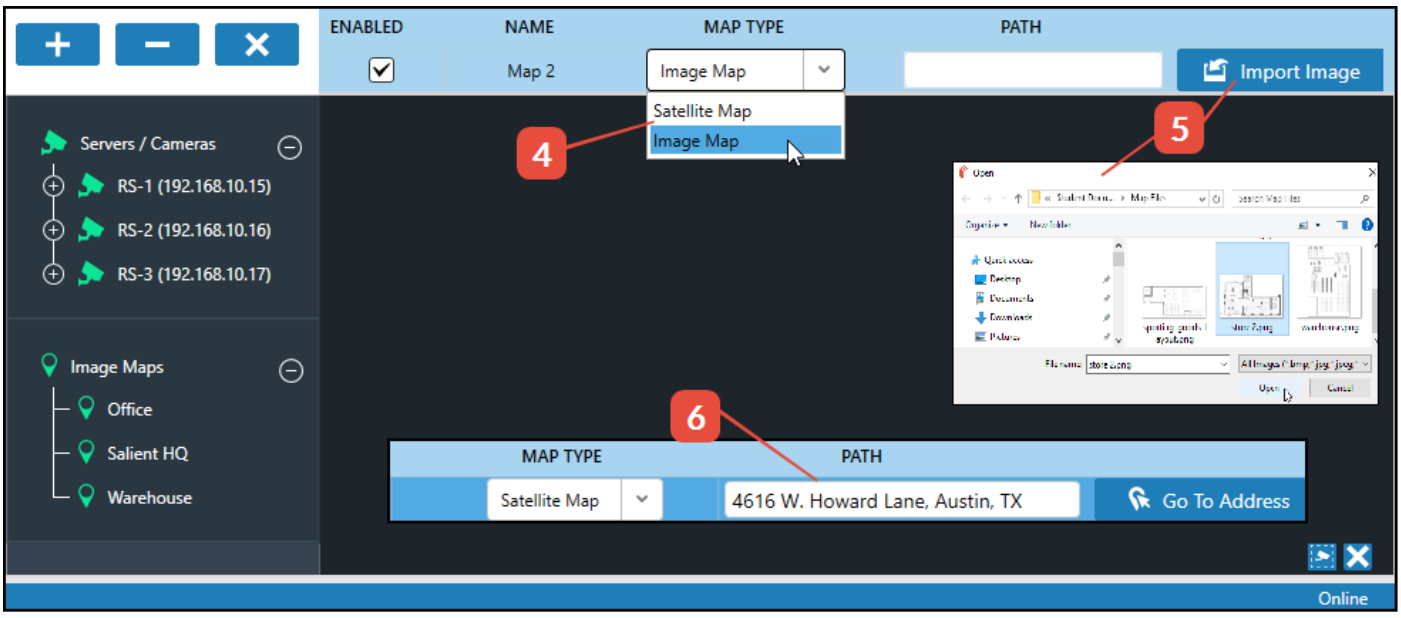
Steps:

1. Within Custom/Favorites, locate Views and Maps
2. Right-click on Maps, a menu will appear
3. From the menu, select New Map



4. When the Map Construction screen opens, select from the Map Type menu the type of map for construction.
5. Select import Image (for a static map image) to access the windows explorer. In explorer, navigate to the image you wish to use.
6. If using a satellite Map, enter the mailing address, place of interest name, or landmark name into the Path.

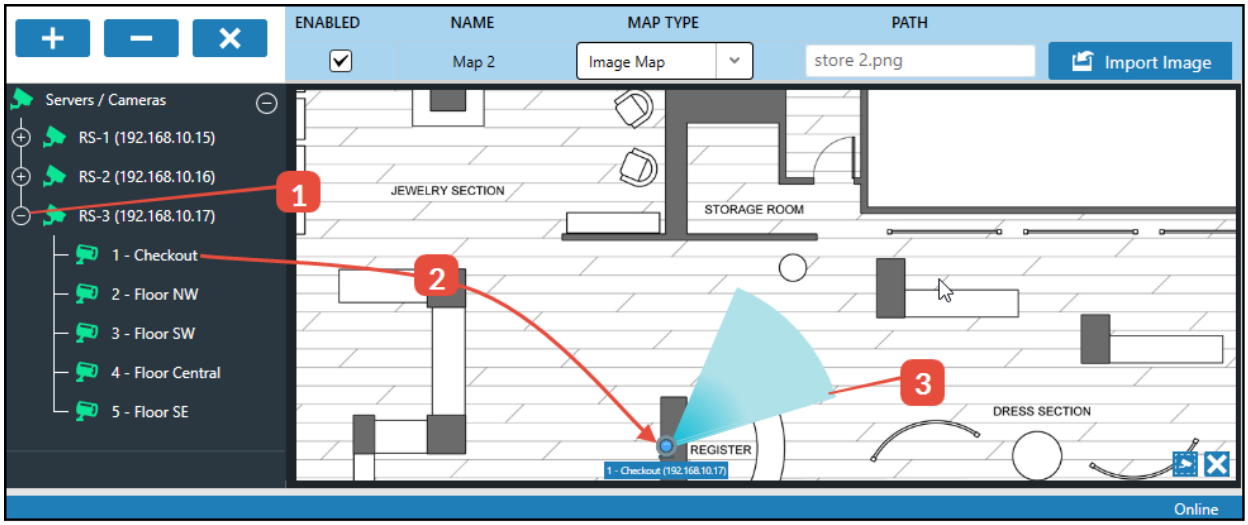
   Note: the dynamic button to the right of the path bar. It will reflect the type of image being utilized (Go To Address or Import Image).



7. Once your map is selected and displayed, save the configuration.

Add Cameras to the Map

Place cameras on the map in order to most accurately represent the real world physical locations and fields of view of the cameras.

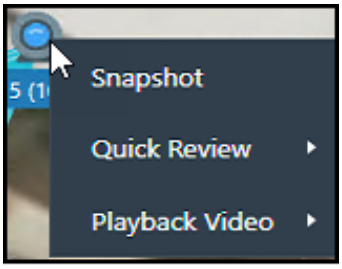


Steps:

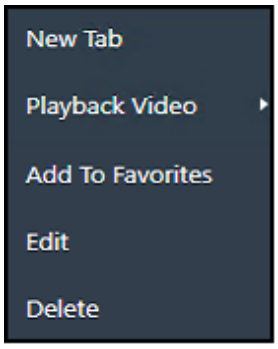
1. With the map image in place and centered as desired, open the server hosting the cameras to be placed on the map.
2. Drag and drop the cameras from the appropriate server.
3. Adjust the camera's cone to proper orientation, field of view, and distance.
4. Save your work by selecting the save icon located at the top right corner of the Toolbar.

Camera Icon Menu Options

The camera icons on a map with video host a right click menu. The icons allow the user to take a snapshot of the video occurring, or to play back recorded video and are similar in functionality to the corresponding Live View options.



Custom Map Menu Options



Option	Description
New Tab	Frees and floats the map panel
Playback Video	Opens Review In Timeline menu. If Review In Timeline is also selected, the user is redirected to Playback
Add to Favorites	Adds the selected map to the favorites group
Edit	Edits the map image and details of the map, including cameras
Delete	Deletes the selected map

Map Icon Tools

At the bottom right corner of many maps are icons (tools) used to make adjustments to the appearance of the map.

View Live Cameras displays the map's cameras in the video display area.

Switch to Satellite map. No action occurs if a satellite map does not exist (i.e. if no Internet connection is present).

Select Cameras.

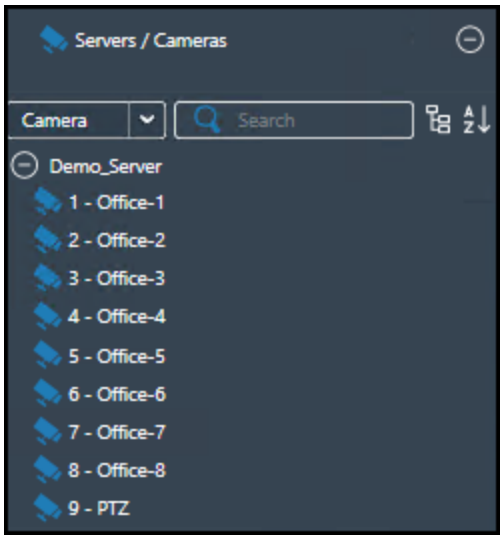
Zoom in.

Zoom out.

Scale to Fit.

Servers/Cameras

The Servers/Cameras sub-panel provides access to servers and cameras in order to alter Views or drag and drop cameras into a pre-configured view for temporary viewing. Multiple cameras may be selected using traditional cntrl/shift +click and drag methods.

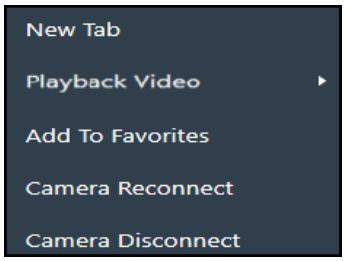


Servers/Cameras Right Click Menu

Right clicking a Camera produces a dynamic submenu, the features of which are defined below.

Right clicking a Recording Server with bandwidth control enabled will allow starting and stopping of event monitoring.

New Tab	Creates a floating window and is present in many Client- Live View right click menus
Playback Video	Permits the user to select Review in Timeline.
Add to Favorites	Permits the user to add the selected camera to favorites, located in the navigation menu under Custom/Favorites.*
Camera Reconnect	Stops streaming the selected camera to Live View
Camera Disconnect	Resumes streaming the selected camera to Live View



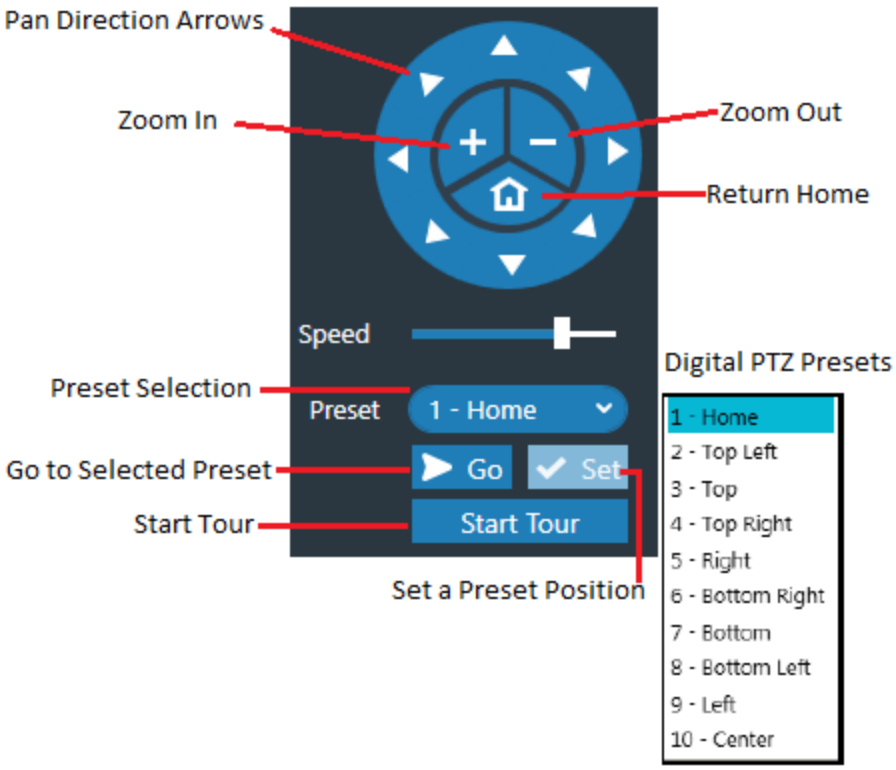
*Favorites are available on the local Desktop Client on which they were created. To create a Favorite, a user must be given specific access to the camera and/or view. Access to a camera or view through a group is not sufficient to add the camera or view to a Favorite.

To learn more about adding servers and cameras to CompleteView, Click Recording Servers Adding a Recording Server.

PTZ / 360

There are several methods to Pan, Tilt, and Zoom (PTZ) both digital and mechanical PTZ cameras in the Live View panel. Each video tile provides the user with “Click to Center” digital or true PTZ movement. In addition, pre-configured tours may be started and stopped by pressing the Start/Stop Tour button wherever it appears.

PTZ Controls



Digital PTZ is the default PTZ condition for all IP and analog fixed and mechanical PTZ cameras. Mechanical PTZ cameras that are configured with a Digital PTZ protocol will display the illustrated list of presets. Additionally, mechanical PTZ cameras may or may not be configured with PTZ preset positions. Therefore, when making a preset selection from the PTZ/360 panel for mechanical PTZ cameras, the resulting list of presets will be based on the camera that is selected. PTZ preset changes require permissions to set and are typically predefined by the Administrator or a management level user. To learn more about configuring PTZ presets, Click Recording Servers Camera PTZ.

Click-to-Center PTZ Control

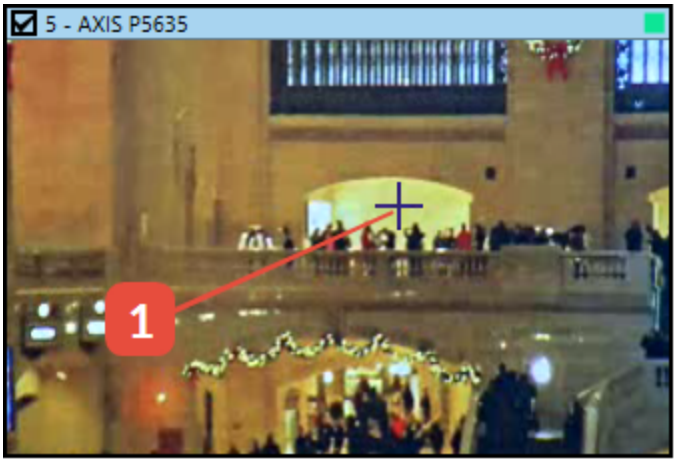
Clicking within a camera's field of view window will center the camera on that spot. Zoom is controlled using the mouse scroll wheel.

Digital PTZ Note

Digital PTZ requires the user to first zoom into the video stream using the mouse roller or PTZ joystick control before panning. The Pan and Tilt controls will allow you to move to the edges of the fixed camera's field of view.

Steps:

1. Left-click on a video stream and look for the crosshair.
2. Use the mouse roller to zoom into the video.
3. Move the crosshairs to and click on the area of interest or the object to be tracked.

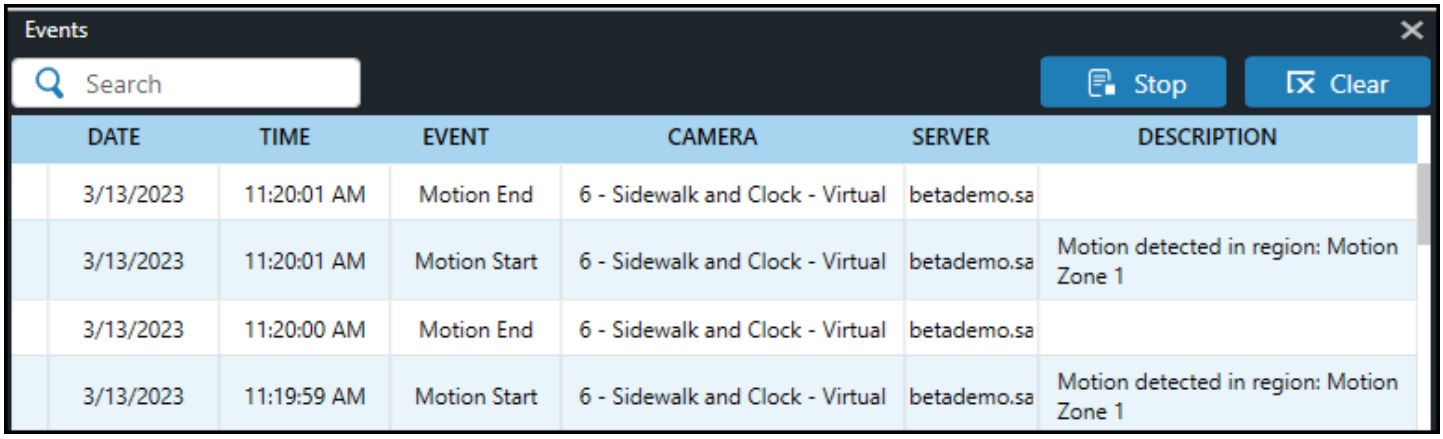


Fisheye PTZ Operation

On certain fisheye cameras, the pan and tilt functions may be inverted through the on-screen PTZ control. Those options will automatically appear when the camera is selected for viewing. In addition, the type of dewarped view to be displayed is selectable here, if available.

Events Panel

The Events Panel displays a text description for each motion or alarm event, also providing the user with a date, time, camera name, and the camera's server information.

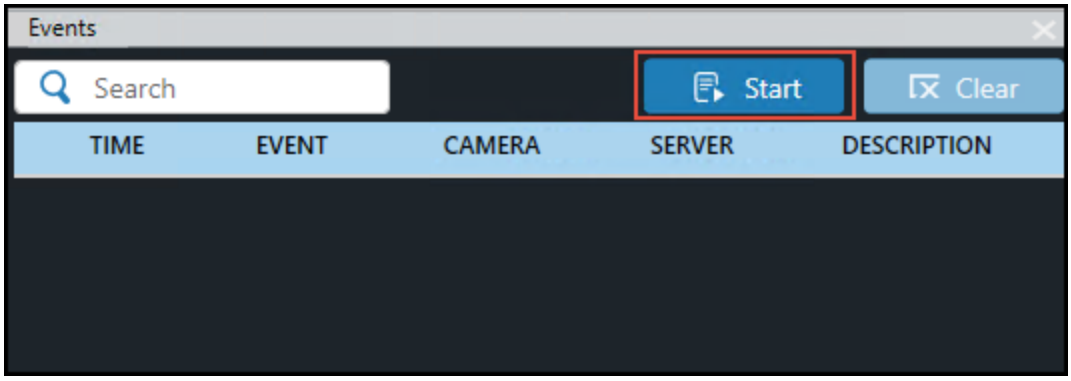


Search Event

Users may search for a particular event by name, event description, camera name, server name or time (hh:mm) by typing the criteria into the Search field in the upper left of the Event Panel and pressing Enter. Multiple values may be entered, separated by commas.

Stop/Start Function

In low bandwidth deployments, Recording Servers may be configured to report events only on demand. If events are not being displayed, events may be restarted by clicking the Start button in the Events panels of the relevant modules. See Bandwidth Control for more information.



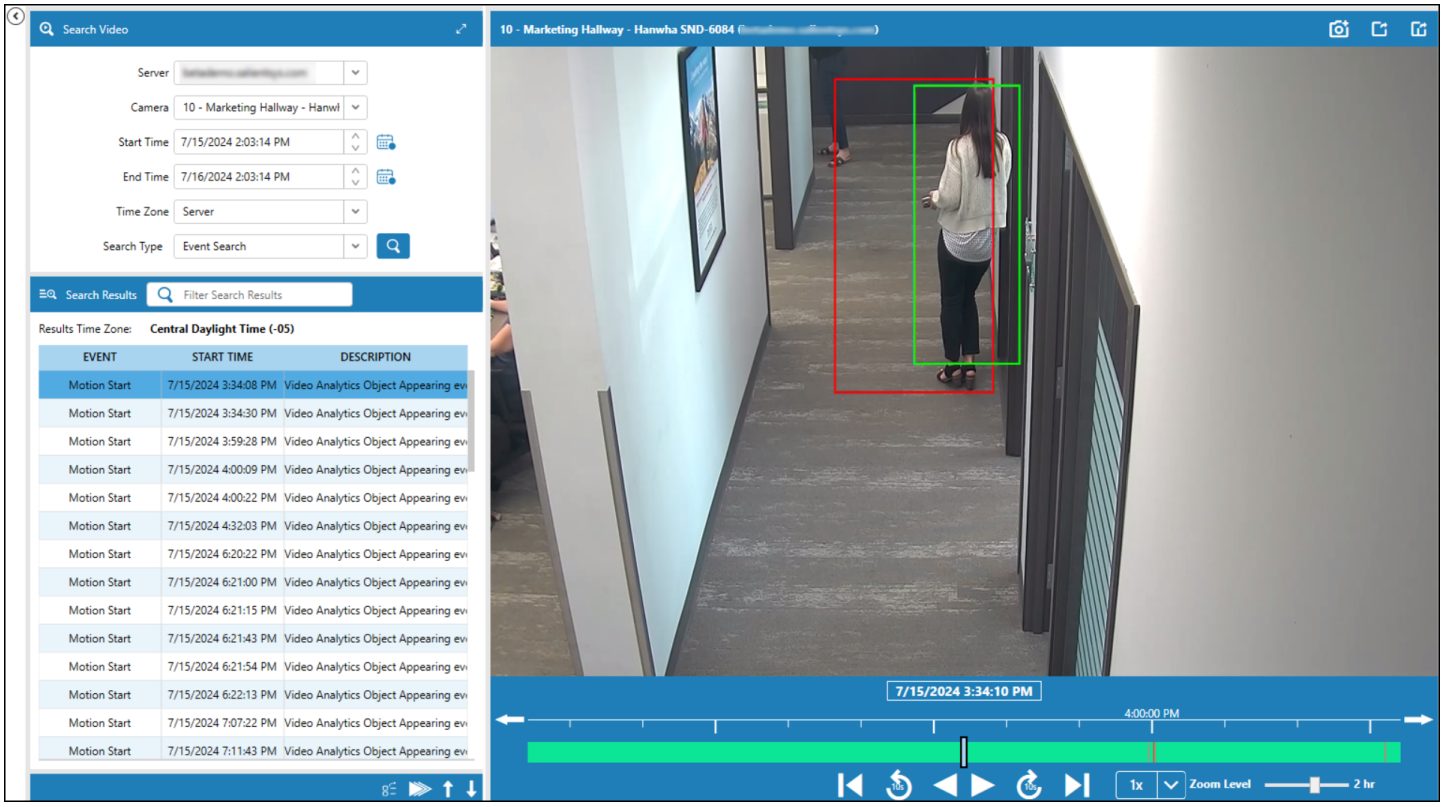
Note: Live events will not update in the Events Panel with search criteria in the search box. Clear the search with the Clear button.

Displaying an Event's Video

Selecting an event from the Events panel will both show a live view of the associated camera and begin playback of the event in the Event Details panel, discussed in the next section.

Playback Overview

CompleteView's Playback module allows for the search, review, and exportation of video recorded to a Recording Server. Each function will be discussed in its own subsequent section.



Playback Toolbar

Playback hosts a toolbar in the top right corner of the interface. Icons in the toolbar are unique to Playback.

Playback Video takes the user to the camera search screen from which cameras, views, and maps may be searched

Search Video launches a video search for specified cameras, servers, dates, and times.

Export Queue redirects the user to the Export Queue. For more information about the Export Queue, Click Export Queue.

Opens a menu displaying Stretch to Fit, About, Change Password and Logout options.

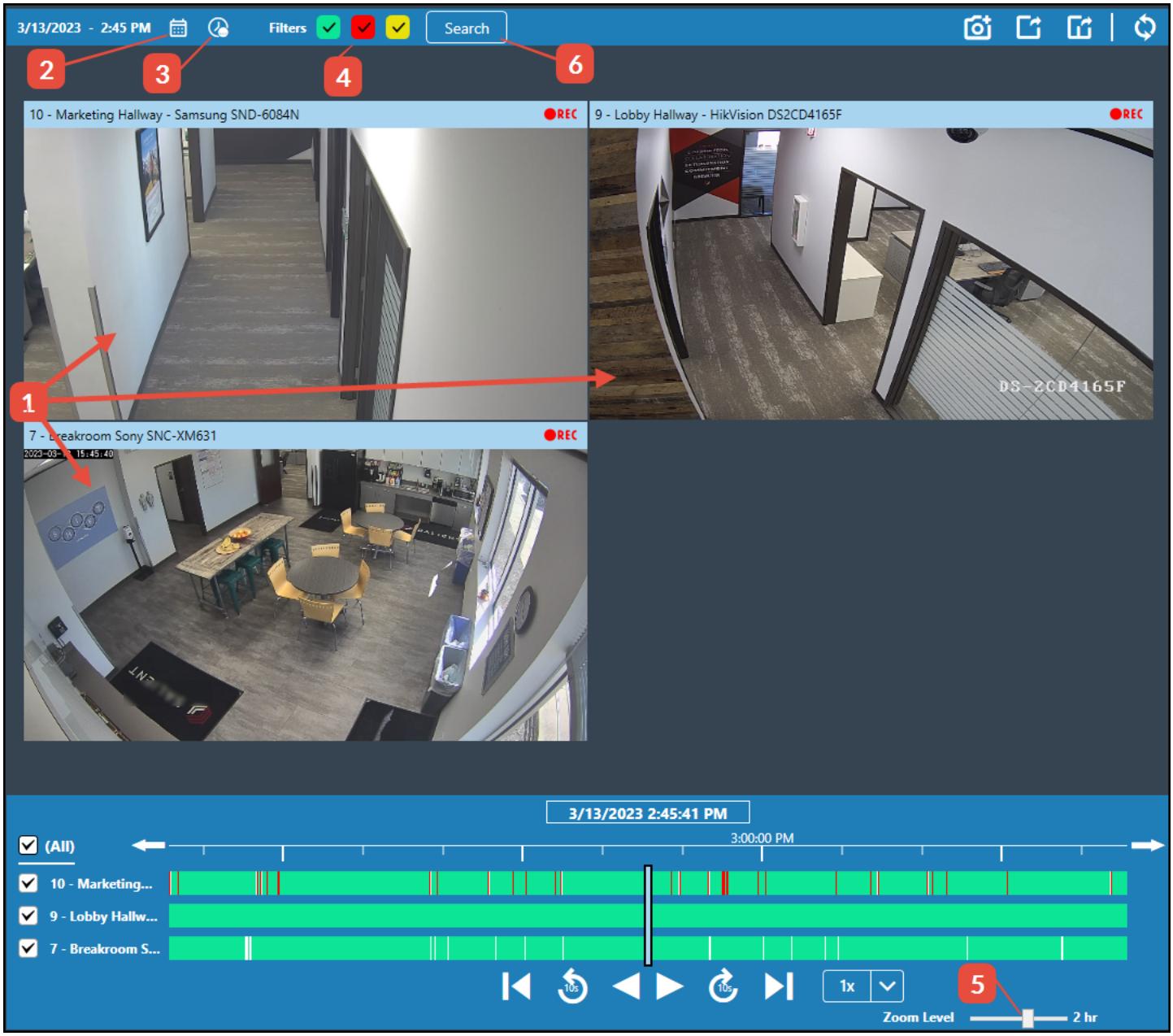
Playback Video

This section steps through the functionality of Playback Video and details its controls. Playback Video allows operators to easily review video from one or more sources in a single screen. This functionality differentiates it from Search Video, which allows for searching a single camera over the course of multiple days.

Playback Video Search

Playback Video allows an operator to go to a specific start time and date to begin reviewing video for the selected View, Map, or by selecting one or more cameras. A maximum of 16 total cameras may be reviewed at a time. If a View or Map contains more than 16 cameras, the operator will be prompted to select the 16 cameras to be displayed in playback. By default, the timeline will populate 2 hours of video; 1 hour before and 1 hour after the selected start time. The timeline may be adjusted to see up to 24 hours using the Zoom Level slider, described below.

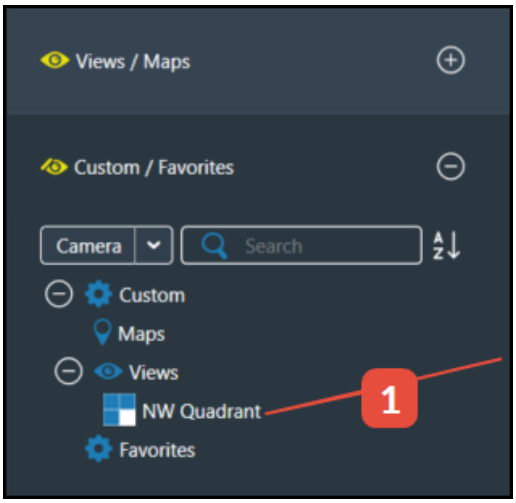
Performing a Search



The following steps are enumerated below and in the image above.

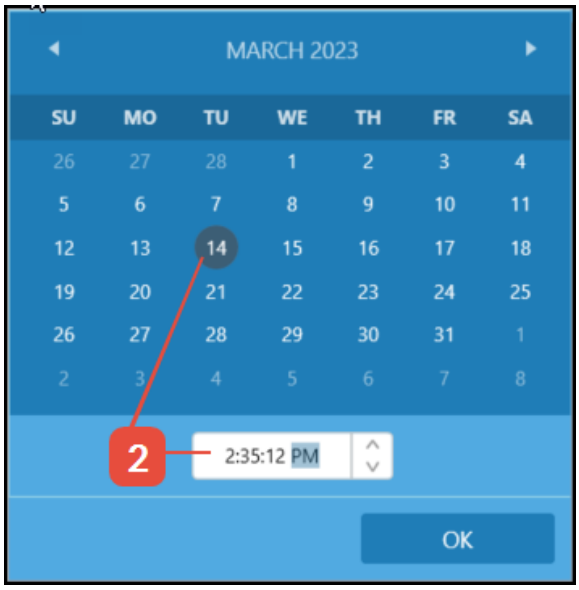
Steps:

1. Begin by dragging over a View, Map, a single or multiple cameras into the Playback Review Panel.



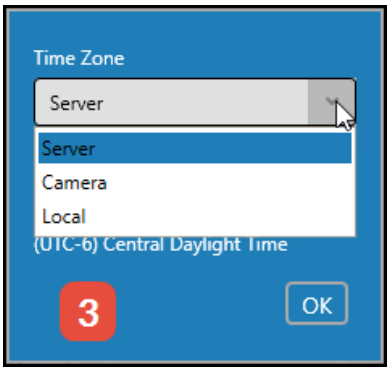
Multiple cameras may be dragged over one at a time or via standard cntrl+click/shift+click methods. Only one View or Map may be reviewed at a time, but cameras may be added to the Playback Review Panel once a Map or View has been added, for a total of up to 16. If a different Map or View is dragged in, then any currently displayed cameras, Maps, or Views will be replaced and the operator will be required to perform a new search.

2. Select the date and enter the starting time for the search .



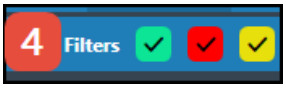
Playback Video is used to search video from a single day. The current position marker will be set at the midpoint of the returned timeline. For example, if a time of 2:35pm is entered with a Zoom Level of 2 hours (discussed below), the displayed timeline will begin at 1:35pm, end at 3:35pm, and display the current position marker at 2:35pm.

3. Select the desired Time Zone.



The Time Zone setting is configurable to use the time of a Recording Server via the Server option (default), a selected Camera, or the Local time zone, as determined by the time zone setting of the Desktop Client machine on which the search is being performed.

4. Select the type of recorded video to be displayed in the resulting timeline.



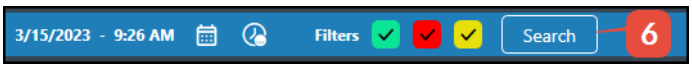
- Green - Continuous Recording
- Red - Motion Recording
- Yellow - Alarm Recording

5. Select your Zoom Level (optional).

The zoom level determines the initial duration of the displayed results, is adjustable from 1 minute to 24 hours, and defaults to 2 hours.

The Zoom Level can be adjusted after the results have been returned. Zooming out past the initial search duration may require refreshing the results by clicking the Search button again.

6. Click Search



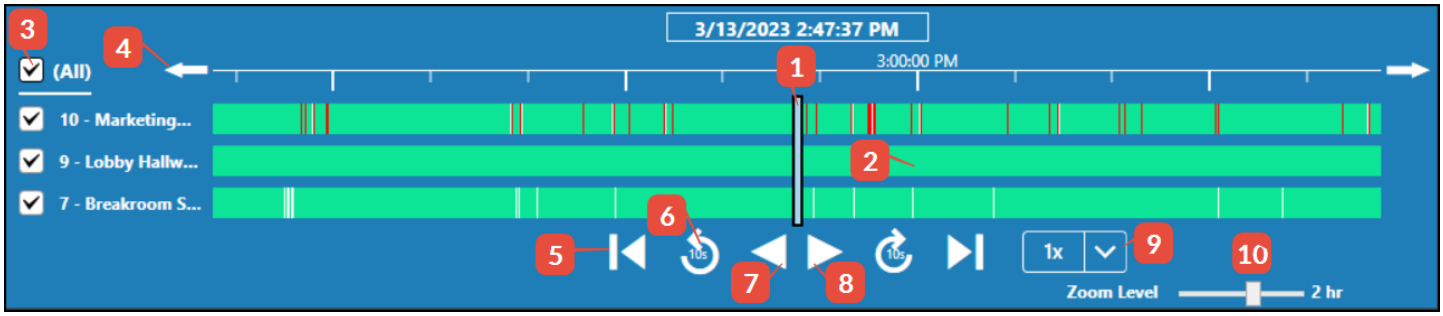
If needed, clicking the Reset icon will clear all current cameras and search criteria.

Playback Video Functions

Once search results have been returned, Playback Video provides powerful tools to provide useful, actionable information to investigators.

Playback Controls

Playback Video's playback controls largely follow standard conventions with some additional enhancements.



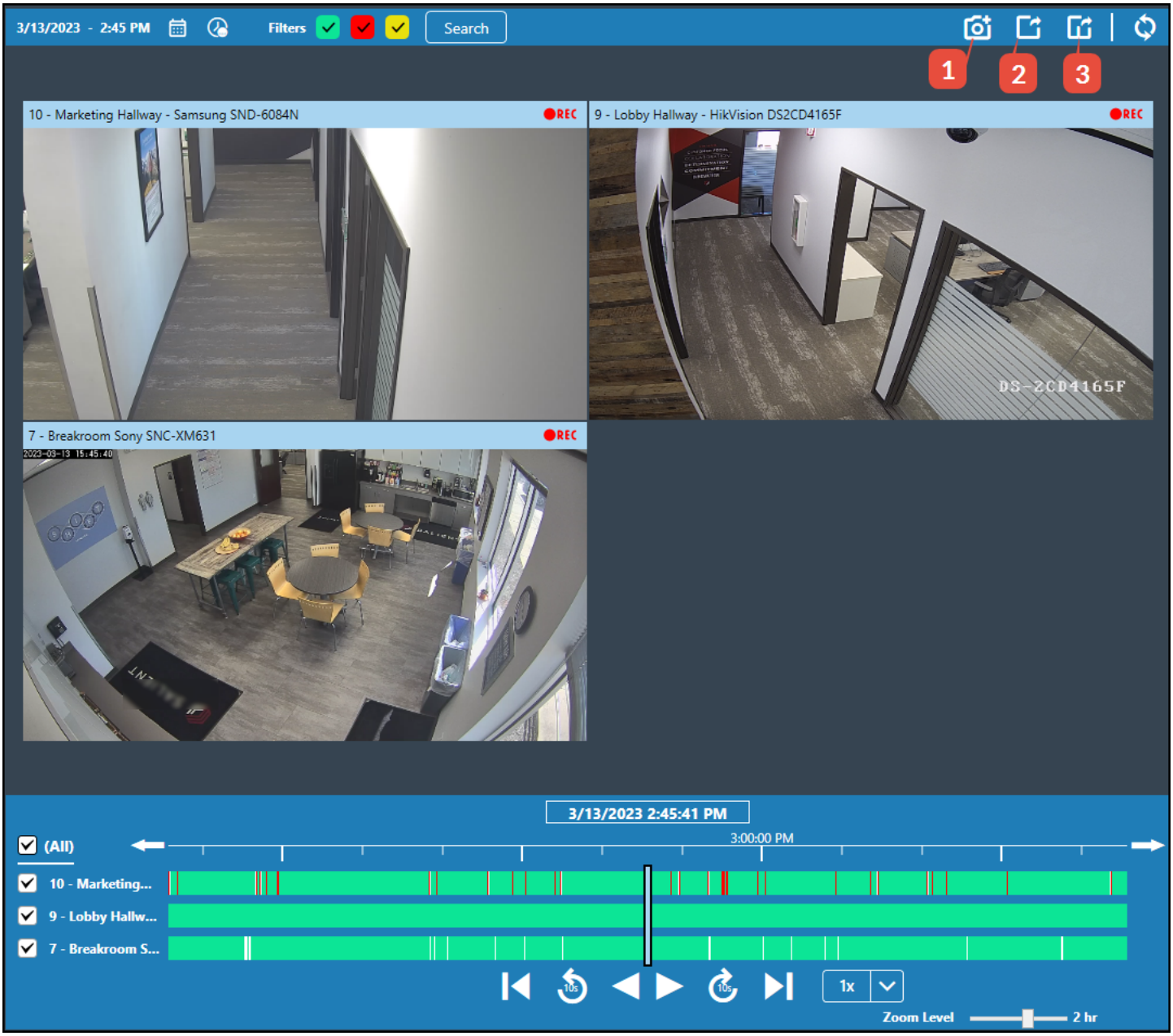
1. The current position marker indicates the moment in time being displayed in the video pane.
2. The timeline is color coded to indicate the type of video (continuous, motion, or alarm) recorded at various points in the search results. The timeline can be scrubbed forward and backward by clicking and dragging with the mouse. If a timeline is scrubbed past either the start or end time of the initial search, the video data will refresh to populate the newly added time.
3. Selects All or individual cameras. Camera selection can also be made in the Playback Review Panel by clicking or cntrl+clicking individual video tiles. A scrollable vertical slider will be displayed if more than 4 cameras are present.
4. Clicking either arrow sets the current position marker to the time indicated when the arrow is rolled over. The time increment is dynamic, contingent upon the Zoom Level.
5. The Previous or Next event controls will move the timeline to set the current position marker to the beginning of either the previous or next event. The controls work for either single or multi-camera results. If events overlap, the previous event button moves the timeline to set the current position marker to the earliest starting point of the events, as does the next event button for groups of events forward in time.

6. Clicking the Jump Back or Jump Forward buttons will rewind or advance the timeline the indicated amount of time. Jump time is configurable from 5 seconds* to 1 hour by right clicking either control and selecting from the menu. The jump time is not individually configurable per control.

   *Jump time may be set from 1 frame to 1 hour in the **Search Video Playback Pane**.
7. Clicking Reverse will start playing the currently displayed cameras backward. Reverse playback can be played at 1x speed.
8. Clicking Play will start playing the displayed cameras. Video may be played from .5-8x speed.
9. Select forward playback speed, ranging from .5-8x.
10. Zoom Level selects the amount of time in the timeline. If adjusted past the initial search duration, the Search button may have to be clicked to refresh the new timeline.

Export Functions

The following functions are available in Playback Video once results have been returned from a search.



The numbers below correspond with the numbers in the image above.

1. Take Snapshot

If multiple cameras are selected, clicking Take Snapshot will save the current frame of all selected tiles to a selectable folder as multiple .jpg files. If only one tile is selected, the frame can be saved as either a .bmp or .jpg file, title and notes information may be entered in the popup screen, and the image may be printed.

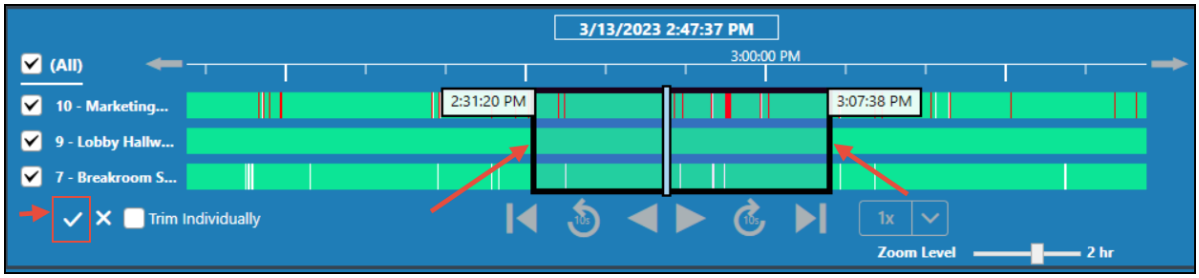
2. Export full Timeline

Places the selected camera(s) in the Export Queue. This option uses the entire length of the selected clip(s).

3. Trim and Export

Trim and Export allows for all selected cameras' start and end times to be set for export.

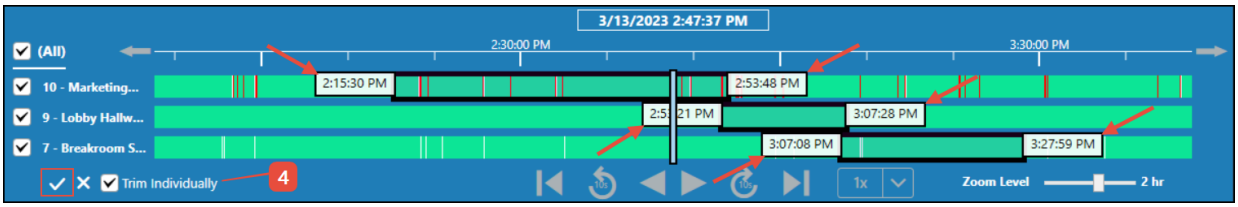
Drag the sliders to the desired start and end times, then click the checkmark to send the trimmed video to the Export Queue. A scrollable vertical slider will be displayed if more than 4 cameras are present.



4. Trim Individually

Allows individual cameras' start and end times to be set for export. This feature is useful in capturing action moving across multiple cameras sequentially.

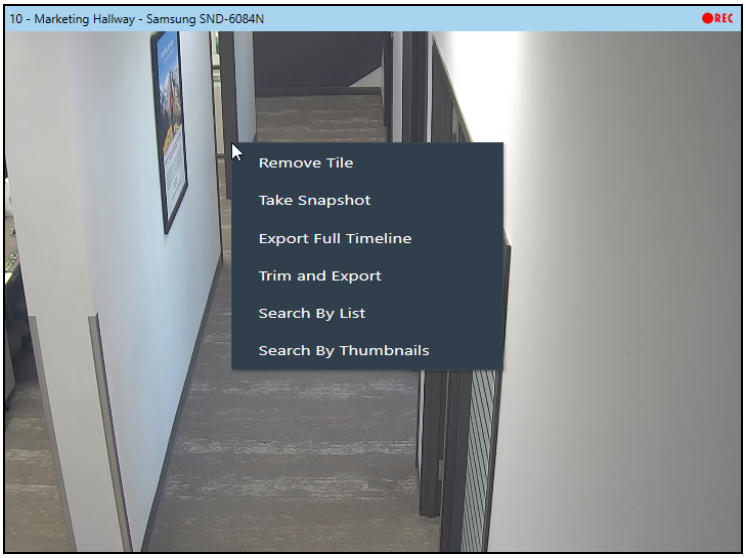
Select Trim and Export as above, then check Trim Individually. Set start and end times for each camera. Start and end times do not need to overlap. Finally, click the checkmark to send the trimmed video to the Export Queue.



Resets the search process to the starting state.

Video Tile Right Click Menu

Right click on a video tile to display the right click menu.



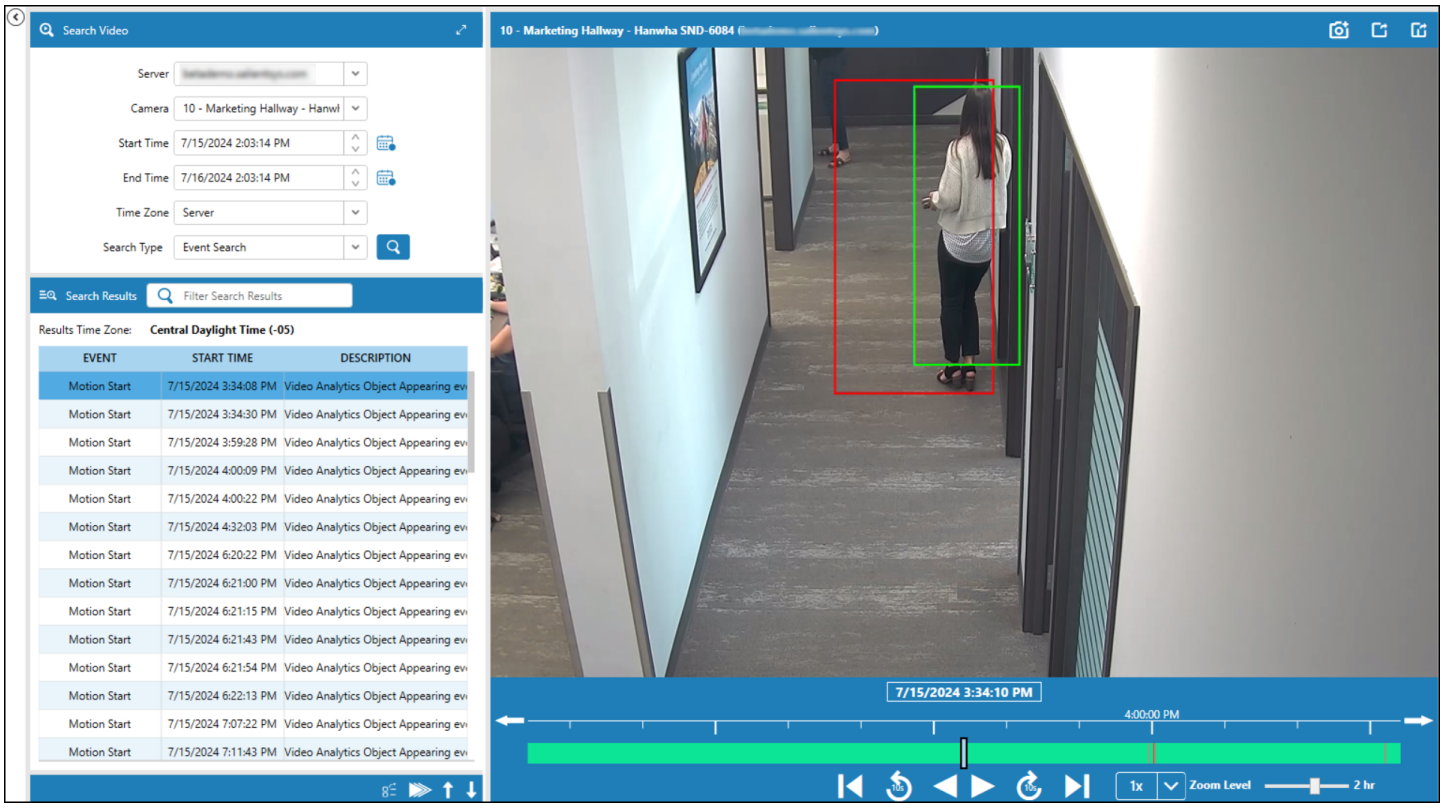
Video Tile Right Click Menu

Option	Description
Remove Tile	Removes the video tile from the Playback Review Panel
Take Snapshot	If multiple cameras are seletecd, clicking Take Snapshot will save the current frame of all selected tiles to a selectable folder as multiple .jpg files. If only one tile is selected, the frame can be saved as either a .bmp or .jpg file, title and notes information may be entered in the popup screen, and the image may be printed.
Export Full Timeline	Adds that video tile's full timeline to the Export Queue
Trim and Export	Launches the Trim and Export interface for that tile's video. See above for details.
Search by List	Opens the Search by List interface for the selected tile. See Search Video for more information.
Search by Thumbnail	Opens Thumbnail Search for the selected tile. See Search Video for more information.

Search Video

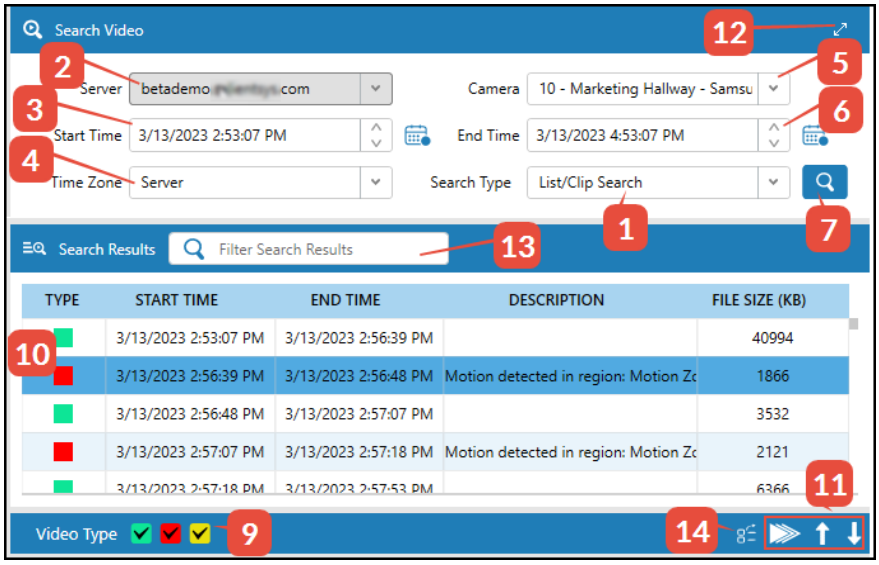
Search Video is capable of conducting multi-day investigations on individual cameras by searching for events, recording type (lists/clips), as well as SmartSearch for motion and Thumbnail Search. The results may then be sent to the Export Queue and exported to a hard disk, thumb drive, or optical media. If multiple camera search is required, Playback Video provides that functionality.

The search parameters and results can be collapsed to allow for greater screen area for video review by clicking the chevron in the upper left corner of the panel. Finally, results can be filtered by using the Filter Search Results text box.



List/Clip Search

CompleteView provides powerful and flexible search tools for video from a single camera by date, time, server and camera.

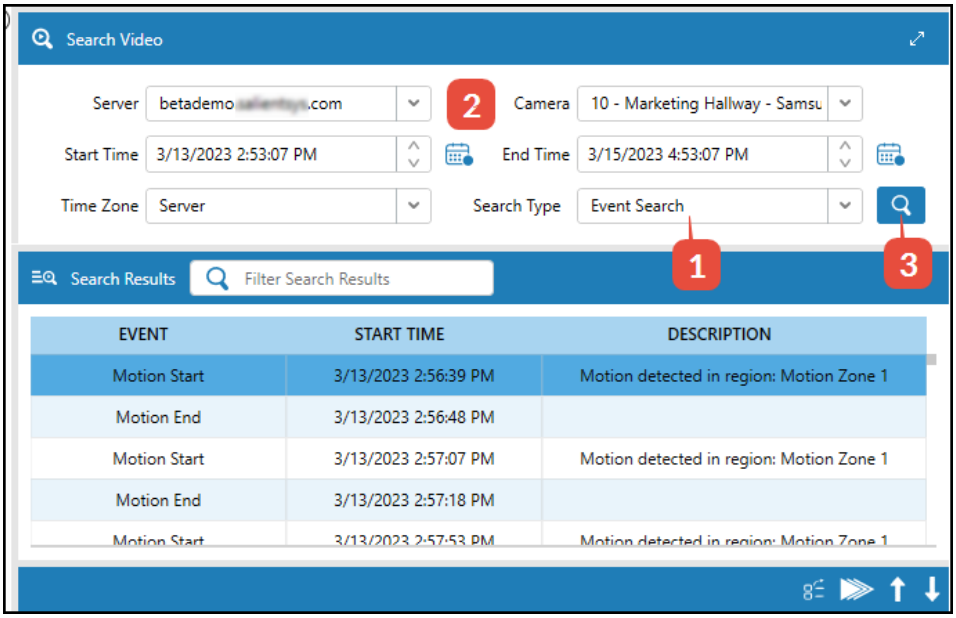


Steps:

1. Select List/Clip Search
2. Select the Server
3. Select the Start Time and Date
4. Select the Time Zone. The Time Zone setting is configurable to use the time of the selected Recording Server via the Server option, the selected Camera, or the Local time zone, as determined by the time zone setting of the Desktop Client machine on which the search is being performed
5. Select the desired camera.
6. Select the end time and date
7. Click Search
8. Wait for the results to appear in the Search Results Window
9. Select or deselect the recording type(s) to establish the correct video review: Green-Continuous, Red-Motion, or Yellow-Alarm.
10. Double click on any of the listed results to display video or...
11. Use either the Sequential Play or arrow controls to play all or step through each of the results.
12. Toggles between Enlarged and Collapsed views
13. Filter the results by typing in keywords, dates, times, etc.
14. Optionally, use the Export Clip/Event icon to send selected items to the Export Queue.

Event Search

Event Search finds a camera's configured events for the given parameters and returns the associated video clips.



Steps:

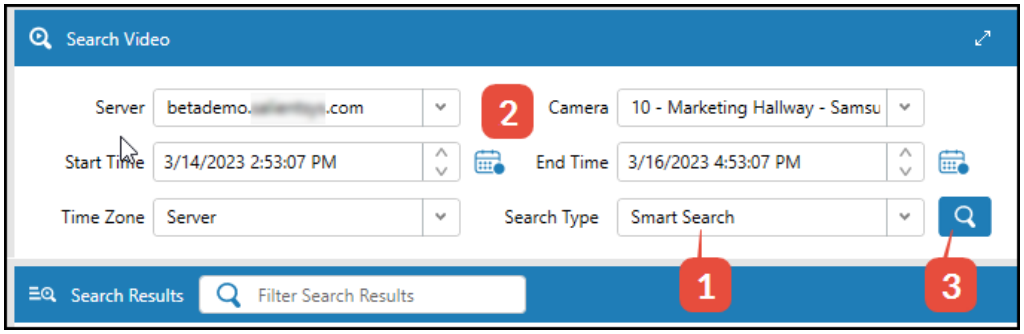
1. Select Event Search
2. Enter information to perform a search as described above.
3. Click Search

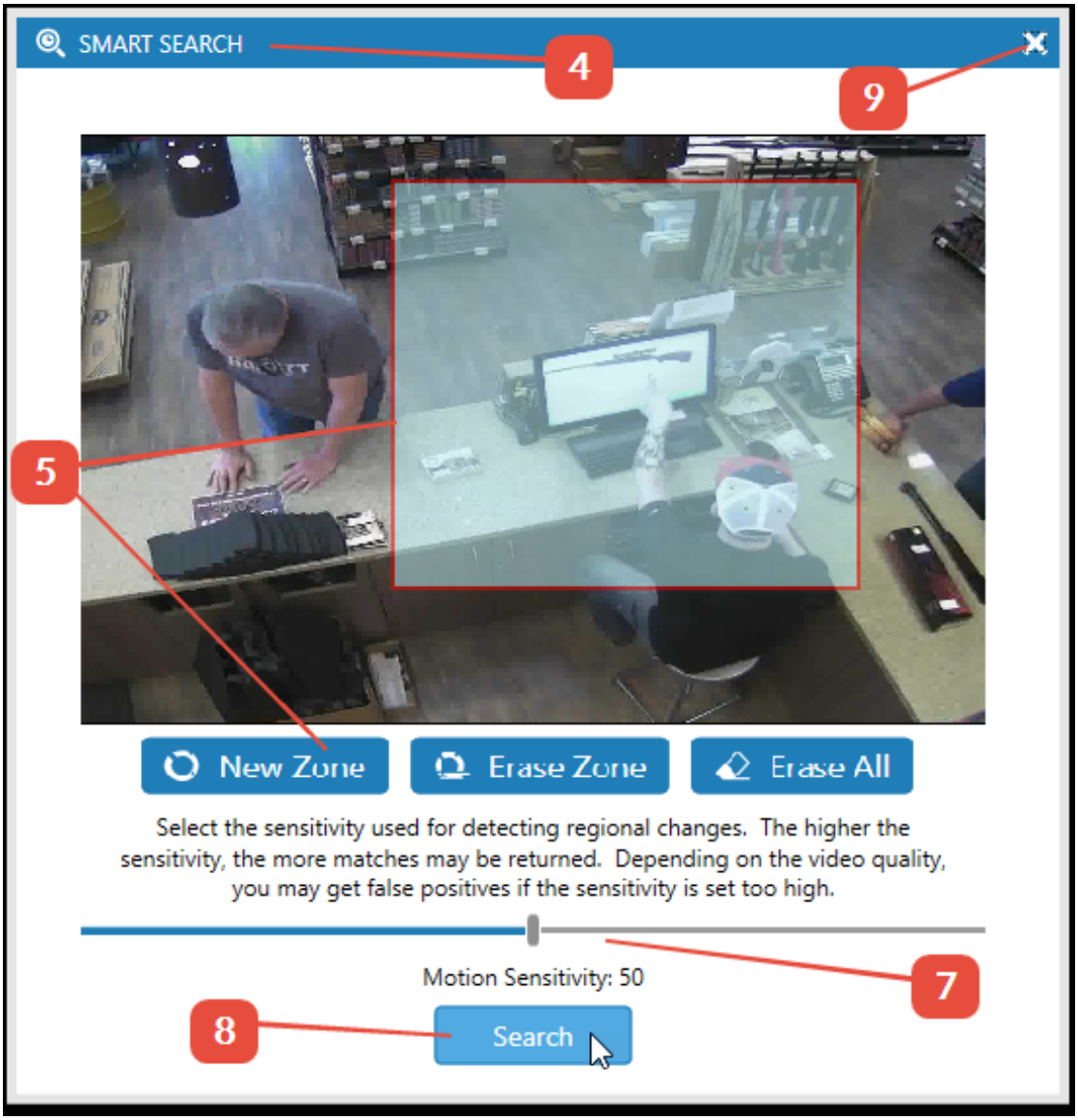
The results will include the type of event, time of the event, and description of the event. The results are filterable from the Filter Search Results box.

Click on a result to play it in the Video Playback panel.

Smart Search

Smart Search searches recorded video to determine if motion has occurred at an earlier point in time at a location specified by the user. Smart Search accomplishes this by using video motion detection algorithms on previously recorded video events.



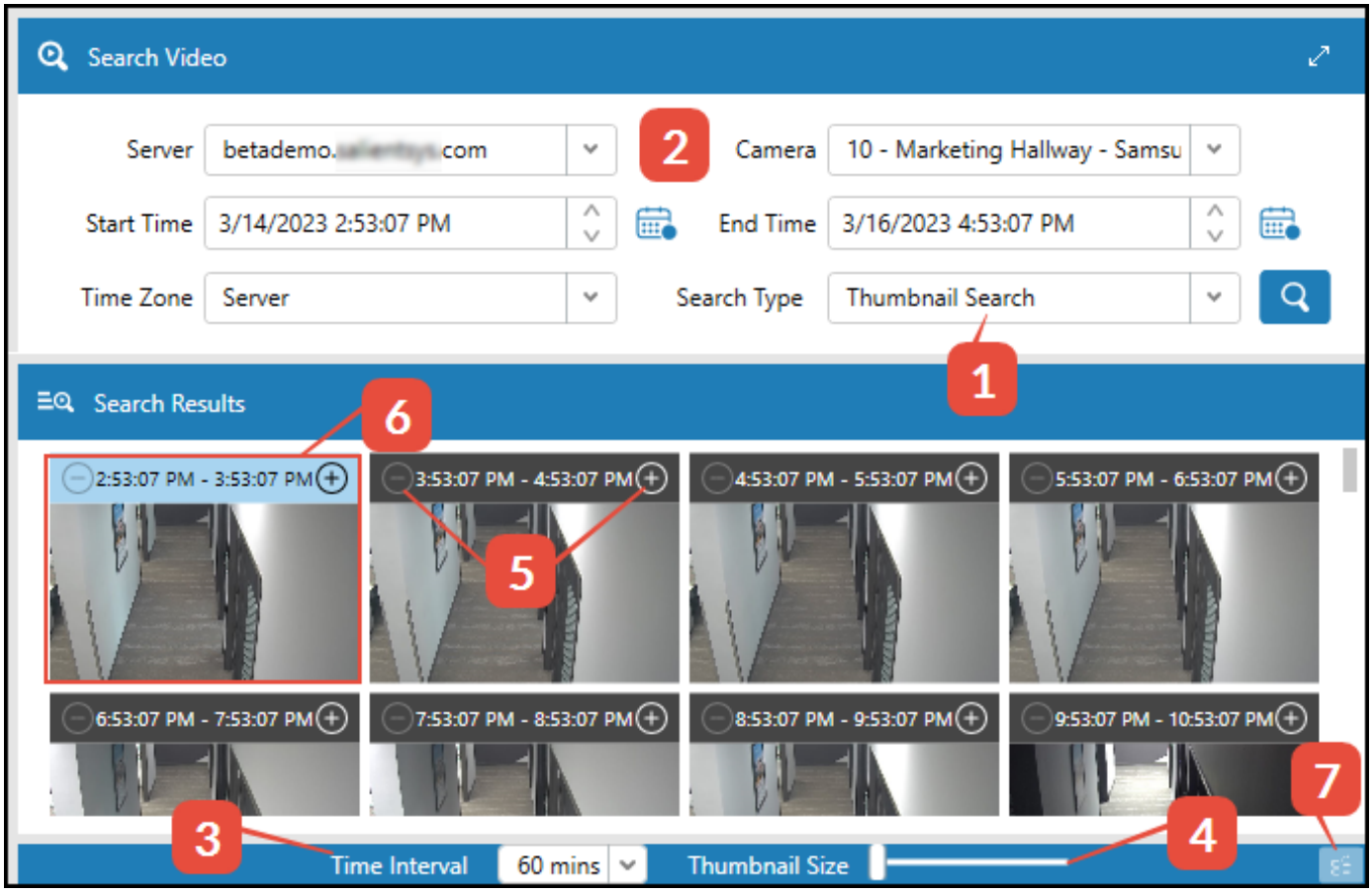


Steps:

1. Select Smart Search.
2. Enter information to perform a search as described above.
3. Click Search
4. The Smart Search interface window will open
5. Create a zone within the video area to search for motion. Only one zone can be created.
6. The zone can be moved and resized. To move the zone, place your cursor in the middle until it displays 4 arrows, then click and drag. To resize the zone, place your cursor on the perimeter of the motion zone, when directional arrows appear, click and drag.
7. Set the motion sensitivity for the detection area. 50 is the default, but this setting may require adjustment to ensure accurate search results.
8. Select the search button to begin the smart search
9. The status of the search will be displayed at the bottom of the Smart Search window. When it completes, close the window.
10. Results of the Smart Search will be displayed in the Search Results panel.

Thumbnail Search

Thumbnail Search generates chronological thumbnail images of a single camera/video stream, searched by server, camera, time zone, date, and time.

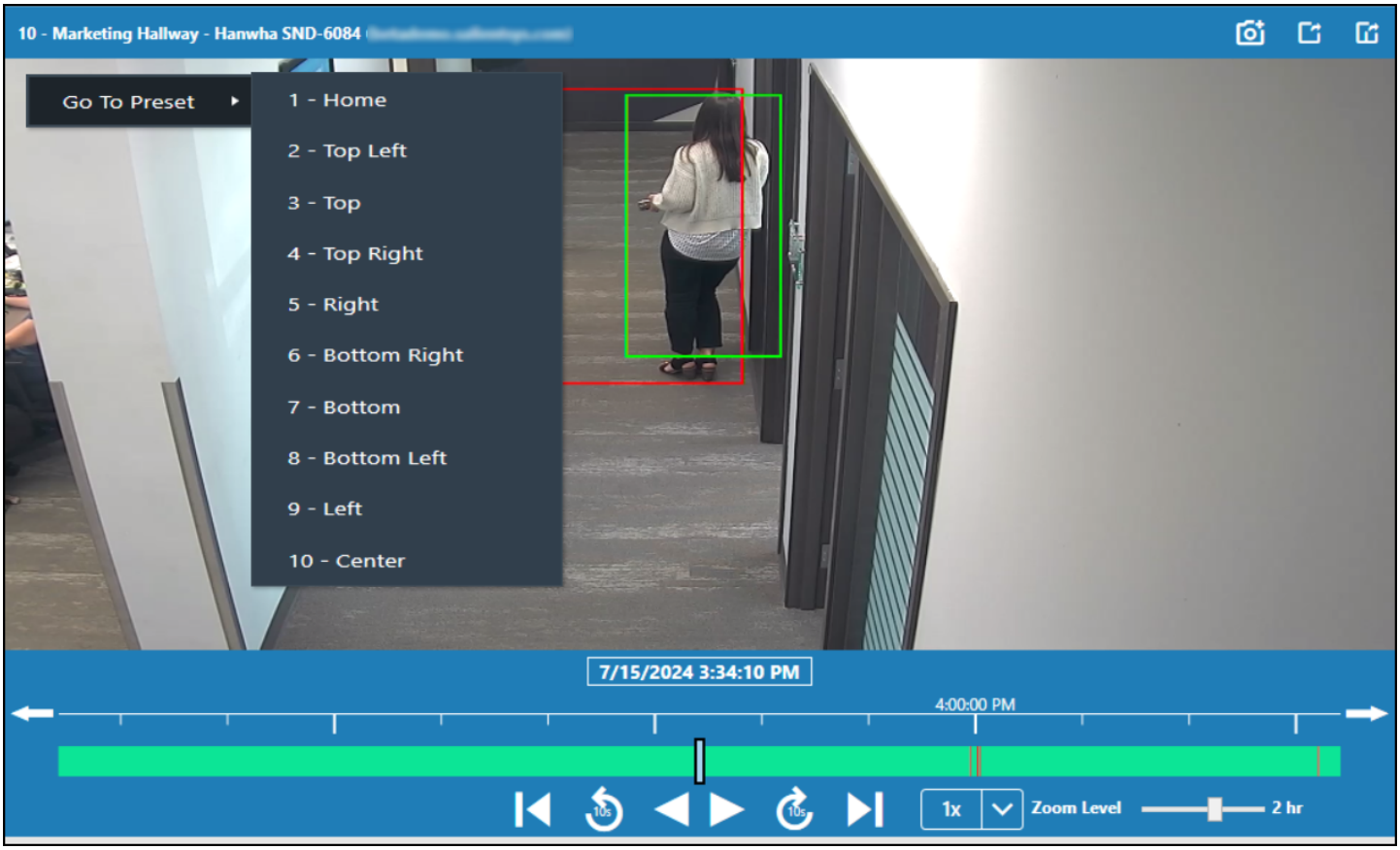


Steps:

1. Select Thumbnail Search
2. Complete a search as described above
3. Adjust the Time Interval as desired. The Time Interval sets the duration of the clips. Consequently, shortening the Time Interval will produce more clips, and the available Time Intervals will depend on the duration of the search.
4. Adjust Thumbnail Size as desired.
5. Clicking the + or - icons will increase or decrease the thumbnail's time granularity, respectively.
6. Clicking a clip will begin playback.
7. Optionally, use the Export Clip/Event icon to send selected items to the Export Queue.

Search Video Playback Pane

After performing a search, selected clips are viewed in the Search Video Playback Pane. Controls are discussed in Playback Video Functions.



Right clicking will produce the Go To Preset menu.

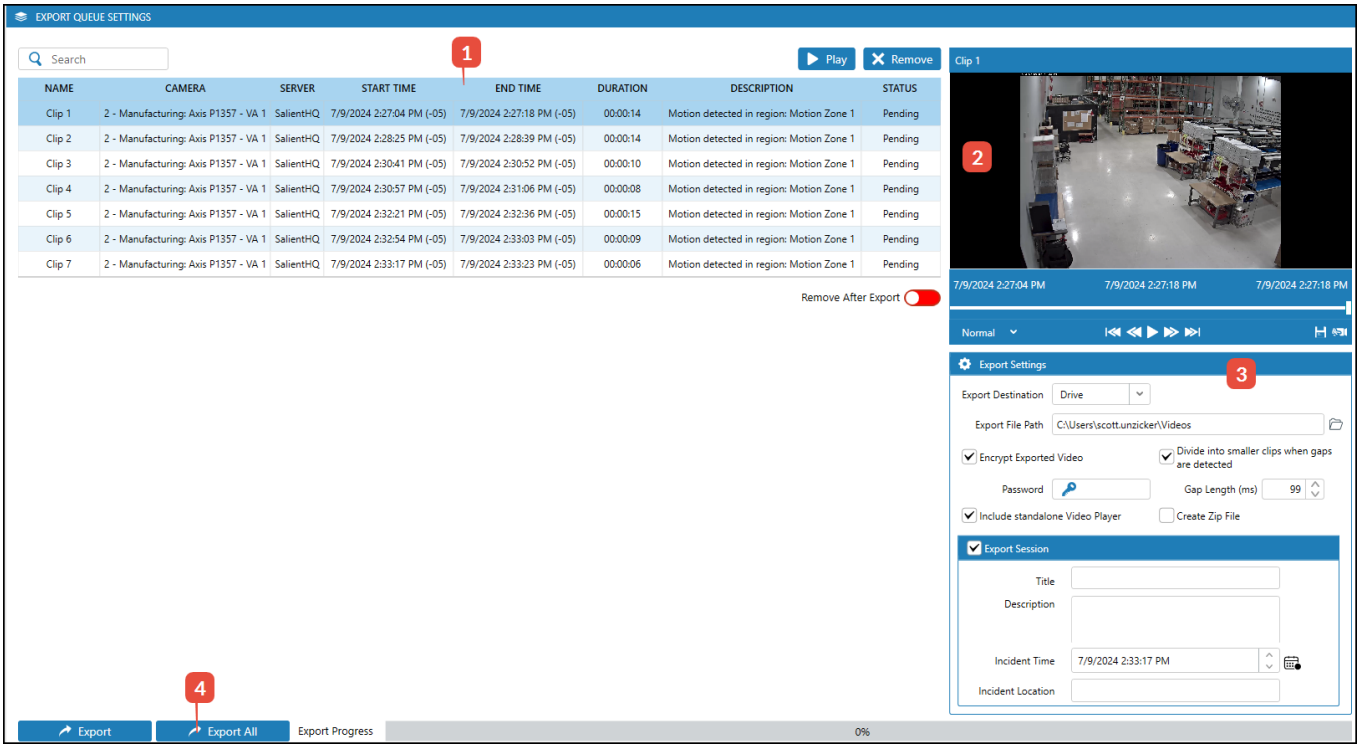
Export Queue

In CompleteView, all exportation of recorded video is conducted from the Export Queue Panel, which has all of the features necessary to export video to CD/DVD, thumb drives, local, and network file locations.

The Export Queue is divided into four sections:

1. The Export Queue, where all items are listed and held when they are sent for Export from any other location within CompleteView. Clips may be played or removed from the queue here, or removed from the queue after export.
2. The Export Playback Panel, which allows any user to select and view any video clip from the Export Queue using all of the typical playback tools. In the lower right corner of the Export Playback Panel is a Trim Video Tool that allows the user to define a start and end date and time for the clip prior to export.
3. The Export Settings Panel, where export destination, video play attachment and Export Session Descriptions are configured.
4. The Export, Export All buttons and the Export Progress Indicator all reside at the bottom of the Export Queue Panel.

Each will be detailed below.



Encrypt Exported Video Export Setting

When the Encrypt Exported Video option is checked, CompleteView encrypts the selected video and audio clips during the export process as .avix files. The exportation encryption is completely independent of any encryption that may have been implemented on the Recording Server. A password is required for encryption during exportation. The password should not be the same password used for any Recording Server encryption configuration. The exported clips may only be viewed in the included Video Player and are not playable in 3rd party applications. If multiple clips are exported with different

passwords, Video Player will prompt the user for each password before playback begins. If the same password is used for all clips, the password only needs to be supplied once to the Video Player.

Clip Gap Export Setting

CompleteView can divide clips selected for export into separate .avi (or encrypted .avix) files based on the presence and length of gaps in the video. If the "Divide into smaller clips when gaps are detected" option is left un-checked, any gaps will be represented by a "No Video" message during playback. When enabled, CompleteView will create a new file for each clip after detecting a gap exceeding the Gap Length threshold, and each of those clips may also include "No Video" for gaps. Any gaps shorter than the threshold will not initiate the creation of a new file and will also be displayed during playback as "No Video." If using encryption, the entered password will be applied to all files generated during the export process.

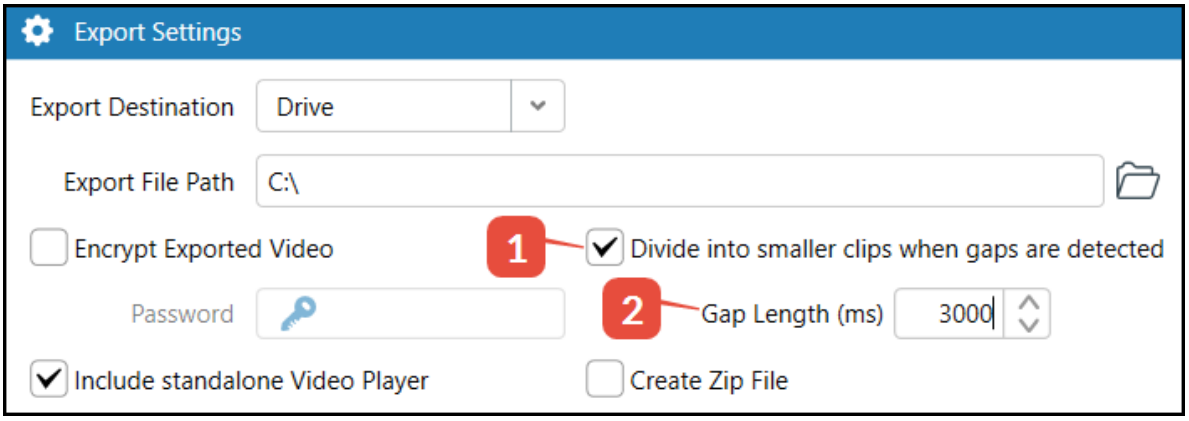
Examples

If a 10 minute clip with 3 gaps is exported with the "Divide into..." option un-checked, the entire clip is exported as one contiguous file. During playback, a "No Video" message will be displayed where the gaps are present.

If that clip is exported with the option selected and none of the gaps are longer than the configured threshhold, a single file will be generated as above, and "No Video" will appear during playback to represent the gaps.

If that same clip is exported with the option selected and 2 of the 3 gaps are longer than the configured threshhold, a total of 3 files will be generated, all of which will also display "No Video" during playback to represent the gaps.

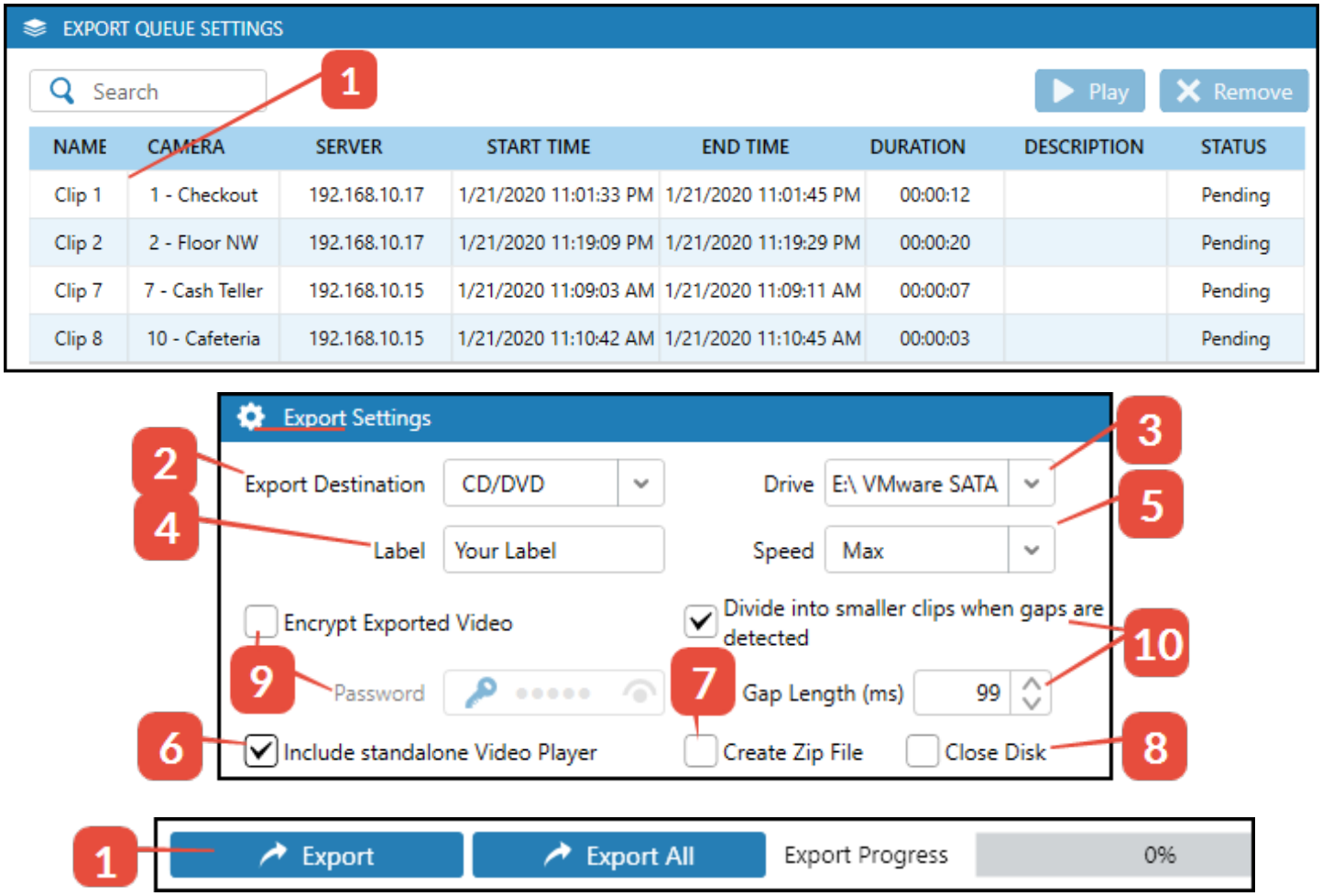
To enable:



1. Select the box
2. Enter a value in milliseconds (1000 ms = 1 second)

Export Single or Multiple Clips Directly from Queue to CD/DVD

Steps:

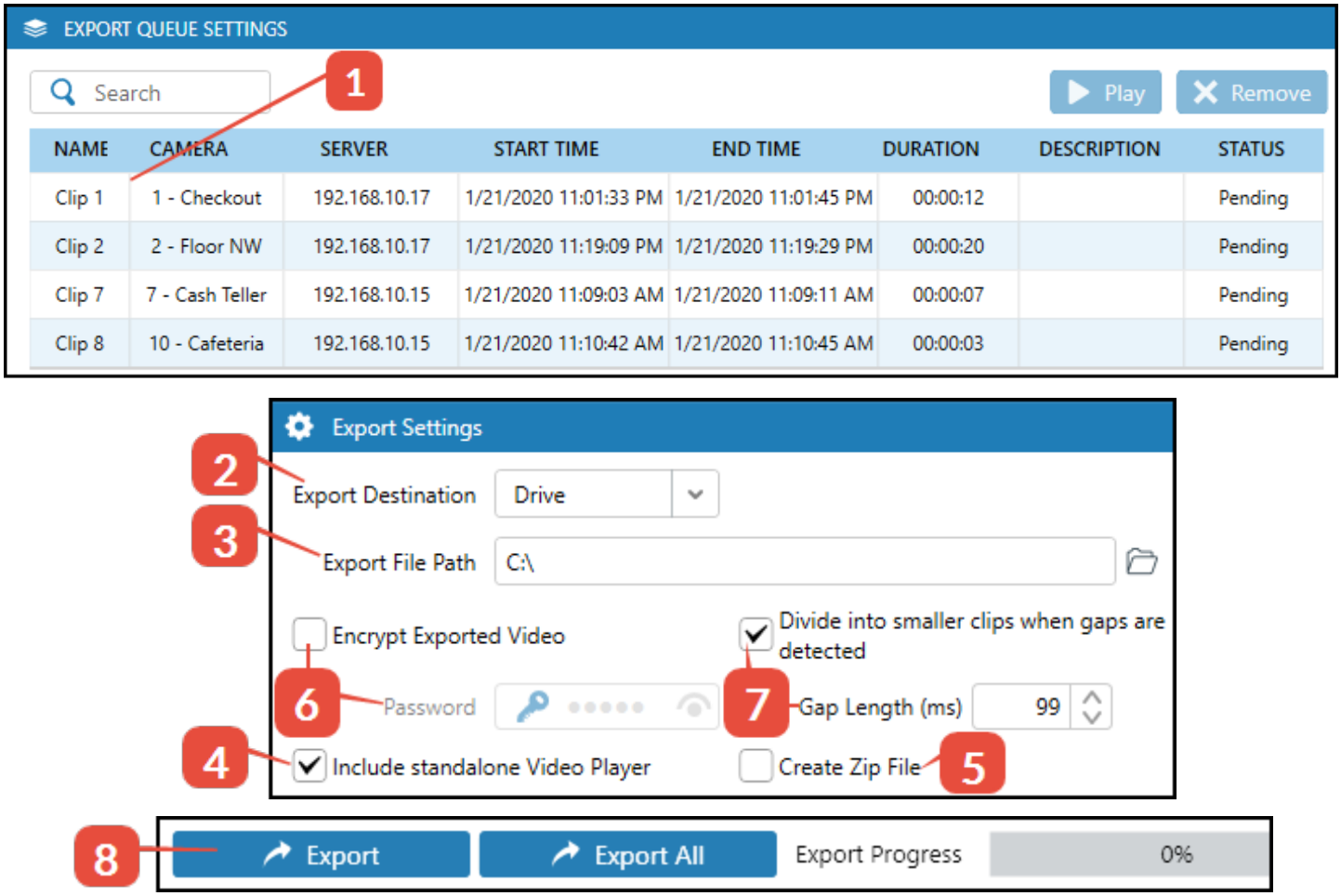


Steps:

1. Select a video clip(s) from the Export Queue (multiple clips can be selected using ctrl+click or shift+click).
2. Set the Export Destination to CD/DVD.
3. Select the destination drive of your CD/DVD.
4. Optional: Enter in a label for the CD/DVD
5. Select Min or Max for the burn speed.
6. Select to include the standalone Video Player.
7. Determine if you wish to create a zip file that contains the exported video and player (if selected).
8. Determine if you wish to close the disk or leave the disk open.
9. Optionally encrypt the exported video, described above.
10. Optionally mitigate clip gaps as described above.
11. Select the Export or Export All Button, as applicable.

For more information on playing the exported file(s), launch the Video Player and consult the Video Player User Manual by selecting Help -> View Help.

Export to File on Local Disk /Network/Thumb drive



Steps:

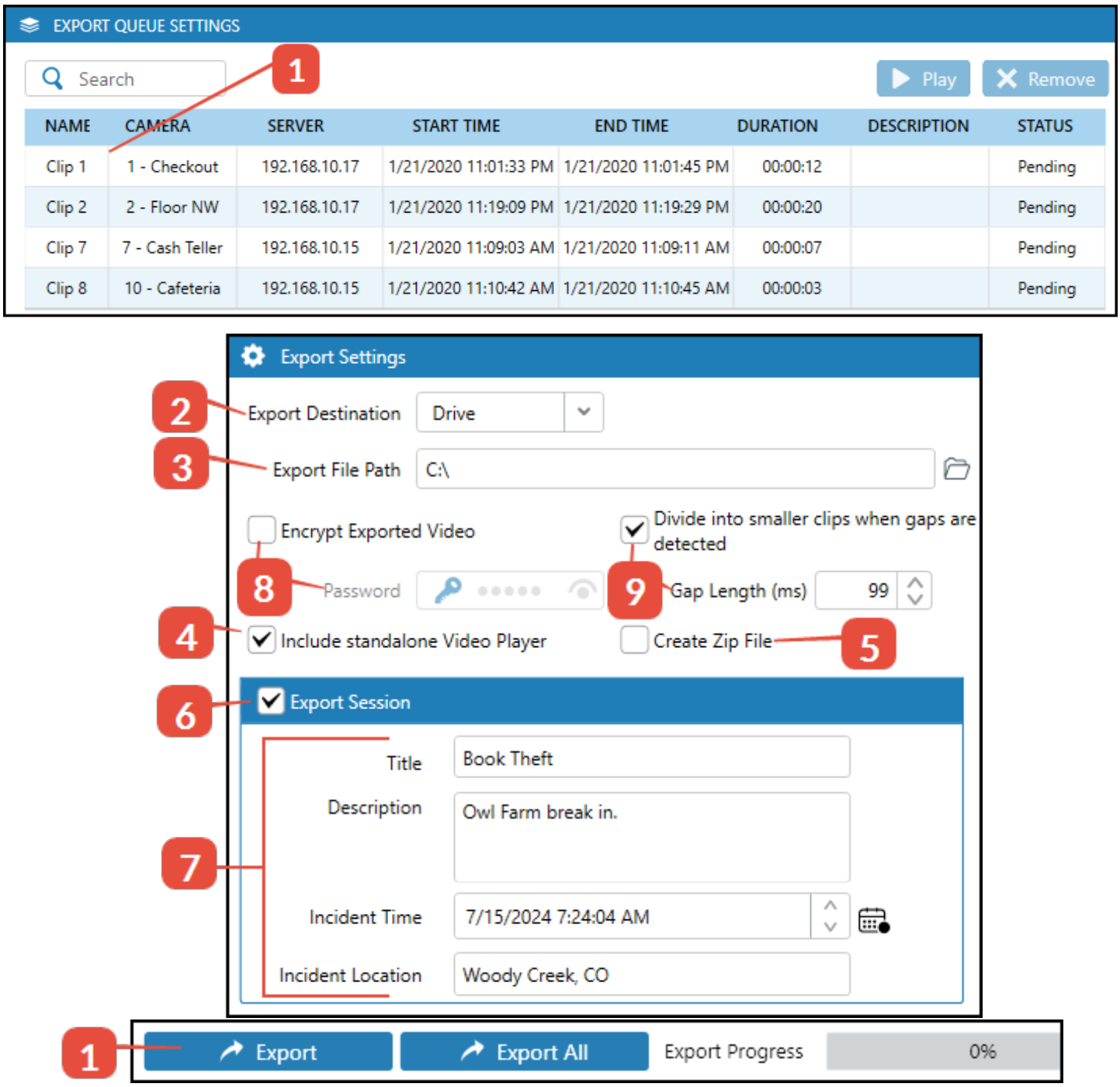
1. Select a video clip(s) from the Export Queue (multiple clips can be selected using ctrl+click or shift+click).
2. Set the Export Destination to Drive.
3. Browse and select or enter the Export File Path.
4. Select to include the standalone video player.
5. Determine if you wish to create a zip file that contains the exported video and players.
6. Optionally encrypt the exported video, described above.
7. Optionally mitigate clip gaps as described above.
8. Select the Export or Export All Button, as applicable.

For more information on playing the exported file(s), launch the Video Player and consult the Video Player User Manual by selecting Help -> View Help.

Exporting a Session File

Session exporting is used to create a file (with the .esf extension) that links multiple video clips related to a specific incident together, in addition to exporting the selected clips as individual .avi (or .avix for encryption) files. Multiple files are grouped together as a *.esf file, which allows a user, using the Video

Player, to view all the exported video of an incident in a chronological playback. The video included in an Export Session may be verified to ensure that the exported video has not been changed.



Steps:

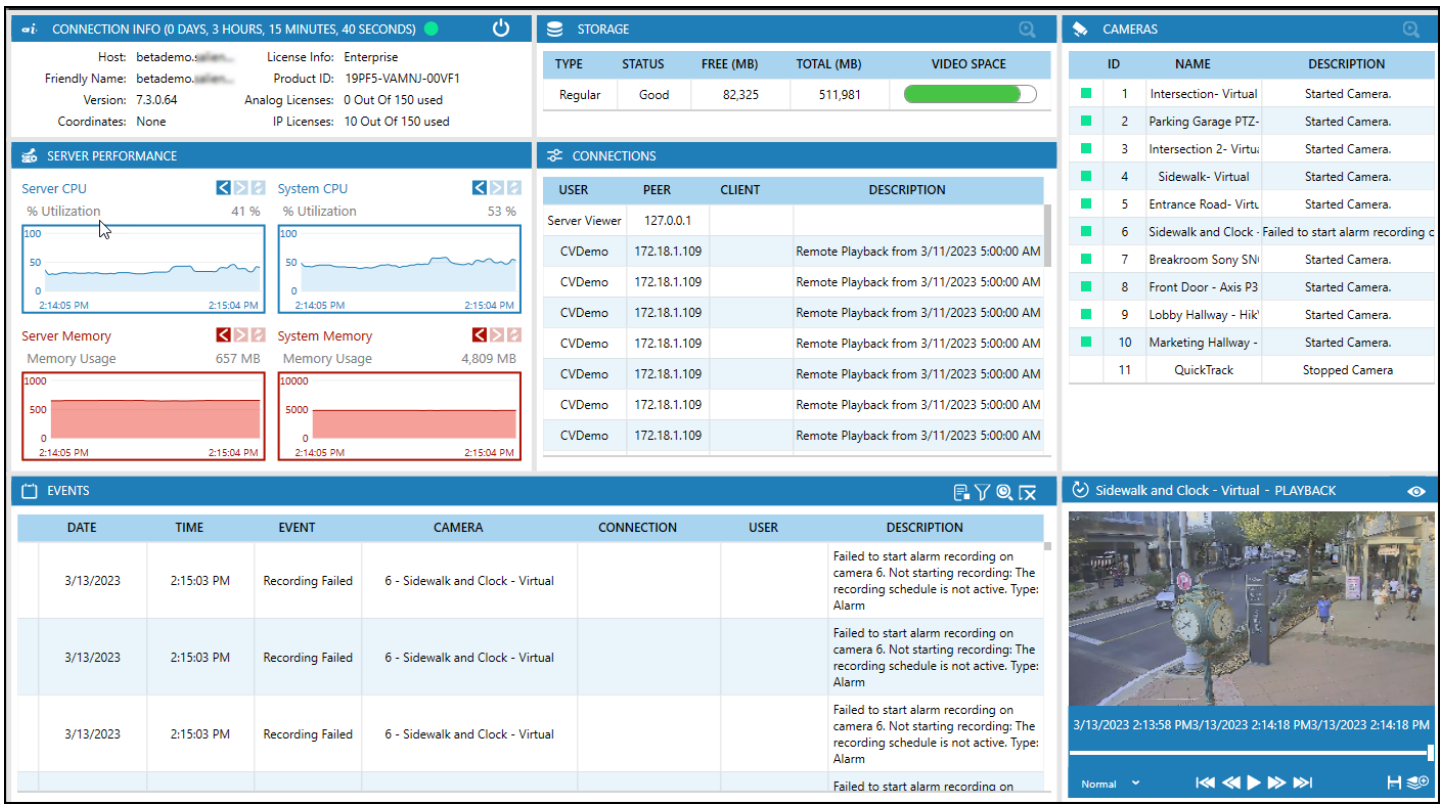
1. Select a video clip(s) from the Export Queue (multiple clips can be selected using ctrl+click or shift+click
2. Select the export destination for your session file. In this example a drive is used.
3. Browse and select/enter the destination path.
4. Select to include the standalone video player.
5. Determine if you wish to create a zip file that contains the exported video and player.
6. Select the Export Session box.

7. Enter in the applicable information including title, description, time and location. All blanks must be filled.
8. Optionally encrypt the exported video, described above.
9. Optionally mitigate clip gaps as described above.
10. Select export or export all as applicable.

For more information on playing the exported file(s), launch the Video Player and consult the Video Player User Manual by selecting Help -> View Help.

Dashboard Overview

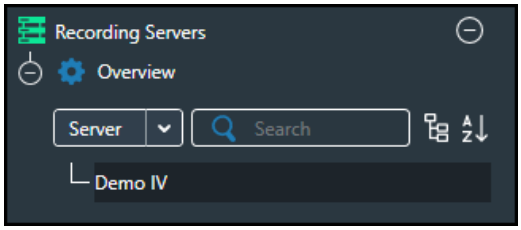
The Dashboard provides information allowing review and assessment of the health of all Recording Servers, the servers' assets, and activities. The Dashboard's panels are intended for use as diagnostic tools. They continually display information relating to licensing, storage status, storage use and availability, server CPU and memory use, real-time remote and live user connections, real-time events and playback of a server's live or recorded video from any of the server's cameras. When used to their full potential, the tools within the Dashboard may be used to identify potential problems before a system failure occurs.



Navigation Pane

The Dashboard Navigation Pane enables selection and viewing of a server's operational information. In the illustration, Demo IV server is selected. This pane is searchable and sortable, as described in [Desktop Client Initial Launch](#).

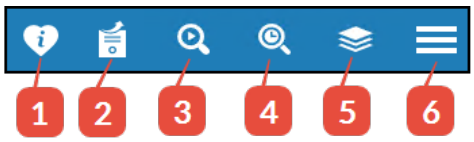
CompleteView supports CompleteView 4.X servers, which are displayed as Legacy Servers.

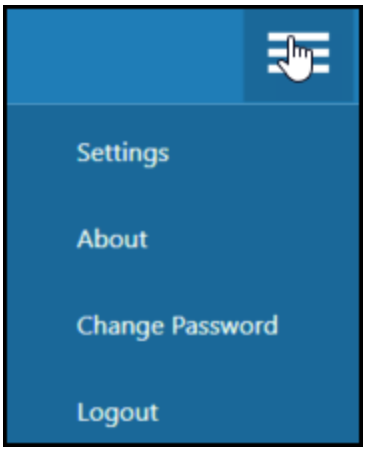


Dashboard Toolbar

The toolbar resides at the top right corner of the Dashboard Task screen.

1. **Server Status** displays status of all Recording Servers attached to the current Management Server. See below for more details.
2. **Server Overview** presents the Dashboard screen.
3. **Search Video** launches playback for video retrieval.
4. **Search Events** presents a list of motion, alarm, etc., events for playback.
5. **Export Queue** displays a lists of videos marked for export.
5. **Menu** presents the following options:
   a. **Settings** displays video stream options, detailed below.
   b. **About** displays version and other information about CompleteView
   c. **Change Password** launches the VMS change password window
   d. **Logout** logs out of the client.

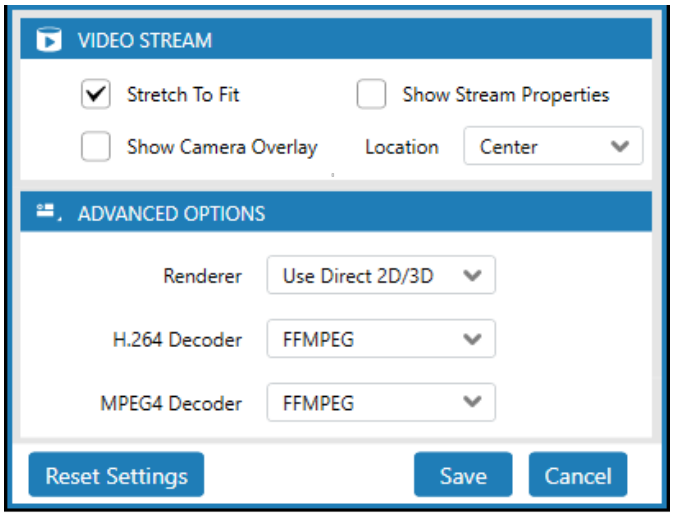




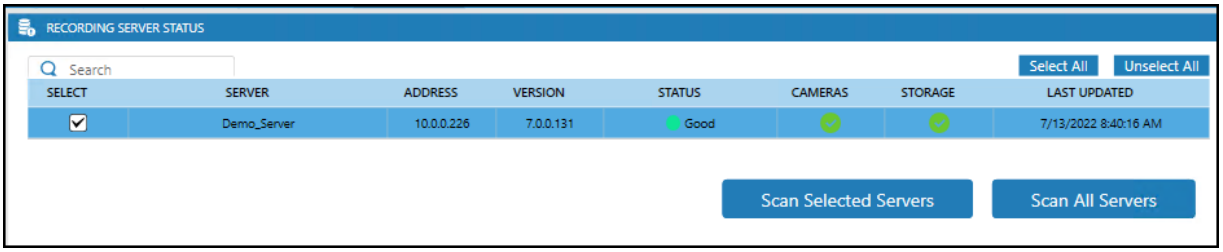
Video Stream Settings

Selecting Menu then Settings will produce the Video Stream menu. This panel allows the user to configure the appearance options for the Dashboard's Live View Panel.

Stretch To Fit, Show Camera Overlay, Show Stream Properties, and settings in **Advanced Options** are described in detail in Live View Overview.



Server Status



Selecting the Server Status icon will present a list of all Recording Servers currently attached to the deployment's Management Server. Either select the desired servers and click Scan Selected Servers or click Scan All Servers. The server list is searchable and sortable.

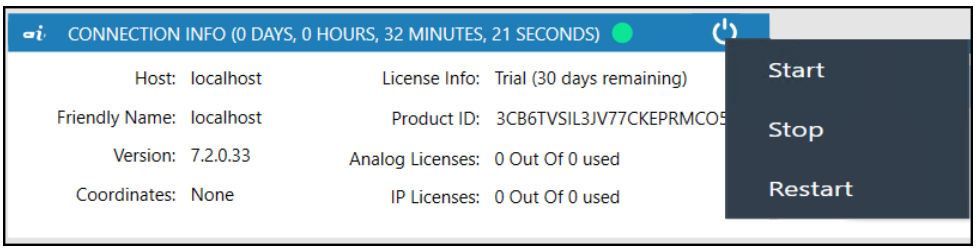
Status Color	Meaning(s)
Green	**Good** - Server is online, no issues found
Yellow	**Issues detected** - Server is online, issues with either cameras or storage found
Red	**Scan error** - Server is online, internal error when scanning for issues **Unable to connect** - Could not connect. Usually indicates the server is offline.
Black	**Not yet connected** - The server has not been scanned **Pending scan** - Scanning in process **Scan interrupted** - Scanning process was interrupted, and results may be incomplete

The Cameras and Storage columns will display either a red X or a green checkmark. Cameras are flagged if not recording to disk due to being disabled, sync lost, or a recording failed error. Storage is flagged if it is offline or if no free space is available.

Double clicking a listed Recording Server will display its Dashboard.

Connection Info Panel

The Connection Info Panel is located in the top-left of the Dashboard and displays information about the selected server. The current up time from the server's last restart and a colored status indicator dot are displayed in the top bar of the panel. The colored dot shows the connection status of the selected server. The Server Info screen also provides analog and IP license information, the Friendly Name, Product ID, and software version of the server. All of the information in the Server Info Panel may be requested by technical support personnel to assist in troubleshooting.



Server Status

- Connected
- Attempt Connection
- Not Connected

In addition, servers may be started, stopped, or restarted from within the Connection Info Panel using the virtual power button.

Storage Panel

The Storage Panel is located in the top-center of the Dashboard. The panel displays the type, status, free and total storage space, as well as a graphical representation of the percentage of the storage pools in use.

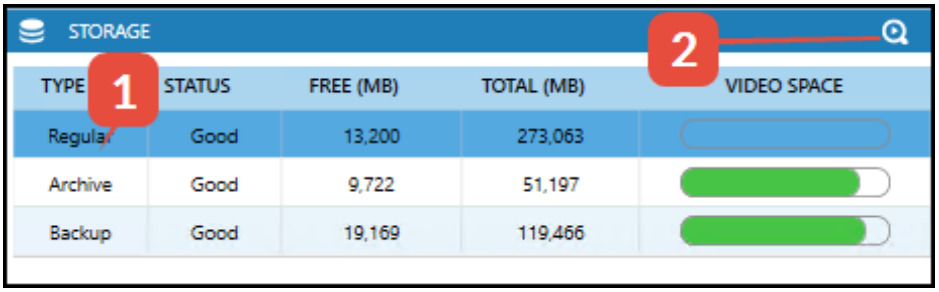
At the top of the Storage screen is a darker band, referred to as the Title Bar. Within the Title Bar on the far right is a spy-glass icon, which is a virtual button that will redirect the user to a search video screen.

Search For Video

The search encompasses all cameras for the selected server, or for a specific pool that is selected in the Dashboard's Navigation Pane. The storage search feature is intended for troubleshooting video recording storage issues. Video investigations or export should be conducted from the CompleteView Playback function. Click Here for more information about Playback search.

Steps:

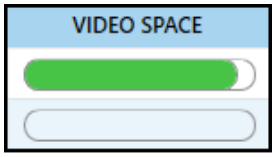
1. Select a Storage Pool. Note that the selected type will turn a darker color, and the spyglass will brighten.
2. Select the Search Video icon



Video Space

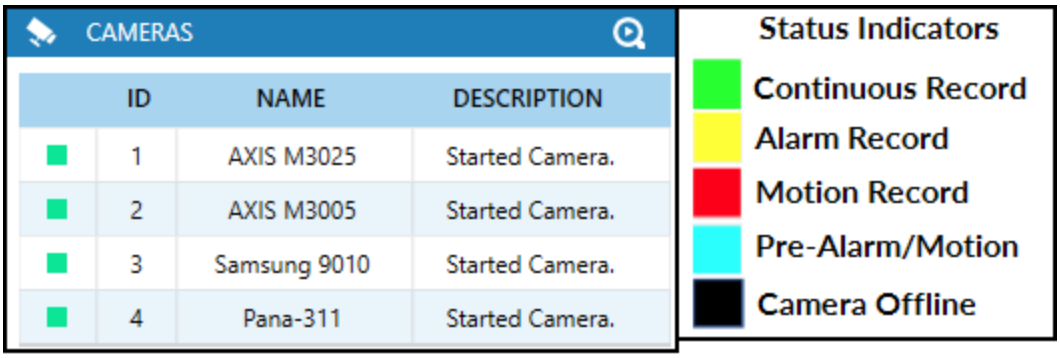
The Video Space indicator displays used versus available recording storage space. Green indicates used space, while white indicates available space.

New pools will show as a white bar. As the pool fills with video, the green indicator will increase, and the white indicator will decrease as a green bar with a progressively smaller white slice on the right to indicate free space, which is reserved for first in, first out (FIFO) video operation.



Cameras Panel

The Dashboard Cameras Panel provides a list of the selected server's cameras. The camera panel's default location is the top right corner of the Dashboard.



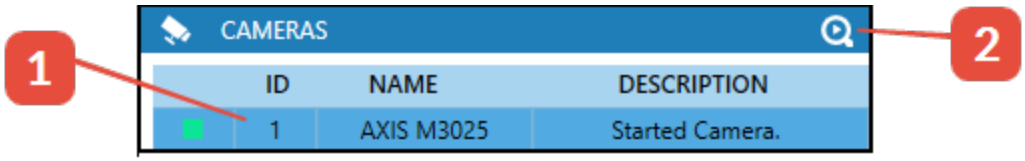
Camera Headings

The headings include:

- **Status** displays a color code indicating the recording status of the camera (see indicators above).
- **ID** displays the order of the cameras listed on the server. The camera ID is the unique identifier by which CompleteView identifies cameras, and may be used in third party integrations.
- **Name** each camera has a friendly name that may be changed. Changes are completed in the Recording Server's configuration. Click Recording Servers Cameras for more information about changing the Name.
- **Description** displays the state of the camera.

Search Video from Cameras Panel

Camera Search Video is intended for troubleshooting video recording and camera connection issues.



Steps:

1. Select a Camera
2. Select the Search Video icon

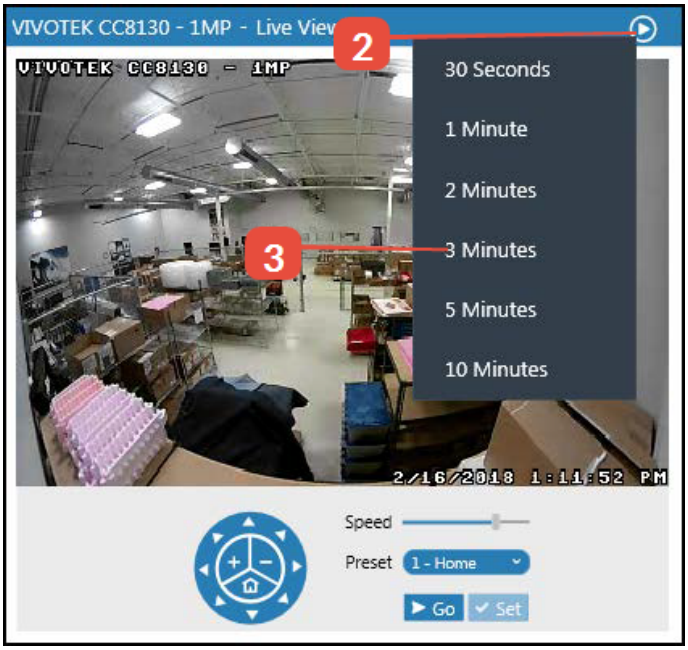
Return to Dashboard from Search Video

1. Select the Server Overview icon, located in the Dashboard toolbar  .

Dashboard Live View

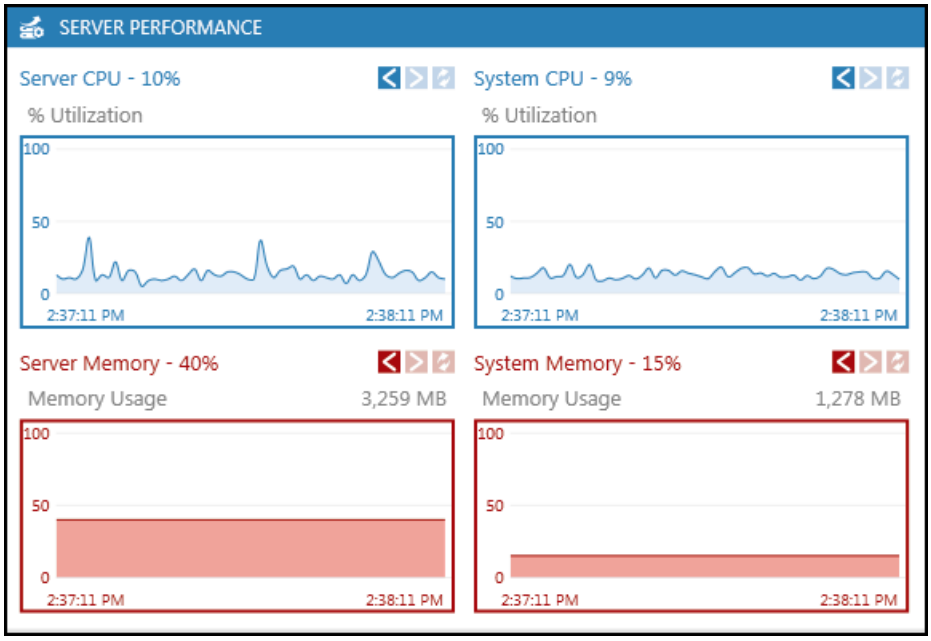
Selecting a camera from the Cameras List will display its live video. This feature is provided for administrators to validate that the camera is streaming as expected. For convenience, PTZ and preset con-

trols are included below the live video. For a quick review, click the Search Video icon (2), then select the review period (3).



Server Performance Panel

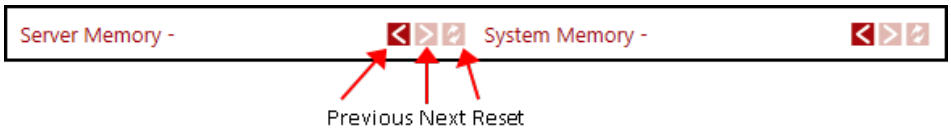
The Server Performance panel displays real time server and system CPU and memory utilization percentages in both digital displays and analog graphical charts, informing those seeking such information of the overall health of the VMS. The memory and CPU information is displayed for the Recording Server selected in the Dashboard's Navigation pane. Three buttons for each of the four displays allow the user to look at previous data, next data, as well as resetting the display to the current status. The information provided by the Server Performance panel would be useful in determining, for example, the performance impact on the VMS due to camera frame rates, data rate, or compression changes.



Server vs System CPU and Memory

Within the Server's Performance panel are both (recording) server and (total) system CPU and memory statistics. The information is differentiated. **Server** CPU and Memory statistics are specifically relevant and exclusive to the Recording Server, and are distinct from any MS Windows functions.

System CPU and memory statics include both Recording Server and overall system CPU and memory load performance statistics. System CPU and memory should be the determining factor when considering changes that may impact total load. The System CPU load should remain at or below 75% when either adding cameras or making camera setting adjustments. The 25% headroom is useful for live view, playback, and other user and server functions. The memory and CPU statistics displayed are a forward rolling, one-minute period.



Previous increments the data display and statistics time backward one minute for each button click.

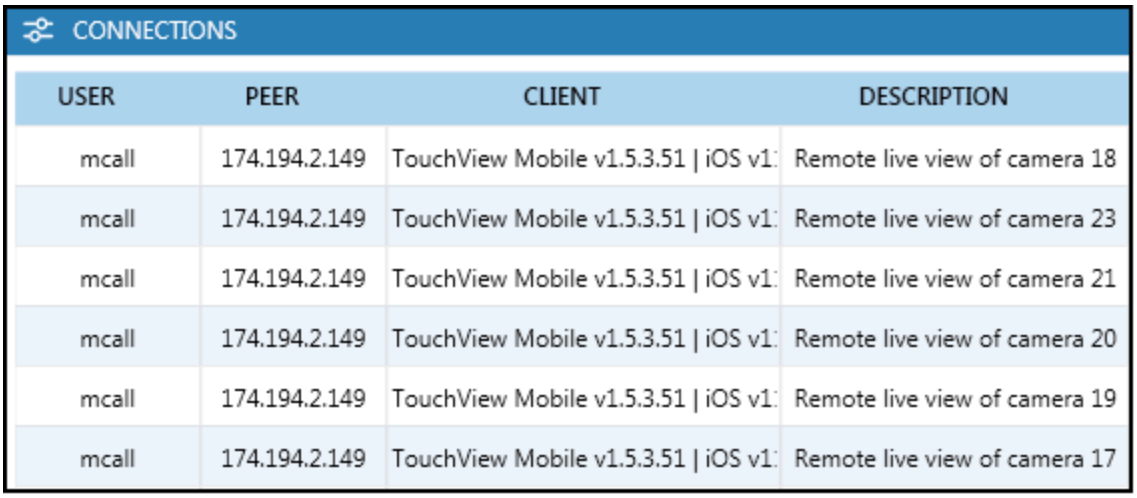
Next brings the data display and statistics forward from the previous position by one minute for each click, until the current data time is reached.

Reset resets the data display to current time and statistics.

The navigational functionality is the same for both System and Server information.

Connections Panel

The Connections Panel displays real time information indicating which client application is being used by whom. The connection panel shows a camera's data for as long as the camera's connection is active.



User indicates the login account that is connected to the server or viewing live video.

Peer displays the IP address of the source delivering the video to the live view client. Could be useful in determining the cause of unauthorized access.

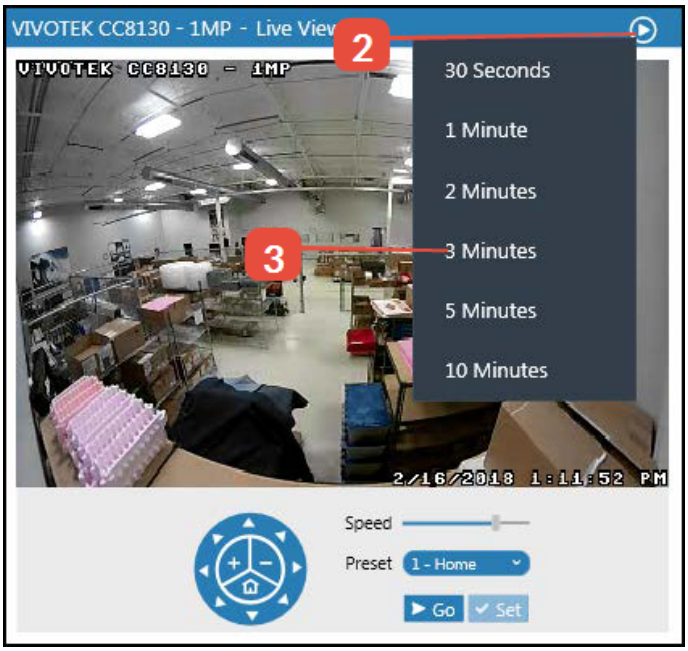
Client relates the type of client in use. Blank indicates that the client is CompleteView Client, and not a live viewing client.

Description describes what the connection is doing. The top listed item of the connection panel is most often the first CompleteView Client.

Live View Panel

The Live View panel is located directly below the Cameras Panel. In Live View's title bar's top right corner is a virtual button that allows a Quick review of video, selectable from the last thirty (30) seconds to ten (10) minutes of recorded video. The Video Review Panel is intended as a quick verification of camera connectivity and functionality. For CompleteView's full live viewing capabilities, Click Here.

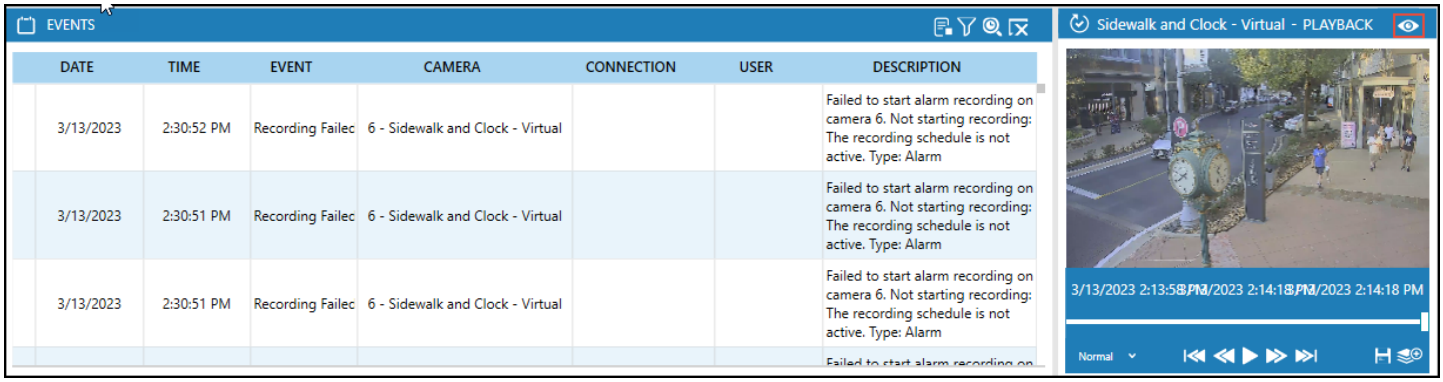
Steps:



1. Select a camera.
2. Click on the button in the video review panel.
3. Select one of the review options.

Events Panel

The Events Panel displays a list of events in real time. Double-clicking on any event in the list will cause recorded video associated with the event to display in the video Playback window. The video can be toggled between Playback or Live View in the Playback window by clicking the icon in the top right corner. Events, such as a camera off-line, may not have associated video. If a camera is not configured to record continuously, and an event comes in for which recording video is not turned on, a “no video found” message will be displayed if playback is attempted.



Date indicates the date the event occurred.

Time indicates the time the event occurred.

Event shows a brief technical description of the event.

Camera displays the camera name for a motion or other integrated analytic event.

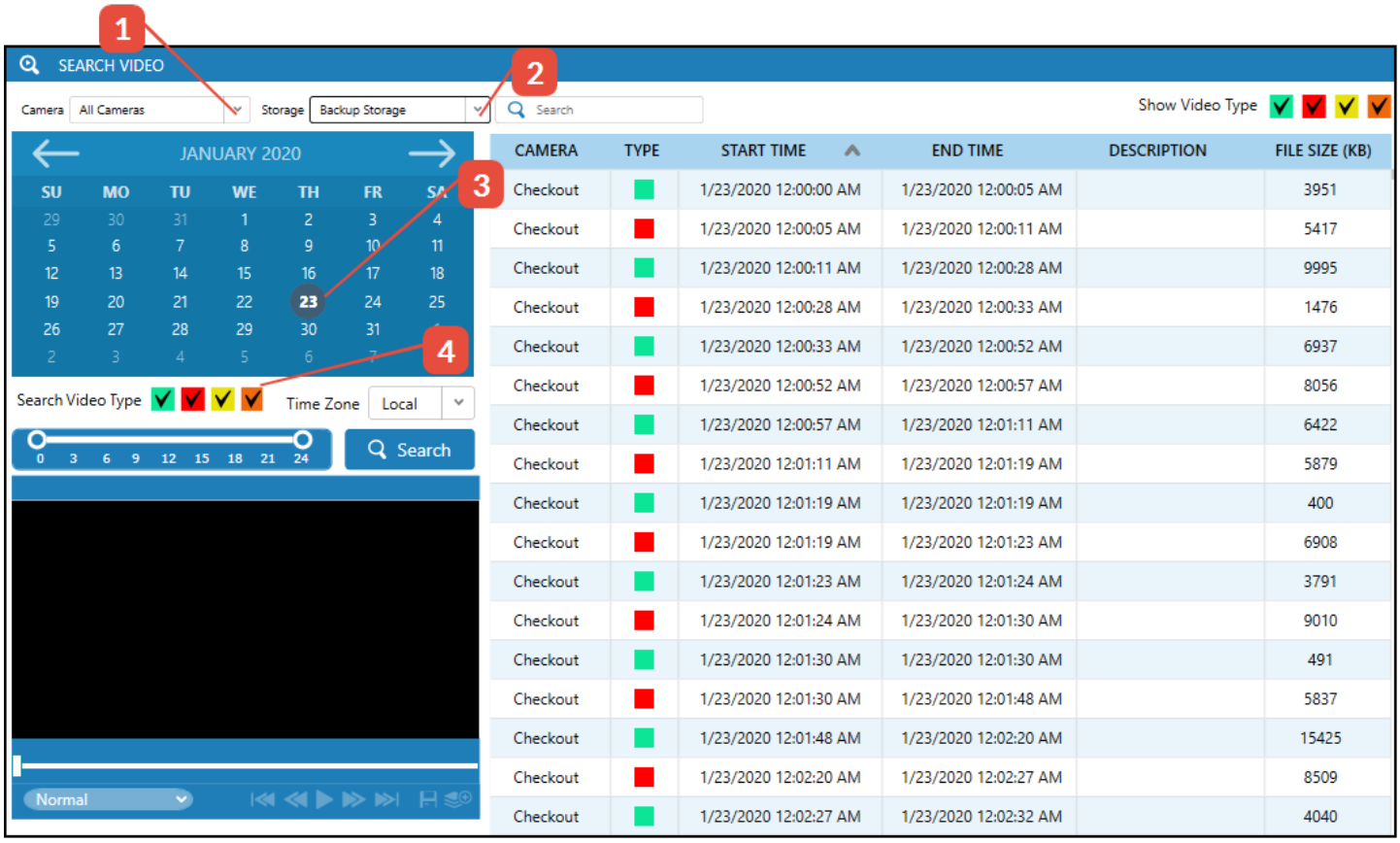
Connection displays the ID number of a connection to the Recording Server. Connections could include Desktop Clients, 3rd party video streaming software, attached devices, etc.

User denotes the person that is logging into or out of either a Recording Server or into a server’s connection into active directory.

Description contains a clear text description of the event. Some, but not all events, will display a description.

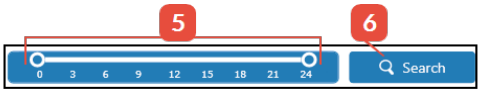
Search Video Panel

Dashboard Search Video allows users to both confirm video availability and enables video search, playback, and export to the video playback queue. Search Video may be selected from the server's status, camera-list title bar icon, or independently from the Dashboard's Title bar icon.



Select Video and Playback

Steps:

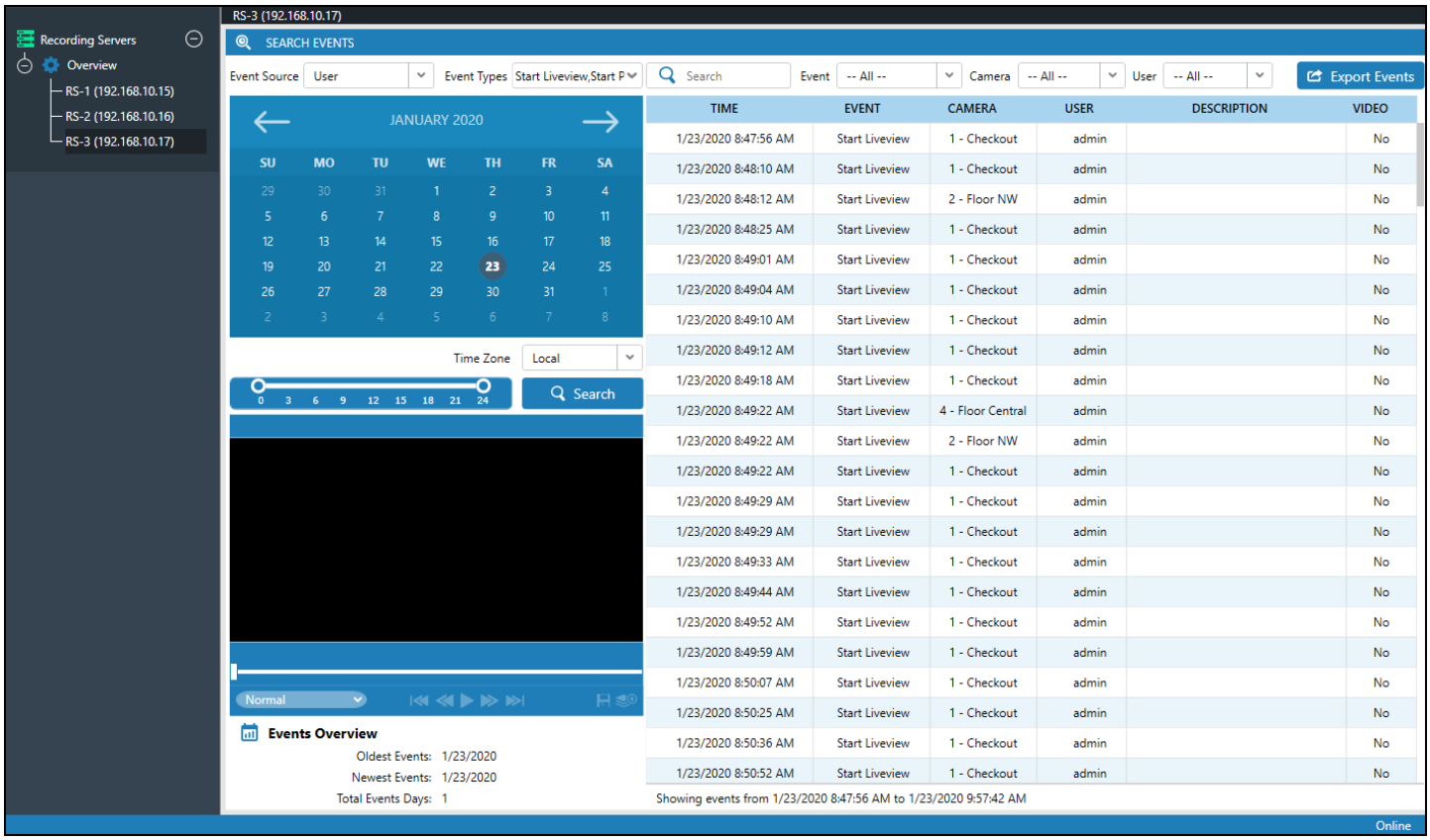
1. Start at the top of the Select Video panel, select one or all cameras, from the Camera pull-down list; the default choice is all cameras.
2. Select, to the right to of the camera pulldown, a specific storage pool type, or all storage; the default choice is all storage.
3. On the calendar, select a date that you wish to search. Note: Bolded dates indicate days that have recorded video.
4. Below the calendar, check the Video Type box next to the video type for which you are searching. Leaving all boxes checked is the default choice and will display all video types for the date and selected camera(s).
5. On the timeline, use the left and right sliders to choose the video search start and end time.
6. Select Search. 

7. Search through and double-click on one of the resulting video clips that you wish to playback.

For more information about video playback controls, **Click Here**.

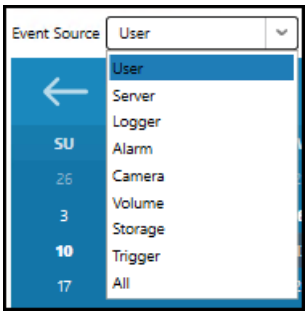
Search Event Panel

The Search Events panel enables users to search for and play back events and event-related video. Dashboard Search Events may be selected from the server's status, camera list title bar icon, or independently from the Dashboard's Title bar icon.



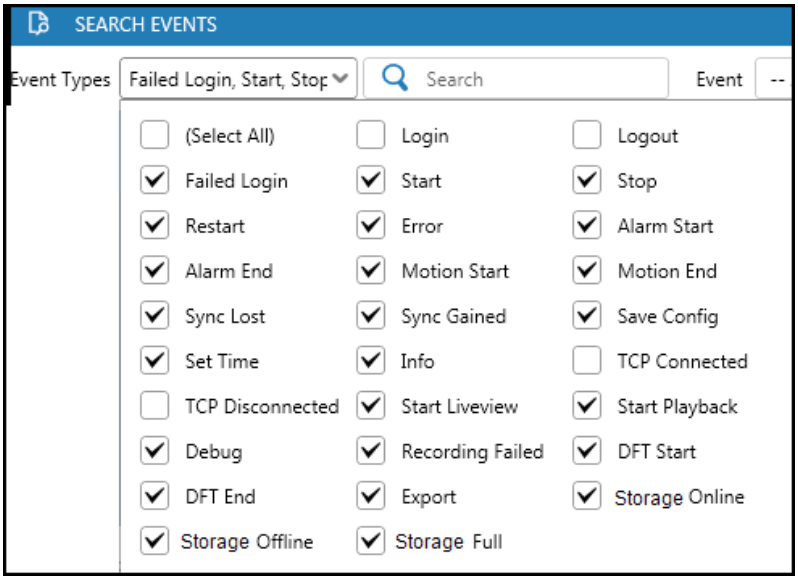
Search Events - Event Sources & Types

Events are categorized according to their origin. The event source dictates the specific list of event types that can be searched.



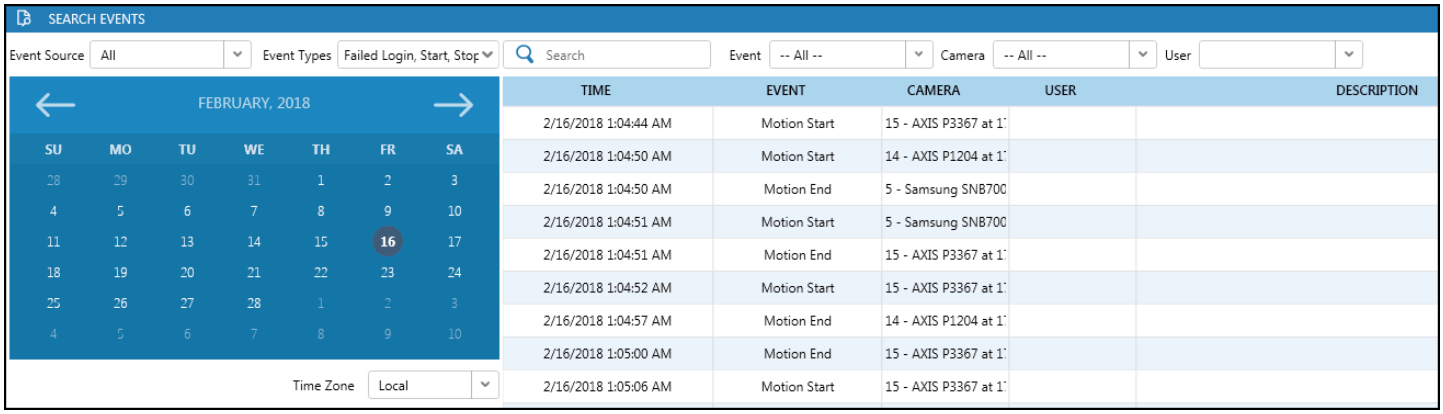
Search Events - Event Types

Events that are checked in the "Event Type" box are placed into the database as the event occurs and retained. The event list box is opened by selecting the pulldown menu. Boxes that are checked are searched, and boxes that are not checked omitted.



Search Filters

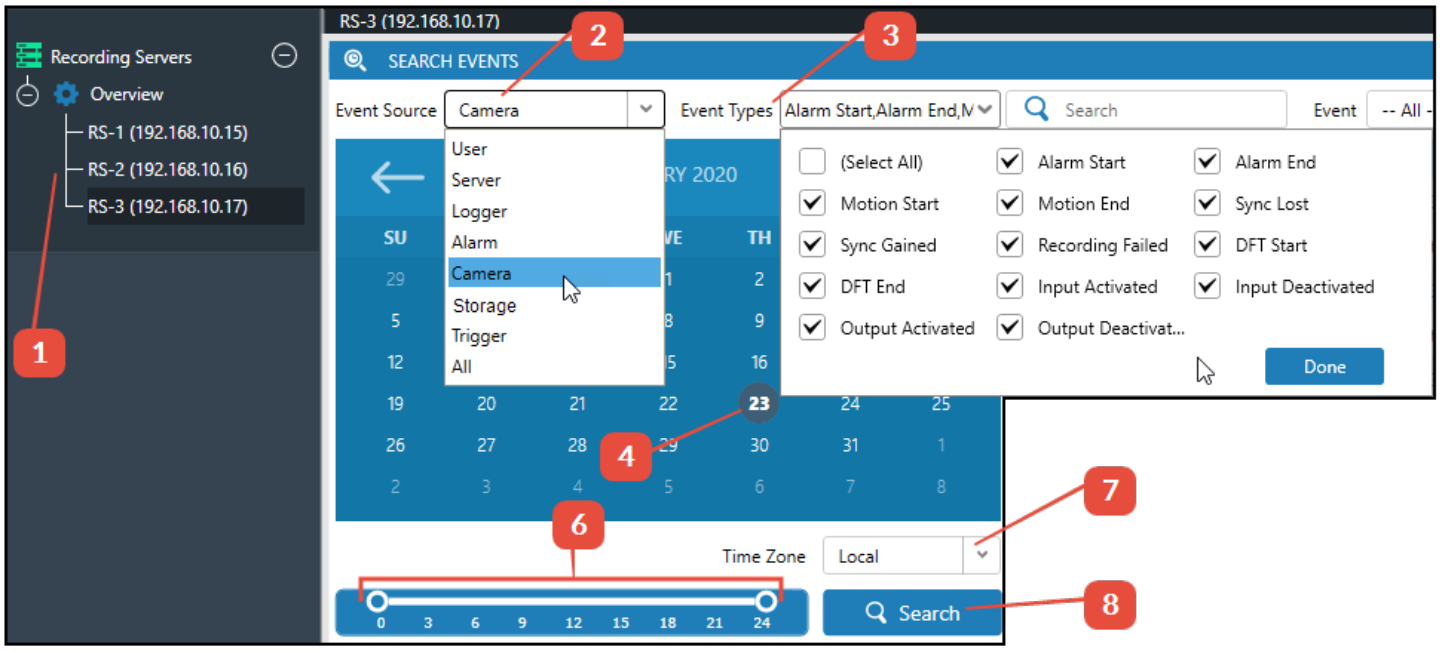
Additional search filter menus at the top of the display may be employed to search for events related to a specific camera, event (from the list), storage, alarm, logging, and/or user.



Filter Selection Chart

Second Search Menu	Third Search Menu	Expected Results
Camera	Select All or a specific camera	List of events for the selected day, time, and camera(s) are displayed.
Event	Select All or a specific listed event	List of all or particular events for the selected day and time are displayed.
User	Select All or a specific listed user account	List of all or particular events specific to the user account or all user accounts, and for the day and time are displayed.

Search Events

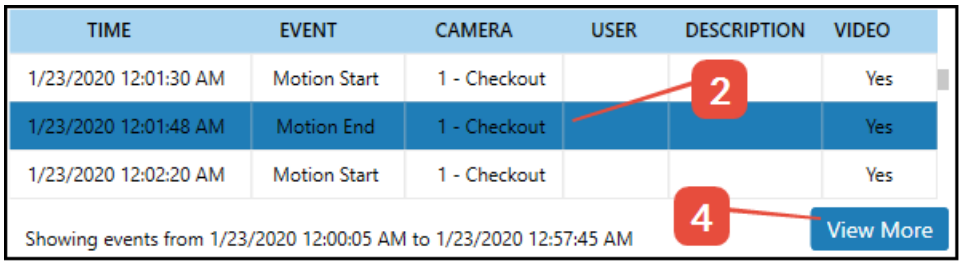


Steps:

1. Select the recording server to be searched.
2. Select the event source
3. Select the event types
4. Select the date you wish to search.
5. Bold text dates indicate event data is available for that day.
6. Set the start and end search time sliders to establish a search window.
7. Select the time zone for the search. (local or server time)
8. Select search.

Typically, cameras and any of the six events (Motion End, Motion Start, Failed Login, Stop, Start, Info) that have associated video may be played back and viewed in the video playback window, located below the calendar.

Playback Event Related Video



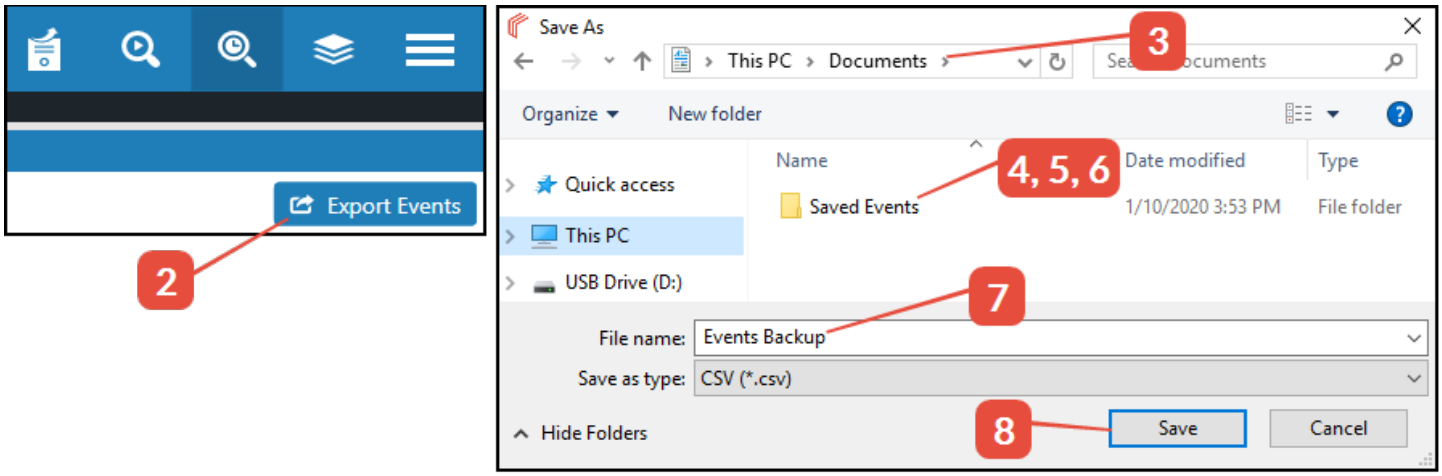
Steps:

1. When the events list is populated, search it.
2. Double-click on the result.
3. Wait for the video to display in the playback window.

4. If you do not see the event for which you were searching, look in the bottom right-hand corner of the Search Events panel and select the View More button.

Search and Export Event List

Events may be exported, saved, and displayed as a CSV file. Microsoft's™ Excel® or other CSV display tools may be used to show the file.



Steps:

1. Complete an event search
2. Select the button entitled "Export Events," which is located in the top right-hand corner
3. When the "Save As" box opens, determine where the events should be saved
4. Create a new Windows folder
5. Name the folder; suggested name, "Saved Events"
6. Open the new Saved Events folder
7. Name the saved Events file
8. Select Save

Illustrated is part of a Motion Start and Motion Stop event search report. The report was saved and shown in Microsoft's™ Excel®. A time-date search was executed to generate a Motion-Start and Motion-Stop report.

	A	B	C	D	E	F
1	TIME	EVENT	CAMERA	USER	DESCRIPTION	VIDEO
2	1/23/2020 7:34	Motion Start	Axis-3025			Yes
3	1/23/2020 7:34	Motion End	Axis-3025			Yes
4	1/23/2020 7:35	Motion Start	1 - Checkout			Yes
5	1/23/2020 7:35	Motion End	1 - Checkout			Yes
6	1/23/2020 7:35	Motion Start	Pana-311			Yes
7	1/23/2020 7:35	Motion End	Pana-311			Yes

Maintenance

The Maintenance module provides access to push updates, logging functions, camera diagnostics, and server configuration information. Use the following icons to access their respective functions, which will be discussed in subsequent sections.

 Updates

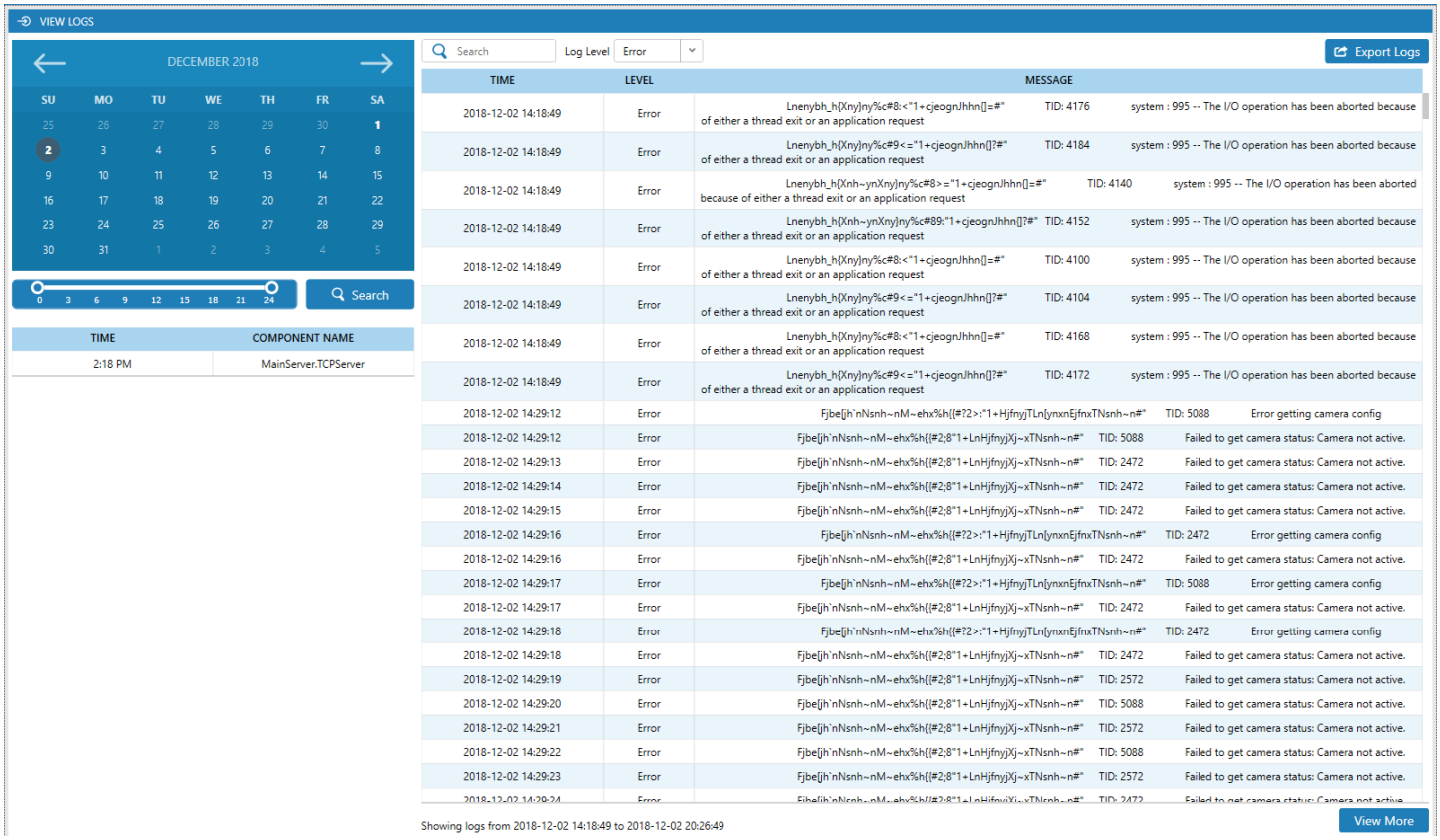
 Logging

 Camera Diagnostics

 Server Configuration

Maintenance Logging

The Logging function displays a list of searchable server event log entries, and allows for exportation of events. Click Export Logs to save as a .csv file.



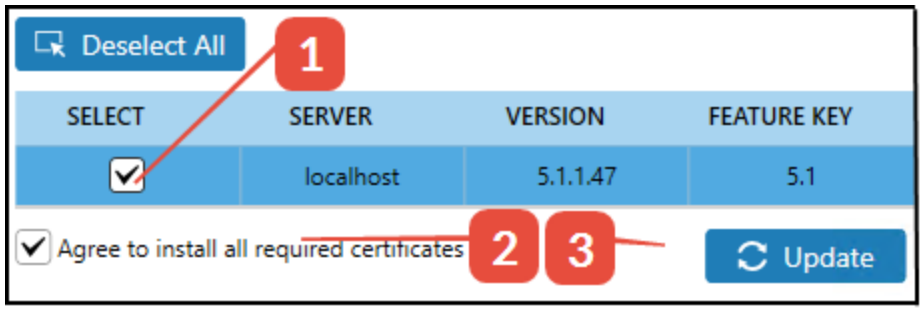
Maintenance Updates

The Updates function allows administrators to push software updates to both local and remote Recording Servers connected to the deployment's Management Server.

Note: Legacy servers must be running version 4.8.2 or newer and have a 5.1 or newer feature key applied to accept remotely pushed updates. Locally update the legacy server to 4.8.2 or newer and apply a 5.1 feature key before attempting to remotely push an update.

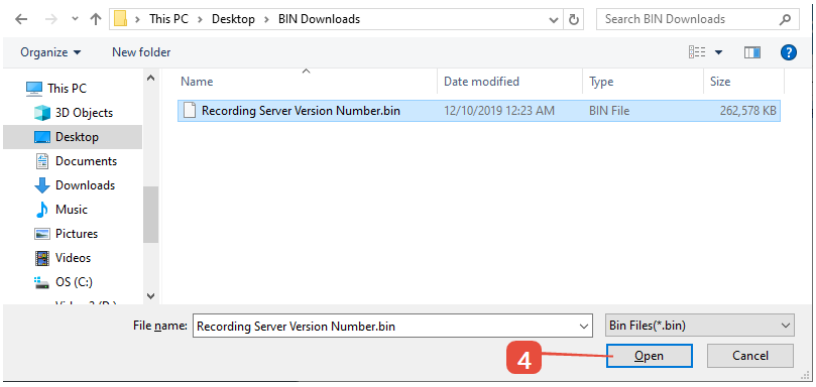
Applying Updates

The process to apply updates to single or multiple Recording Servers is identical. Simply select the server(s) to be updated, agree to install all required certificates, select Update, and choose the .bin file. Progress for each server will be displayed in the right pane.



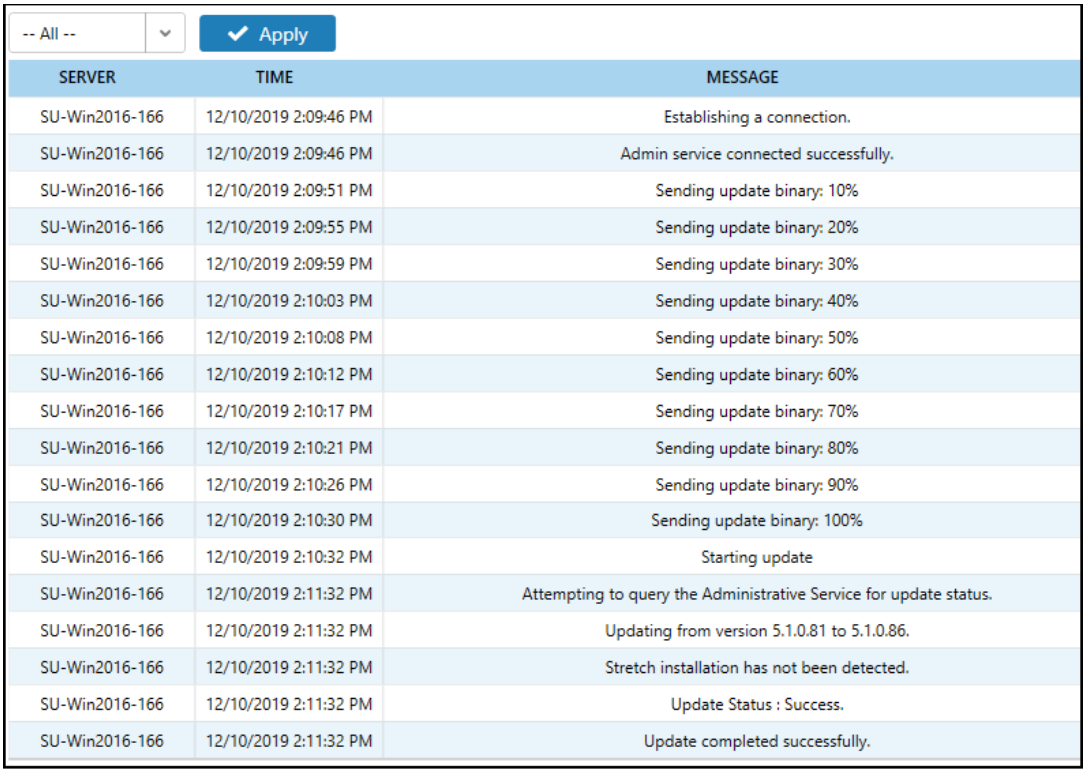
Steps:

1. Select the server
2. Check Agree to install all required certificates
3. Select Update



4. Select the .bin file and click Open

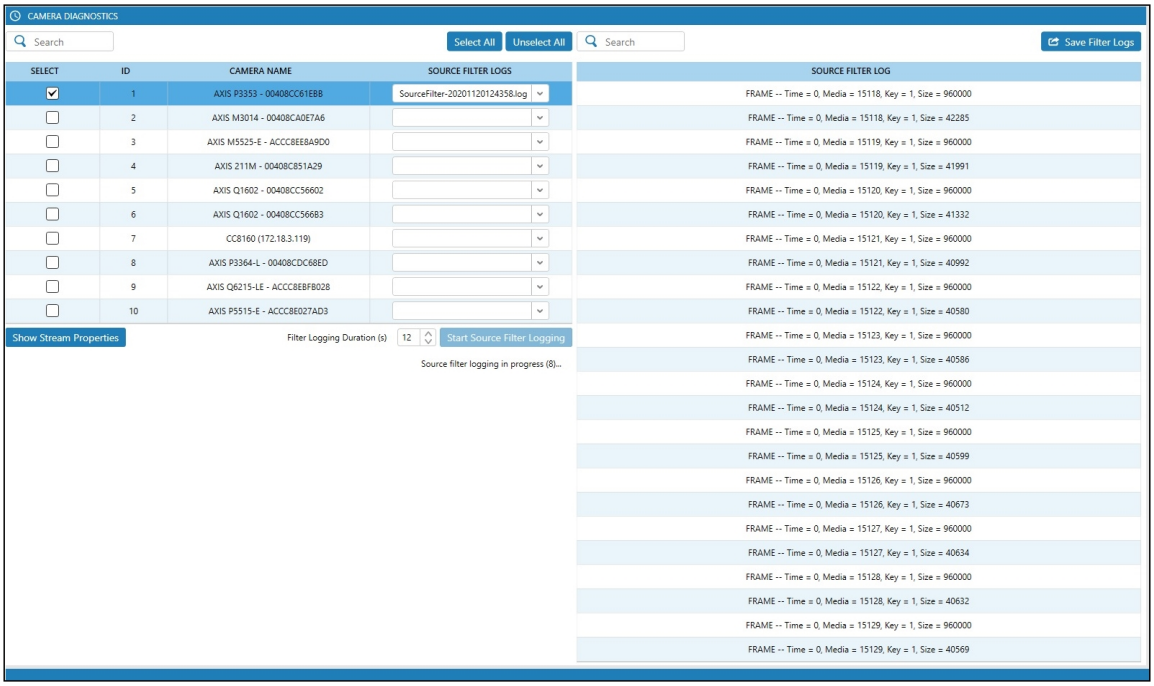
The right pane will display update progress and success or failure messages for each server to which the update was pushed. If multiple servers have been updated, use the drop down menu to select a server and click Apply to check its update status.



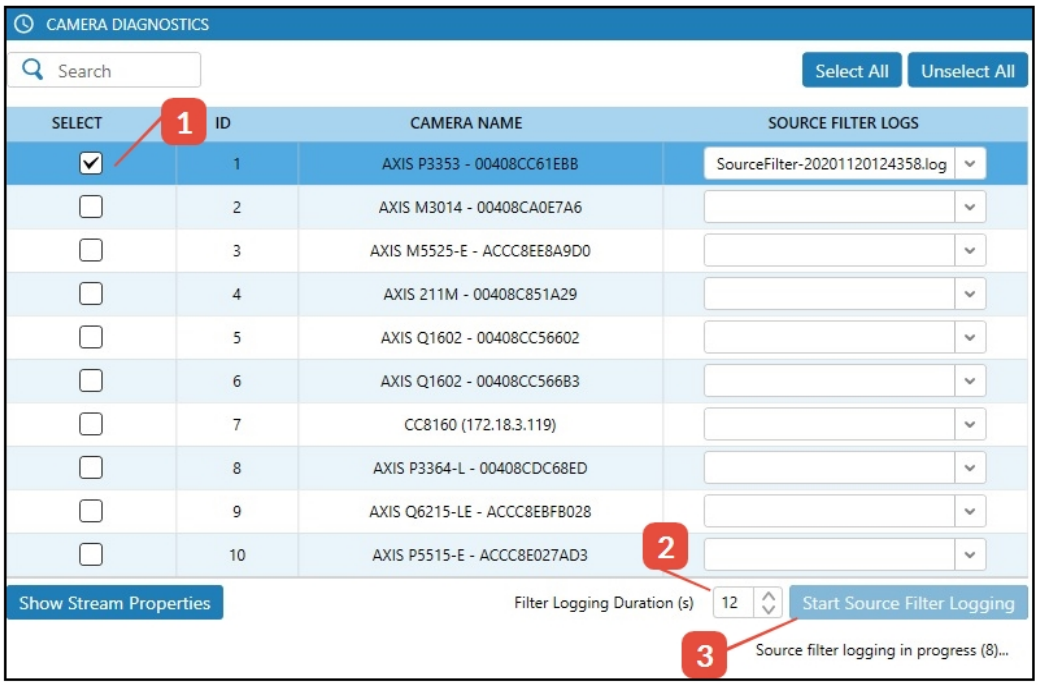
SERVER	TIME	MESSAGE
SU-Win2016-166	12/10/2019 2:09:46 PM	Establishing a connection.
SU-Win2016-166	12/10/2019 2:09:46 PM	Admin service connected successfully.
SU-Win2016-166	12/10/2019 2:09:51 PM	Sending update binary: 10%
SU-Win2016-166	12/10/2019 2:09:55 PM	Sending update binary: 20%
SU-Win2016-166	12/10/2019 2:09:59 PM	Sending update binary: 30%
SU-Win2016-166	12/10/2019 2:10:03 PM	Sending update binary: 40%
SU-Win2016-166	12/10/2019 2:10:08 PM	Sending update binary: 50%
SU-Win2016-166	12/10/2019 2:10:12 PM	Sending update binary: 60%
SU-Win2016-166	12/10/2019 2:10:17 PM	Sending update binary: 70%
SU-Win2016-166	12/10/2019 2:10:21 PM	Sending update binary: 80%
SU-Win2016-166	12/10/2019 2:10:26 PM	Sending update binary: 90%
SU-Win2016-166	12/10/2019 2:10:30 PM	Sending update binary: 100%
SU-Win2016-166	12/10/2019 2:10:32 PM	Starting update
SU-Win2016-166	12/10/2019 2:11:32 PM	Attempting to query the Administrative Service for update status.
SU-Win2016-166	12/10/2019 2:11:32 PM	Updating from version 5.1.0.81 to 5.1.0.86.
SU-Win2016-166	12/10/2019 2:11:32 PM	Stretch installation has not been detected.
SU-Win2016-166	12/10/2019 2:11:32 PM	Update Status : Success.
SU-Win2016-166	12/10/2019 2:11:32 PM	Update completed successfully.

Maintenance Camera Diagnostics

Camera Diagnostics allows for the capture and exportation of detailed camera information and display of stream properties.



Capturing Camera Stream Data

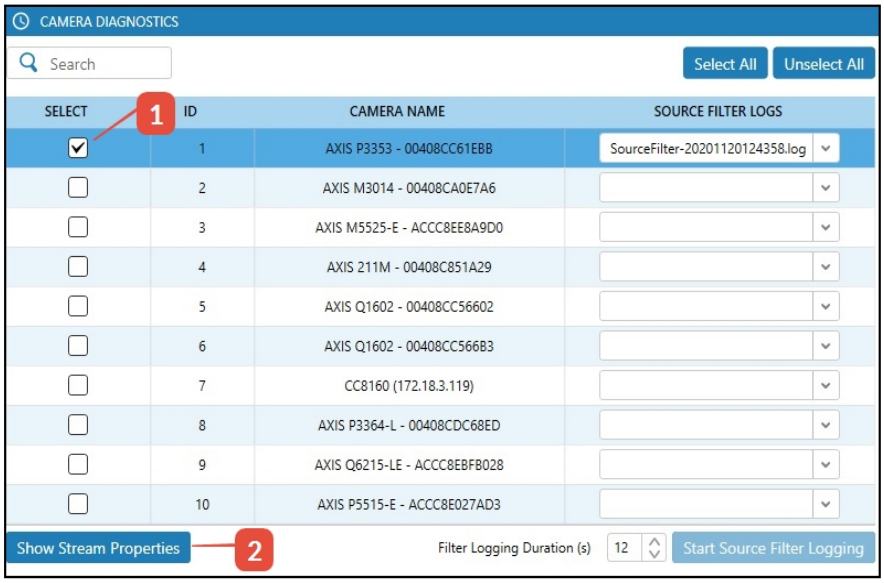


Steps:

1. Select the camera
2. Select the duration of the capture (in seconds)
3. Click Start Source Filter Logging

The camera's information will be displayed in the Source Filter Log pane to the right. Click Save Filter Logs to save the data.

Show Stream Properties



Steps:

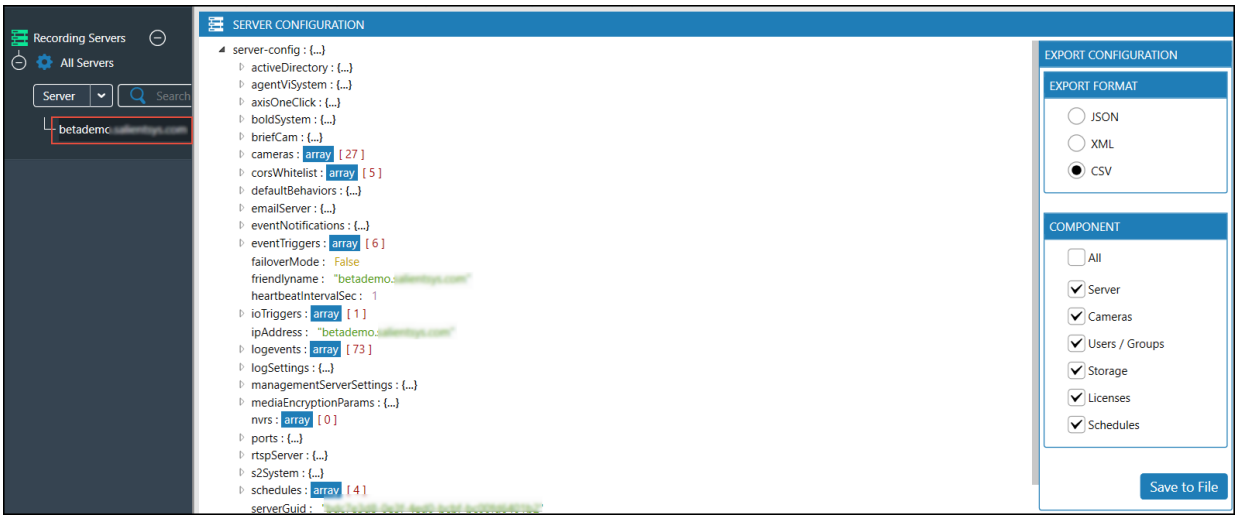
1. Select the desired camera
2. Click Show Stream Properties

The stream properties will be displayed in the right pane. Click Save Stream Properties to save the data.

Maintenance Server Configuration

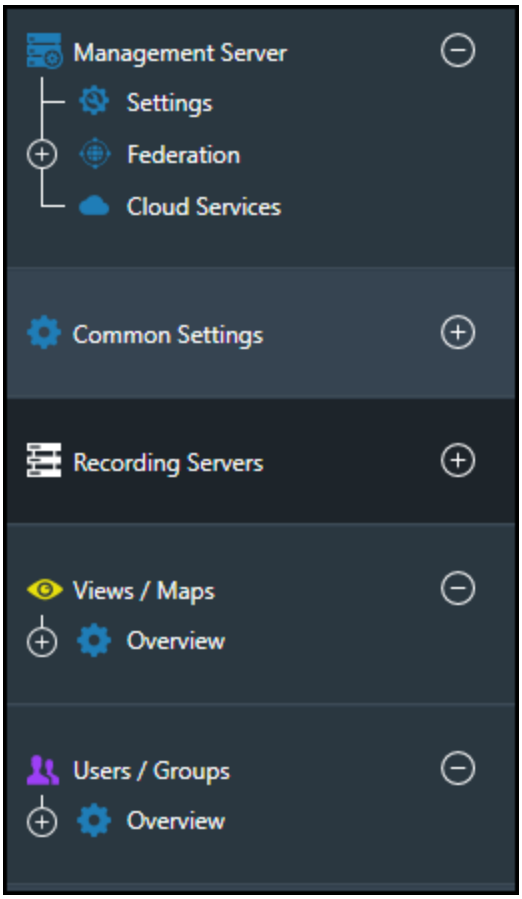
Server Configuration provides detailed, exportable information about the selected Recording Server.

Select the desired server, and click the carat to expand the information tree to view. The data may be saved as a .json, .xml, or .csv file. In addition, various components' configurations may be selected for inclusion in or exclusion from the exported file.



Configure Module Introduction

The Configure module is divided into the following subpanels: Management Server, Common Settings, Recording Servers, Views/Maps, and Users/Groups. Each subpanel has been designed and labeled to clearly identify its purpose. From here, administrators may adjust the settings for each of those areas of functionality.



The Navigation Pane within the Configure module may be locked to prevent changes. Click on the icon to lock and unlock the Navigation Pane.

Configuration Menu

Saves the current server configuration

Adds a new server

Toggles between editing and monitoring the selected server

Allows addition of a Volume, Storage Pool, NVR, Camera, I/O, Trigger, or Schedule to the select server

Allows addition of a new View, Auto View, or Map to the selected server

Allows addition of a new User or Group to the selected server

Quick links to Servers, Cameras, Storage Pools, Volumes, I/O, Licenses, Views, Maps, GPS, Users, Groups, and Active Directory configuration areas

Settings, About, Change Password, Logout

Common versus Recording Server Specific Settings

The Client and every individual Recording Server include settings that host Ports, Security, Operations, and Integrations. Services are located only on the Management Server. When configured and implemented from Common Settings, Ports, Services, Security, Operations, and Integrations may be applied to all CompleteView Recording Servers, generally by selecting Apply to All Servers. If configuring an individual Recording Server and the given setting has come down from the Management Server, a check mark will be displayed next to "Inherited" in the upper right corner.

When applied to the individual Recording Server, Ports, Operations, and Integrations, are applied exclusively to that Recording Server. Security certificates are applied to both individual Recording Servers and the Management Server.

Information about Saving Configuration Changes

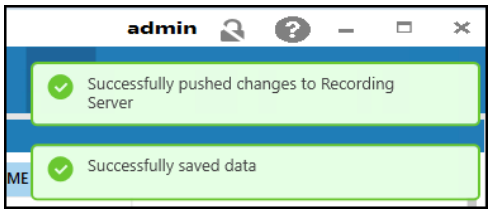
The Management Server keeps a copy of a Recording Server's configuration and device information. The Recording Server also keeps a copy of the configuration and device information and uses its local copy of the configuration so that it doesn't have to rely on Management Server availability. The Client maintains a local copy of Management Server's data to improve response time and maintain functionality in the event the Management Server goes offline.

When a Legacy Server is added to the Client, a record of it is kept in the Management Server. However, the server's configuration file is kept in the Legacy Server's CompleteView 4.X folder.

Saving the Configuration to the Management Server

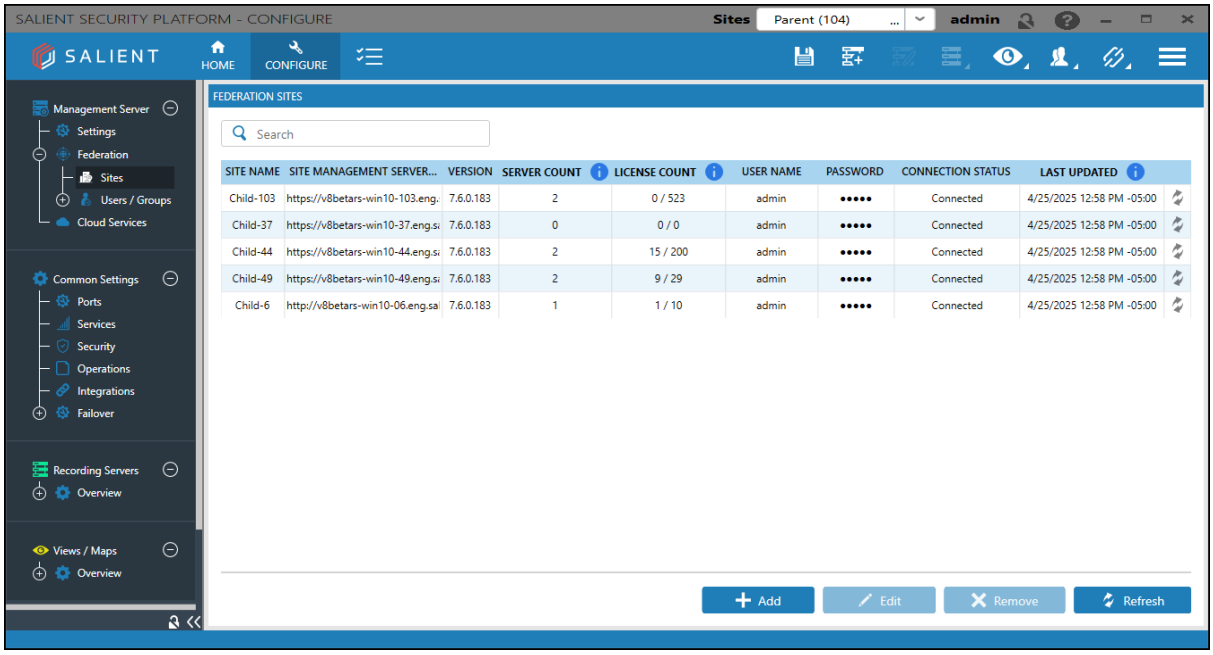
Each time configuration changes are made, they must be saved in order to take effect. Selecting Save Configuration saves all unsaved changes to the Management Server.

Any confirmation, informational, or error messages will be displayed near the save button.



Federation Overview

The Management Server configuration pane contains Management Server and Cloud details and allows for the configuration of Federation, described below.



Federation Architecture: Parent and Child Sites

The Federation architecture is characterized as a single-tier, hybrid model consisting of a single Parent and many Child Management Servers (also referred to as Sites) that allows for centralized oversight while maintaining local autonomy at individual sites. A Child site consists of a Management Server and any number of Recording Servers. A collection of federated servers is known as a Deployment.

The Parent Management Server acts as the central credential authority within the federation, managing per-site access for federation groups. Recording Server permissions for those federated groups are handled locally, on a per-site basis. Once established on the Parent Management Server as a federated user in a federated group, credentials are propagated to the Child servers. Federated users can then connect directly to any site they have access to and seamlessly switch between sites without needing multiple credentials. Each time a user connects to a site, authentication is managed locally, minimizing the need to send every authentication request to the Parent Management Server after initial credential verification. Child Management Servers manage local resources and provide granular user management for site-specific access control.

This architecture enables centralized oversight from the Parent Management Server while allowing individual sites to operate autonomously. If the Parent Management Server becomes unavailable, Child sites continue operating normally, ensuring uninterrupted access for both federation and site users. Additionally, each Child site maintains a list of its sibling sites, allowing federation users to switch between Child sites and authenticate locally—even if the Parent Management Server is offline.

An example of creating a Parent and Child sites will be shown in the Federation Implementation section.

Federation Users and Groups Overview

The purpose of creating a Federation User and associating it with a Federation Group is to allow that user access to both the Parent and Child sites in a Deployment. Like traditional CompleteView Users,

Federation Users can be either VMS users or AD users. It is not required to use Federation Users and Groups. However, if Active Directory is not in use, a VMS user would need to be created and managed for each Child site where access is required, individually. Employing Federation Users and Groups reduces this burden by allowing management of the Federation VMS User and Groups on the Parent Management Server.

If using Active Directory, ensure each site in the Deployment can authenticate to the same Active Directory instance. AD users will be imported from the Active Directory Domain the Parent Management Server is associated with. Again, it is critical when using AD users and Groups that the Child site can authenticate the AD users to the same domain that the Parent Management Server is associated with.

While either Federation Users or Groups may be created first, the process will be more streamlined by defining Federation Users when implementing new systems. An example of creating Federation Users and Groups will be shown in the **Federation Implementation** section.

Prerequisites

Federation is available for new Deployments running version 7.5.0 or newer. With the introduction of version 7.6.0, existing Deployments may be migrated to a federated configuration.

While there are no licensing fees associated with Federation, it is important to note that enabling this feature may necessitate the deployment of additional Management Servers to establish the Federation environment.

Configuration of a Federation requires administrative credentials for each of the Management Servers to be federated. A Management Server needs to be designated as the Parent, and connectivity with the Child sites is required.

Federation Solution Guide

For in-depth information, planning and design considerations, use-cases, lifecycle management, implementation guidelines, and migration instructions, refer to the Federation Solution Guide, located on the Salient website, or contact support.

https://www.salientsys.com/download/federation-solution-guide/

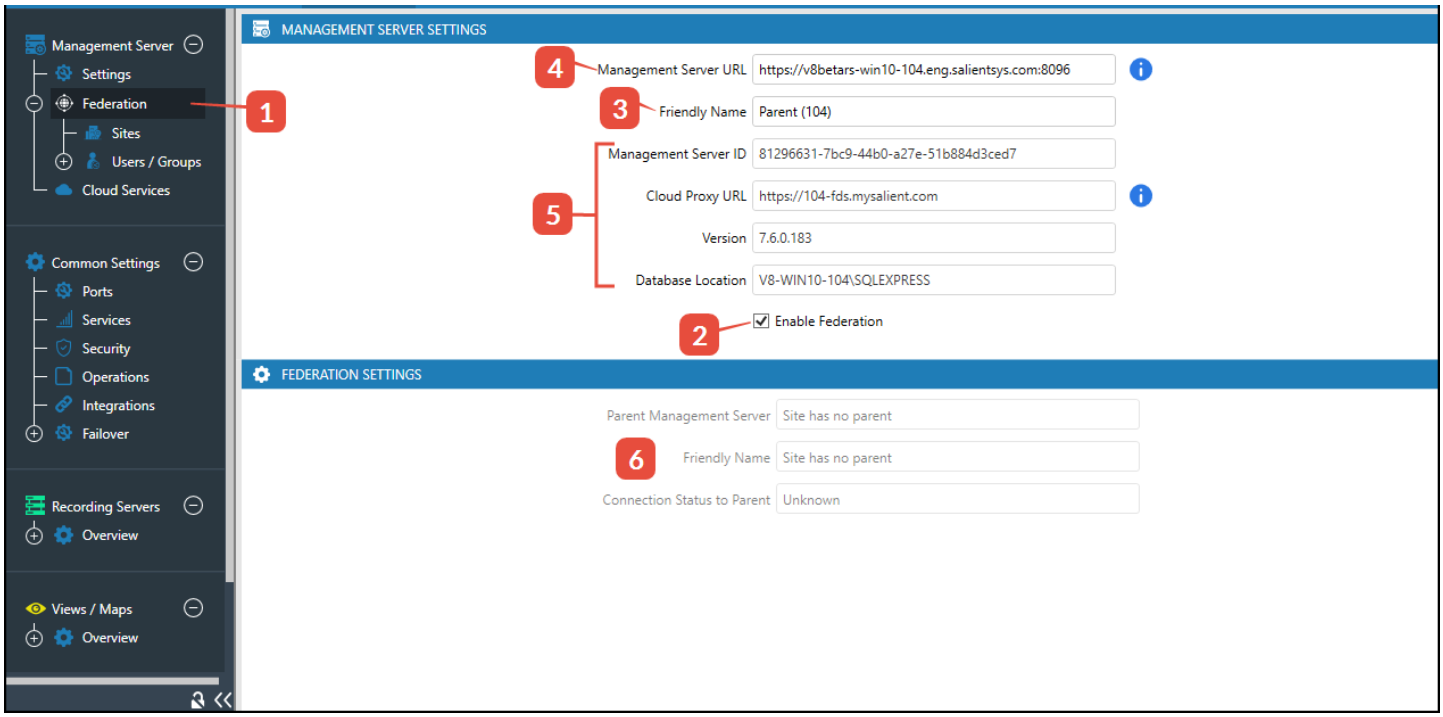
Federation Implementation

The following section provides general procedures and guidelines for creating and configuring a Federated Deployment. Because of the scope and level of complexity involved, it is strongly recommended that the Federation Solution Guide discussed in the previous section be downloaded and studied before proceeding. If migrating an existing traditional Deployment to a Federation, contact Salient support for more information as that process is not detailed in this documentation.

Parent Management Server Configuration

Log in to the Management Server to be designated as the Parent with administrative credentials.

Before enabling Federation, verify that the Management Server URL is correct in either the Settings or Federation nodes, as it defines how other Management Servers in the Deployment will connect to it. The Desktop Client will auto-populate this field based on the Management Server's system. If a different URL is desired, it should be configured prior to enabling Federation, although it can be updated later.



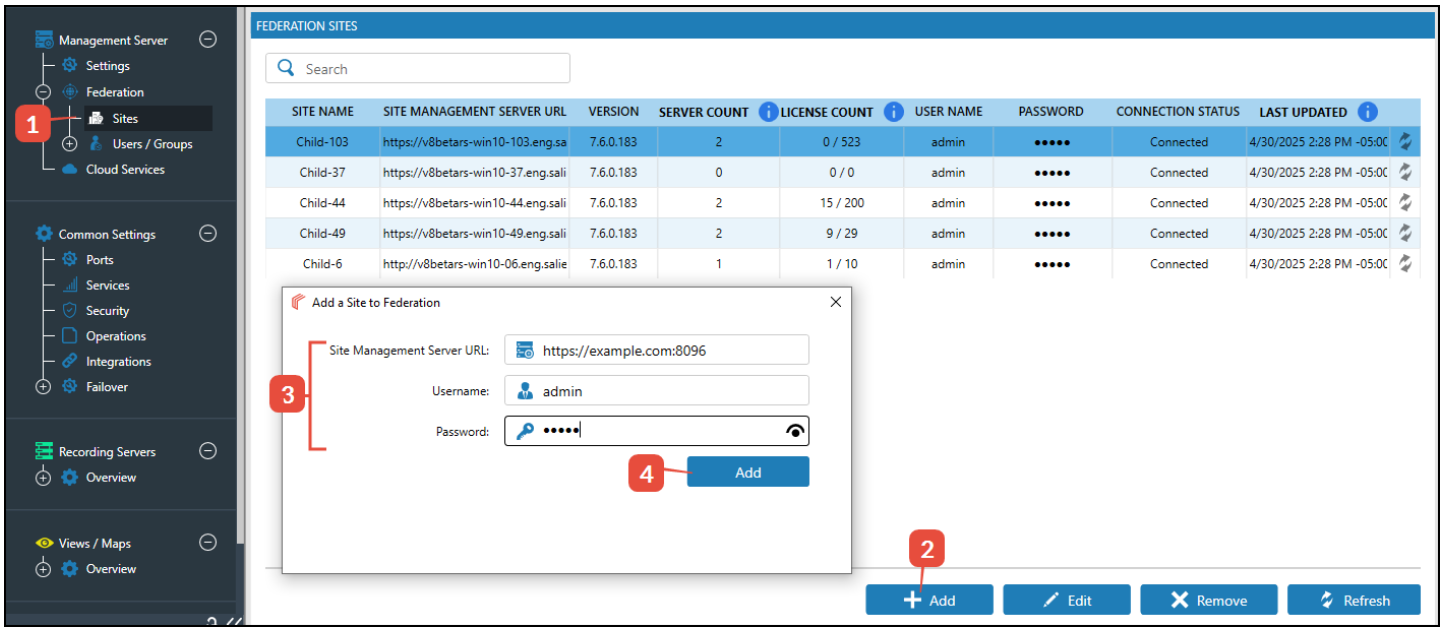
1. From the Management Server left navigation pane, select Federation.
2. Select Enable Federation.
3. Optionally provide a meaningful Friendly Name, which will be used for both Site Switching and as the Site Name in the Sites pane, discussed below. The field is populated by default, usually with the computer's name.
4. The Management Server URL auto-populates and is the value used to connect to the Management Server via the Desktop Client, other Management Servers, and Recording Servers. If the computer name, IP address, network security settings, etc., are changed in the string (e.g. TLS is enabled at a later date), the field must be updated with the new information (e.g. changing from http: to https:, port from 8095 to 8096, etc.).
5. Management Server ID, Cloud Proxy URL, Version, and Database Location fields are auto-populated, non-editable, copyable, and are provided for informational purposes.

6. The Federation Settings pane will not populate for the Parent.
7. Save when done.

Adding Sites to the Parent

After configuring the Parent Management Server, add sites to define and build the federation. Note that the sites must be online, reachable, and functioning in order to successfully add them.

The URL of the Child Management Servers should be confirmed before attempting to connect them to the Federation. This can be confirmed by connecting to each Child Management Server and viewing the Management Server Details page. The URL can be verified and updated, if needed, in the same manner as described above for the Parent Management Server. There is no need to enable Federation at the child, as this will be done by the parent. If the URL of the Child Management Servers is known, then there is no need to connect to the Child Management Server prior to adding it to the Parent Management Server.



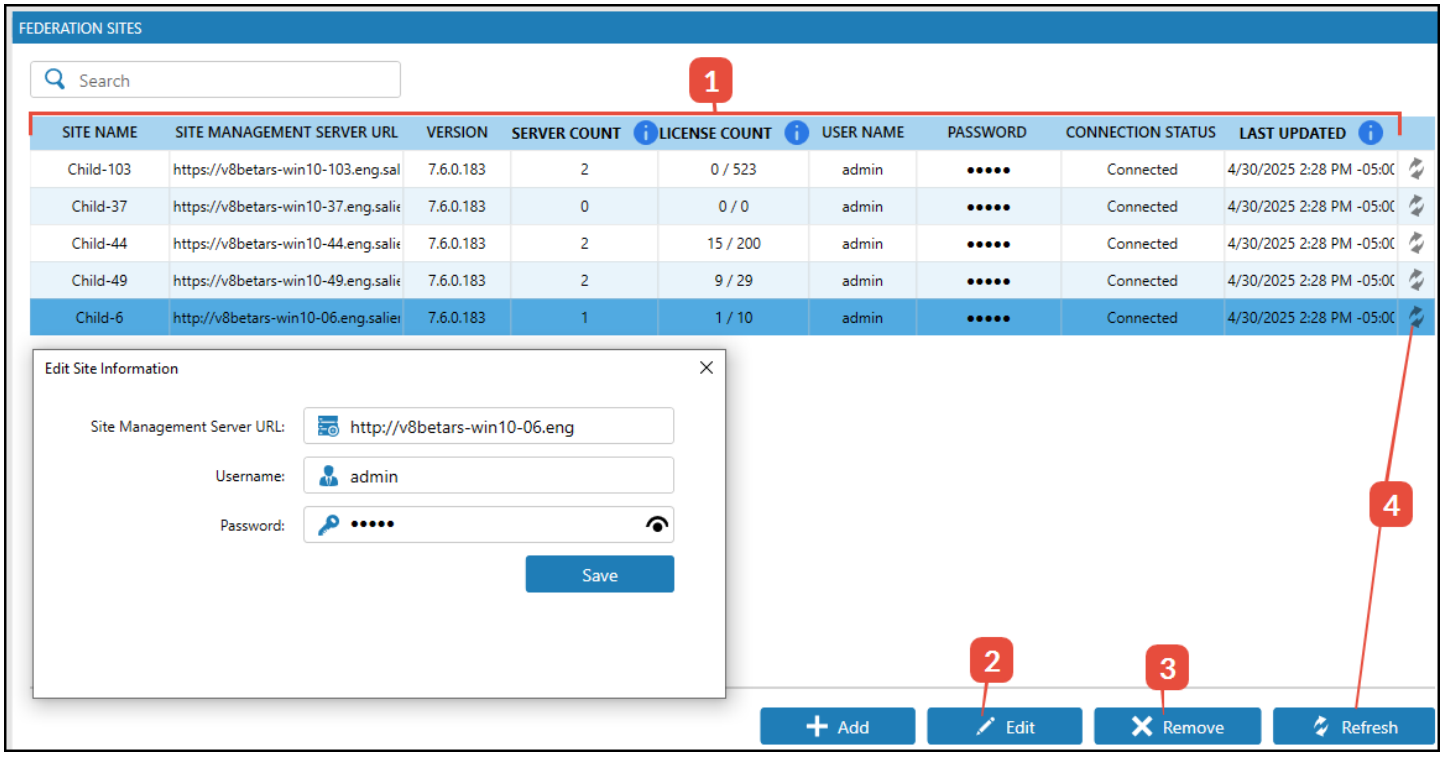
1. From Management Server, Federation, select Sites.
2. Select Add.
3. Fill in the Site Management URL, Username, and Password fields. The credentials must have full administrator privileges.*
4. Select Save.

*To establish a connection between the Child and Parent, an admin level account will be needed when adding the Child site. This account will be used for polling between the parent and children. If the password for this admin account is changed, update the site to reflect the new password.

After clicking Save, the Parent will contact the Child Management Server, authenticate the provided credentials, enable the federation setting, and add that Site to the Deployment.

Federation Sites Pane

Added Child Management Server (Site) information may be viewed and modified from the Federation Sites pane. Sites may be added or removed and statuses checked from here. The pane will only be populated on the Parent Management Server. Child Management Servers will display a message prompting the user to log in to the Parent Management Server.



1. Federation Site Fields

Site Name	The Friendly Name as configured in Management Server, Settings
Site Management Server URL	The value used to connect to the Management Server via the Desktop Client, other Management Servers, and Recording Servers. If IP address, computer name, network security settings, etc., are changed (e.g. TLS is enabled at a later date), the field must be updated with the new information (e.g. changing from http: to https:, port from 8095 to 8096, etc.).
Version	The CompleteView Management Server version
Server Count	The number of attached Recording Servers to that Management Server
License Count	The number of analog and IP camera licenses used over the number available
User Name	The User Name supplied to connect with the server
Password	The Password supplied to connect to the server
Connection Status	Indicates the current connection status and last attempted connection to the Child Management Server. See Refresh Status below for more information.

2. Click to edit the selected server's URL and credential information.
3. Click to remove the selected server(s).
4. Click to refresh the connection status between the Parent and Child Management Servers either individually or for all sites. See below for more information.

Refresh Status

The Parent Management Server periodically polls all the Federated Children servers about their connection status, Site name, and the time and date of the last attempt.

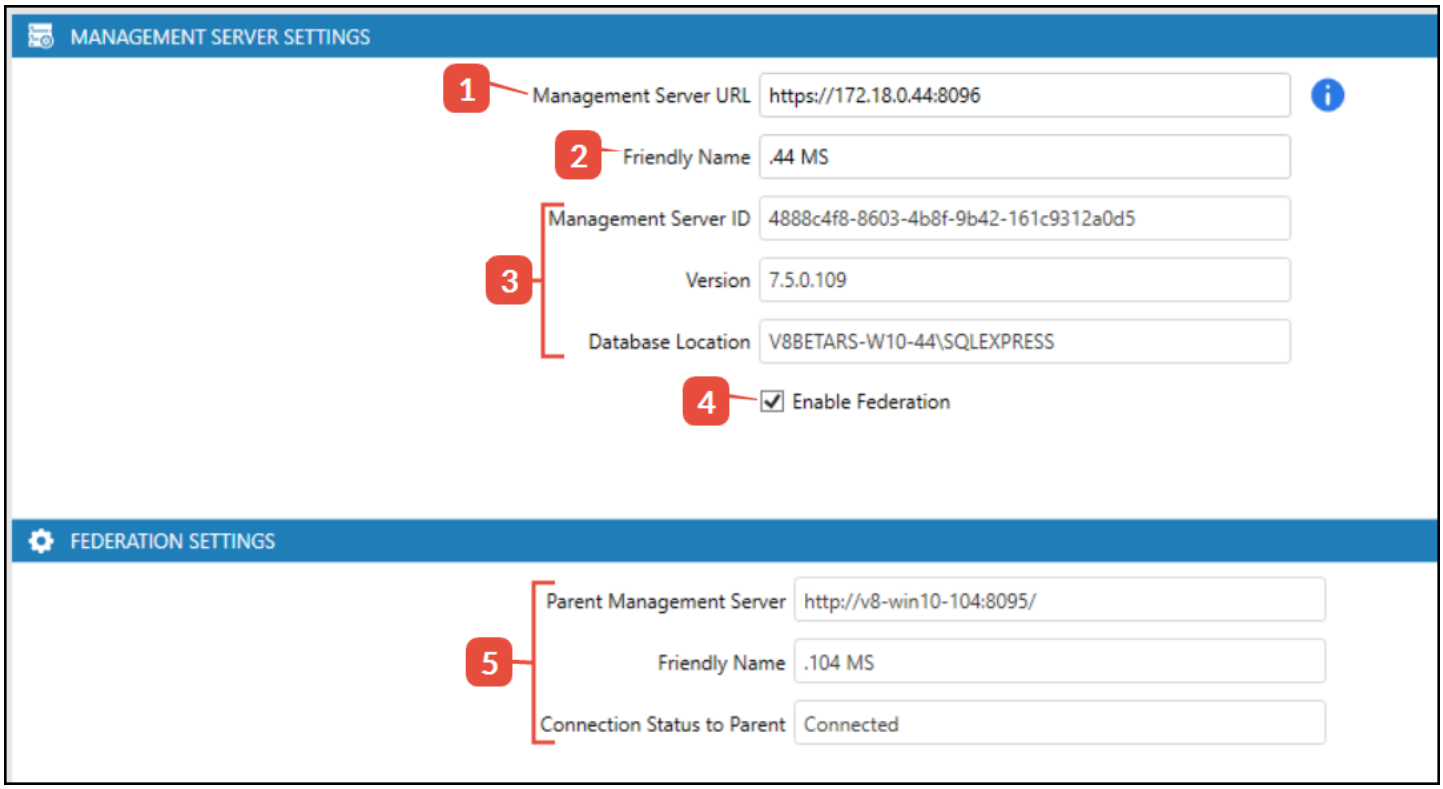
Selecting a server and clicking Refresh Status will update all the fields above (if necessary) for the selected site, and will also poll the server for version, server count, and license count information as well. Polling is also done from the Parent at an interval, but the displayed values will not be refreshed until the page is reloaded by navigating away and returning to the page.

Possible connection statuses include:

Connected	Successful connection and authentication
In Progress	The Parent is attempting to connect and authenticate with the Child server
Failed Authentication	The Child is reachable, but the Parent failed to authenticate. Check credentials.
Unreachable	The network on which the Child resides is unreachable
Not Connected	The Parent is not currently connected with the child. The Child may have disabled Federation.

Child Management Server Configuration

Child servers may update their URL information and Friendly name and may block the Parent from access when necessary. In addition, connection status with the Parent is displayed in the Federation Settings pane, but is not editable.



1. The Management Server URL auto-populates and is the value used to connect to the Site Management Server via the Desktop Client, other Management Servers, and Recording Servers. If IP address, computer name, network security settings, etc., are changed (e.g. TLS is enabled at a later date), the string must be updated with the new information (e.g. changing from http: to https:, port from 8095 to 8096, etc.). **After the change, the new URL information must be manually updated on the Parent Management Server**.
2. Optionally provide a meaningful Friendly Name, which will be used for both Site Switching and as the Site Name in the Sites pane. The field is populated by default, usually with the computer's name. Any changes to the Friendly Name will automatically be detected by the Parent and updated.
3. Management Server ID, Version, and Database Location fields are auto-populated, non-editable, copyable, and are provided for informational purposes.
4. Selecting Enable Federation will allow Parent access to the Child, which enables the Site for Site Switching, discussed below.

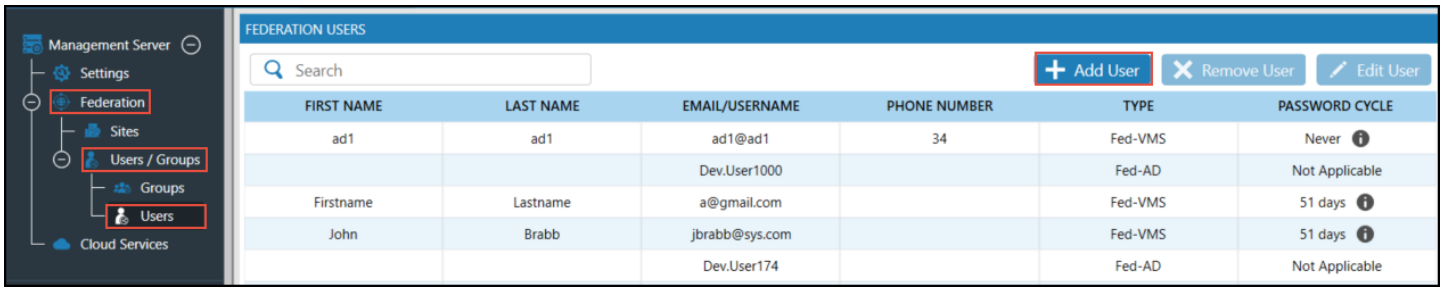
   Disabling Federation prevents federation actions from taking place on the Site, such as Site Switching, until re-enabled.

Creating Federation Users

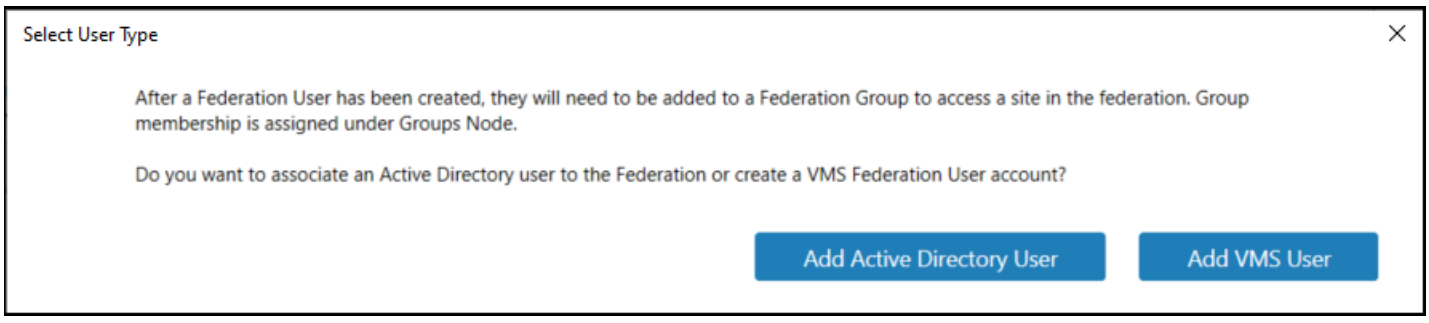
With the Parent and Child sites created, the next step is to define Federation Users and Groups. As indicated previously, it is not required to use Federation User and Groups. However, if Active Directory is not in use, then a VMS user will need to be created and managed at each site where access is needed. Once again, ensure each site can authenticate to the same instance if using Active Directory.

Note that while either Federation Users or Groups may be created first, the process will be more streamlined by creating Federation Users before Groups when implementing new systems.

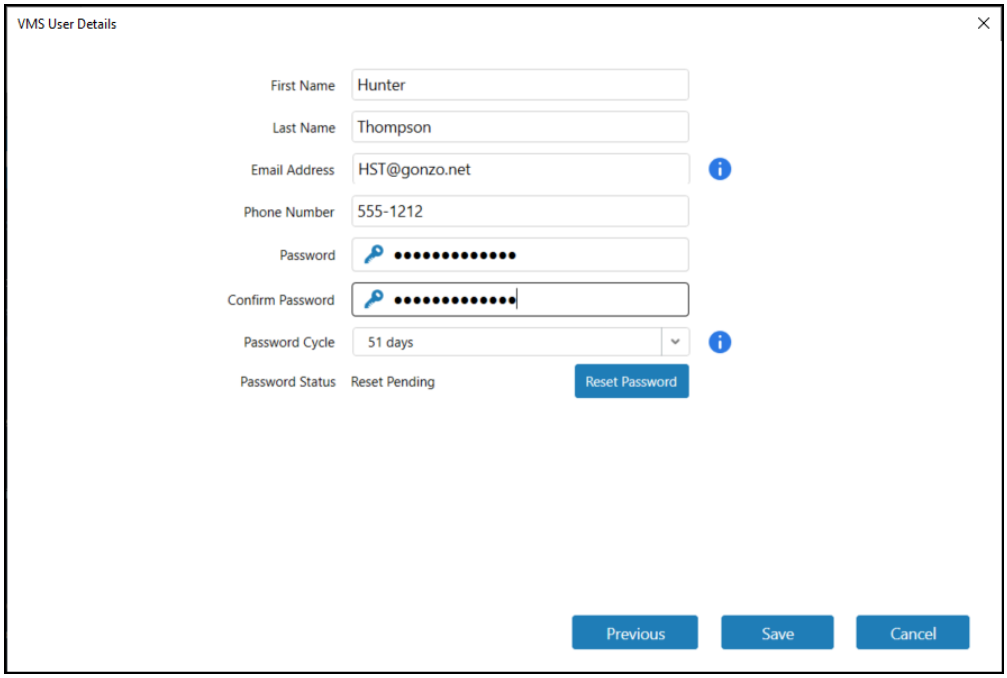
The creation of either a VMS or Active Directory Federated user begins by first expanding the Federation node then the Users / Groups node of the Parent Management Server. Select the Users branch and click Add User. Note that Password Cycle information will be visible if password policies have been enabled. For more information, see Password Policy in Common Settings Operations.



From the pop up dialog window, select which type of user to create.



Creating a Federated VMS User

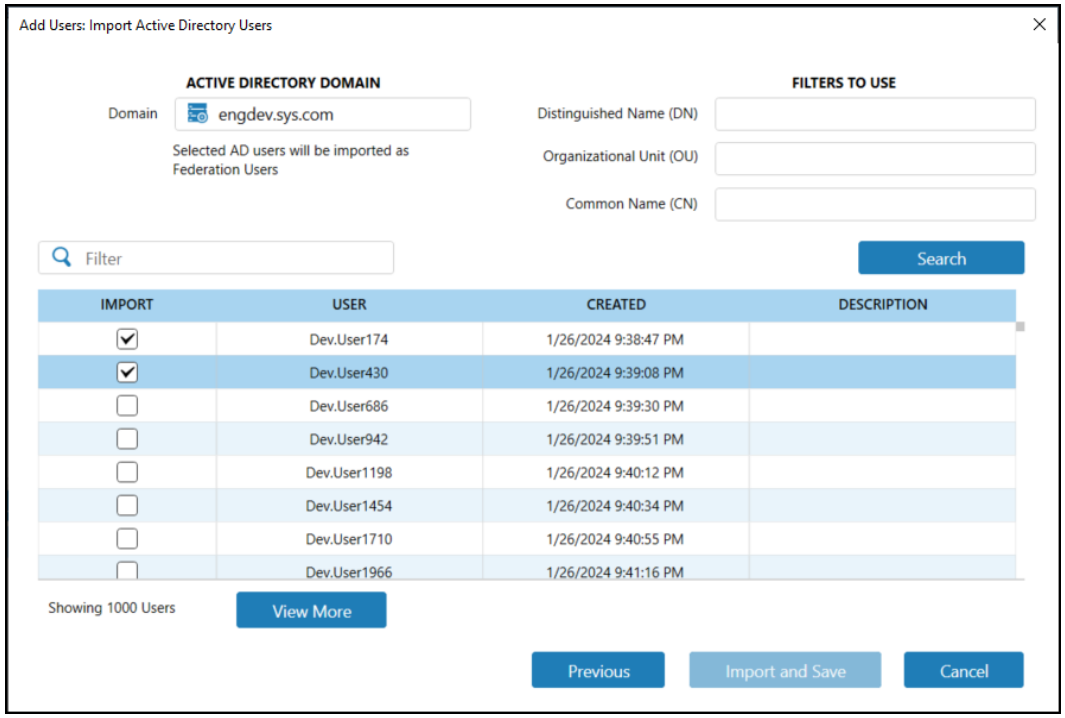


In the dialog box, fill out the required fields, including the first and last name, email address and password. The phone number can optionally be included. Once the required fields are populated and the password is confirmed, click the Save button. Set the desired Password Cycle.

It is important to note that a Federation User's username will be the email address entered at the time of creation. This is a departure from CompleteView's traditional users which did not use an email address for that purpose.

Once the user is saved, additional users can be added or Federation Groups can be defined.

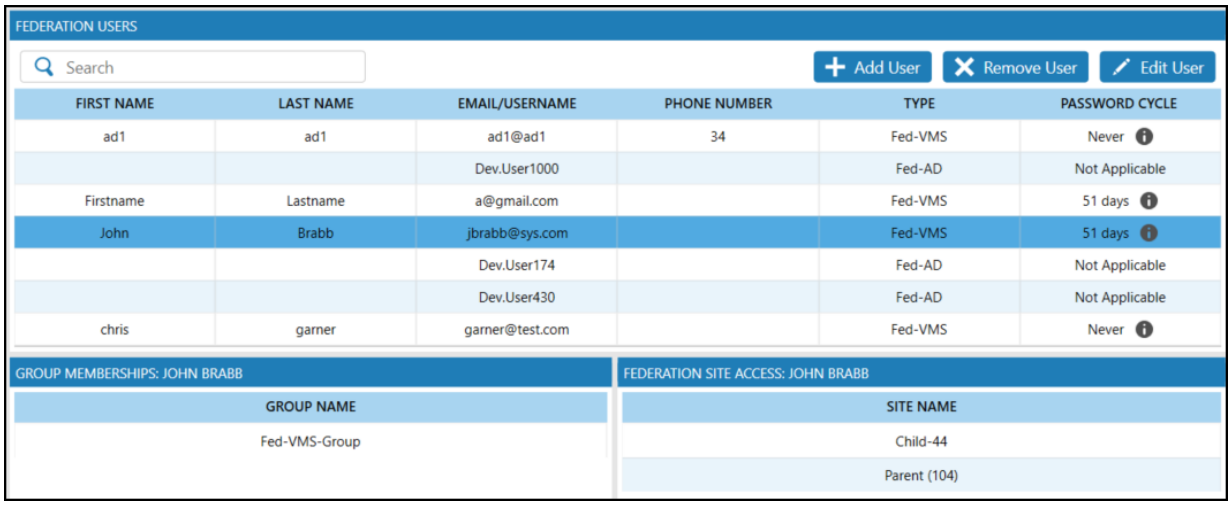
Importing an AD User



To import an AD user, select Add Active Directory User from the Select User Type dialog. The Domain will be pre-populated with the Active Directory domain defined in the Common Setting -> Services -> Active Directory page of the Configure Module. The page allows filters to be applied for the Distinguished Name, Organizational Unit, or Common Name when searching for Active Directory users.

Once the desired Active Directory users have been selected, the Import and Save button will become active. Click it to perform the action and close the dialog.

Federation Users Page



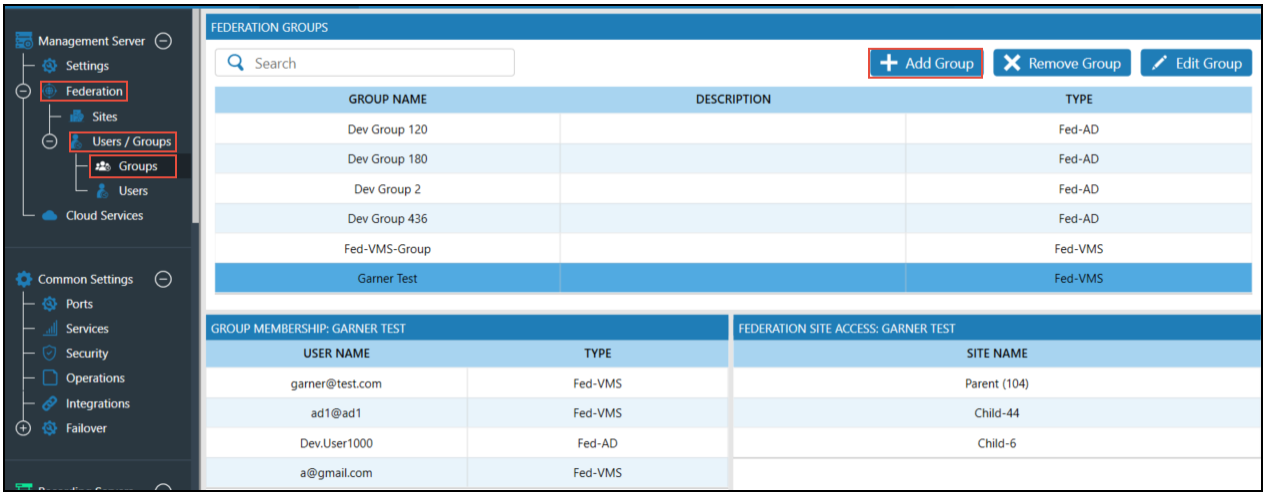
The Federation Users page displays a user's group membership and site access information. It also allows for adding, editing, and removing users. Modifying or removing users can only be performed one user at a time by selecting a user and then the appropriate button for the desired action. Further, only Federation VMS Users can be edited. If an Active Directory user needs to be modified, it must be performed in Active Directory. The potential consequences of removing a user are discussed in the Federation Solution Guide. Finally, unlike traditional VMS users (non-Federated), if Password Policy is ernabled on the Parent Management Server, all Federated VMS Users' password cycles will be automatically updated to align with the global cycle.

Creating Federated Groups

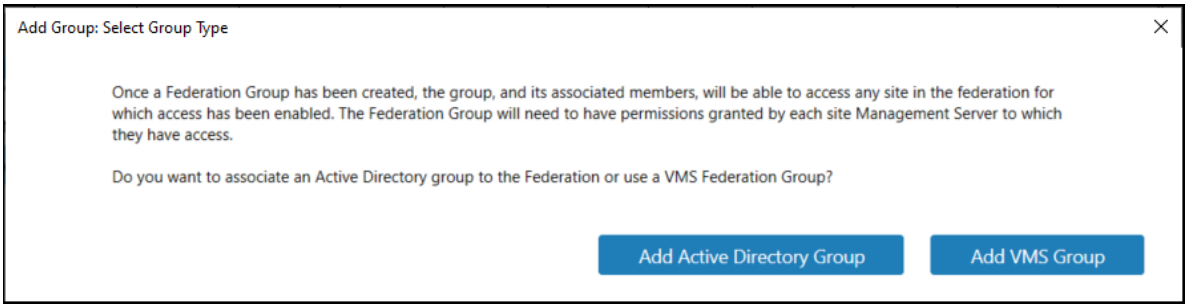
After creating Federation Users, they need to be associated with either a VMS or AD Federation Group. If a Federation User is not associated with a Federation Group or if the group to which the user belongs has not been granted access to a site, the Federation User will not be able to log into a site. Using Active Directory does create some exceptions to this rule, discussed in the Federation Solution Guide.

This section details the creation of a Federation Group, associating Federation Users to that group, and granting the Group access to the various sites in the Deployment.

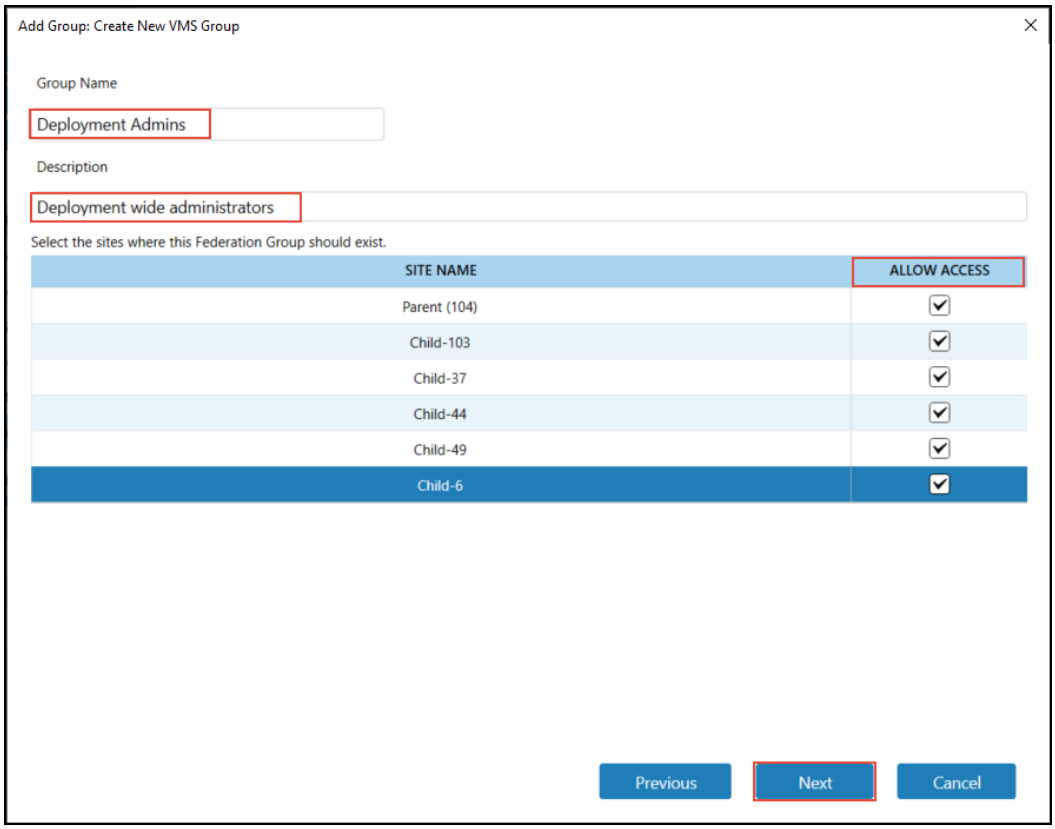
The creation of either a VMS or Active Directory Federated group begins by first expanding the Federation node then the Users / Groups node of the Parent Management Server. Select the Groups branch and click Add Group.



From the pop up dialog window, select which type of group to create.

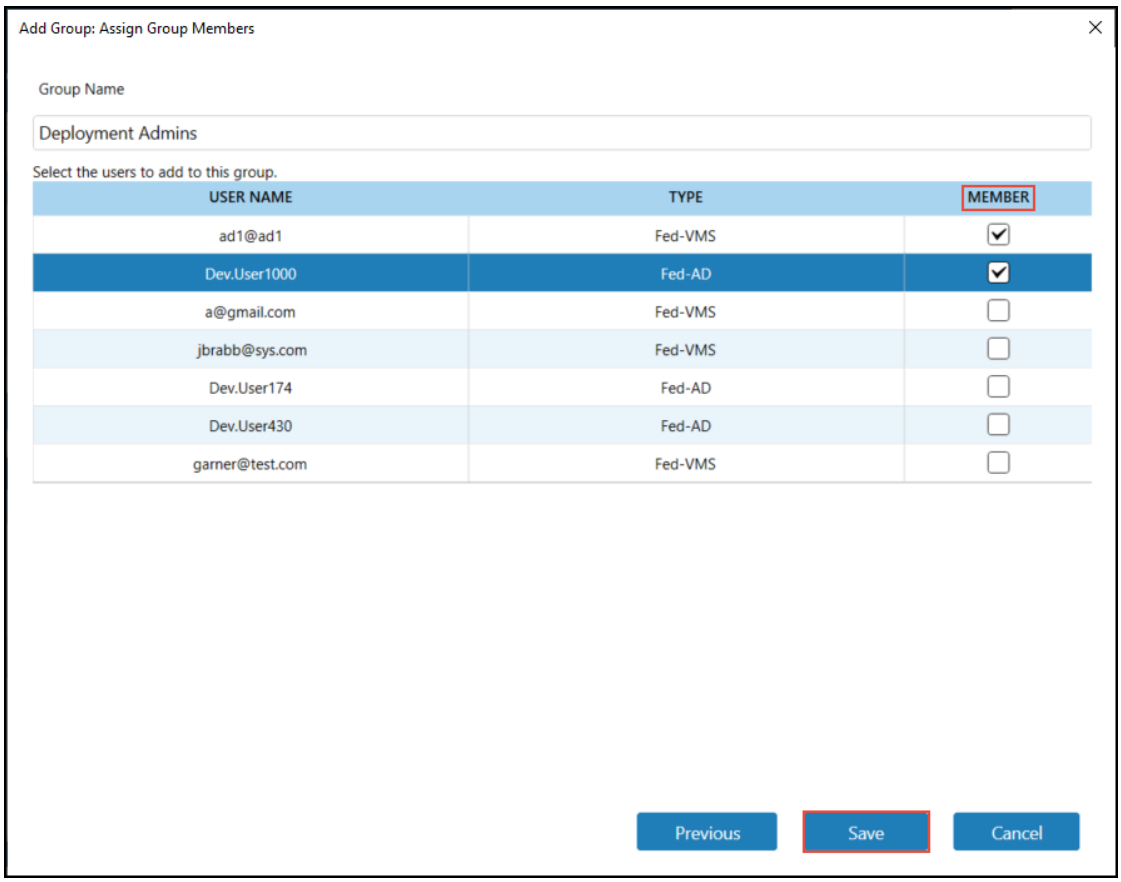


Create a Federated VMS Group



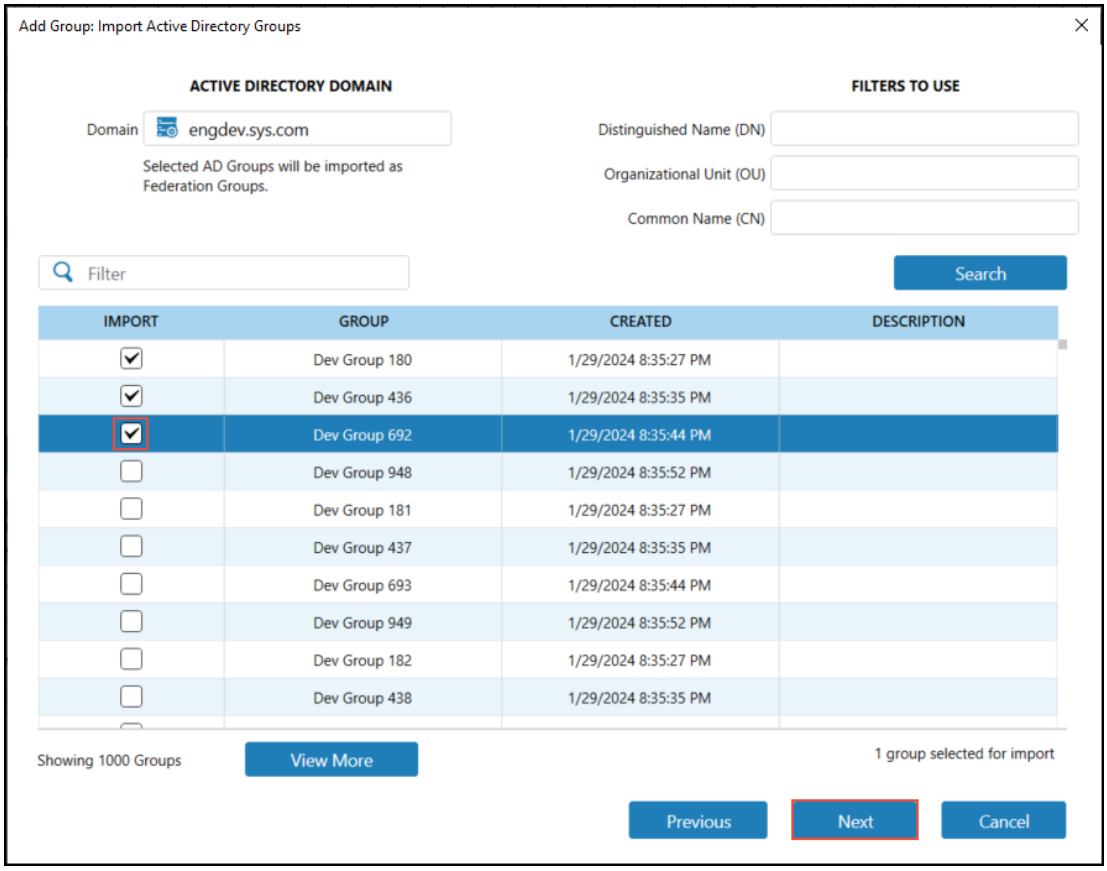
After selecting Add VMS Group, the Add Groups: Create New VMS Group screen will be displayed. This dialog allows you to enter the group name as well as an optional description of the group.

Additionally, this allows selection of the site(s) the group should have access to. Select Next to proceed to adding Federated Users to the Group.



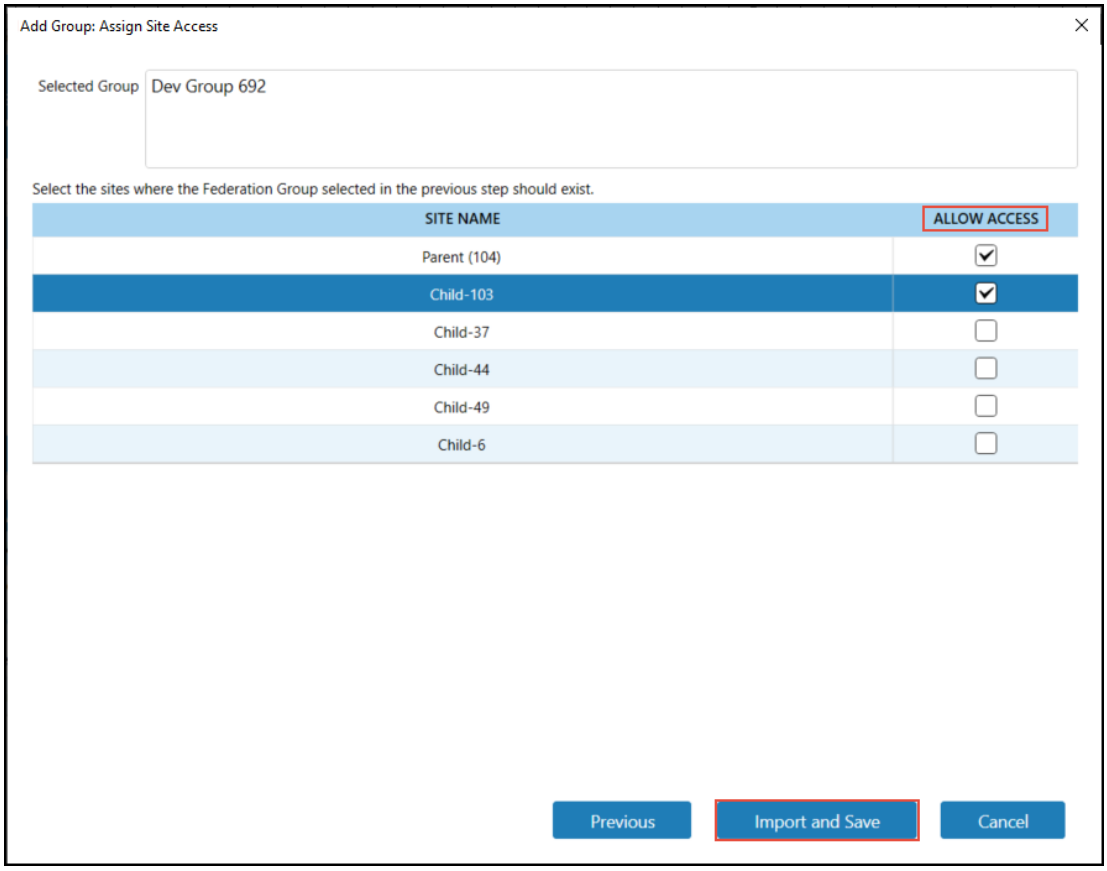
The Add Group: Assign Group Members screen will display all the Federation Users which have been created. Federation Groups support both Federation VMS and Federation AD user types to be assigned to a Federation VMS Group. Select users from the list to add them to the group. Pressing the save button will save the settings and will push changes to the sites where the groups have been provided with access.

Add a Federated Active Directory Group



The process to add an Active Directory group to the Federation is similar to adding an Active Directory user. From the Add Group: Select Group Type screen, select the Add Active Directory Group button. This opens the Add Group: Import Active Directory Groups screen.

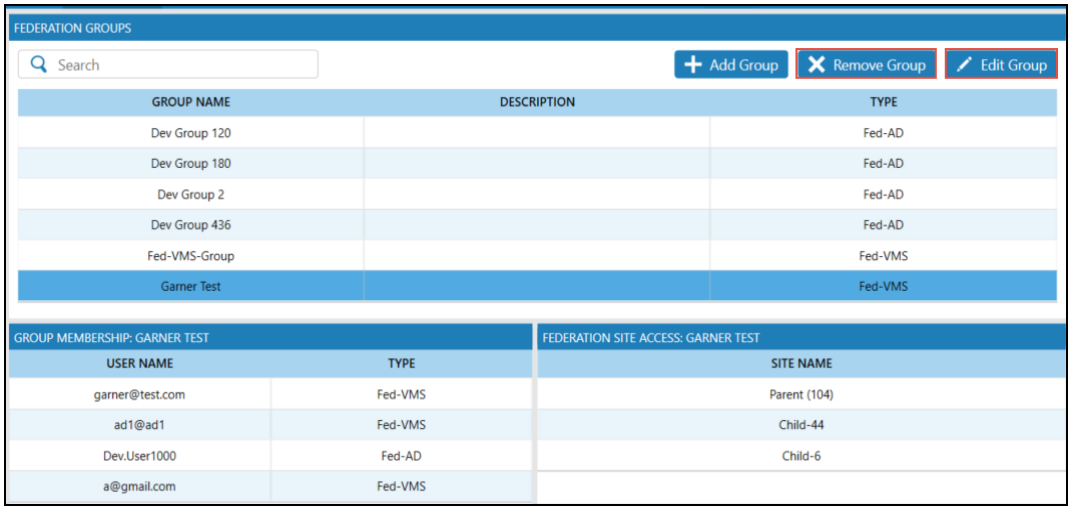
This screen will have the Active Directory domain pre-populated with the domain configured for the Parent Management Server's Active Directory settings. Optional filters are provided to refine the parameters of the search criteria prior to submitting the search. Leaving these filters blank will return all groups from the domain. The screen provides a filter field which can be used to find specific groups in the results. The search will display the first 1000 groups returned from Active Directory. If the domain contains more than 1000 groups, the View More button will retrieve more groups from the domain. Select one or more groups to import from Active Directory into CompleteView. Click Next when complete.



When granting access to sites in the Add Group: Assign Site Access step, it is important to note that if more than one group is selected, the access will be granted to all selected groups . It is advisable to only select groups which will need access to the same sites if selecting multiple AD groups to import. Unlike Federation VMS Groups, there is no ability to select individual users to import. All members of the AD group as configured in AD will be imported. Further, there is no ability to associate a Federation VMS User with a Federation AD Group.

Select the sites to grant access to and select Import and Save. When the Import and Save button is pressed, the AD group will be imported into the Federation and the sites which were selected for access will be updated with the Active Directory group(s).

Editing Federation Groups



After a Federation Group has been added, there is the ability to edit or remove the group. This can only be performed one group at a time. Select the Federation Group to edit or remove and press the desired button. By selecting the edit button, the ability to select the sites the group has access to can be modified for either VMS or AD Federation Groups. Additionally, for Federation VMS Groups the Group name and group members can be modified.

When selecting the delete button, the Federation Group will be deleted, removing that Federation Group from all sites it was given access to. However, that action does not remove or delete Federation Users from the Federation User section. Further, if a Federation User is a member of more than one Federation Group which has been given access to a site, the Federation User will still retain access to the site until the last Federation Group they are a member of on that site is removed.

Site Management Servers are updated at the end of the process of creating and saving a Federation Group. When Federation User and Groups are added, modified, or deleted, the Parent Management Server will send this information to the Child sites. This is an automated process that is started when the Save button is pressed in the dialog screen. In the event a child site is unavailable, the changes will be placed in a queue and will be automatically pushed to the site when it is accessible.

Federation Site Switching

Federated Users have the ability to switch between Sites and perform normal CompleteView tasks for which they have permissions, such as administration, viewing cameras, playback, etc., all from a single log in.

Site Switching Prerequisites

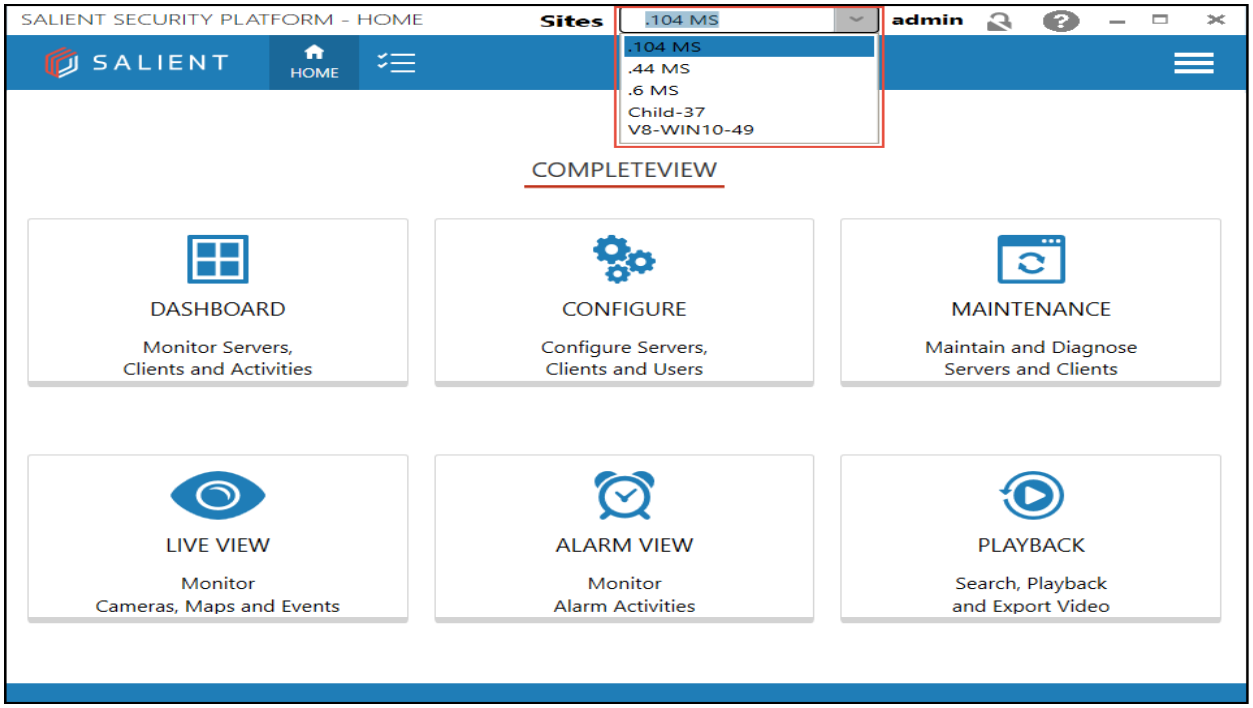
For site switching to function, the following prerequisites must be met:

1. Federation is enabled and working on all servers in the Deployment to which access is desired.
2. Either the user's credentials are a member of a Federated User Group (as described above) OR the credentials used to log in to the Desktop Client **exist and are maintained on all Child servers to which access is desired.***

The user's permissions must be set per Site and may be different for each one. For example, the user may have complete administrative permissions on Site 1, allowed only access to the Live View and Playback modules on Site 2, and Dashboard only on Site 3. See **Users & Groups Configuration** for more information.

*Active Directory may also be used, but each Site must resolve to the same AD instance. That is, each Site must use the same Active Directory user configuration. See above and/or the Federation Solution Guide for more information.

Switching Sites

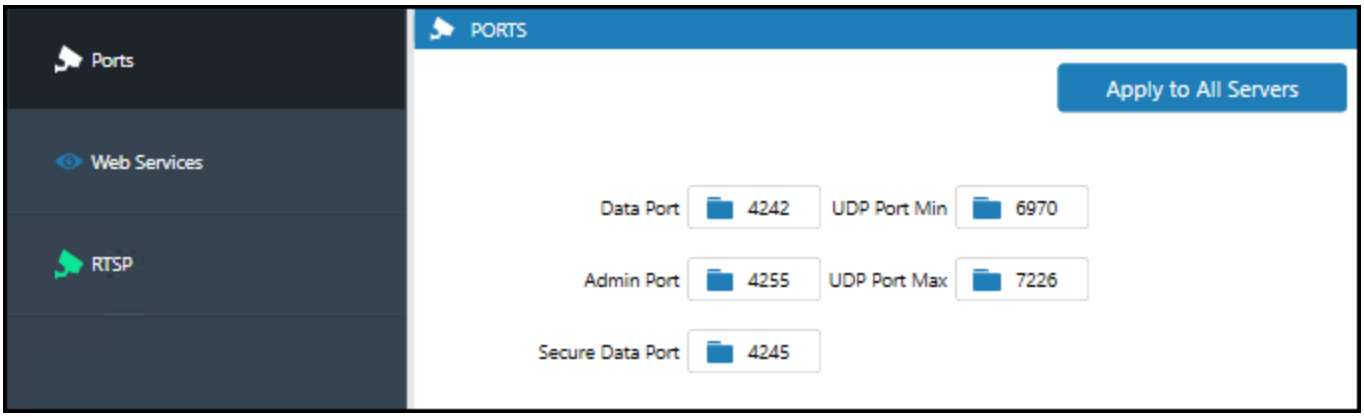


After logging in to the Desktop Client, click the dropdown menu, and select the desired Site. Presuming the user has proper module and site permissions, the Desktop Client will switch to the new Site and display the same CompleteView module the user was previously viewing. If site permissions have not been granted, an error message will be displayed.

Common Settings Ports

Ports include the TCP/UDP ports for both CompleteView and the unsecured/secured Web Server. The Administrator/Installer may globally apply the port numbers entered in the Port Panel to all recording servers that are also members of the Client.

Ports



Ports Table - Port Number Defaults and Purpose

Name	Default Port	Purpose
Data Port	4242	Used by the clients to communicate with the recording server through TCP protocol
Admin Port	4255	Used by clients to communicate with admin service
Secure Data Port	4245	Used for secure communication between Recording Server and client
UDP Port Minimum	6970	Minimum and Maximum UDP port range employed to connect to a UDP camera
UDP Port Maximum	7226	See note regarding UDP above

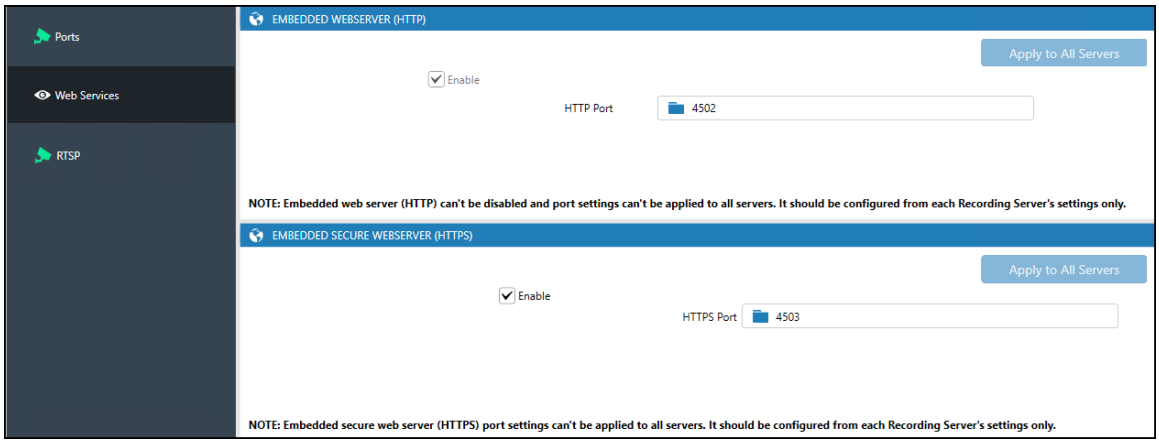
Ports Web Services

Web Services enables the HTML Web Client and/or TouchView to remotely view live and recorded video from multiple servers. After version 5.5, the Web Client is compatible with the following browsers on the listed operating systems:

- Firefox 68
- Chrome 81
- Edge 81
- Windows 10+
- MacOS 10.11+

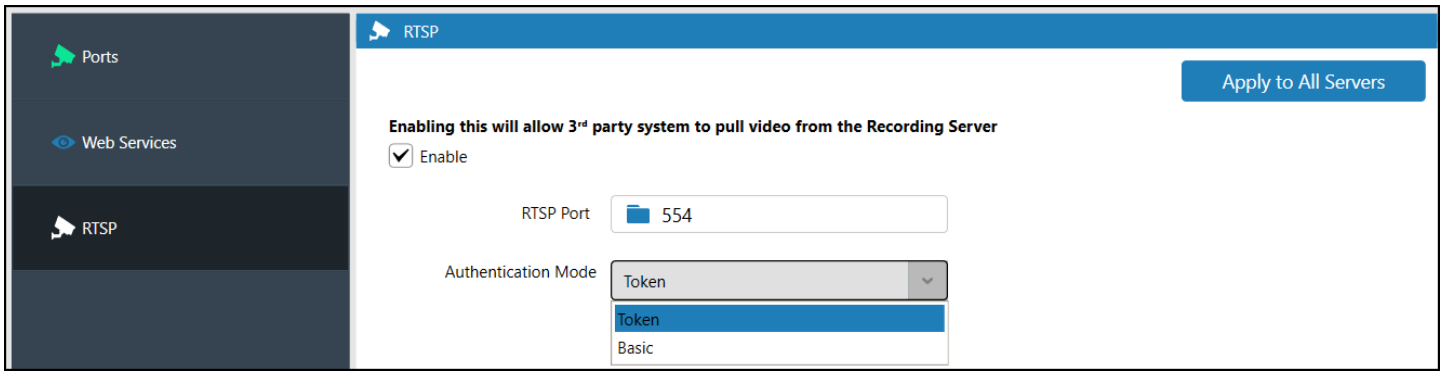
The permitted TCP port ranges for Web Services is 4502-4535, inclusive. By default, Web Services is enabled for both HTTP (non-security HTML video streaming) and HTTPS (Secure HTML video streaming).

HTTPS requires a Security Certificate to be correctly signed by a signing authority to be secure.



Ports RTSP

CompleteView's RTSP server allows for streaming video and audio data from Recording Servers to 3rd party clients, analytics engines, media players, etc. The server may be either enabled in Common Settings and applied to all Recording Servers, or per individual Recording Server.



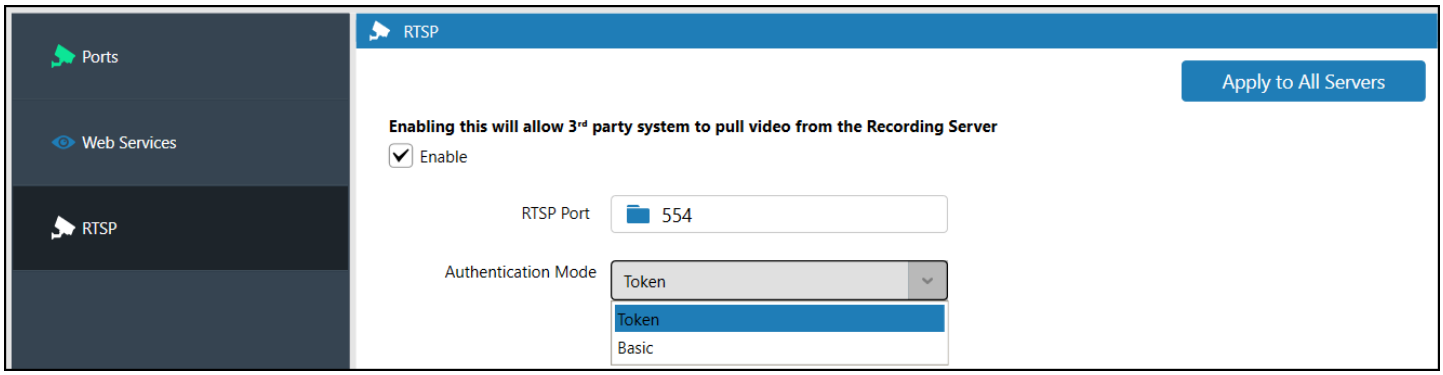
RTSP Server and client information is detailed in its own documentation and available through the Salient support website.

RTSP Server

The CompleteView integrated RTSP Server is intended to allow analytics engines, 3rd party video clients, media players, etc., to access a Recording Server's video streams via RTSP. It's intended that connectivity will largely be achieved programmatically, with each organization implementing its own scripts and applications to suit its environment as the required parameters, strings, and tokens can be quite lengthy to deal with manually.

RTSP Configuration

The RTSP Server may be enabled either in Common Settings and applied to all Recording Servers, or per individual Recording Server. If configured within Common Settings and applied to all servers, all will use the same port unless manually changed.



RTSP Authentication

Clients must authenticate with CompleteView before video data may be delivered. CompleteView supports both token and basic authentication. Token authentication requires the client to request a token from the deployment's Management Server and provide it in the request to stream video, whereas basic authentication requires the client to send valid VMS credentials with camera permissions to access the requested stream. Select the Authentication Mode from the drop down menu in either the Management Server under Common Settings, Ports, RTSP, or via an individual Recording Server's Ports, RTSP pane.

Token Authentication

The authentication token must be acquired from the deployment's Management Server via CompleteView's REST API. The token must be included in all new RTSP requests using token authentication. REST clients must utilize the OAuth 2.0 authorization protocol to communicate with CompleteView. The REST client requests an authentication token from the Management Server, which is then copied and pasted into the RTSP request string. The tokens do expire, but if video is being actively viewed, the connection will not be broken upon expiration, and a new token will not be needed until a new connection is attempted. Note that the VMS credentials must have camera permissions to access the desired streams.

REST API Token Request

Use the following parameters to request an authentication token from the deployment's Management Server.

POST /connect/token

Grant Type: Password Credentials
Access Token URL: https://managementserverIP:8096/connect/token
Username: (e.g. admin)
Password:
Client ID: (see below)
Client Secret: secret
Scope: management-server.configClient
Authentication: Send as Basic Auth header

The Client ID may be any one of the following:

ClientId = "client.desktop"
ClientId = "client.video-wall-agent"
ClientId = "client.android"
ClientId = "client.ios"
ClientId = "client.web"

Example

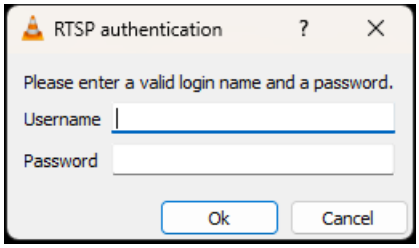
Once the token is returned from the Management Server, include it in the RTSP request to the desired Recording Server. The following example illustrates a new RTSP request including access to camera 1 (a multistream camera), stream 1, in H.265 at 10 frames per second, with an overlay, and includes the (truncated) access token. See below for a full list of available parameters and request format information.

rtsp://recordingserverIP:554/live/1?streamId=1&codec=h265&fps=10&overlay&access_token=eyJhbGciOiJSUzI1NiIsImtp...

Basic Authentication

CompleteView accepts VMS credentials for RTSP requests. The VMS user must have access to the camera in CompleteView in order to stream video. After making the RTSP request, a client should prompt the user for the CompleteView credentials.

Note: Active Directory users are not supported at this time.



RTSP Parameters

Utilize the following parameters to specify how CompleteView delivers the requested video. For clients using basic authentication, the access token parameter is not required.

Request Format

The request must begin with the protocol (rtsp) followed by the Recording Server's IP address and RTSP port (default 554), followed by "/live/" then, at a minimum, the camera ID (discussed below). Optional parameters must be preceded by a "?", but subsequently separated by a "&", but do not need to be in any particular order. The example below is requesting live feed from camera 1 as an 800x600 MPEG4 stream.

rtsp://recordingserverIP:554/live/1?codec=mpeg4&height=600&width=800

Parameters

cameraid	Denotes the numeric value CompleteView has assigned to a given camera, is a required parameter, and must come after the /live/ entry in the request. Instead of the value assigned by CompleteView, cameraid may also be satisfied by using a camera's GUID. rtsp://recordingserverIP:554/live/**1** or rtsp://recordingserverIP:554/live/**692c68cc-ea6a-4640-bfd1-6d410e89a3fd**
streamid	For multistream cameras, specifies which stream to use. If left unspecified, CompleteView will send the "Primary" stream as assigned by an administrator. rtsp://recordingserverIP:554/live/1?**streamId=0**
fps	Specifies the desired frame rate of the live stream (1-30). The framerate cannot exceed the original rate coming from the camera. rtsp://recordingserverIP:554/live/1?**fps=5**
codec	The Recording Server can transcode the original stream coming from the camera. RTSP Server currently supports transcoding to MPEG4, H.264, and H.265 streaming (mpeg4, h264, and h265). rtsp://recordingserverIP:554/live/1?**codec=h265**
height & width	Specifies the dimensions in pixels of the video stream to be sent to the client. The RTSP Server cannot upsize the resolution from the original stream. rtsp://recordingserverIP:554/live/1?**height=600&width=800**
overlay	Toggles the overlay containing framerate, codec, etc., on or off. If not included, the default is no overlay. rtsp://<serverIpAddress>:554/live/1?**overlay**
access_token	The authentication token requested from the Management Server. All new stream requests must inlcude the access token. See RTSP Authentication section above for more details. rtsp://172.18.1.109/live/1?**access_token=eyJhbGciOiJSUzI1NiIsImtp...**

Common Settings Services

Services include Active Directory and Email Server configuration settings. Services configuration is only available through Common Settings and not per Recording Server.

Services Active Directory

Active Directory (AD) allows the Administrator to import users and groups to the Client from Active Directory, establish camera user and viewing permissions, and provide a quick, efficient, and secure login validation process to the Client's users and groups.

Active Directory groups that are imported to CompleteView are stored in the Management Server database. AD users can be provided CV permissions via group association. The Management Server uses an authentication token to track a logged in user. When the token expires, the Management Server will attempt to re-authenticate the user by calling AD (to either find the user directly or find by group association). This re-authentication process is invisible to the user. However, if the user was removed from AD (or the group the user is associated to) the user will encounter errors.

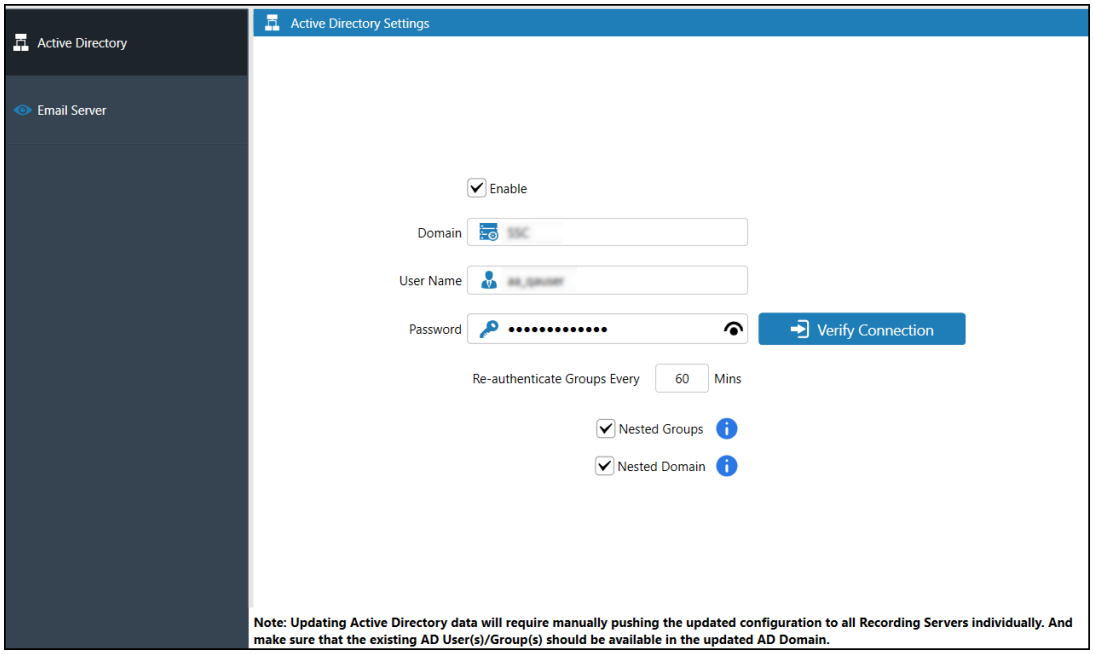
The Recording Server will authorize access of resources (such as cameras) with each access. If the user's permissions are based on AD group association, the Recording Server will use the "Re-authenticate Groups" value. The Recording Server will use this value to cache the authorization of the AD user based on the group association. This reduces the communication from the Recording Server to the Active Directory.

The Re-authenticate Groups entry is shown in minutes, with a default of 60. The time may be shortened or lengthened as necessary.

Nested Resources - Groups & Domain

Users can belong to a AD group directly or to a group under a group. If your AD structure is such that users who require access to CompleteView exist under multi-level groups, Nested Groups should be enabled.

With the use of Nested Domain, members of child domains associated with the root domain can be authenticated through Universal Groups. During the login process, the CompleteView attempts to authenticate the user from within the root domain. If that fails, CV works its way through the child domains to find the user. If found, the user is authenticated. In larger organizations where the user may be far down the child domain structure, some authentication performance slowdown may be experienced consequent to the search.



Benefits of Active Directory

- Active Directory user login Authentication is managed by the IT organization
- Time savings by importing users and groups that already exist in Active Directory, rather than manually adding individuals or groups to the Client.
- Group creation and changes are all managed by the IT organization and imported into the Client.
- Windows Single Sign-on for the users; no need for separate CompleteView login names and passwords.

Automated User Name and Password Change Avoidance

The username and password should be a Service Account so that the Active Directory Domain Controller username and password remain the same when a regularly scheduled password change is required by Active Directory. If this is not adhered to, CompleteView will disconnect from Active Directory when the scheduled username or password change occurs.

For more information about Active Directory, see Active Directory Connector.

Services Email Server

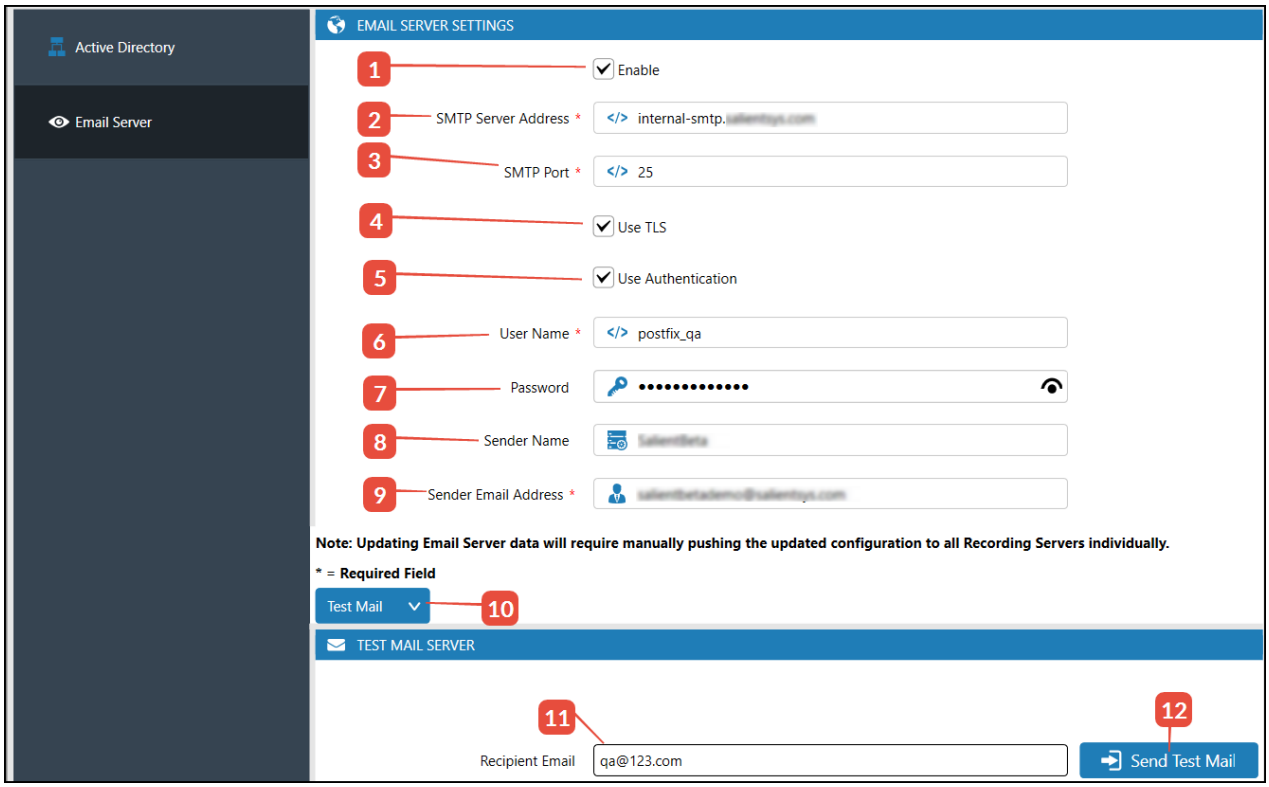
Email notification may be set up to enable email and SMS notification of the following:

1. Alarms
2. Camera sync loss
3. Camera sync gained
4. Camera motion sensed
5. Recording failures
6. Recording Server offline

For email notification to function correctly, there must be an established Simple Mail Transport Protocol (SMTP) account that is dedicated to both the Client and email notification. Email notification is a

Common Setting that may be applied to all Recording Servers listed in the Client at the time email settings are entered.

Email Notification Setup

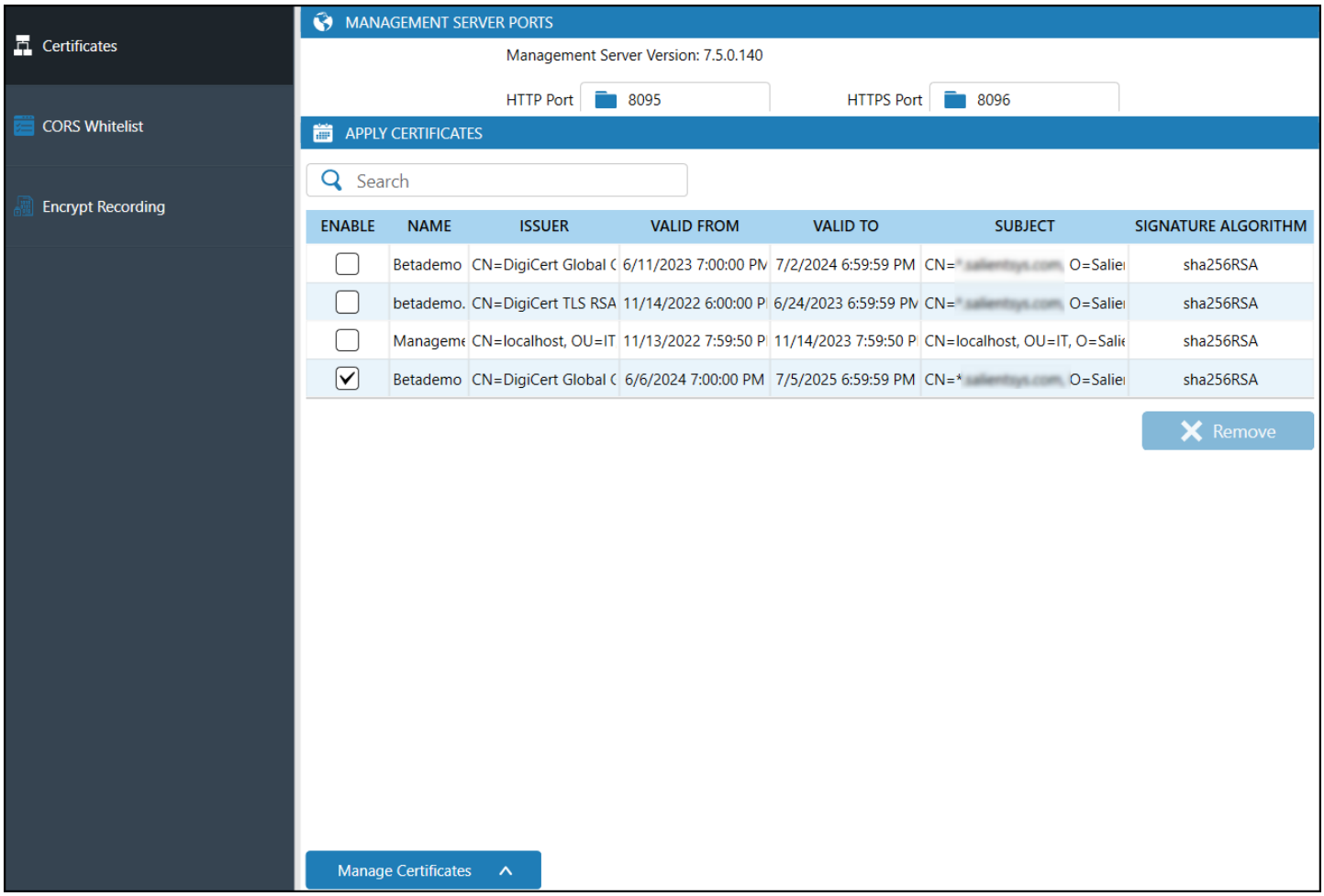


Steps:

1. Check the Enable check box
2. Enter the SMTP mail server domain information
3. Enter the port that is required by the employed SMTP account
4. Select TLS if it is required by the SMTP account
5. Select Authenticate if a username and password are required to use the SMTP service
6. Enter the SMTP user account name that was set up for email notification
7. Enter the SMTP password that was set up for email notification
8. Enter the Sender name
9. Enter the Sender's email address; it may be the same as the username
10. Optioinally, select Test Mail
11. Enter a test email address
12. Click Send Test Mail
13. Save the configuration

Common Settings Security

Security protocols may be implemented system-wide from the Common Settings Security screen, or per individual Recording Server. Recording Servers share similar settings with those located in Common Settings, but some features are limited to the Management Server. Settings changed at the Common Settings level may be applied to all Recording Servers in the deployment, while Settings changed at the Recording Server level impact only that specific Recording Server.



Certificates Overview

CompleteView contains facilities for secure web-based communications via HTTPS. To be used properly these security facilities require local, per site management of digital certificates. This section of the manual deals with the practicalities of creating and configuring both self-signed certificates and certificates from a certificate authority. For more information, see Digital Certificate Management and More.

A digital certificate must be enabled on each Recording Server that will employ secure (HTTPS) web-based video streaming, and for the Management Server in the Security tab.

In addition to security certificate creation and addition, the CompleteView Management Server maintains a configurable list of approved host addresses with witch various clients and Recording Servers may communicate, referred to as a Cross-Origin Resource Sharing (CORS) Whitelist.

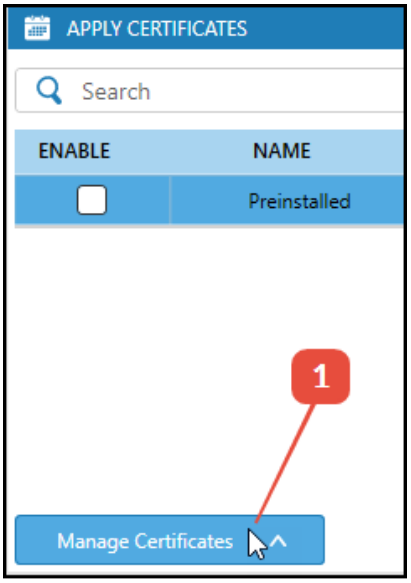
Create Self Signed Certificate

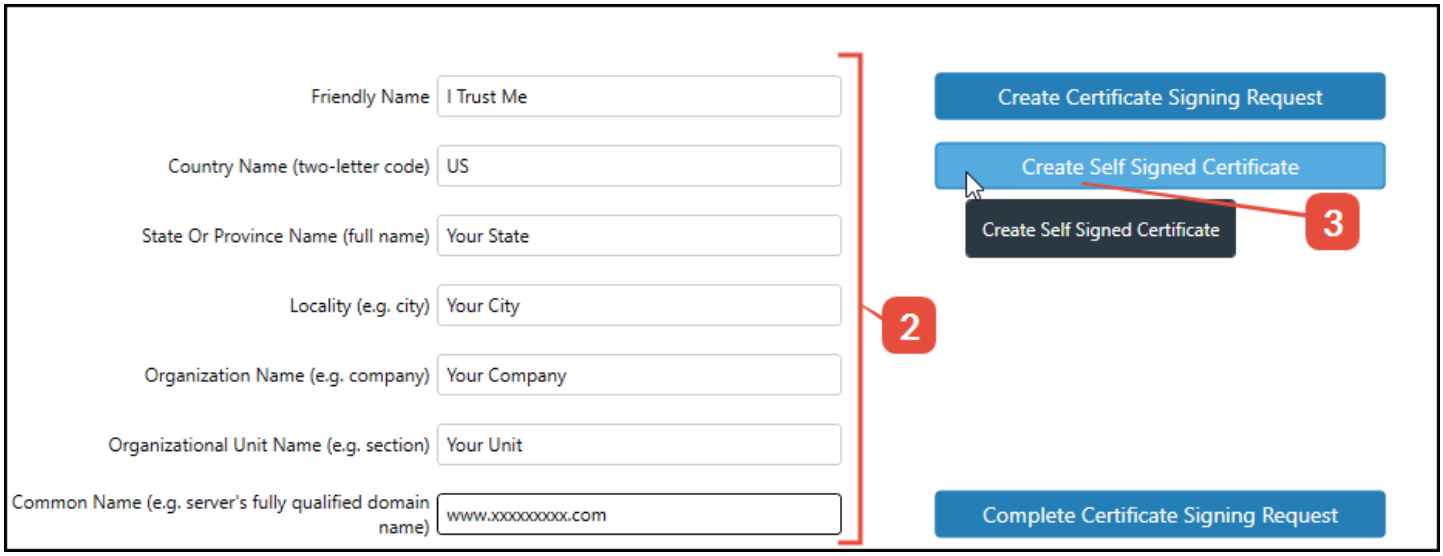
CompleteView comes with a pre-installed certificate, which has a number of limitations that should preclude its use in a production environment. First, it is formally associated with the CompleteView Recording Server, and not the site-specific server on which it resides and for which it is to serve as credentials. Second, it is self-signed as opposed to coming from a certificate authority.

CompleteView supports the quick creation of a certificate that suffers only from the second of these limitations.

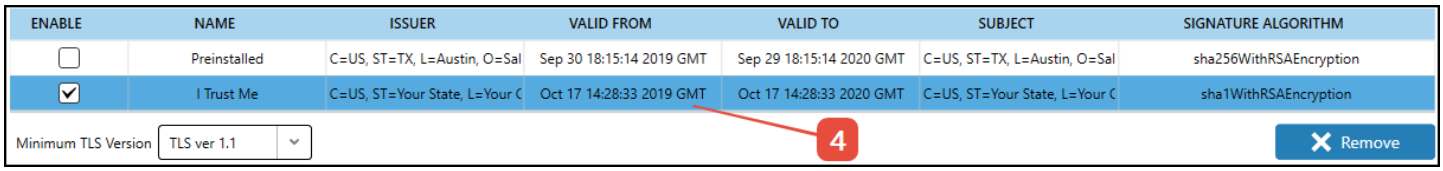
While logged into the Desktop Client, select the Configure module. Either select Common Settings or the desired Recording Server, select Security, then click the Manage Certificates button near the bottom of the window. It is recommended that you fill in all fields with reasonable values, except possibly the organizational unit name (which is commonly omitted in certificates). For the common name (the last field), it is important that you use the name by which the server will be accessed over the web. Enter a friendly name for the certificate. This value is used merely to distinguish among the certificates managed by CompleteView. Any string is legal, though it is recommended to avoid the empty string and to generally keep the friendly names distinct and recognizable. Click Create Self Signed Certificate when done, and Save the server configuration.

1. At the bottom of the Apply Certificates window, click on Manage Certificates.
2. Enter the proper information in the fields.
3. Click the button labeled Create Self Signed Certificate.



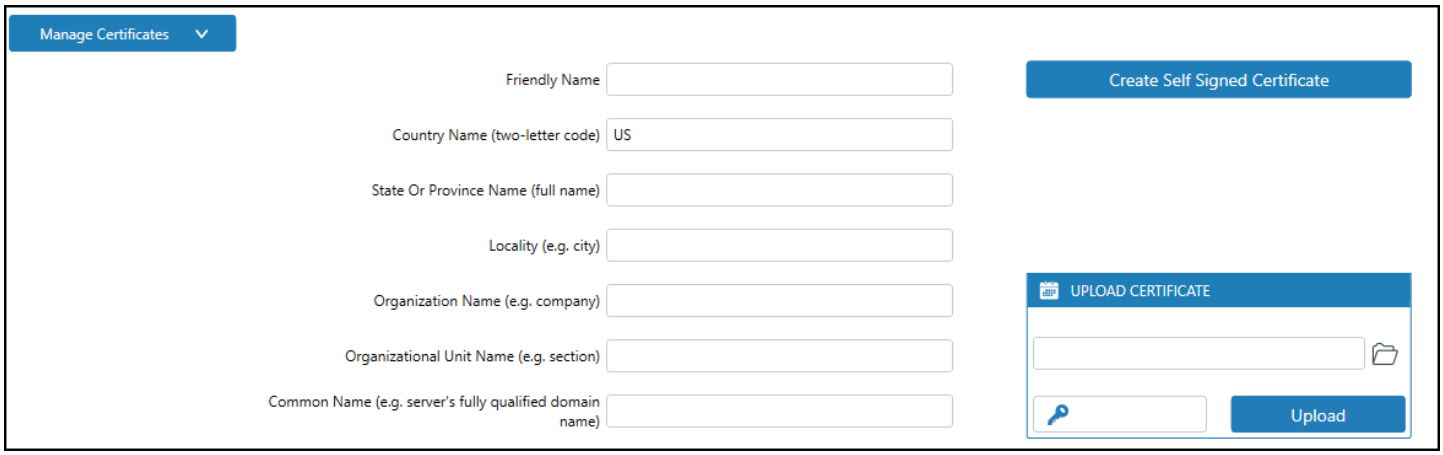


4. Your Self-Signed Certificate will be visible in the certificate list.
5. Save the Configuration.

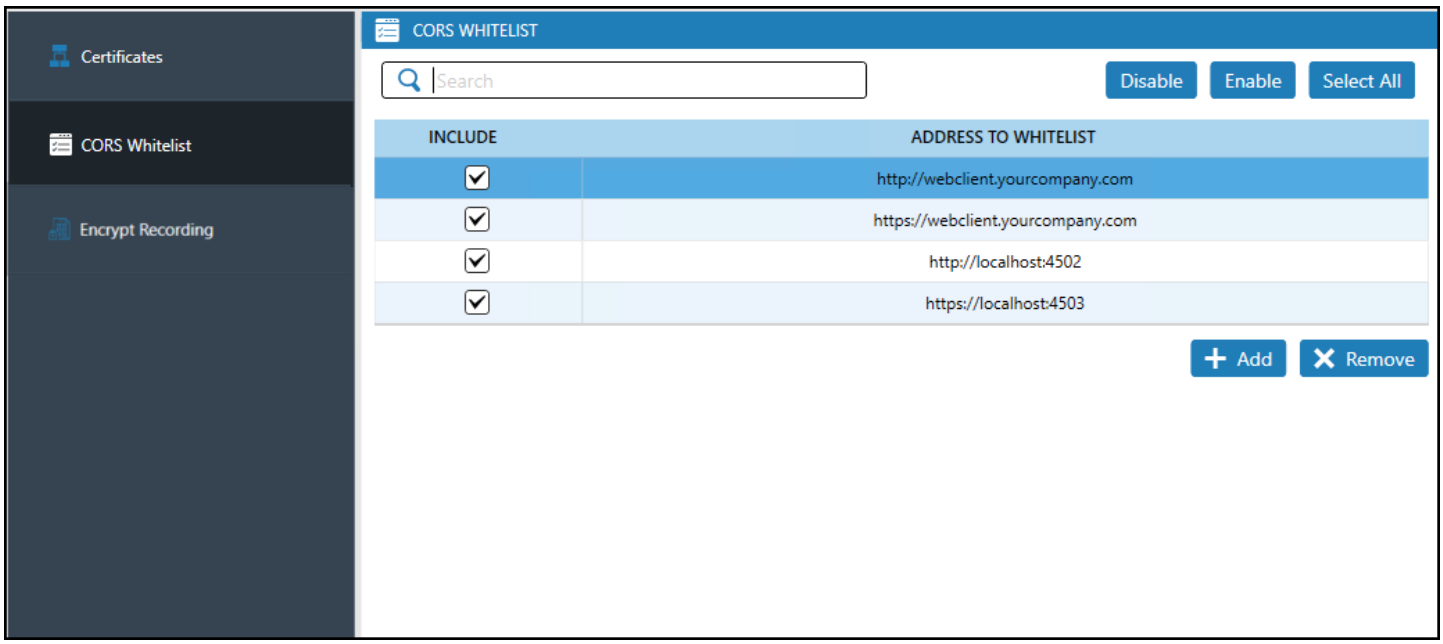


Applying Signed Certificates from a Certificate Authority

Note that Signing Requests may only be generated from within CompleteView for individual Recording Servers, and not via Common Settings. It is beyond the scope of this document to detail the process of creation of a signing request, as it varies from organization to organization. Once a signed certificate has been received from an authority, click Upload in the Upload Certificate pane, select and open the file. Save the configuration.



CORS Whitelist



CompleteView Management Server maintains a configurable list of approved host addresses with which the Web Client, mobile application, and Recording Servers may communicate, referred to as a

CORS Whitelist. For example, if the Web Client must first communicate with a web hosting site to access the video from a deployment's Recording Servers, that web hosting site must be added to the whitelist.

Administrators have the ability to add, remove, or update addresses to or from this list. Each entry should be in the following format:

- http://{address}[:port]
- https://{address}[:port]

Addresses may be either IPv4 or IPv6, or a hostname may be used. When a new Recording Server is added with "Auto Provision" enabled, the whitelist from the Management Server is automatically applied. When "Apply to All Servers" is selected, the Management Server applies the whitelist to all Recording Servers.

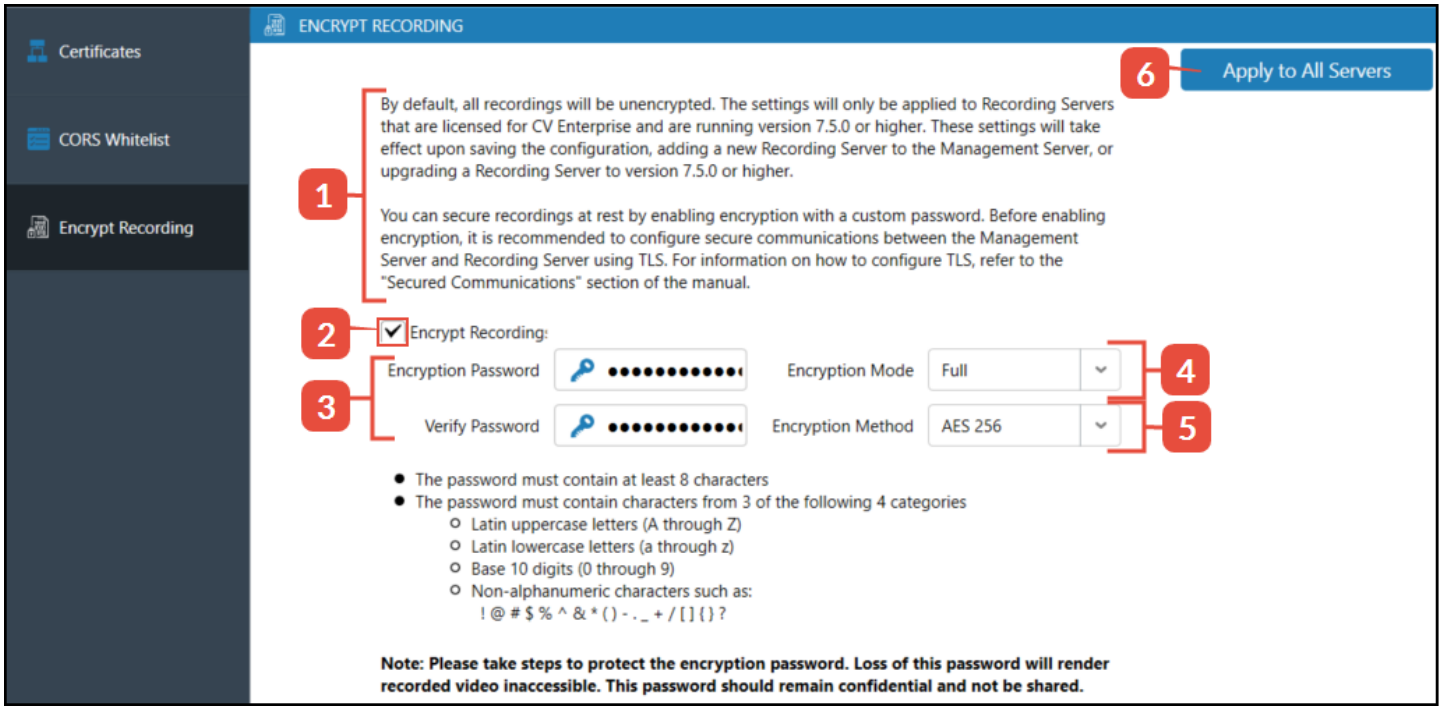
Encrypt Recording Overview

CompleteView allows for the encryption of video and audio data that is being written to disk, also known as encryption at rest. Encryption is applied to all storage types (Regular, Backup, Archive, etc.) for either Volumes or Storage Pools, and may be implemented deployment-wide or per Recording Server. See **Recording Server Storage EncryptionRecording Server Storage Encryption** for more information. Enabling encryption does not affect failover operation. It is strongly recommended enabling TLS communications between Recording and Management servers for optimal security. See **Secured Communication** for more information. After enabling encryption from Common Settings, all newly added Recording Servers will be encrypted. By default, recording encryption is not enabled. Encryption may be enabled and disabled over time, and both encrypted and non-encrypted video will still be accessible.

Note: Encrypted Recording Servers may be moved within a single Management Server without losing access to encrypted video, but cannot be moved between Management Servers. Reach out to support if a Recording Server needs to be moved to a new Management Server.

Enabling Encrypt Recording

Use the following steps to enable deployment-wide encryption at rest. Note that enabling encryption applies only to newly written video and audio data, and cannot be applied to existing data.



To enable Encrypt Recording:

1. Read the disclaimer in the UI
2. Select Encrypt Recording
3. Enter the Encryption Password then Verify the password

   Take steps to protect the encryption password. If the password is lost, the encrypted data will no longer be accessible. The password may be changed at any time.

4. Select the Encryption Mode

   Either Full or Lite encryption modes are available. Full mode encrypts both I and P video frames, where Lite mode encrypts only the I frames. Full encryption is recommended and is the default selection.

5. Select Encryption Method

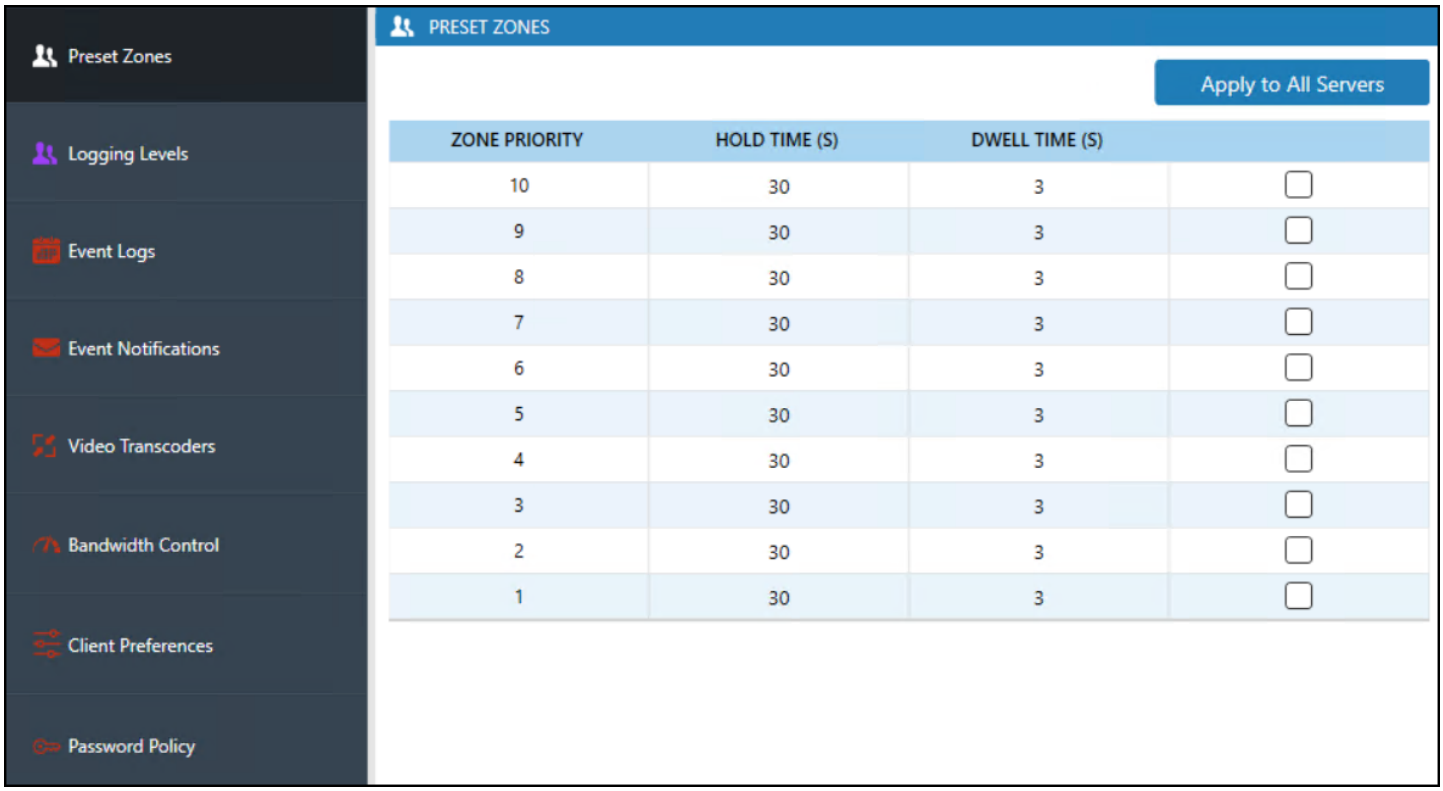
   Either AES 128 or 256 bit encryption is available. AES 256 is the more secure option, and is the default selection.

6. Select Apply to All Servers

Common Settings Operations

Using Operations from Common Settings in the Client, an Administrator may establish Operations for all Recording Servers. Operations may also be applied to individual servers. Operations include Preset Zones, Logging Levels, Event Logs, Event Notifications, Video Transcoders, and Bandwidth Control configuration.

Preset Zones



Operations permit the Administrator to define and configure PTZ preset zone priorities along with their hold and dwell times for all Recording Servers. Preset Zones are actionable PTZ preset virtual video areas within a video scene. Preset Zones are configured to send a PTZ camera to a specific preset position when motion is sensed by another camera.

The Preset Zone illustration below shows a truck moving through the fixed camera motion area; the fixed camera detects the motion, which triggers CV to send a designated PTZ camera to the Preset Zone position and hold in that Preset Zone for a predetermined period. Motion from any object can trigger Preset Zone activation. The settings to configure this are located in Common Settings/Operations.

1. Fixed coordinating camera
2. Motion Detection Area-red rectangle
3. Preset Zone-blue oval
4. PTZ Camera

Preset Zone Settings

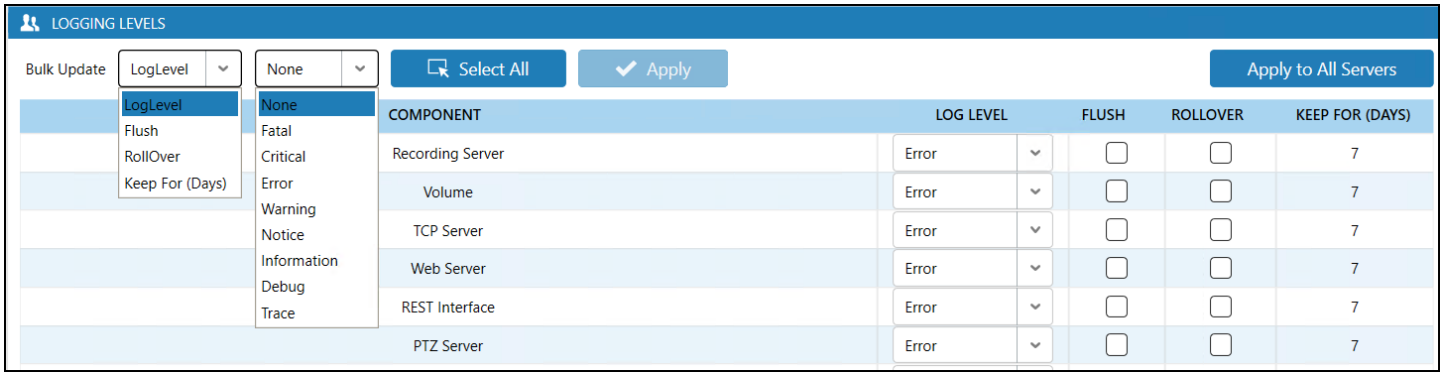
1. **Zone Priority** sets a zone's priority relative to other presets. There are ten (10) distinct priority levels. Ten is the highest priority, and one is the lowest priority
2. **Hold Time** defines the total number of seconds that the PTZ camera is to remain at a Preset Zone
3. **Dwell Time** is the time that one PTZ camera stays in a Preset Zone when the PTZ camera is working with two or more coordinating cameras that have the same priority level.
4. **Cycle** is used to cycle the same PTZ camera between two or more Preset Zones that have the same Zone Priority number.

Two or More Coordinating Cameras

It is possible to assign one PTZ camera to service two or more coordinating cameras. Zone Priority determines which coordinating camera has the higher priority and receives the first response from the PTZ camera.

Logging Levels

Event Logs define default logging levels of all subsystems of Recording Servers as well as log file duration. This information can be used to troubleshoot system issues.



Log Levels

None	Fatal	Critical
Error	Warning	Notice
Information	Debug	Trace

Event Logs

Administrators can select and configure all event types to be logged by the Recording Server. Event Logs provide time and date of an event, how often the event occurred and, in some instances, the person using the system at the time of the event. Event Logs can help the service technician discover and possibly isolate events by looking for correlations between events and hardware operation or system use.

Events with selected checkboxes will be logged for all Recording Servers and kept in the Management Server's database. Exceptions for all Recording Server settings may be established for individual Recording Servers by configuring the exception at the Recording Server's Settings/Event Logs Panel.

Logged Events

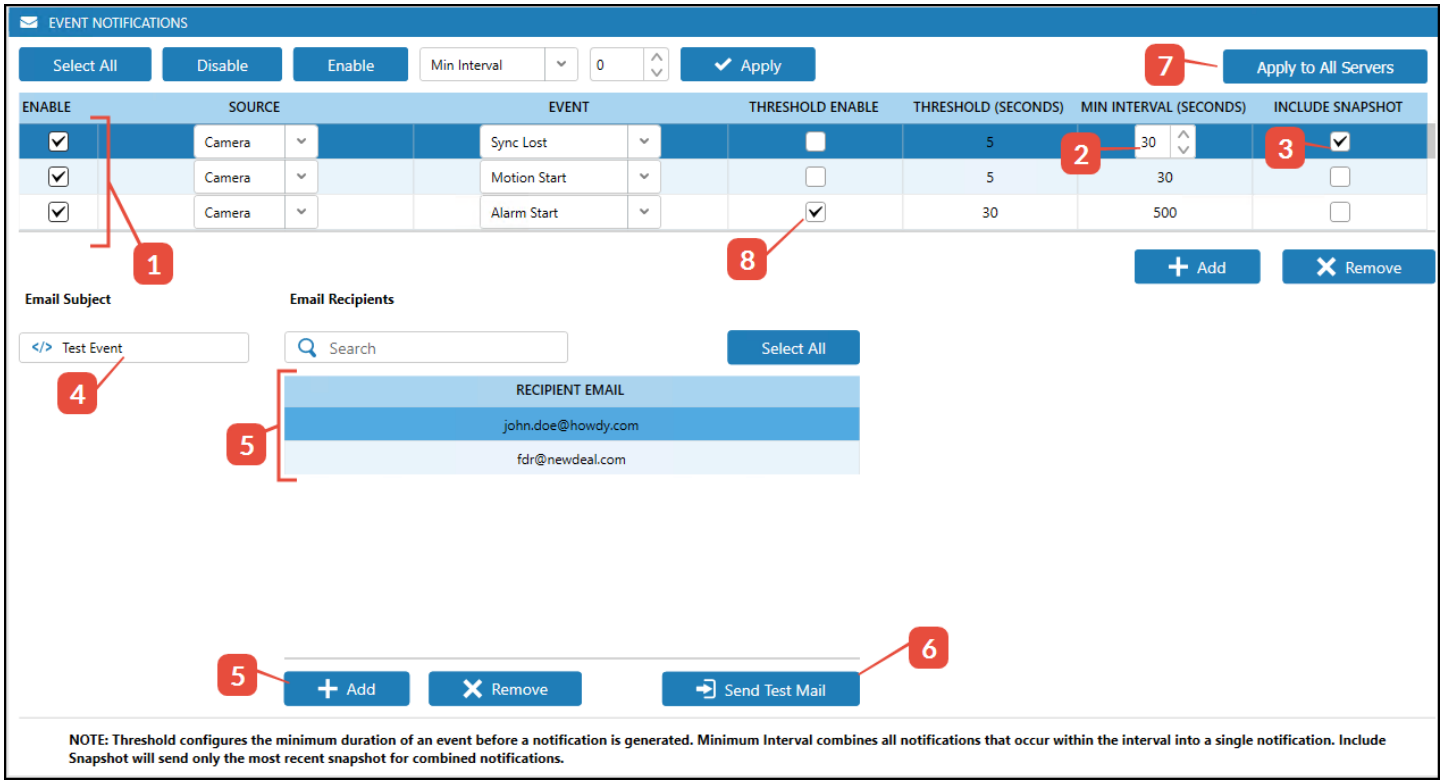
Alarm End	Alarm Start	Debug (Logging)

DFT End	DFT Start	Error (Logging)
Export (Video)	Failed Login (user)	Info (Logging)
Input Activated	Input Deactivated	Login (user)
Logout (user)	Motion End (camera detect)	Motion Start (camera detect)
Output Activated	Output Deactivated	Recording Failed (volume)
Restart (server)	Save Configuration (server)	Set Time (server)
Start (server)	Start Live View	Playback
Stop	Sync Gained (camera)	Sync Lost (camera)
Delete Failed	Free Pool Space Failed	Insufficient Retention
Minimum Camera Retention Active	Minimum Retention Violation	Minimum Storage Violated
No Event	Overflow Drive Active	Overflow Drive Inactive
Pool Drive Offline	Pool Drive Online	Recording Started After Failed
RTSP Channel Created	RTSP Channel Destroyed	RTSP Live Connected
RTSP Live Disconnected	RTSP Playback Connected	RTSP Playback Disconnected
Start Playback	Storage Threshold Met	Storage Write Failed
Sync Gained	Sync Lost	TCP Connected
TCP Disconnected	Trigger Activated	Trigger Deactivated
Video Export	Volume Full	Volume Offline
Volume Online		

Event Notifications

Event Notification enables the Administrator to configure automated emails for events caused by Cameras, Storage Pools, Volumes, Servers, Alarms, and Users. The Email Server must be configured with an SMTP account in Services. Emails may be customized with a subject and recipient list, and a test email may be sent to ensure that the email account information is correct. A complete list of events with their sources and descriptions is enumerated below.

Event Notification Selection/Configuration



Steps:

1. Enable or disable events as desired
2. The Min Interval setting allows for consolidation of all notifications occuring within the configured time span into one email. If 10 Sync Lost events happen in 29 seconds and the interval is set to 30, only one email will be sent containing all 10 Sync Lost events.
3. Check the box if a snapshot should be included with the notification
4. Enter an email subject in the line provided
5. Enter one or more email recipients, selecting Add after each one (note that the list may be searched)
6. Send a test email, and make any corrections to the email setup if the email fails
7. If Event Notification is desired for all servers, select the Apply to All Servers button
8. Enable or disable Notification Threshold. See below.
9. Save the configuration (if complete)

Event Notifications

Source	Event	Description
Server	Start	Recording Server Service Start
	Stop	Recording Server Service Stop
	Restart	Recording Server Service Restarted
	Save Config	Recording Server Configuration Saved
	Set Time	Recording Server Time Set

Source	Event	Description
Camera	Alarm Start	Indicates start of an alarm recording due to a trigger, such as a camera event
	Alarm End	The end of alarm recording
	Motion Start	Indicates start of motion recording due to a trigger, such as a camera event or server-side motion detection
	Motion End	The end of motion recording
	Sync Lost	Camera Connection to Recording Server Lost
	Sync Gained	Camera Connection to Recording Server Regained
	Recording Failed	The Recording Server failed to write a video clip to the volume or pool
	DFT Start	Dynamic Frame Throttling engaged on Recording Server
	DFT End	Dynamic Frame Throttling deactivated on Recording Server
	Recording Started After Failed	The Recording Server resumed attempting to write to the volume or pool after a previous failure.
Volumes & Storage Pools	Recording Failed	Video Recording failed to write to the volume or pool
	Volume Online	Volume available for use
	Volume Offline	Volume not available for use
	Volume Full	Volume has reached capacity
	Minimum Storage Violated	Volume is nearly full
	Minimum Retention Violation	Pool minimum retention policy not met
	Insufficient Retention	Not enough pool space to meet current retention requirements
	Pool Drive Offline	A drive for a given storage pool has gone offline
	Free Pool Space Failed	Write error to storage pool
	Overflow Drive Active	Drive marked for overflow operation in a pool receiving data from full pool
	Overflow Drive Inactive	Enough pool space has been cleared to no longer need use of a designated overflow drive
	Storage Threshold Met	Allocated video space in a pool has been used up
	Storage Write Failed	Failed to write video data to a storage pool
	Pool Drive Online	Pool drive reported online after being offline
	Minimum Camera Retention Active	Deletion of video occurring while respecting minimum retention policies
Alarm	Alarm Start	Indicates start of an alarm recording due to an IO device trigger

Source	Event	Description
	Alarm End	The end of alarm recording
	Input Activated	The alarm device's input pin was triggered/activated
	Input Deactivated	The alarm device was deactivated
	Output Activated	The alarm device's output pin was triggered/activated
	Output Deactivated	The alarm device's output was deactivated
RTSP	RTSP Channel Created	External request for RTSP communication recieved and established
	RTSP Channel Destroyed	Communication with external request terminated
	RTSP Live Connected	RTSP live stream established
	RTSP Live Disconnected	RTSP live stream disconnected
	RTSP Playback Connected	RTSP playback established
	RTSP Playback Dis-connected	RTSP playback stream terminated
User	Login	A User has successfully logged in
	Logout	A User has successfully logged out
	Failed Login	A User has failed to log in
	Start Live View	A User has begun viewing live video
	Start Playback	A User has begun viewing recorded video
	Video Export	A User has exported recorded video - applicable only to an Export volume
	Output Activated	An IO device's output was activated by a user (software triggers)
	Output Deactivated	An IO device's output was deactivated (software triggers)

Notification Threshold

The Threshold Enable setting allows for a configurable minimum amount of time to elapse before a notification is sent for the selected event. For example, if an Alarm Start event is set with a 30 second Threshold but an Alarm End occurs after 29 seconds, no notification will be sent. The event will still be logged and searchable even if a notification is not sent. The results of the Threshold configuration can be combined with the Min Interval setting. In the example above, all Alarm Start events longer than 30 seconds that transpire over the following 500 seconds will be bundled into 1 email notification. Currently, Notification Threshold is available per event type and per camera. For example, in a 50 camera deployment with Alarm Starts, CompleteView would generate 50 emails for each 500 second interval as configured above. By default, this feature is turned off.

Notification Threshold is applicable to the following events:

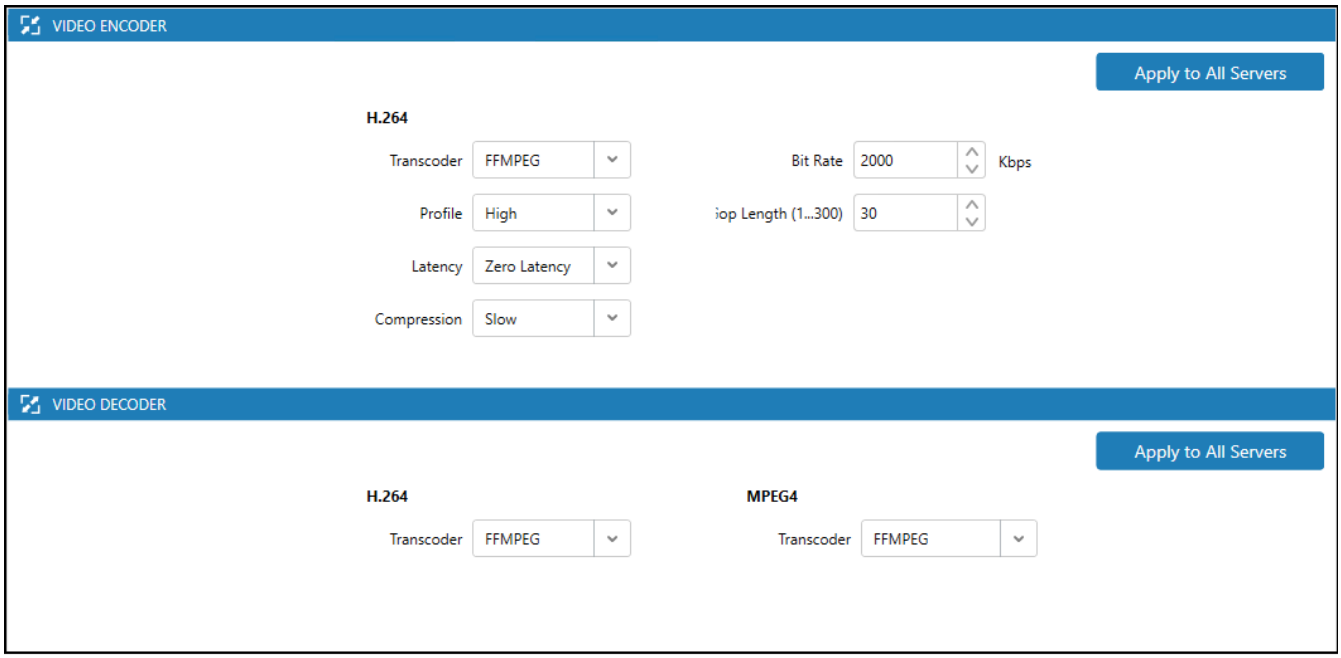
- Sync Loss (reset by Sync Gain)
- Sync Gain (reset by Sync Loss)
- Motion Start (reset by Motion End)

- Alarm Start (reset by Alarm End)
- Recording Failed (reset by Recording Started after Failed)

Discontinue an Event Notification

1. Uncheck the event that is to be discontinued
2. Save the configuration

Video Transcoders



This section allows configuration of the video transcoders to be used for decoding and encoding video streams. The optimized defaults are pre-configured, and only an experienced user should make changes upon the recommendation of technical support.

Either IPP or FFMPEG codecs are currently supported. For encoding, the selection will only apply to H.264, while for decoding the selections will apply to both H.264 and MPEG4. In short, the settings within the Video Transcoders pane allow system administrators to tailor video encoding and compression options to suit both the type of content and on what type of device it will be displayed.

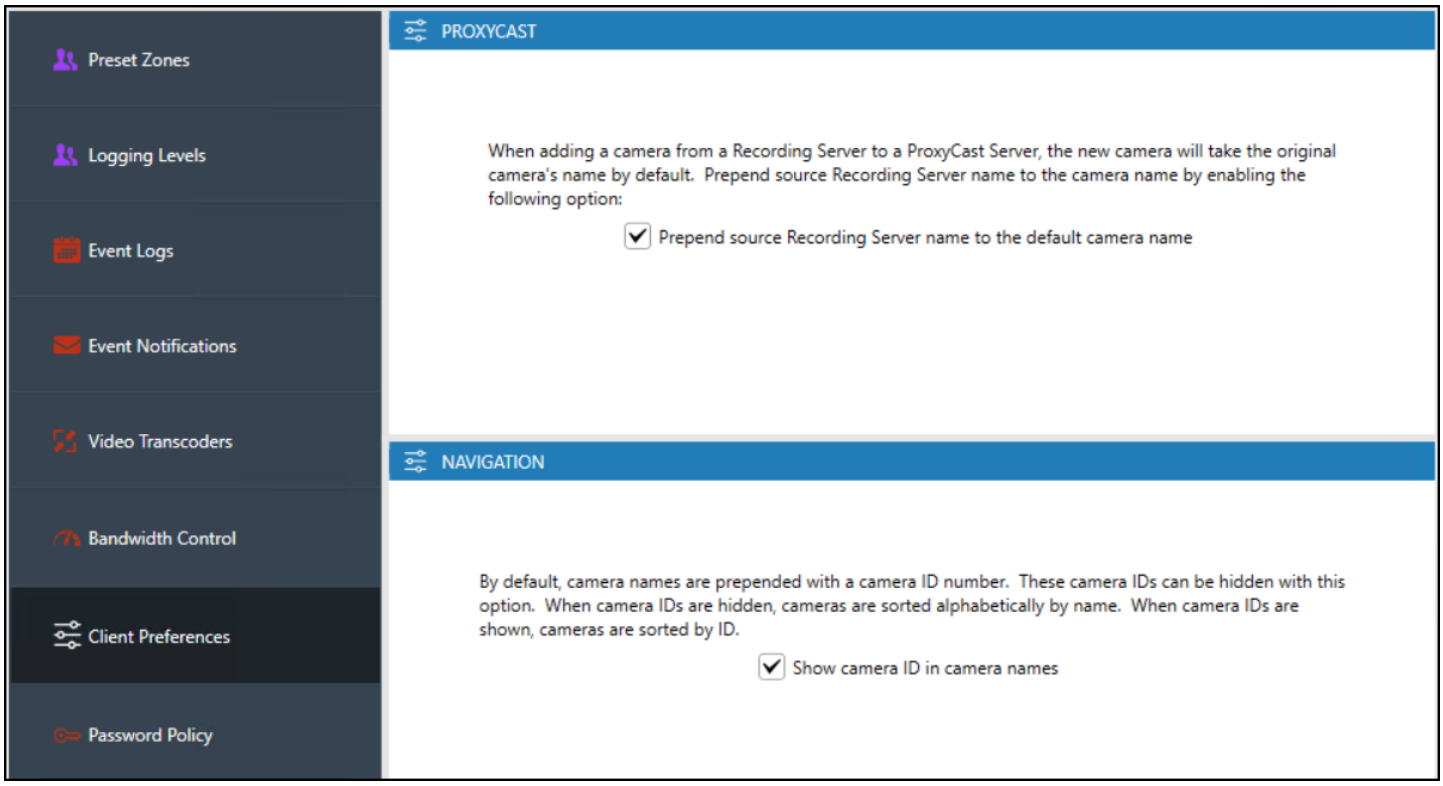
Once configured and the server configuration saved, the cameras configured for either H.264 or MPEG4 will utilize the selected codec and its options.

At this time, H.265 utilizes hard-coded parameters which are not user-configurable.

Bandwidth Control

CompleteView allows for the configuration of individual Recording Servers to operate in low-bandwidth environments, such as found on oil-platforms, Ranger stations, and other remote locations where connectivity may be restricted. See the following Bandwidth Control section of the documentation for detailed information.

Client Preferences



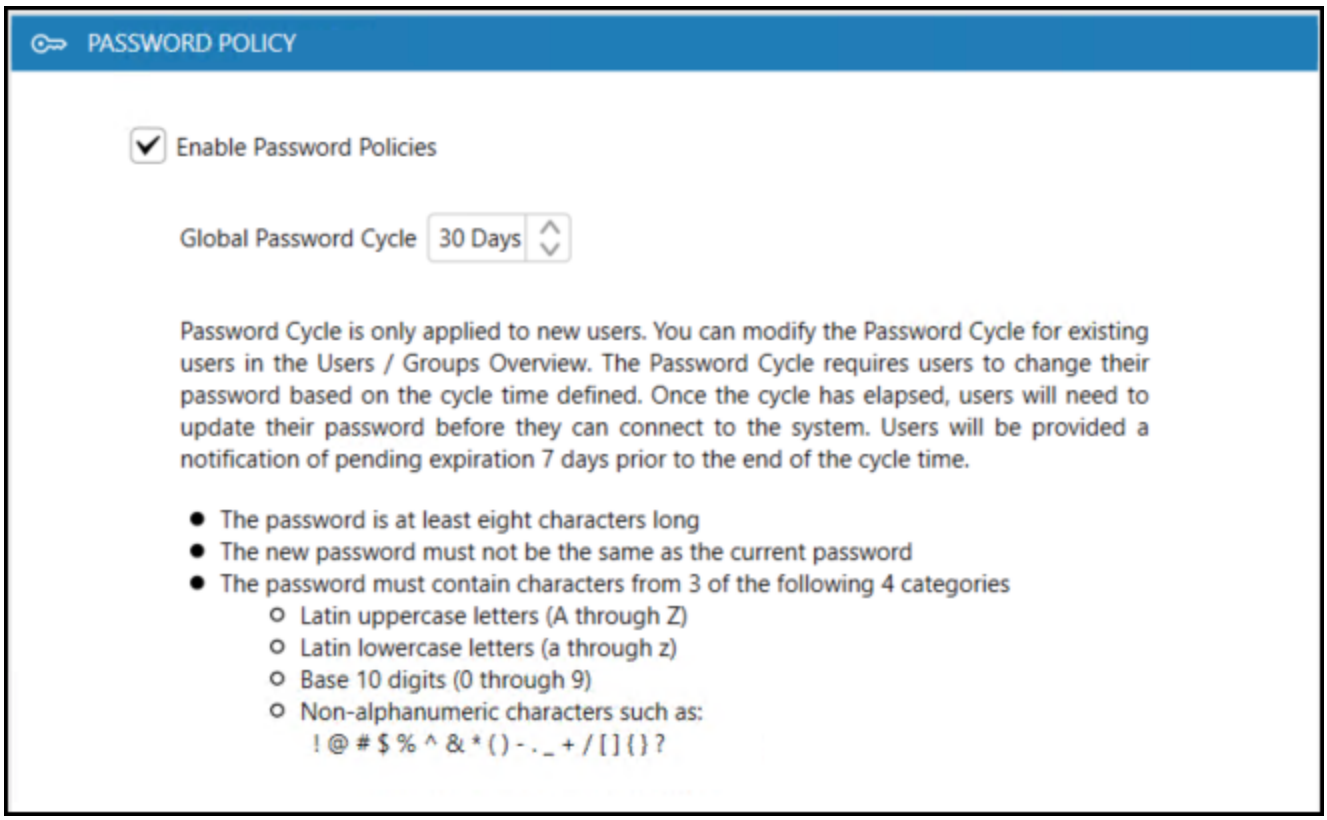
Client Preferences relates to toggling the camera ID on or off camera names. Client Preferences settings are global, applied to Desktop Clients per Windows user on a given system, and stored in the local cache (app data) folder.

Client Preferences Navigation

If the box is selected, the camera ID assigned by CompleteView will be included as part of the camera name. Any camera sorting will include the camera ID. If the camera ID is not included in the name (box is not checked), then sorting will be done by the camera name, whether it be customized by the user or left as the make and model of the camera, automatically populated by CV. This setting is global and overrides the Live View Settings -> Show Camera ID checkbox. If left unchecked, then Live View Settings -> Show Camera ID will be disabled and grayed out.

Password Policy

CompleteView provides administrators with the ability to enforce password policies, which includes password complexity and password cycle time. By default, password policies are disabled. Enabling the policy will cause CompleteView to check the password complexity of existing users. If a given user's password does not meet the complexity rules, CompleteView will force a password reset. When the Global Password Cycle is enabled or changed, the policy will apply only to new users. See the **Users & Groups Configuration** section for detailed information.


PASSWORD POLICY
Enable Password Policies
Global Password Cycle
30 Days
Password Cycle is only applied to new users. You can modify the Password Cycle for existing users in the Users / Groups Overview. The Password Cycle requires users to change their password based on the cycle time defined. Once the cycle has elapsed, users will need to update their password before they can connect to the system. Users will be provided a notification of pending expiration 7 days prior to the end of the cycle time.
The password is at least eight characters long
The new password must not be the same as the current password
The password must contain characters from 3 of the following 4 categories
Latin uppercase letters (A through Z)
Latin lowercase letters (a through z)
Base 10 digits (0 through 9)
Non-alphanumeric characters such as:
! @ # $ % ^ & * ( ) - . _ + / [ ] { } ?

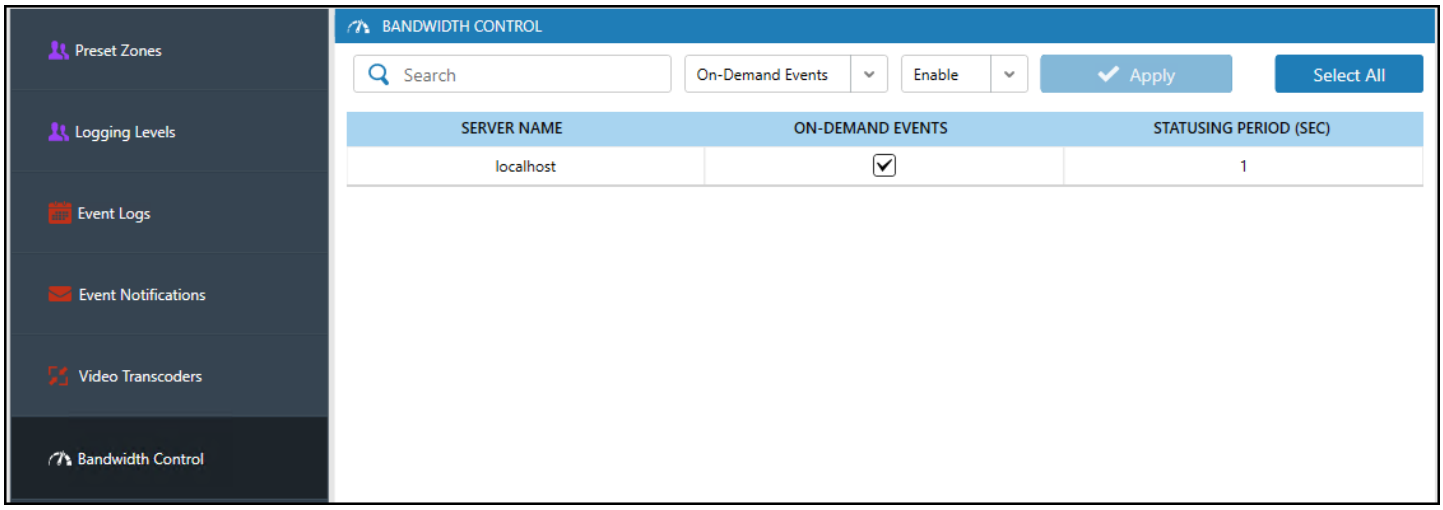
Bandwidth Control

When a Recording Server is monitored actively from the Desktop Client in the Dashboard and Configure modules, the Desktop Client polls the Recording Server for updates such as CPU usage, volume or storage status, and connection information. These status updates are required to show the status and health of the Recording Server in real time.

In addition, the Desktop Client subscribes to events on all Recording Servers to which a logged-on user has access in Live View and Alarm View modules. In Dashboard and Configure modules, events are subscribed only from the Recording Servers that are connected.

All of the activities described above consume bandwidth.

CompleteView allows for parameters to be set to accommodate Recording Servers located in areas of low-bandwidth connectivity. CV allows control of status update frequency, event subscriptions, data queries, and on-demand (as opposed to default) loading of events, camera lists, thumbnails, views, maps, etc. When bandwidth controls are in place, that information is loaded only when the Desktop Client specifically connects to and needs the information, such as when a new View is created using cameras connected to the restricted Recording Server.



Bandwidth Control Configuration

After configuring the selected Recording Server, log out and log back in to the Desktop Client to effect the desired changes.

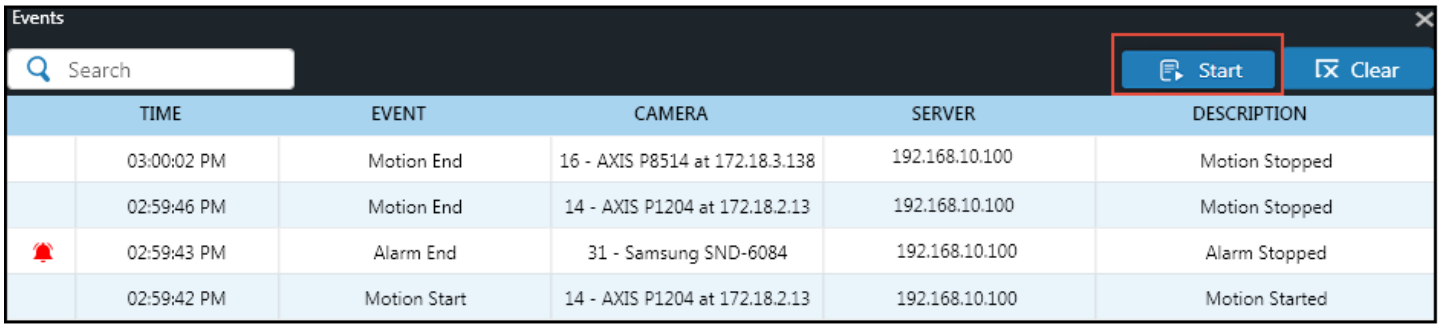
"Statusing" Period

"Statusing" Period determines how frequently the status is received from the selected Recording Server, configurable between 1-60 seconds, and is visible in the Dashboard and Configure modules.

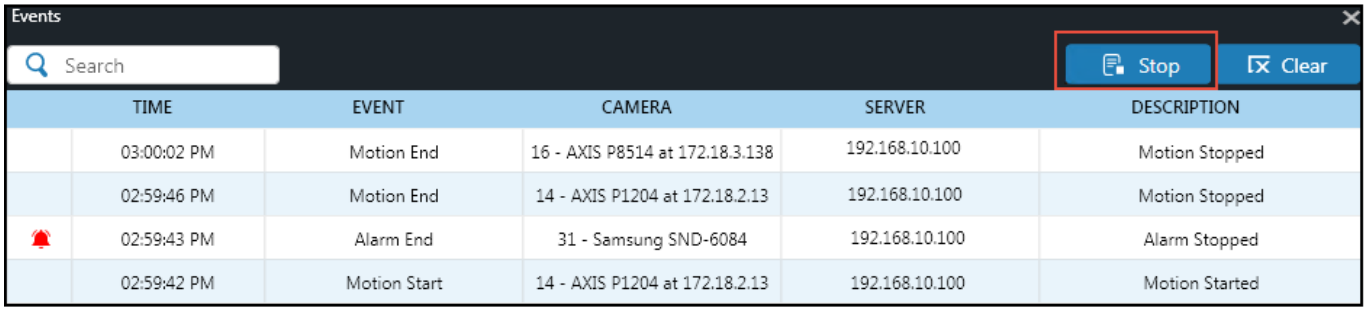
On-Demand Events

On-Demand Events toggles automatic real-time receipt of alarm and other events coming from cameras and other attached devices to the selected Recording Server. The results are visible in the Events panels located in the Dashboard, Live View, Alarm View and Configure modules.

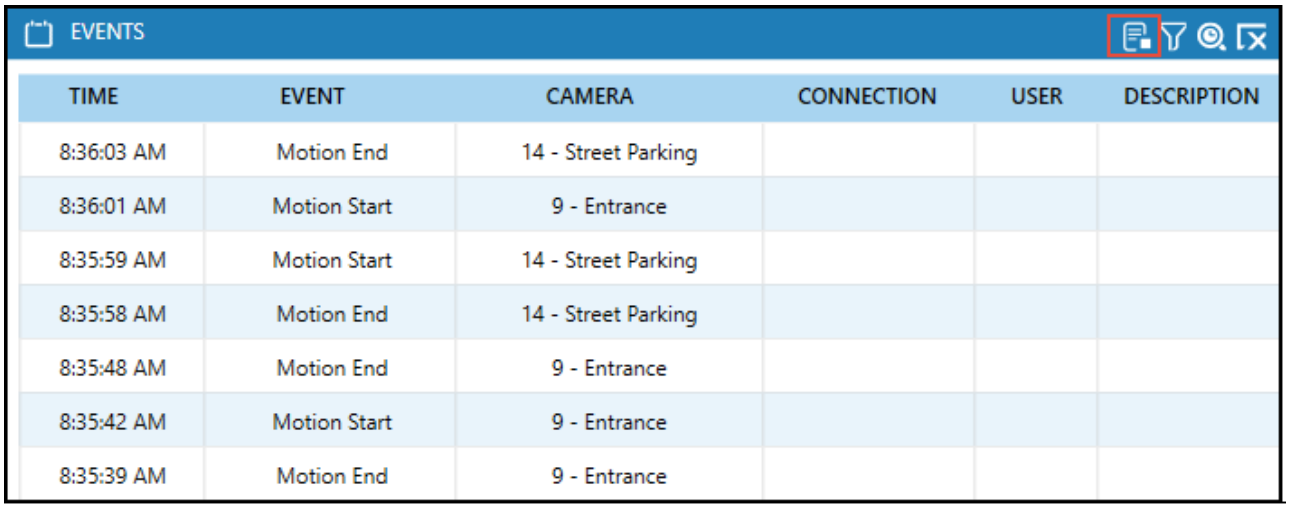
When enabled and saved, no events will be received from or displayed for the selected Recording Server in the various modules' Events panels. Events may be restarted by clicking the Start button in the Events panels of the relevant modules.



To stop the events again, select the Stop button.

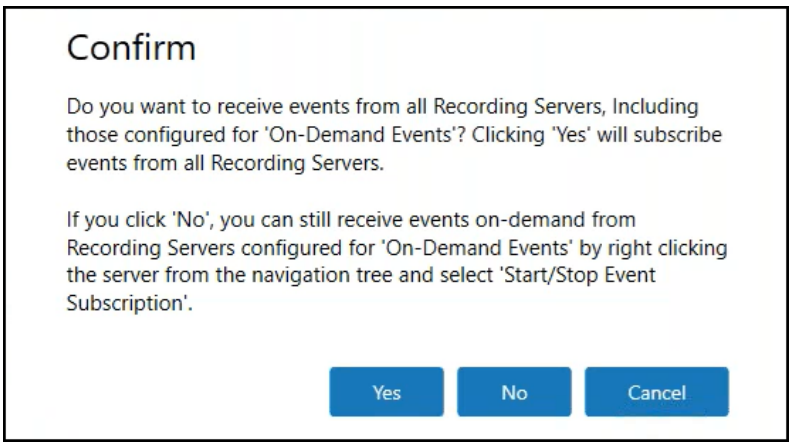


In the Dashboard Events panel, use the highlighted button to start/stop event receipt.



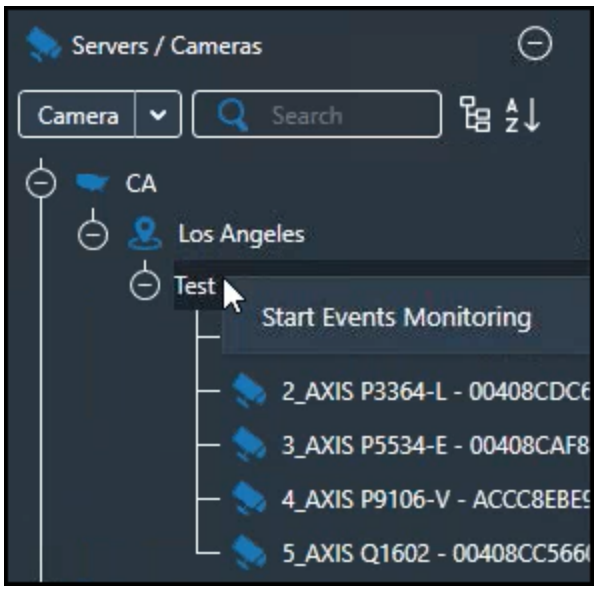
Mixed Environment Events Handling - Live View

When monitoring a mix of Recording Servers in Live View where one server is restricted and one is not, clicking the Start events button as shown above presents a choice.



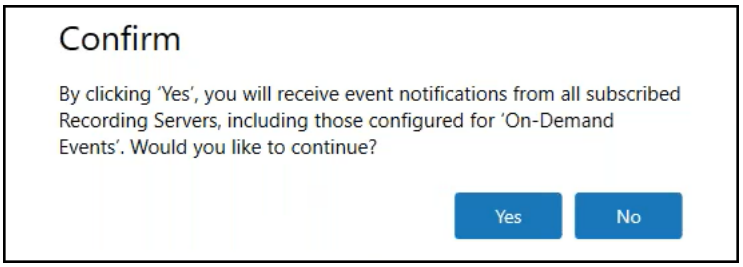
Clicking Yes will allow all Recording Servers being monitored in the window to begin streaming event data as normal, even the bandwidth restricted ones. Clicking No will continue to stream events from normally configured Recording Servers, and allow manual control of events monitoring for the restricted ones.

To manually start monitoring restricted Recording Servers, select the desired Recording Server, right click on it, and select Start Events Monitoring.



Mixed Environment Events Handling - Alarm View

Clicking the Start events button in Alarm View also presents a choice.



In Alarm View, however, there is not currently an option to select an individual Recording Server, therefor clicking Yes will begin events data receipt for all servers, regardless of bandwidth configuration status. Clicking No will continue events data from normally configured Recording Servers.

A Word about Camera Status Data

While CompleteView now utilizes the Management Server to maintain most camera configuration information thus eliminating the need for communication with the Recording Server, certain AXIS and other 360 panomorphic cameras require a direct connection between the Desktop Client and Recording Server, and will utilize the necessary bandwidth for that communication.

Common Settings Integrations

Salient currently integrates with more than twenty access control and other video related products that employ Salient's API integration process.

For specific integrations, please see the Cameras and Integrations Overview section of this documentation.

Integrations Listed in the Client

Axis One-Click, Bold Manitou, S2 Access Control, and Immix Protect all require specific recording server settings to complete their integration. Each of these products has an individual setup panel from which they can be configured to operate with CompleteView. See the following section for information about BriefCam Synopsis.

Integrations Unlisted in the Client

Many Integrations that do not use specific recording server settings are integrated into the Client through the Salient Application Program Interface (API). API functionality is enabled by default. The API can be toggled in User/Groups by selecting the user and then selecting the Recording Server Panel.

Integration Component Downloads

Some integrations will require a stand-alone executable file that is commonly referred to as an Integration Component. The Integration Component must be installed prior to enabling the API in CompleteView. Integration Components are found with other software downloads, and can currently be found at:

https://support.salientsys.com/knowledgebase/integrations/

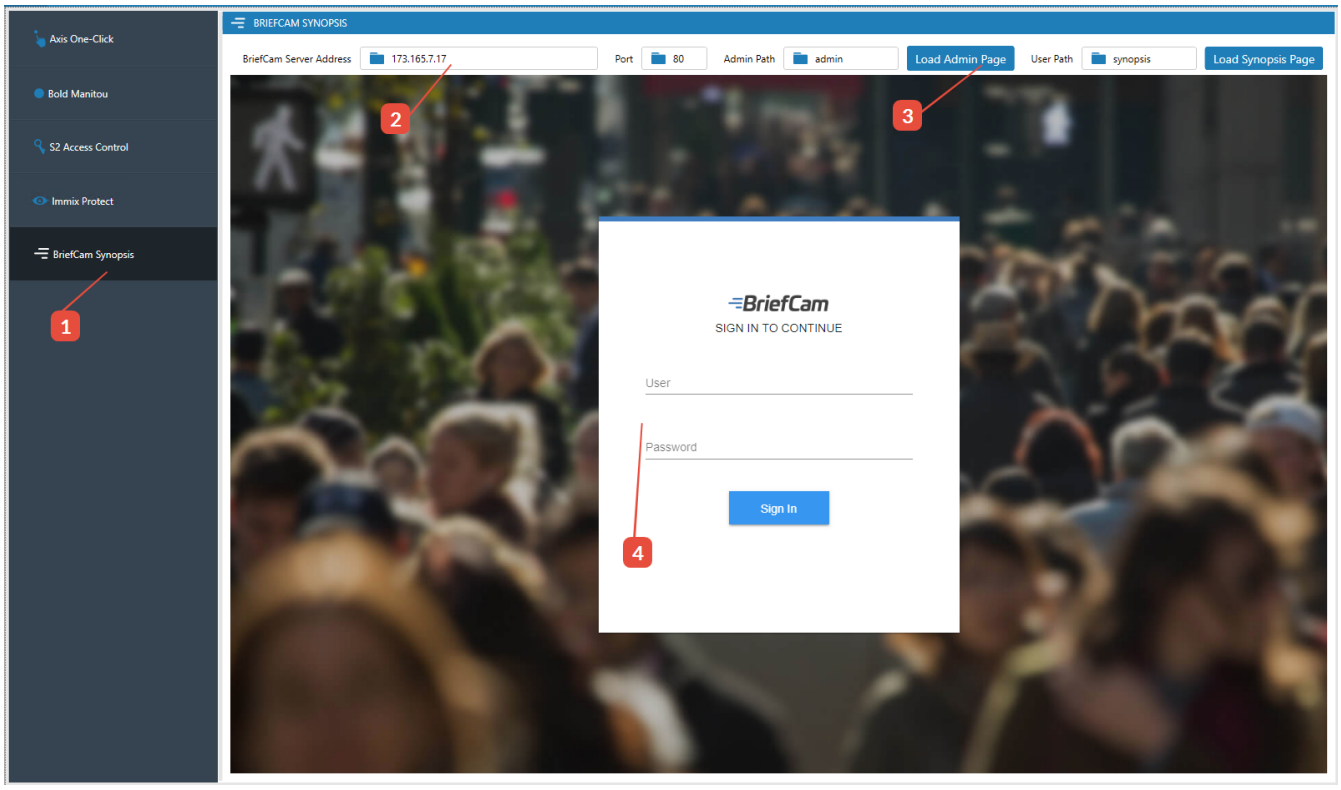
BriefCam Synopsis

BriefCam Synopsis is a powerful analytics tool allowing meta-data within video to be cataloged, stored, and sorted for investigatory playback. Refer to the Synopsis documentation for full functionality information, and refer to the steps below to integrate and access Synopsis from within CompleteView.

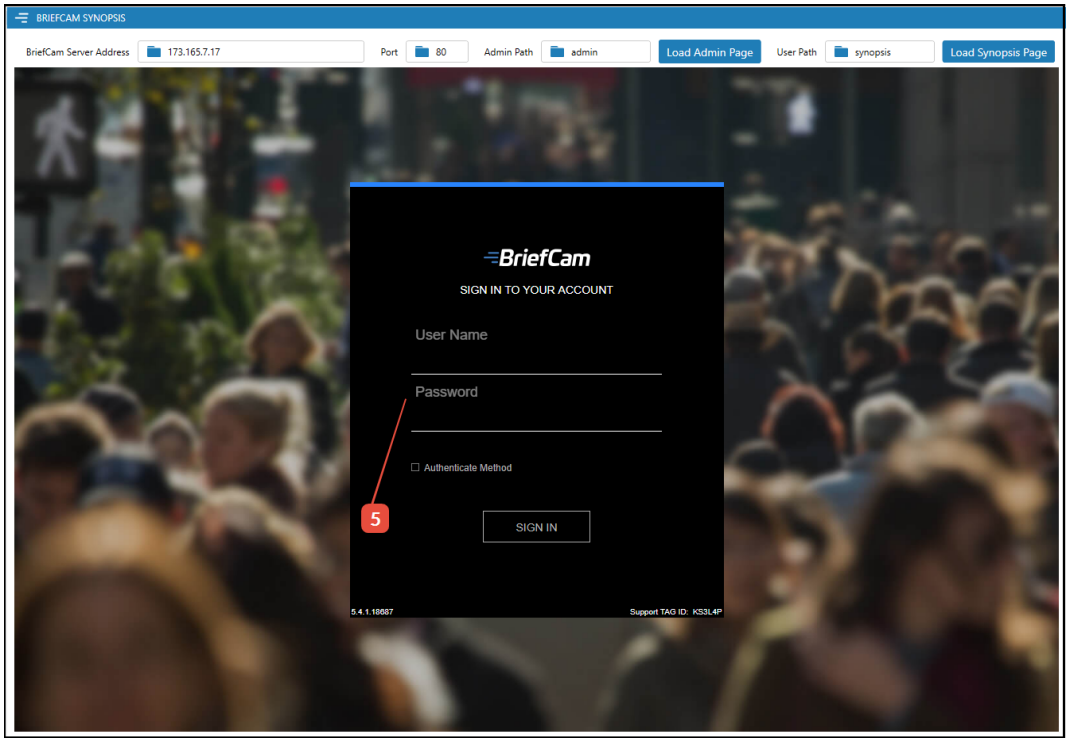
Connecting to the Synopsis Server

Steps:

1. From the Configure Module, expand Common Settings, select Integrations, and select BriefCam Synopsis.
2. Enter the BriefCam Server Address and other required information.
3. Click Load Admin Page. The BriefCam server login screen will appear.
4. Enter the BriefCam server credentials in the window.

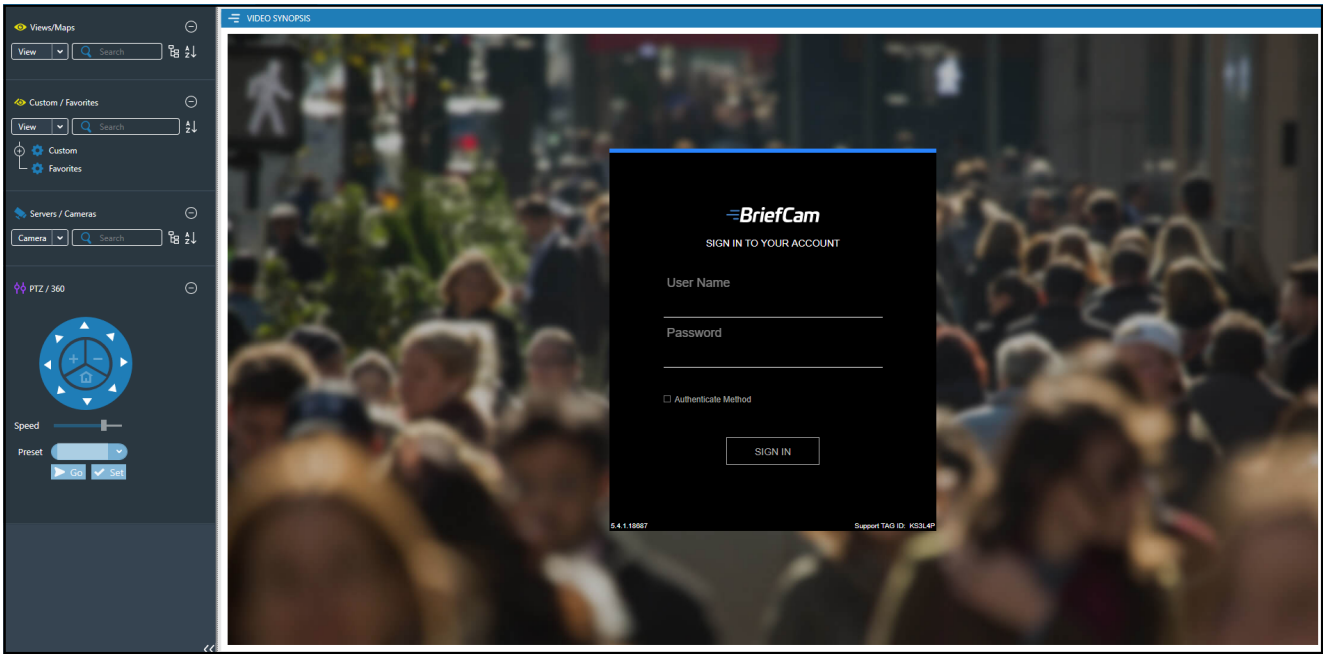


5. In the following screen, enter the BriefCam user account credentials and click SIGN IN.



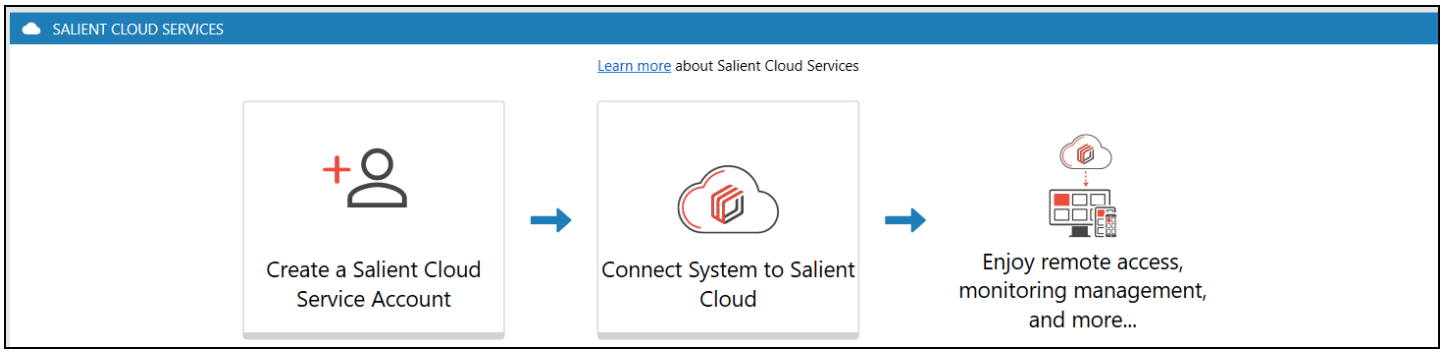
BriefCam Synopsis Playback

After successfully connecting to the Synopsis server, select the Playback Module, select the Synopsis server, enter the user account credentials and click Sign In to access the analytics data.

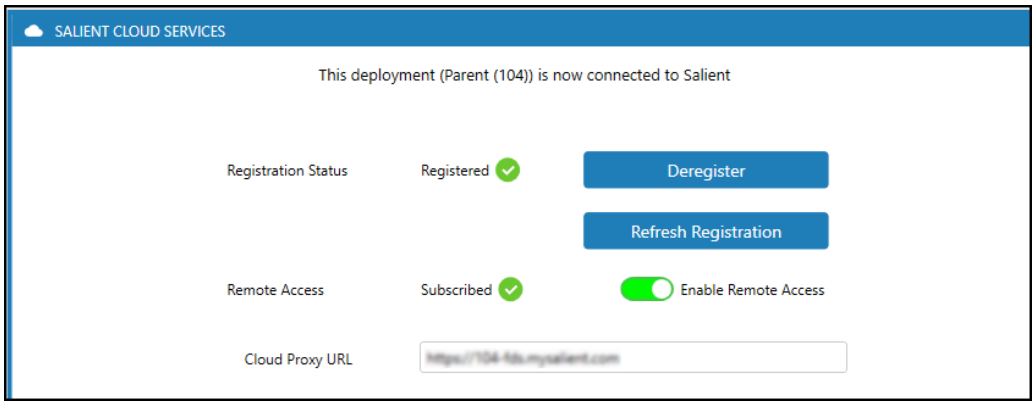


Salient Cloud Services

Salient Cloud Services allow for easy remote access, monitoring, and management of your on-premises CompleteView deployment. From within the Management Server node, select Cloud Services and follow the prompts to set up a Cloud Service account and connect a deployment to the Cloud.



Once registration is complete, select Cloud Services from the Management Server node to display registration and proxy information.



Recording Servers Configuration Overview

A Recording Server's primary function is recording video. In addition, it handles playback, camera schedules, and other functions to be detailed within this documentation.

Settings (Ports, Services, Security, Operations, and Integrations) applies to the individual selected recording server. However, the Client also provides the same configuration options which can be applied to all recording servers.

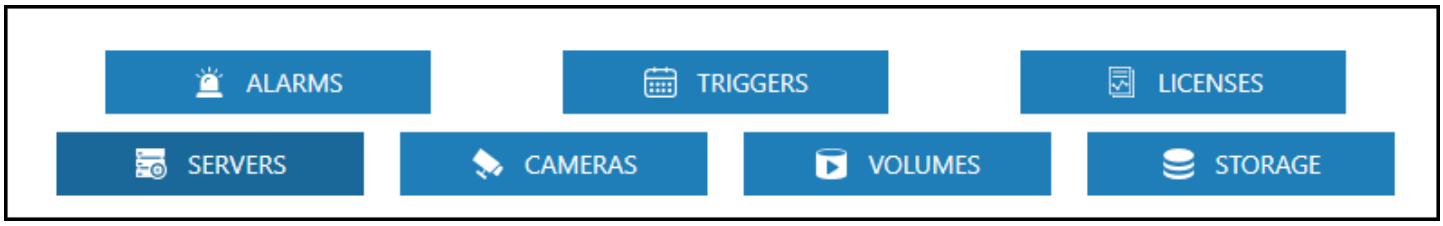
Administrators may configure and apply Settings to all servers from the Client's Common Settings Panel. But, exceptions can be configured from the Recording Servers Settings Panel. For examples, Event Notifications may display an "Inherited" checkbox, indicating that the settings were configured globally. If a change is made locally, the "Inherited" box will automatically be deselected, indicating local configuration.

Recording Server Overview Panel

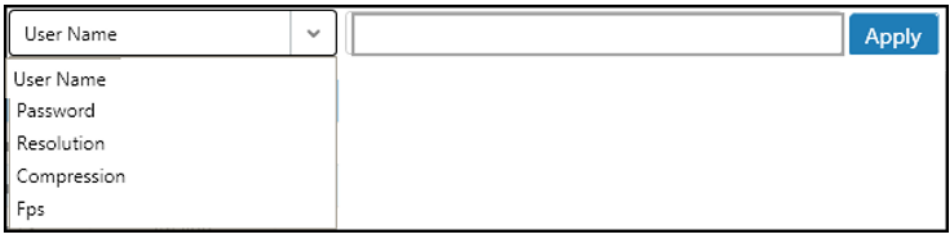
Recording Servers can be added and fully configured through CompleteView. The Overview Panel provides information and configuration access to added Recording Servers.

Overview Panel Top Menu

The six buttons at the top of the Overview Panel redirect the Administrator to relevant configuration options. The center of the panel displays informational columns about the selection.



The pulldown menu is context sensitive, contingent upon the selection.



In addition to the pulldown, users may select which informational columns to display, and, as above, the available columns are contingent upon what has been selected (Servers, Cameras, etc.).

Displays a list of Recording Servers and their information; use the pulldown menu to enter Recording Server's username and password. Selections are applied to all listed Recording Servers or to individual Recording Servers.

Displays camera information for the selected Recording Server; use the pulldown menu to select camera username, password, resolution, compression, and frames per second. Selections may be applied to all cameras or individually to any listed camera.

Displays the Recording Server's recording volumes and their information; use the pull-down menu to select video space, retention type, min. & max storage (in days). Selections may be applied to all volumes or to an individual volume.

Displays the Recording Server's Storage Pools and their information; use the pulldown menu to select and set Video Space.

Displays the Recording Server's available alarm devices and their information; use the pull-down menu to enter username and password.

Displays the Recording Server's available Trigger Devices and their information; use the pulldown menu to enter a description of the device. More detailed information may be found in the **Recording Servers Triggers** section of this documentation.

Displays CV servers and their license information.

Recording Servers Adding a Recording Server

A Word About Regions

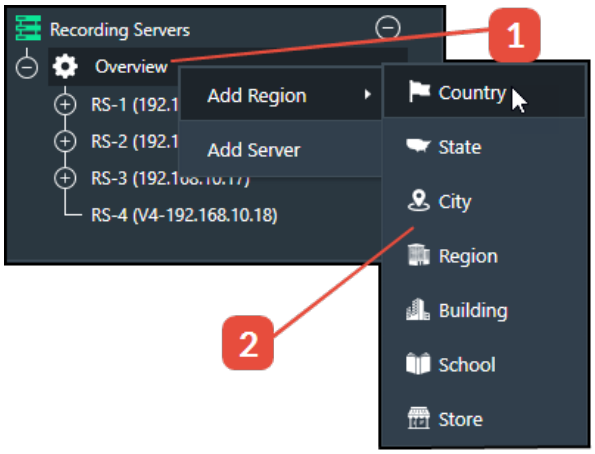
Adding an optional Region enables Administrators to create and place Recording Servers in a geographical hierarchy based on the Recording Server's physical location, which is useful for large, multi-site deployments. The hierarchy can start at any point in the list of Country, State, City, Region, Building, School, or Store. The resulting configuration allows the end-user to view video through a geographically illustrated hierarchy of the entire enterprise. Both the scale of a given installation and the needs of the end user will largely dictate both the necessity and complexity of a regional hierarchy. Recording Servers may be added with or without a Region. The use of Regions is currently limited to Enterprise edition.

For clarity, some UI elements may be omitted from the following information.

Add a Region

Steps:

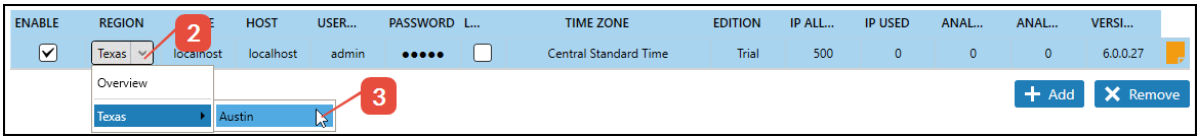
1. Right-click on Overview or an existing Region
2. Select Add Region
3. Select the desired denomination (Country, State, City, etc.)
4. Save the configuration
5. Follow the steps required to add a Recording or Legacy Server (see below)



Note: A hierarchy of denominations can be created to suit the organization's needs (e.g. a City Region can be created under a State Region, etc.).

Change Recording Server Region

A Recording Server's region may be changed after assignment.



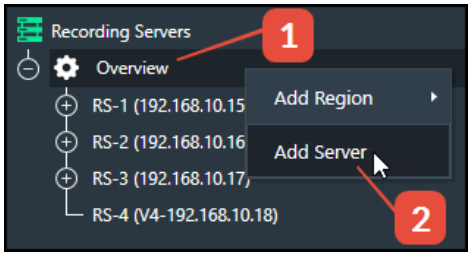
Steps:

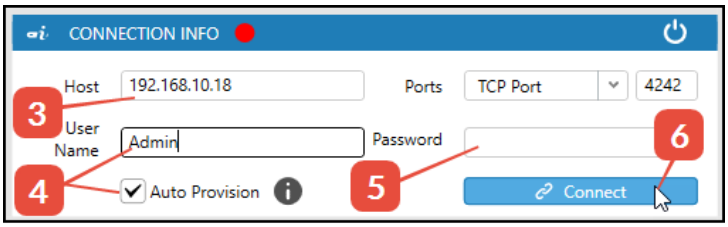
1. Left Click on Overview
2. Select the Region dropdown menu
3. Select the new Region
4. Save the configuration

Add a Recording Server

Use the following section to add a CompleteView Recording Server.

Adding a CompleteView Recording Server





1. Right-click on Overview or any of the created regions
2. Select Add Server
3. Enter the Recording Server's Host HTML address or IP address.
4. Enter the username. The Recording Server's default username is Admin, but if the Recording server is installed on a different machine than the Client, enter the Windows credentials where the Recording Server resides.
   a. Leave Auto Provision checked.*
5. Enter the Recording Server's Password. If the Recording server is on a different machine than the Client, the Windows credentials for that machine are required. Optionally, select Use Common Settings to apply those settings to the newly added Recording Server.
6. Select Connect
7. Save the configuration

Note: When the server connects, the indicator should change from red to green.

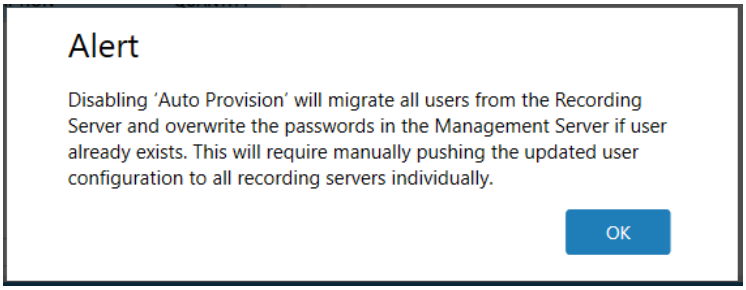
*A Word about Auto Provision

When adding an existing Recording Server to an existing Management Server, CompleteView examines the credentials on the incoming Recording Server. If credentials exist on the incoming Recording Server that already exist on the Management Server, Auto Provision automatically changes the passwords of the credentials on the incoming Recording Server to match the passwords on the Management Server. New credentials coming from the Recording Server are simply added to the Management Server.

Other configuration data such as Active Directory information, users and groups, etc., are handled in the same way. If Auto Provision is checked, the information already on the Management Server will overwrite anything coming in from the Recording Server.

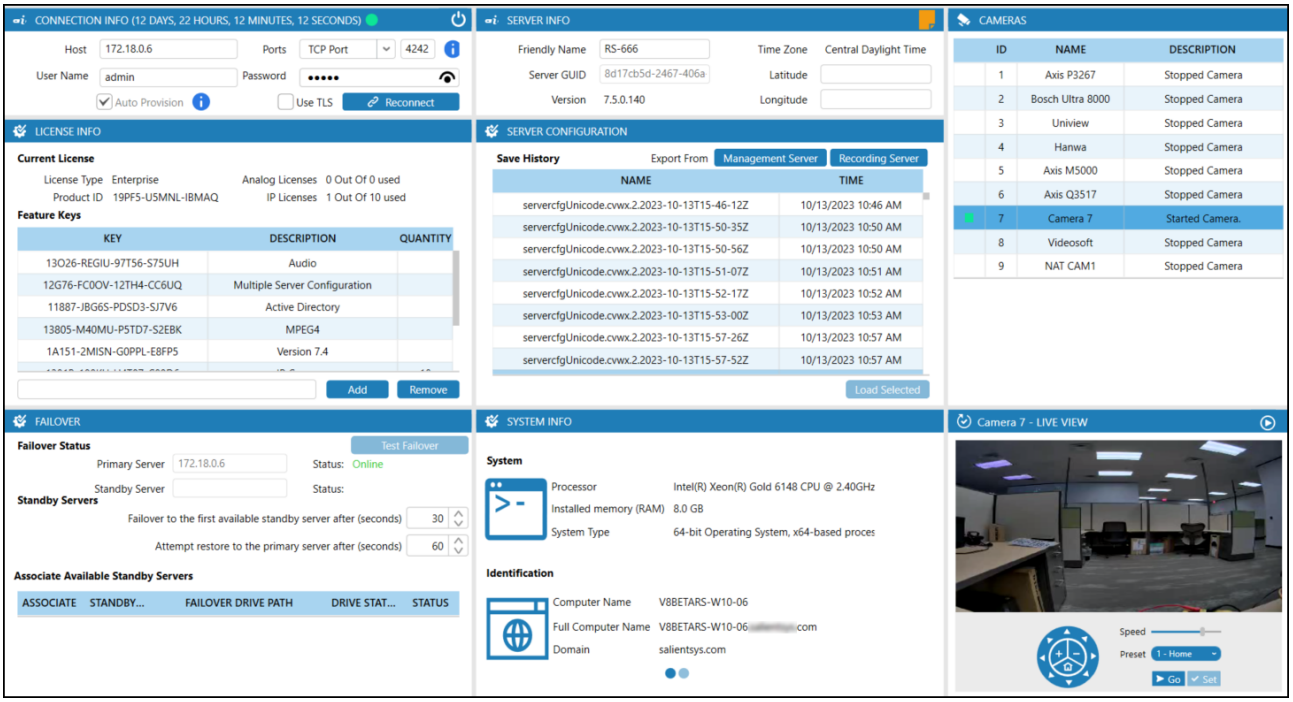
Generally speaking, it is advised to keep Auto Provision checked. However, there are specific instances where disabling Auto Provision may be beneficial, such as when a new Management Server is being implemented and there exists a large pool of users on an existing Recording Server. Disabling Auto Provision and adding the Recording Server will automatically upload the existing Recording Server's users to the new Management Server, credentials intact. After the initial importation, re enable Auto Provision when adding new Recording Servers.

Disabling Auto Provision will generate the following warning message.

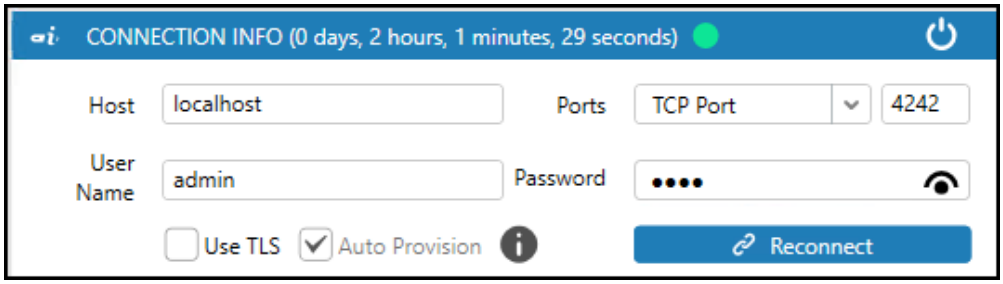

Alert
Disabling 'Auto Provision' will migrate all users from the Recording Server and overwrite the passwords in the Management Server if user already exists. This will require manually pushing the updated user configuration to all recording servers individually.
OK

Recording Servers Edit Settings

By default, the Edit Settings selection is set to Monitor Server. By selecting Edit Settings, many of the Info Panels discussed in Recording Servers Info Panels can be configured.



Connection Info



Connection Info displays the connected Recording Server's up time. To view a given Recording Server's status information, enter its credentials in the pertinent fields, and click Connect (or Reconnect).

Server Info

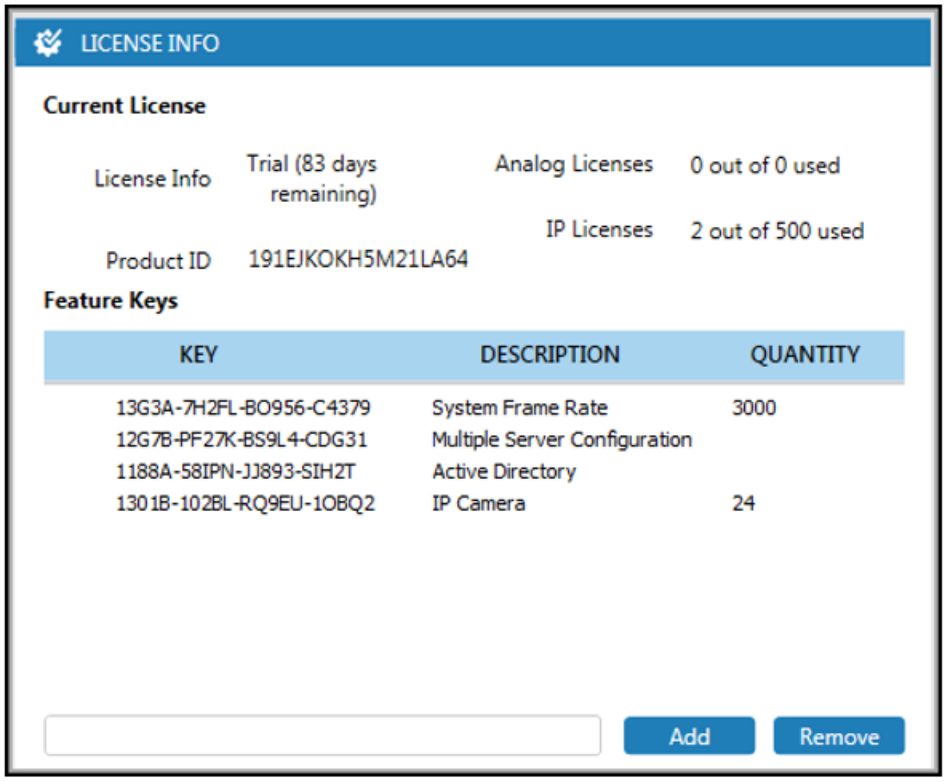
Server Info includes the Friendly Name, Time Zone, Recording Server Version number and Server Coordinates information. From this panel, the recording server's friendly name may be changed.

Change the Recording Server's Friendly Name & Enter Server Coordinates

Steps:

1. Select the desired Recording Server
2. Select the Recording Server Icon from the toolbar
3. Enable Recording Server Edit Settings
4. The current name will display in Server Info
5. Type the new name over the existing server name
6. Optionally enter the Recording Server's latitude and longitude information with up to 6 decimal places precision
7. Save the configuration

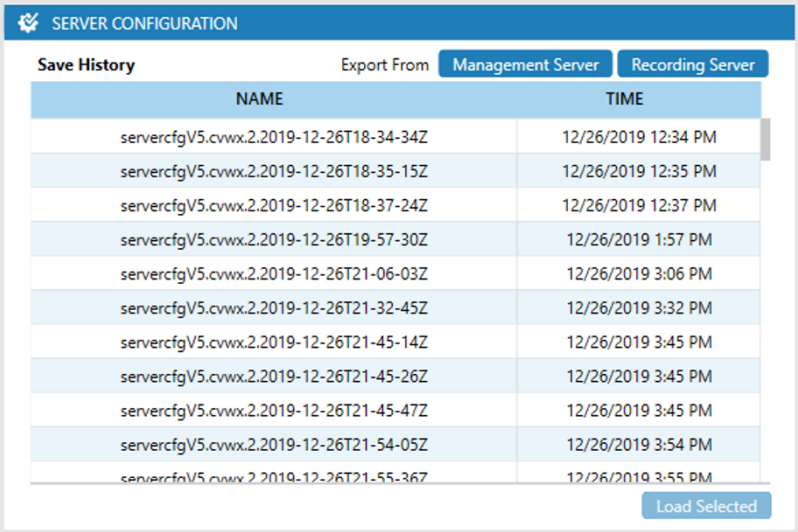
License Info



When Recording Servers Edit Settings is selected, licensing information is displayed here. The top half of the panel displays the Product ID, required information when requesting additional licenses and when contacting technical support. License info describes the license as Pro, Enterprise, or Trial. New camera license feature keys may be added by typing or copying and pasting the key into the field provided, and clicking Add.

Server Configuration

Network Share, Management, and Recording Servers Backup and Backup restoration and exportation are all configured in Server Configuration.



Backup a Server Configuration to a File

Steps:

1. Select a server
2. Backup to a File
3. Select a file location for the backup
4. Select OK

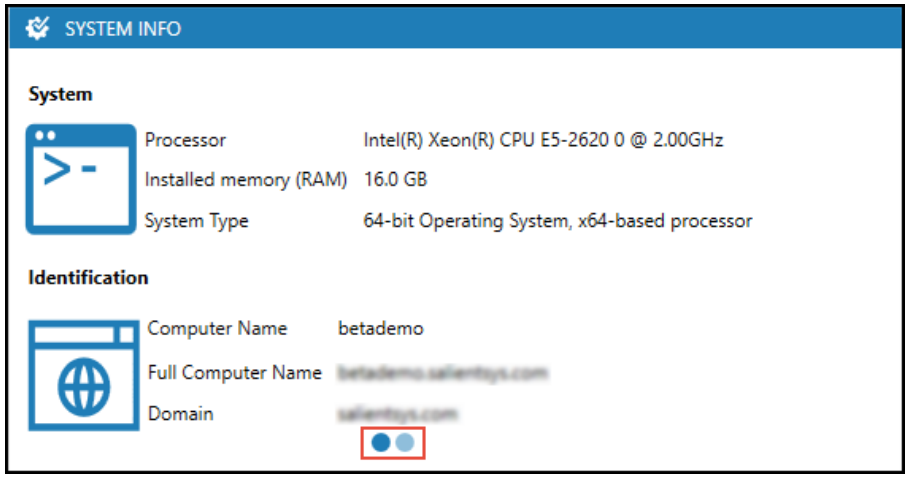
Note: backups will remain listed in the panel for loading. Alternatively, backups may be loaded from a saved file.

Failover

The Failover pane displays Primary and Standy Recording Server information, shared storage paths, and other configuration data related to failover. Please see **Failover Introduction** for more detailed information.

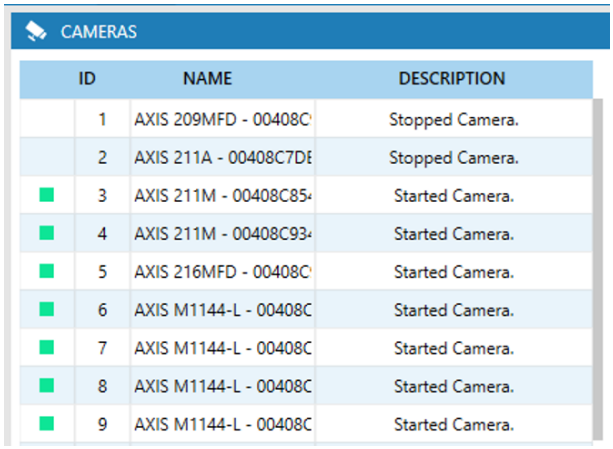
System Info

System Info displays System, Identification, OS, and Network Adapters information for the selected Recording Server. Scroll between multiple screens by using the blue navigation dots.



Cameras

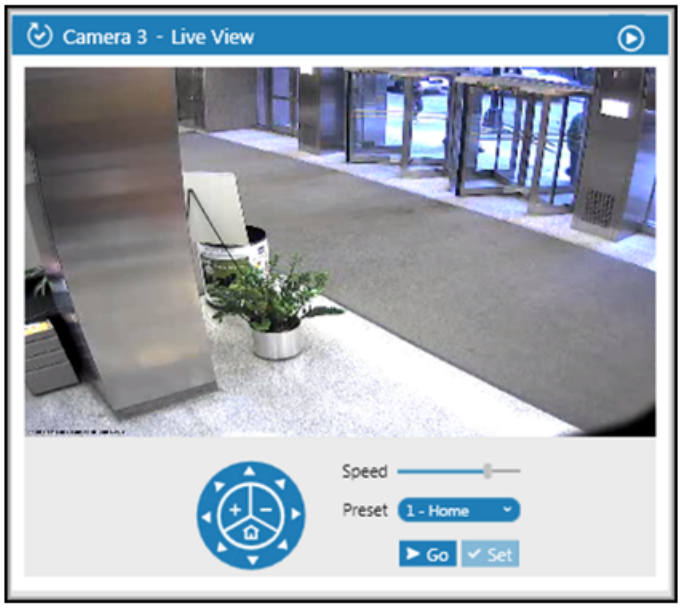
The Cameras Panel indicates the ID, Name, Type, Volume, and recording Status of the cameras connected to the selected Recording Server.



Camera Status	Indication
	Recording Motion
	Recording Alarm
	Recording Continuously
	Pre-Motion or Pre-Alarm Record
	Camera Lost Sync- Not Recording

Live View Panel

Selecting a camera will allow live viewing and quick review of that camera in the Live View Panel.

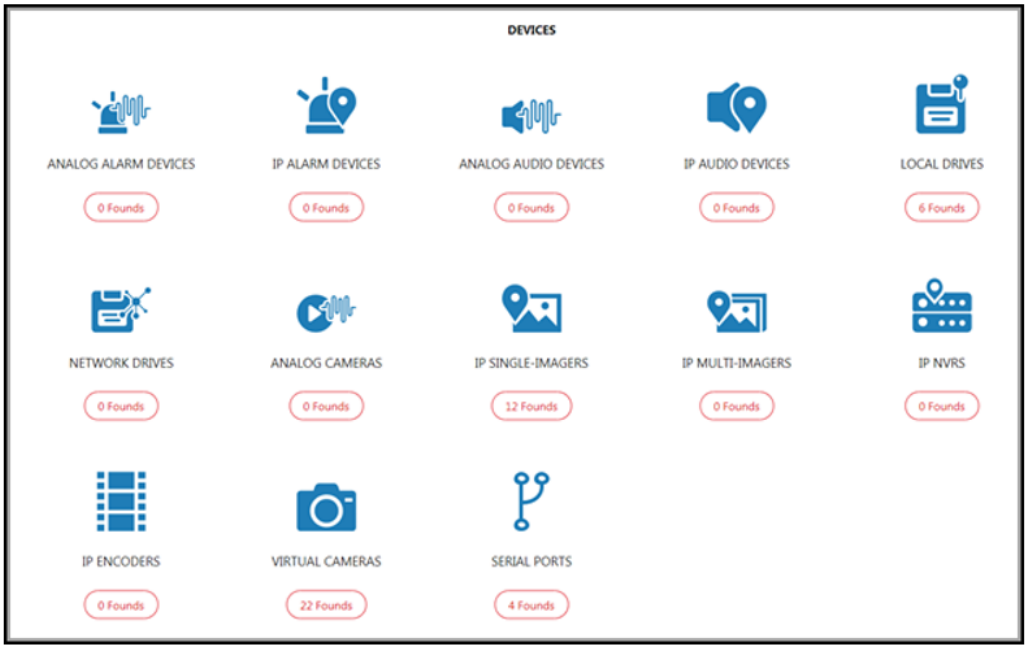


Quick Review

Quick Review permits review of recorded video for the time periods displayed on the menu. The selected time begins when the menu option is selected. A Quick Review menu appears when the button is pressed, allowing users to select between 30 seconds and 10 minutes of the selected camera's most recent recorded video.

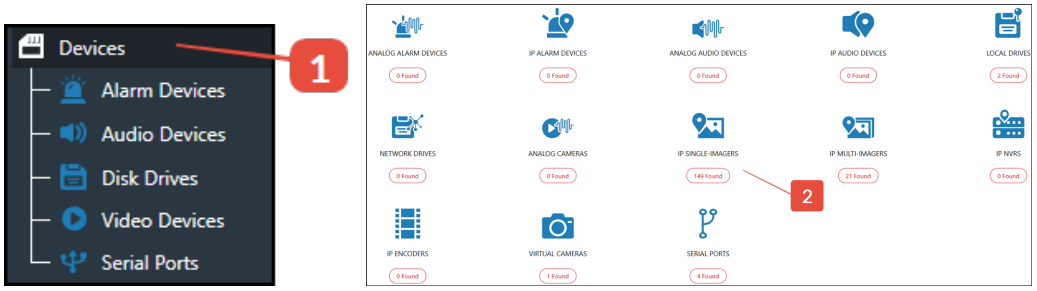
Recording Servers Devices Summary

The Device Summary Panel gives the Administrator a summary picture of all associated alarm, audio, disk drives, video, and other devices that may be attached to the Client by network or direct methods. Pressing any of the buttons directs the Administrator to the associated device group panel. The Device Group Panel is intended to provide an overview of the group's existing discovered devices. Some modifications to existing device parameters are allowed, but the panel is not intended to facilitate major changes or to new device additions to the Client. New devices should be added from the Volumes or Storage, NVRs Cameras, I/O, Triggers and Schedule Management Panels, located below the Device Group panels.



Review a Device

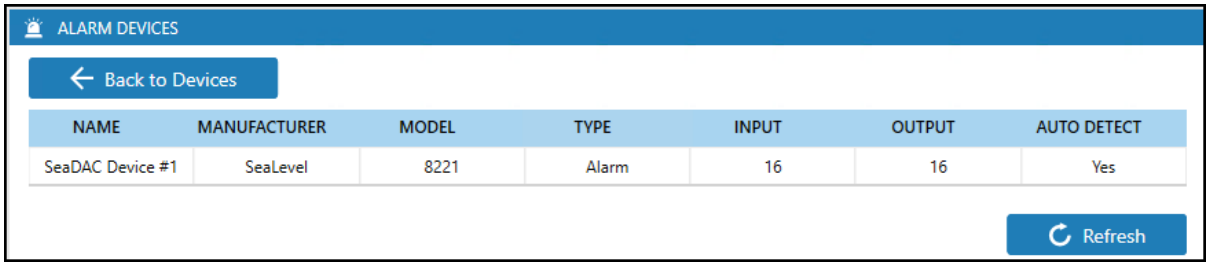
Steps:

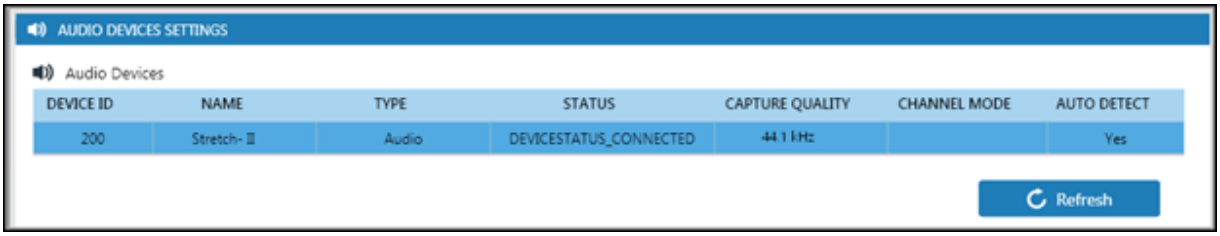


1. Select "Devices" from the Navigation Panel and for the specific server
2. Select the device icon that is to be reviewed

Example Device Information

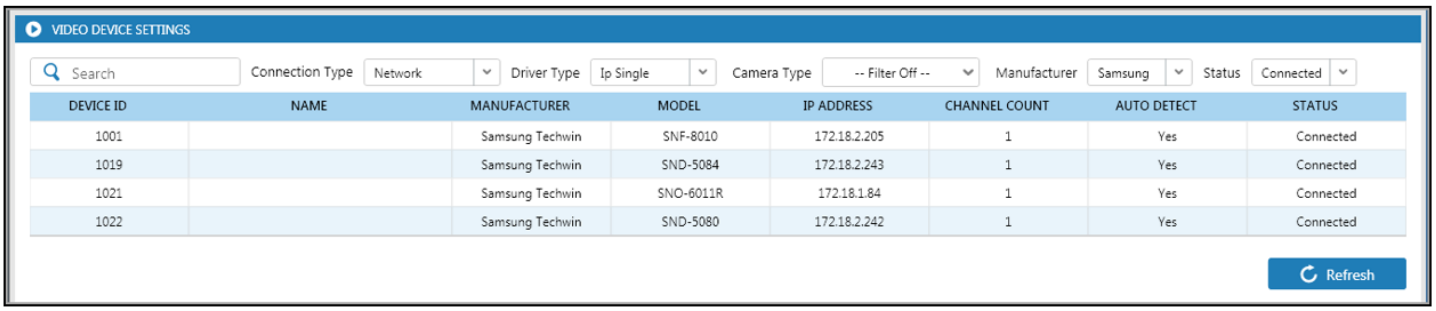
The following images illustrate typical Device Information, alarm, and audio, respectively.





Video Device Panel

The Video Device Panel permits users to select and sort/filter video devices by Connection Type, Driver Type, Camera Type, Manufacturer, and Status.



Storage Pool Introduction

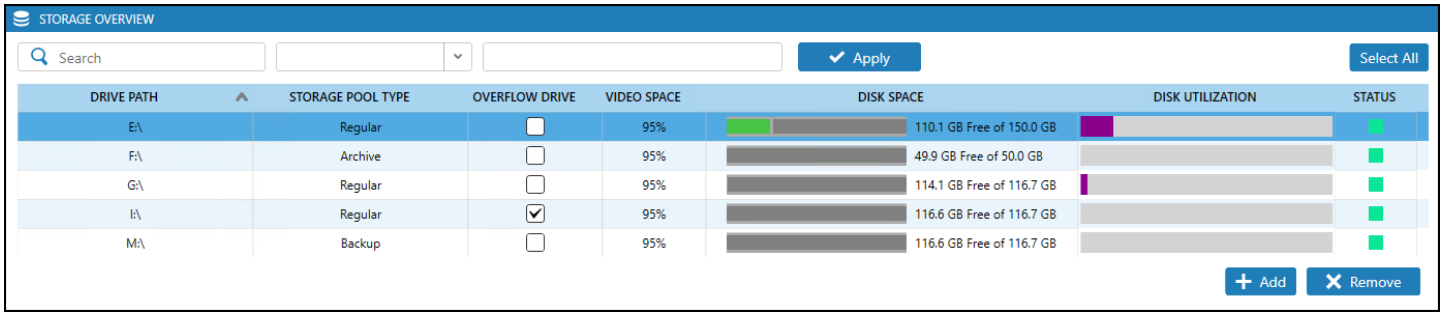
The Storage Pool is a scalable, logical collection of one or more physical drives, providing great flexibility for video storage. Other features of the Storage Pool include incorporation of camera-based video retention policies, storage utilization data, forecasting, and the ability to implement synchronous backup and overflow protection. Any storage location to which a Recording Server has access may be added to the storage pool, including internal drives (JBOD or RAID), NAS, DAS, or Cloud drives as well as individual folders on a given drive may be specified for use as part of the pool. All cameras on a Recording Server have access to the pool, and the drives in the pool may be shared with any other application. Note that a feature key is required to utilize Storage Pools.

Storage Pool Considerations

Once a Recording Server has migrated from volumes to storage pools, there is no ability to revert back. At present, CompleteView does not support the use of Read Only, Export, or Failover storage pools. As such, the functionalities associated with those storage locations are not currently available. Global Server Health does not currently provide individual status information for Regular, Backup, and Archive pools, but rather treats them as one unit in its reporting, and drive utilization information is only available in the Configure module. While forecasting of projected data use is a feature of storage pools, its functionality is limited to currently attached cameras, and cannot be used to estimate the space required for additional cameras. In addition, a given camera's video data may not be configured to write to a specific drive within a storage pool.

Storage Overview

Selecting Storage from the Recording Server tree in the left navigation panel will present the Storage Overview screen. Storage Overview is a high level summary of the configuration and status of the Storage Pool.



Seven columns display various Storage Pool configuration and status information, and will be described below.

Drive Path	The Drive Path indicates the assigned Windows or network path to the physical or logical drive, such as D:\, E:\Shared\, or \\Server\Shared\Video.
Storage Pool Type	Displays to which storage pool type each drive is assigned
Overflow Drive	Overflow storage is utilized when the Regular storage pool runs out of room trying to meet minimum storage requirements. Only drives assigned as Regular storage may be used for overflow, and at least two drives need to be present in the Regular pool for one to be designated as an Overflow drive.
Video Space	This is the percentage of the drive's physical space allocated to CompleteView for use as video storage. The default setting is 95%. While the set-

	ting may be lowered, it is not recommended to increase it above 95%.
Disk Space	Displays a graphical representation of the available space on the drive allocated for storage retention. Rolling over the graphic will display a tooltip with greater detail.
Disk Utilization	Displays a graphical representation of all available space on the storage location, including the amount of storage being used for cameras with and without minimum retention, the safety buffer, available free space, and amount of storage being used by applications other than CompleteView. Rolling over the graphic will display a tooltip with greater detail.
Status	Represents drive health and storage pool status. Rolling over the green, yellow, red, or black indicator will produce a screen tip providing more detailed informaion. Green indicates that the storage pool and its drives are operating normally and have sufficient capacity to function correctly. Yellow indicates one of the following: a. A drive's allocated video capacity is greater than the actual space available to write video. This condition may arise when other apps or data residing on the same drive increase in size, potentially compromising CompleteView's ability to honor the drive's configured Video Space percentage. b. A drive's existing consumed video storage is greater than the video space allocated. Similar to the condition above, this may arise after reducing Video Space percentage following recording of a large amount of video. c. The storage pool is using an overflow drive, or is unable to meet minimum retention requirements for the pool. Red indicates that at least one drive in a pool is offline. Black indicates that a particular drive is offline.

In addition, drives may be added to or removed from the pool from the Overview pane by selecting the appropriate button. Detailed instructions on adding a drive can be found in the following sections.

Storage Pool Types

There are three storage types available in CompleteView. Utilization of the various types is accomplished via Retention Policies, and each type will be discussed in its own section. Many concepts applicable to all of the storage types are detailed in the Regular storage section, so a thorough reading and understanding of that section is advisable.

Regular	Utilized by all cameras for scheduled recording, including continuous, motion, and alarm video. Individual Regular storage drives may be selected for Overflow recording, used to ensure video retention policies are met.
Archive	Archiving is the automated transfer of recordings from Regular storage to Archive storage. Archiving frees up space in the Regular pool to meet retention policies. Archiving is performed after a specified number of days, and can selectively move any combination of continuous, alarm, and motion video.

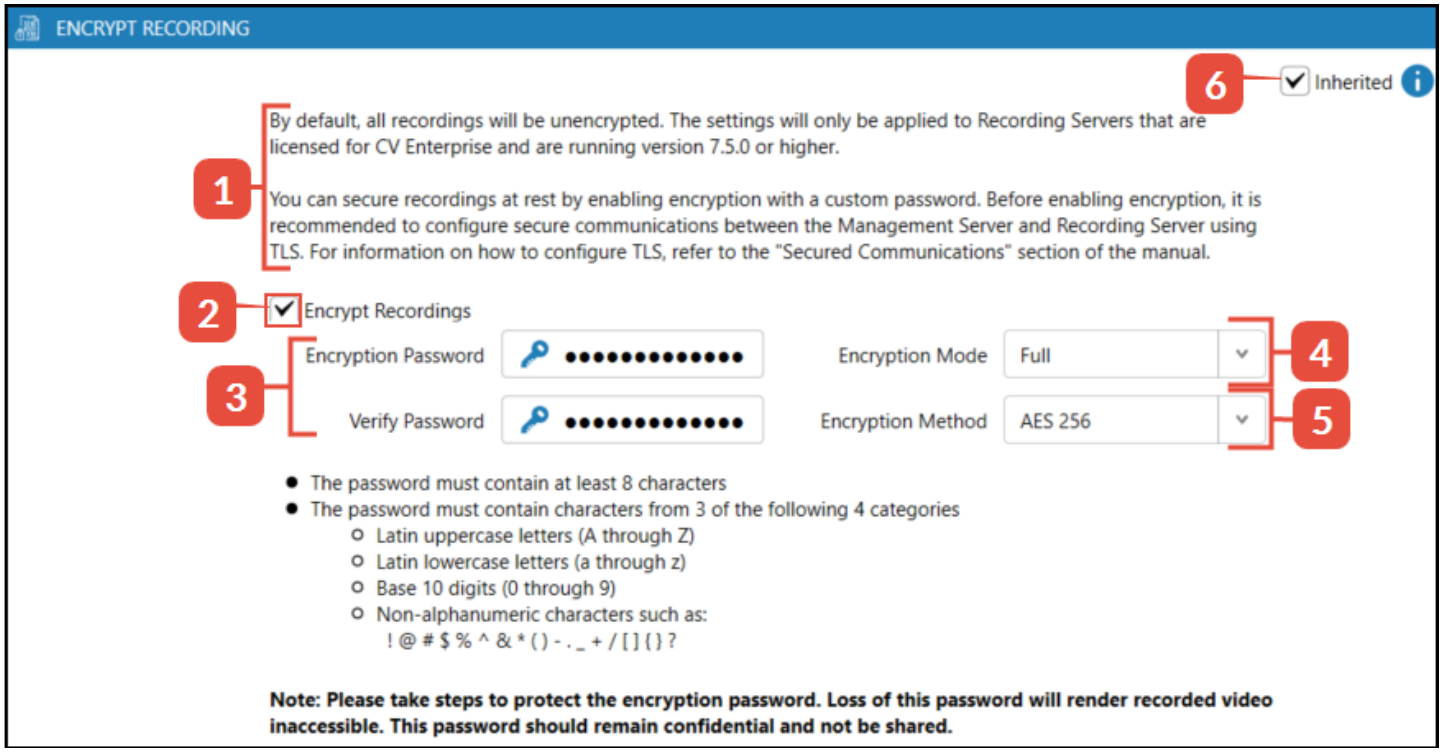
Backup	Backup provides a means of redundancy for the Regular pool. Backups automatically duplicate continuous, alarm, and motion video from the Regular pool to the Backup pool.

Recording Server Storage Encryption

CompleteView allows for the encryption of video and audio data that is being written to disk, also known as encryption at rest. Encryption is applied to all storage types (Regular, Backup, Archive, etc.) for either Volumes or Storage Pools, and may be implemented deployment-wide or per Recording Server. Enabling encryption does not affect failover operation. It is strongly recommended enabling TLS communications between Recording and Management servers for optimal security. By default, recording encryption is not enabled. Encryption may be enabled and disabled over time, and both encrypted and non-encrypted video will still be accessible. This section details enabling encryption on an individual Recording Server. For deployment-wide encryption instructions and for more information, see Common Settings Security

Enabling Recording Server Encryption

Select Storage (or Volumes) from the left navigation pane and use the following steps to enable encryption at rest for the selected Recording Server. Enabling encryption applies only to newly written video and audio data, and cannot be applied to existing data. Note that if the Inherited box has been checked, the Recording Server's encryption has already been configured at the Management Server level. Before enabling encryption on the local Recording Server, it is best practice to verify connectivity with the deployment's Management Server.



To enable Encrypt Recording Server encryption:

1. Read the disclaimer in the UI
2. Select Encrypt Recordings
3. Enter the Encryption Password then Verify the password

   Take steps to protect the encryption password. If the password is lost, the encrypted data will no longer be accessible. The password may be changed at any time, and the passwords for various Recordings Servers, within Common Settings, etc., may be unique.

4. Select the Encryption Mode

   Either Full or Lite encryption modes are available. Full mode encrypts both I and P video frames, where Lite mode encrypts only the I frames. Full encryption is recommended and is the default selection.

5. Select Encryption Method

   Either AES 128 or 256 bit encryption is available. AES 256 is the more secure option, and is the default selection.

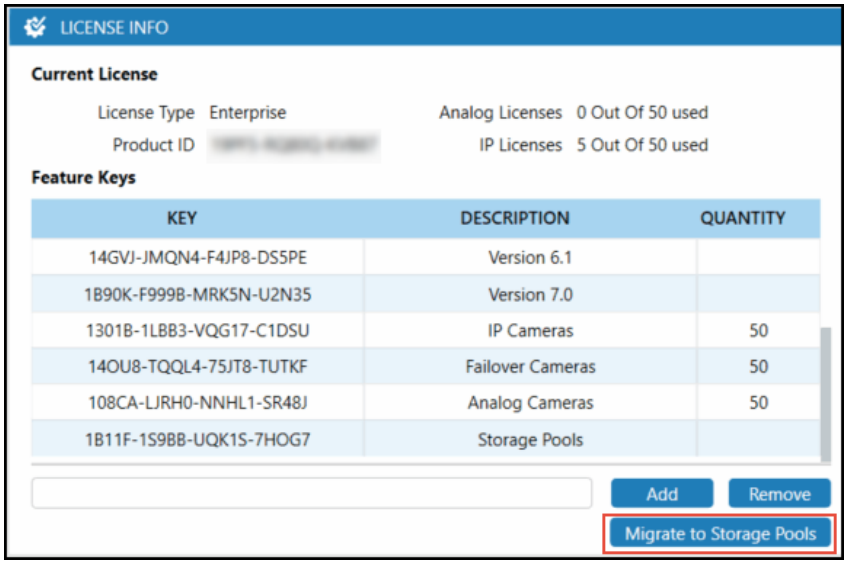
6. If the Inherited box is checked, the Recording Server's encryption has already been configured at the Management Server level. See **Common Settings Security** for more information. If changes are made at the Recording Server level (e.g. a new password, Encryption Method, etc.), the box is de-selected.

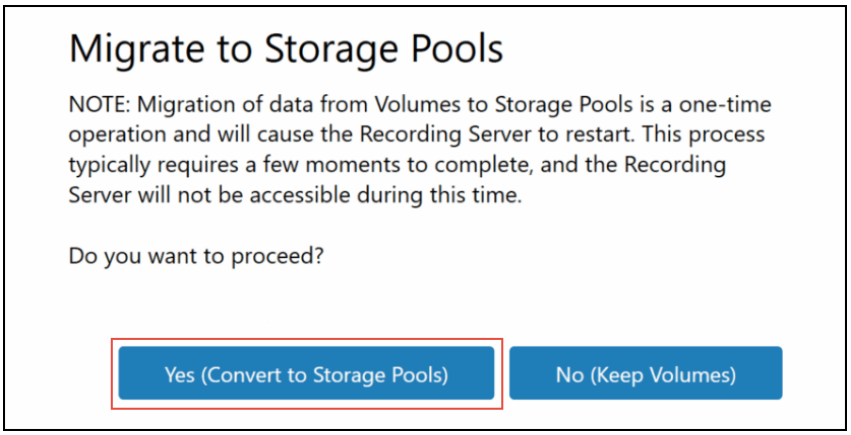
Note: Encrypted Recording Servers may be moved within a single Management Server without losing access to encrypted video, but cannot be moved between Management Servers. Reach out to support if a Recording Server needs to be moved to a new Management Server.

Storage Pool Migration

As noted before, a valid feature key is required to utilize Storage Pools in 7.X. Once migrated from Volumes to Storage Pools, it is not possible revert back. Further, migration from Volumes to Storage Pools is done per Recording Server and cannot be done en mass. The migration to Storage Pools will move the video data from its existing location to the new Storage Pool location on the Recording Server, and will apply existing Volume retention policies to the Storage Pools. Note that transferred policies may need to be adjusted to meet the configured retention requirements of the Storage Pools. In addition, Failover and Export volumes will not be migrated. To complete the migration, the Recording Server service will restart, causing a momentary interruption

In the CompleteView Configure module, browse to the Recording Server to be migrated. On the Overview page in the License Info section press the Migrate to Storage Pools button. Doing so display a notification to verify if you want to proceed. Once accepted, the Recording Server Service will restart.

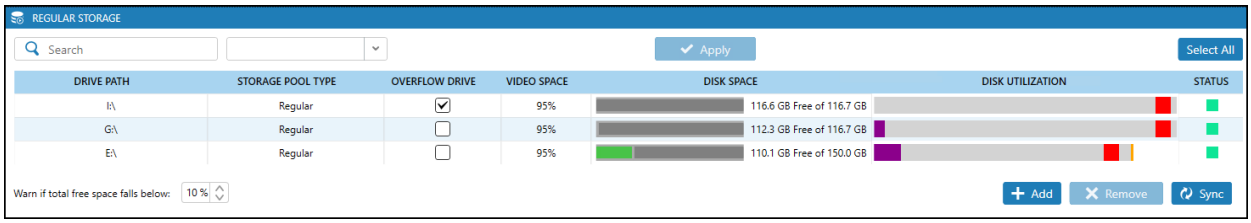




Once the Recording Server Service has restarted you will be able to access the Storage Pools. Video will be automatically written to the Regular Storage Pool and Operators will be able to retrieve video from the Recording Server normally . Repeat the procedure for each desired Recording Server.

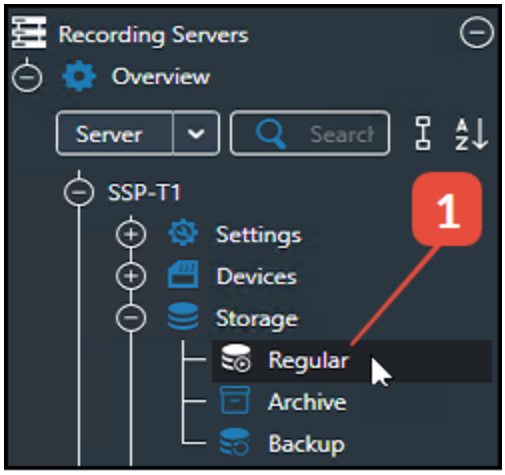
Regular Storage

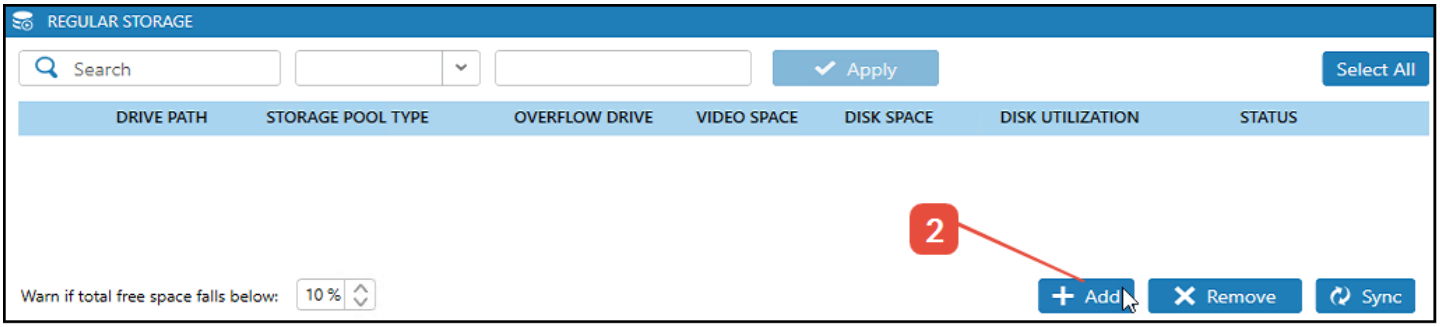
Utilized by all cameras for scheduled recording including continuous, motion, and alarm video, Regular storage is the default storage location for all video for the Recording Server. Cameras added to the Recording Server will automatically begin writing to its Regular storage pool. Individual Regular storage drives may be selected for Overflow recording, used to ensure video retention policies are met.

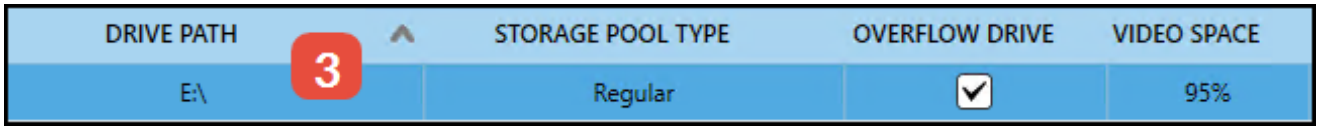


Adding a Drive

Note that the process for adding a drive is the same for any of the storage pool types.







Steps:

1. Select the type of storage to which the drive will be added.
2. Select Add
3. Configure the drive by entering the Path (either absolute or UNC location), optionally designating the drive for Overflow (see below), and select the Video Space.
4. Save the configuration

Finally, adjust "Warn if total free space falls below" if desired. That setting adjusts the minimum percentage of allocated drive space left at which an alarm may be sent. For example, if the value is set at the default 10% and the drive is a 10TB drive, a notification can be configured to be sent when 1TB is left for video storage.

Overflow Storage

Overflow storage is utilized when the Regular storage pool runs out of room trying to meet minimum storage requirements. If configured, CompleteView sends notifications when Overflow operation both starts and stops to alert personnel that the Regular pool may need attention. Only drives assigned as Regular storage may be used for overflow, and at least two drives need to be present in the Regular pool for one to be designated as an Overflow drive.

Regular Storage Retention

Once cameras have been added to the Recording Server and a Regular pool has been created, video retention is set on a per-camera basis. Retention configuration contains three elements: Retention Policy, Retention Estimates, and Storage Utilization.

Regular Storage Retention Policy & Behavior

Storage Retention Policy is used for setting minimum and maximum retention limits on a per-camera basis. Minimum Retention sets the minimum number of days a camera's video is stored in the storage pool. Maximum Retention sets the maximum number of days a camera's video is stored. Setting the Maximum Retention creates a point at which deletion of that camera's video begins, regardless of existing free space. Not configuring both Minimum and Maximum Retention settings results in video being stored until the storage location is full, and FIFO (First In First Out) deletion occurs.

No Minimum Retention Set

In the event that storage space runs out with no minimum retention time set, video older than one day will be deleted across all cameras using FIFO.

Maximum Retention with No Minimum Retention

Video data older than the maximum will be deleted regardless of available storage space.

Minimum Retention with No Maximum Retention

In the event that storage space runs out with a minimum set but no maximum, minimum retention times will be honored as long as possible. CompleteView will delete video older than the cameras' respective minimums using FIFO. If it's not possible to honor minimum retention times, CompleteView will generate an alarm and send an email notification if configured, provide a visual indicator in the Dashboard, and video will begin cascading into drives designated for Overflow.

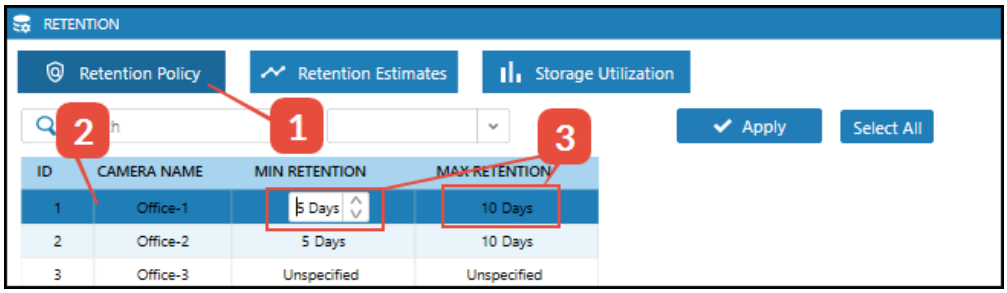
Minimum and Maximum Retention Set

In the event that storage space runs out with both minimum and maximum retention times configured, video older than the maximum retention time is deleted per camera in accordance with the daily schedule. If not enough drive space is recovered, video is deleted across all cameras using FIFO as described above where minimums are honored as much as possible and cameras with no minimum retention time have video deleted down to one day. If minimum retention still cannot be met, CompleteView will gen-

erate an alarm and send an email notification if configured, provide a visual indicator in the Dashboard, and video will begin cascading into drives designated for Overflow.

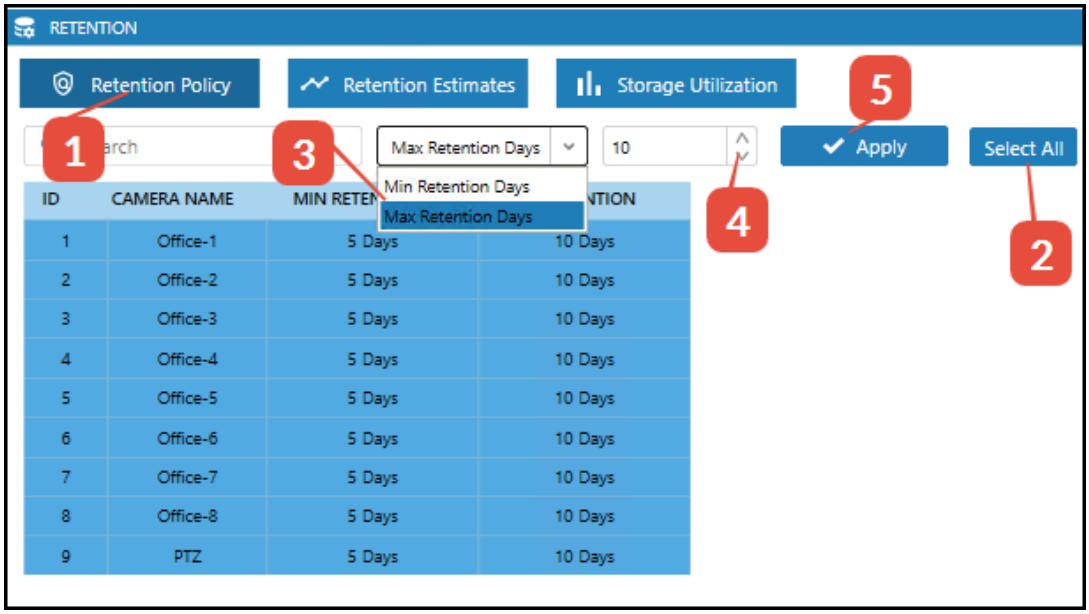
Regular Storage Retention Configuration

Policies may be set one camera at a time or by applying the same policy to multiple cameras at once. Maximum values need to be greater than minimum values.



Steps (for a single camera):

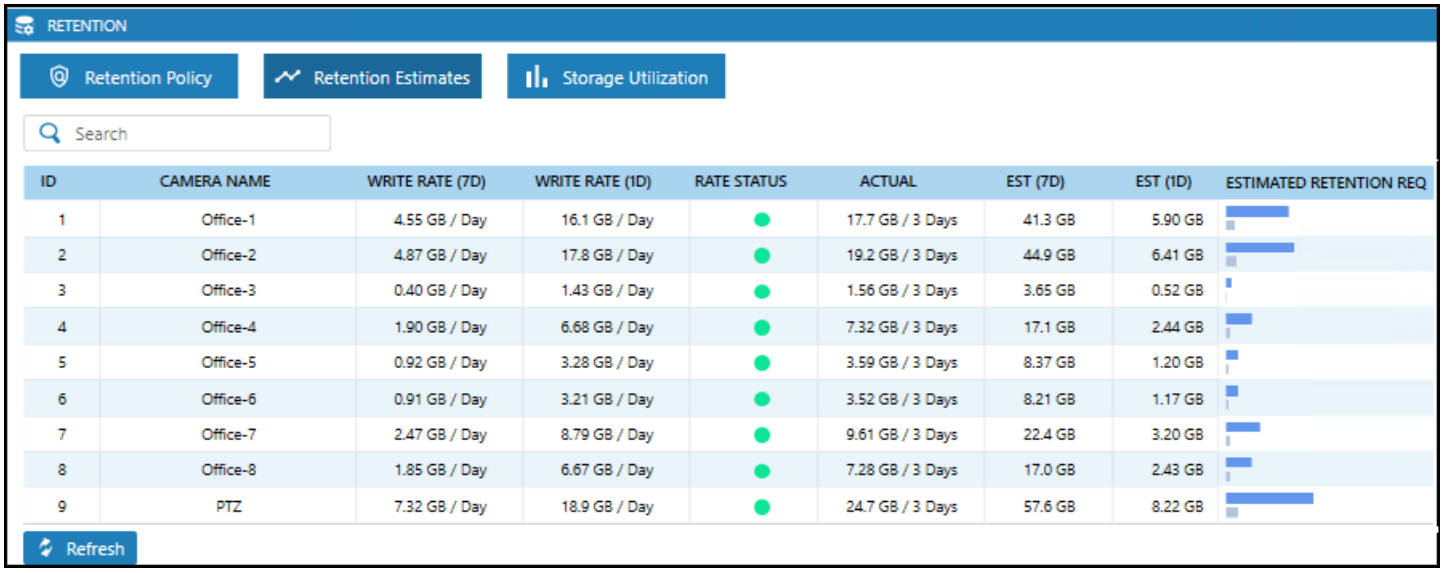
1. Select Retention Policy
2. Select the desired camera
3. Define the Retention (in days)
4. Save the configuration



Steps (for multiple cameras):

1. Select Retention Policy
2. Either use Select All or conventional cntrl/shift+click methods to select the desired cameras
3. Use the dropdown menu to select the desired parameter
4. Use the arrows to select the desired number of days
5. Click Apply
6. Save the configuration

Regular Storage Retention Estimates



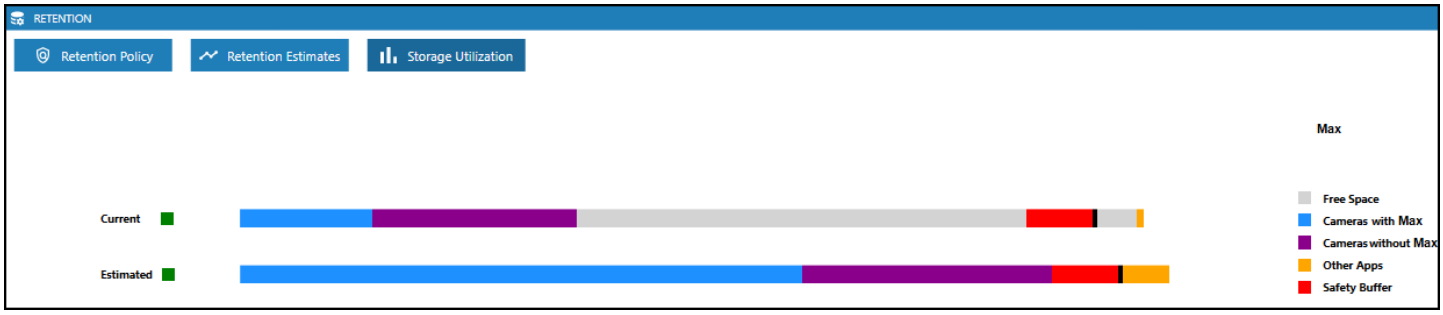
ID	CAMERA NAME	WRITE RATE (7D)	WRITE RATE (1D)	RATE STATUS	ACTUAL	EST (7D)	EST (1D)	ESTIMATED RETENTION REQ
1	Office-1	4.55 GB / Day	16.1 GB / Day		17.7 GB / 3 Days	41.3 GB	5.90 GB	
2	Office-2	4.87 GB / Day	17.8 GB / Day		19.2 GB / 3 Days	44.9 GB	6.41 GB	
3	Office-3	0.40 GB / Day	1.43 GB / Day		1.56 GB / 3 Days	3.65 GB	0.52 GB	
4	Office-4	1.90 GB / Day	6.68 GB / Day		7.32 GB / 3 Days	17.1 GB	2.44 GB	
5	Office-5	0.92 GB / Day	3.28 GB / Day		3.59 GB / 3 Days	8.37 GB	1.20 GB	
6	Office-6	0.91 GB / Day	3.21 GB / Day		3.52 GB / 3 Days	8.21 GB	1.17 GB	
7	Office-7	2.47 GB / Day	8.79 GB / Day		9.61 GB / 3 Days	22.4 GB	3.20 GB	
8	Office-8	1.85 GB / Day	6.67 GB / Day		7.28 GB / 3 Days	17.0 GB	2.43 GB	
9	PTZ	7.32 GB / Day	18.9 GB / Day		24.7 GB / 3 Days	57.6 GB	8.22 GB	

Storage Retention Estimates are intended to provide Administrators with historical and predictive data indicating whether or not adequate storage has been allocated to a given camera to meet the configured minimum retention requirements. Analysis is based on comparing historical averages with current write rates against currently allocated drive space. If the calculated required space is not available, a warning is issued once an hour until enough space is available by either freeing up existing drive space or adding more.

Heading	Data
Write Rate (7D)	The 7 day write rate is the exact amount of data written by the camera in the last 7 days.
Write Rate (1D)	The 1 day write rate is the exact amount of data written by the camera in the last day.
Rate Status	Indicates if the average consumption of storage space based on a camera's write rate falls within current norms. If the 1 day average exceeds the 7 day average, a warning status indicator will be displayed. A write rate increase of 20% will generate a yellow status, while a 40% increase will generate a red status. Note that the status will eventually return to green as the new average becomes the norm.
Actual	Indicates the amount of data written by that camera over the specified number of days.
Est (7D)	Estimated 7 day storage requirements based on historical write rate data, calculated by multiplying the Est (1D) by 7.
Est (1D)	Estimated 1 day storage requirements based on historical write rate data, calculated by divding the total bytes of storage written by the camera by the number of days the camera has been recording.
Estimated Retention Req	The top bar graphically represents the 1 day estimated retention requirements, and the bottom bar represents the 7 day estimated

Heading	Data
	requirements.

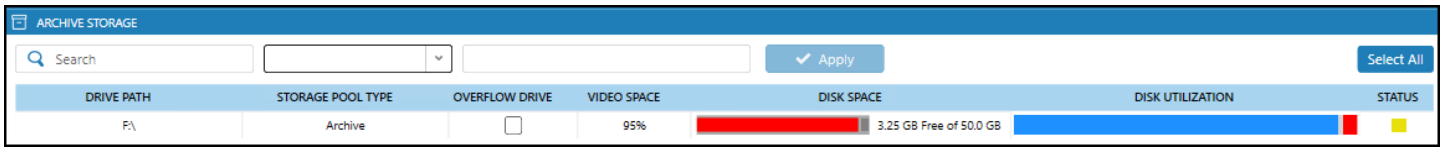
Regular Storage Utilization



Storage Utilization displays a graphical representation of current and estimated storage usage by data type. Rolling over the bars presents either a data type's current or predicted storage usage along with the its color's key information, also available on the right side of the pane. This data allows for a quick visual guide to what types of cameras or apps are utilizing the most and least space so that retention policies may be adjusted accordingly.

Archive Storage

Archiving is the automated transfer of recordings from Regular storage to Archive storage. Archiving frees up space in the Regular pool to meet retention policies. Archiving is performed after a specified number of days, and can selectively move any combination of continuous, alarm, and motion video. Using Archive storage requires a defined Archive Retention Policy.



Adding a Drive

Adding one or more drives to the Archive pool is identical to and described in the Regular Storage section.

Archive Storage Retention

When configured to use Storage Pools, storage retention policies are based on a per-camera configuration as opposed to Volume-wide settings and Scheduled Tasks. Previous versions of CompleteView using simple Volumes would move video data from a Regular to an Archive volume after a set number of days by creating a Scheduled Task. That video data would then be deleted from that Archive volume after the number of days entered into its Max Video Age setting. The length of video retention was therefore based on the configurations of each of the Volumes on which the data was stored. With Storage Pools, the length of time video data is retained is configured at the camera level, as detailed below.

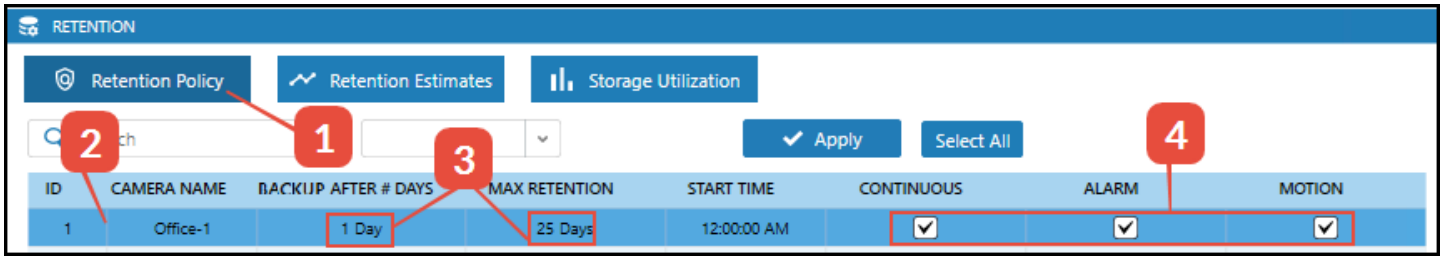
Archive Storage Retention Policy & Behavior

Storage Retention Policy is used for setting minimum and maximum retention limits on a per-camera basis. Minimum Retention sets the minimum number of days a camera's video is stored in the storage pool. Maximum Retention sets the maximum number of days a camera's video is stored. Setting the Maximum Retention creates a point at which deletion of that camera's video begins, regardless of existing free space. Not configuring both Minimum and Maximum Retention settings results in video being stored until the storage location is full, and FIFO (First In First Out) deletion occurs. Detailed retention scenarios are described in the Regular storage section.

Note that the process of archiving video as configured by the Start Time is independent of the process for deletion of expired video as configured by the Max Retention setting, which automatically occurs around midnight. When changing either a Start Time or a Max Retention duration and then saving the setting to the Recording Server, files that meet deletion criteria will be removed.

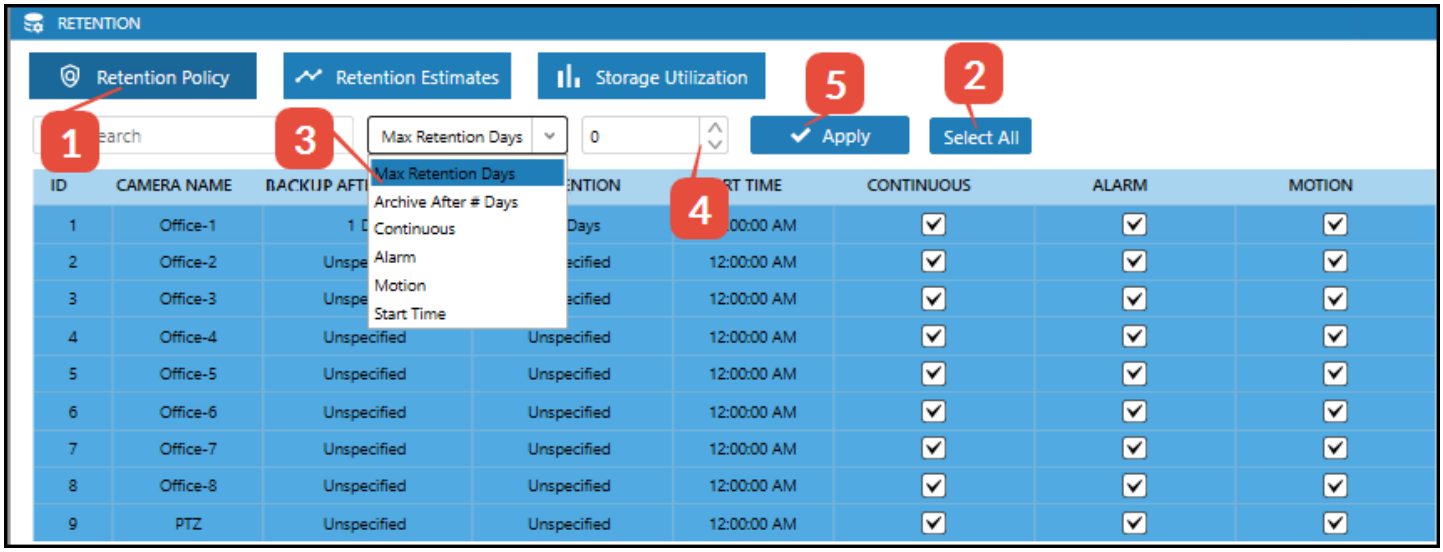
Archive Storage Retention Policy Configuration

The value set for a camera's Regular Minimum Retention policy must be greater than the Archive Storage Archive After # of Days value. If this policy is violated, CompleteView will generate an error message. If left to Unspecified, archiving will not occur.



Steps (for a single camera):

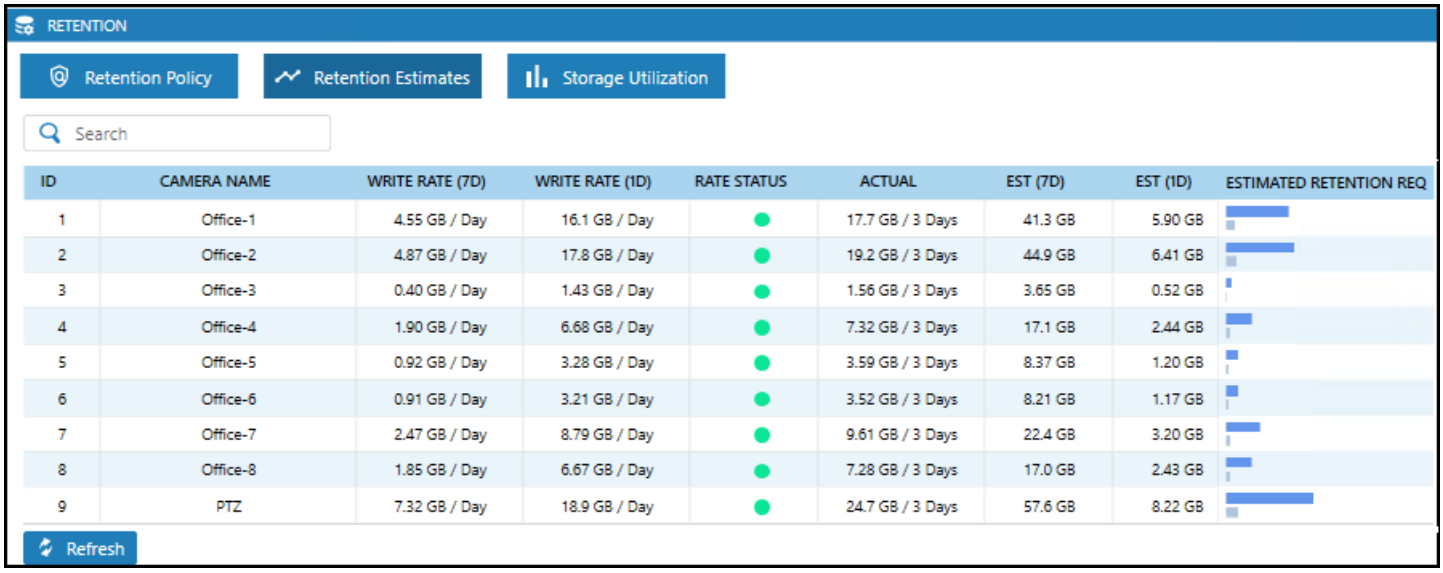
1. Select Retention Policy
2. Select the desired camera
3. Define the Retention (in days)
4. Select the recording type(s)
5. Save the configuration



Steps (for multiple cameras):

1. Select Retention Policy
2. Either use Select All or conventional cntrl/shift+click methods to select the desired cameras
3. Use the dropdown menu to select the desired parameter
4. Use the arrows to select the desired number of retention or archive after days, true/false for a given recording type, and set the start time.
5. Click Apply
6. Save the configuration

Archive Storage Retention Estimates



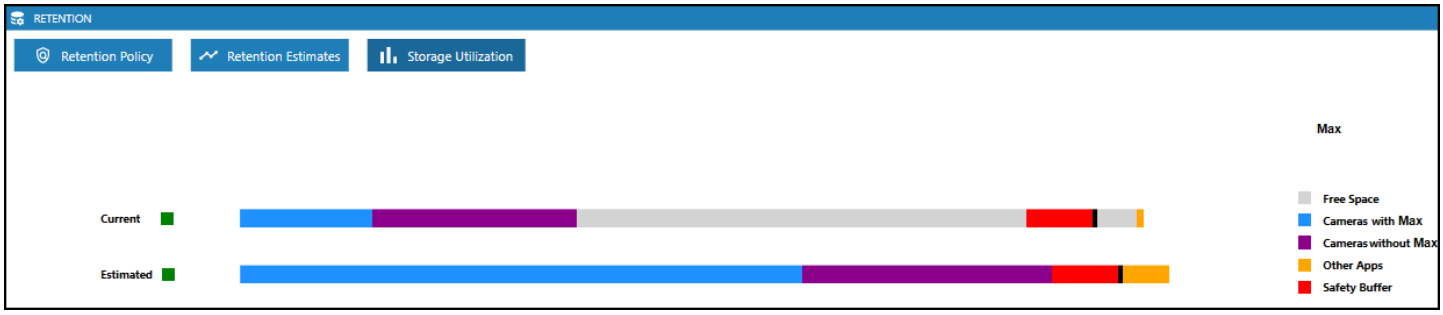
ID	CAMERA NAME	WRITE RATE (7D)	WRITE RATE (1D)	RATE STATUS	ACTUAL	EST (7D)	EST (1D)	ESTIMATED RETENTION REQ
1	Office-1	4.55 GB / Day	16.1 GB / Day		17.7 GB / 3 Days	41.3 GB	5.90 GB	
2	Office-2	4.87 GB / Day	17.8 GB / Day		19.2 GB / 3 Days	44.9 GB	6.41 GB	
3	Office-3	0.40 GB / Day	1.43 GB / Day		1.56 GB / 3 Days	3.65 GB	0.52 GB	
4	Office-4	1.90 GB / Day	6.68 GB / Day		7.32 GB / 3 Days	17.1 GB	2.44 GB	
5	Office-5	0.92 GB / Day	3.28 GB / Day		3.59 GB / 3 Days	8.37 GB	1.20 GB	
6	Office-6	0.91 GB / Day	3.21 GB / Day		3.52 GB / 3 Days	8.21 GB	1.17 GB	
7	Office-7	2.47 GB / Day	8.79 GB / Day		9.61 GB / 3 Days	22.4 GB	3.20 GB	
8	Office-8	1.85 GB / Day	6.67 GB / Day		7.28 GB / 3 Days	17.0 GB	2.43 GB	
9	PTZ	7.32 GB / Day	18.9 GB / Day		24.7 GB / 3 Days	57.6 GB	8.22 GB	

Storage Retention Estimates are intended to provide Administrators with historical and predictive data indicating whether or not adequate storage has been allocated to a given camera to meet the configured minimum retention requirements. Analysis is based on comparing historical averages with current write rates against currently allocated drive space. If the calculated required space is not available, a warning is issued once an hour until enough space is available by either freeing up existing drive space or adding more.

Heading	Data
Write Rate (7D)	The 7 day write rate is the exact amount of data written by the camera in the last 7 days.
Write Rate (1D)	The 1 day write rate is the exact amount of data written by the camera in the last day.
Rate Status	Indicates if the average consumption of storage space based on a camera's write rate falls within current norms. If the 1 day average exceeds the 7 day average, a warning status indicator will be displayed. A write rate increase of 20% will generate a yellow status, while a 40% increase will generate a red status. Note that the status will eventually return to green as the new average becomes the norm.
Actual	Indicates the amount of data written by that camera over the specified number of days.
Est (7D)	Estimated 7 day storage requirements based on historical write rate data, calculated by multiplying the Est (1D) by 7.
Est (1D)	Estimated 1 day storage requirements based on historical write rate data, calculated by divding the total bytes of storage written by the camera by the number of days the camera has been recording.
Estimated Retention Req	The top bar graphically represents the 1 day estimated retention requirements, and the bottom bar represents the 7 day estimated

Heading	Data
	requirements.

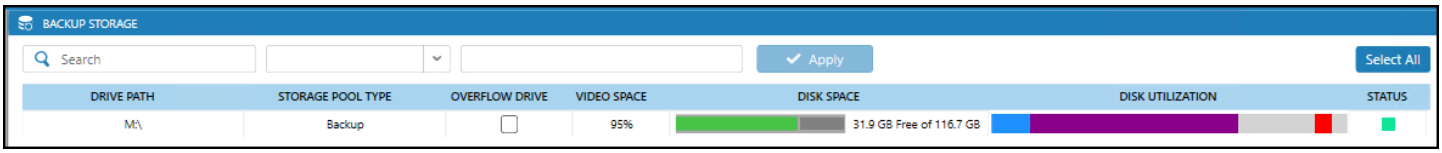
Archive Storage Utilization



Storage Utilization displays a graphical representation of current and estimated storage usage by data type. Rolling over the bars presents either a data type's current or predicted storage usage along with the its color's key information, also available on the right side of the pane. This data allows for a quick visual guide to what types of cameras or apps are utilizing the most and least space so that retention policies may be adjusted accordingly.

Backup Storage

Backup provides a means of redundancy for the Regular pool. Backups can be configured to automatically duplicate continuous, alarm, and motion video from the Regular pool to the Backup pool. Use of Backup storage requires a defined Backup Retention Policy, and writing videos to Backup storage may be configured to take place at the same time as writing video to Regular storage.



Adding a Drive

Adding one or more drives to the Backup pool is identical to and described in the Regular Storage section.

Backup Storage Retention

As with Archive storage, the backup process is cumulative for retention calculation purposes. For example, if a retention time of 30 days is desired, set the camera's Backup Max Retention time to 30 days. If video is backed up from Regular to Backup storage after 5 days and the maximum retention for the camera's video is set for 30 days, the video will be 30 days old from the day of recording before it's deleted, having existed for 5 days in Regular storage then 25 days in Backup.

Backup Storage Retention Policy & Behavior

Storage Retention Policy is used for setting minimum and maximum retention limits on a per-camera basis. Minimum Retention sets the minimum number of days a camera's video is stored in the storage pool. Maximum Retention sets the maximum number of days a camera's video is stored. Setting the Maximum Retention creates a point at which deletion of that camera's video begins, regardless of existing free space. Not configuring both Minimum and Maximum Retention settings results in video being stored until the storage location is full, and FIFO (First In First Out) deletion occurs. Detailed retention scenarios are described in the Regular storage section.

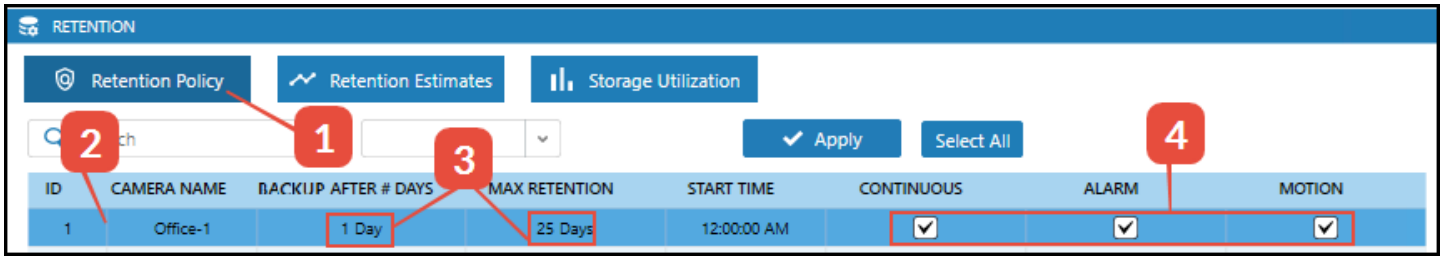
Note that the process of backing up video as configured by the Start Time is independent of the process for deletion of expired video as configured by the Max Retention setting, which automatically occurs around midnight. When changing either a Start Time or a Max Retention duration and then saving the setting to the Recording Server, files that meet deletion criteria will be removed.

Backup Storage Retention Policy Configuration

Backup retention policy configuration is dependent upon the Regular retention policy for a given camera. A camera's Regular Min Retention value must be greater than the Backup policy's Backup After # Days value, and the Backup policy's Max Retention value must be greater than the Regular Max Retention value. CompleteView displays an error message if an invalid configuration is attempted. If Backup After # Days is left Unspecified, backup will not occur.

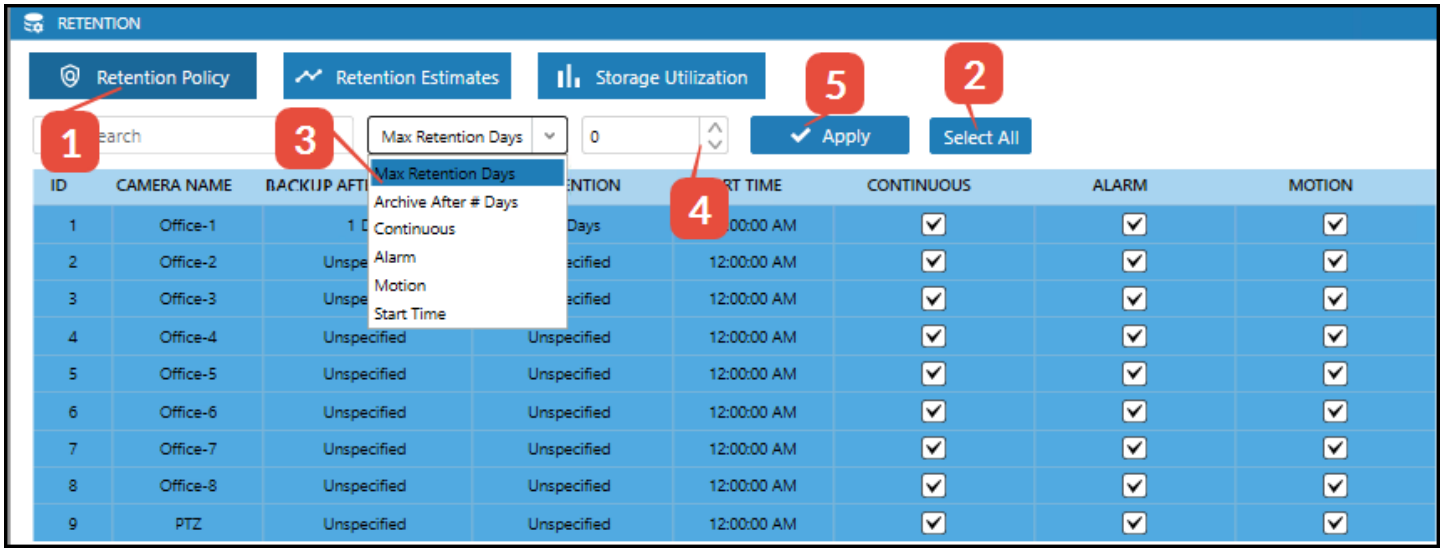
Synchronous Backup

Setting a value of 0 for Backup After # Days will back the camera's video up at the same time as its video is being written to Regular storage, creating a synchronous backup. Time of day does not apply to cameras configured for synchronous backup.



Steps (for a single camera):

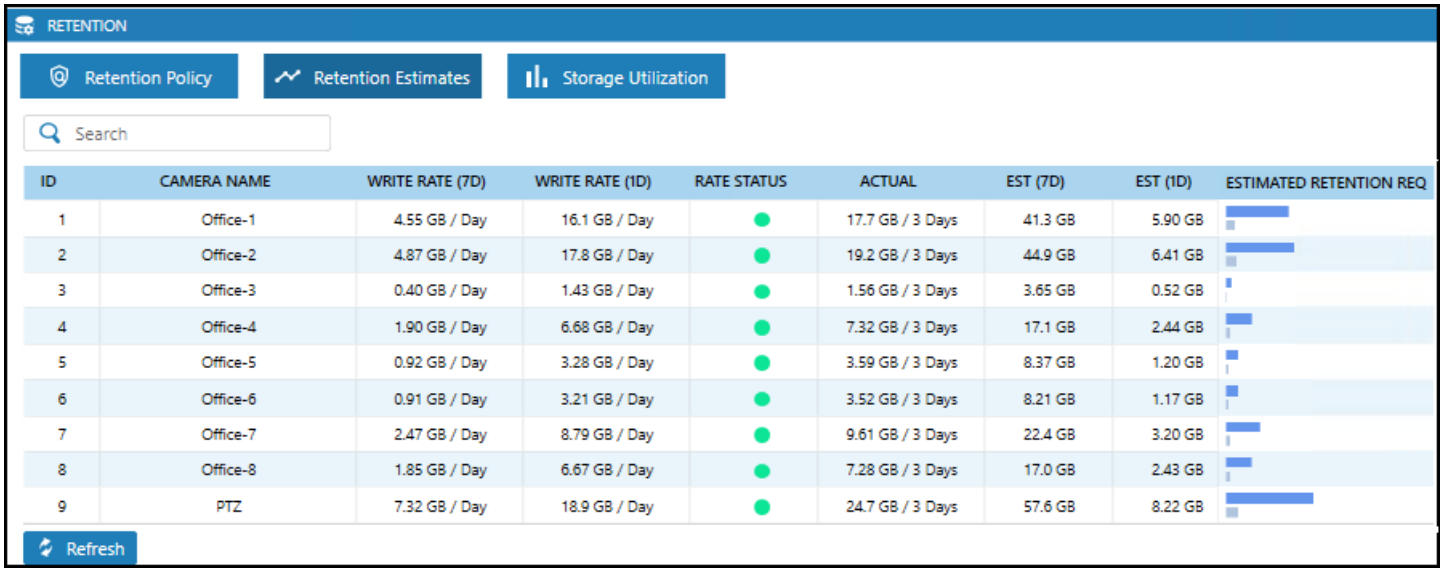
1. Select Retention Policy
2. Select the desired camera
3. Define the Retention (in days)
4. Select the recording type(s)
5. Save the configuration



Steps (for multiple cameras):

1. Select Retention Policy
2. Either use Select All or conventional cntrl/shift+click methods to select the desired cameras
3. Use the dropdown menu to select the desired parameter
4. Use the arrows to select the desired number of retention or Backup after days, true/false for a given recording type, and set the start time.
5. Click Apply
6. Save the configuration

Backup Storage Retention Estimates



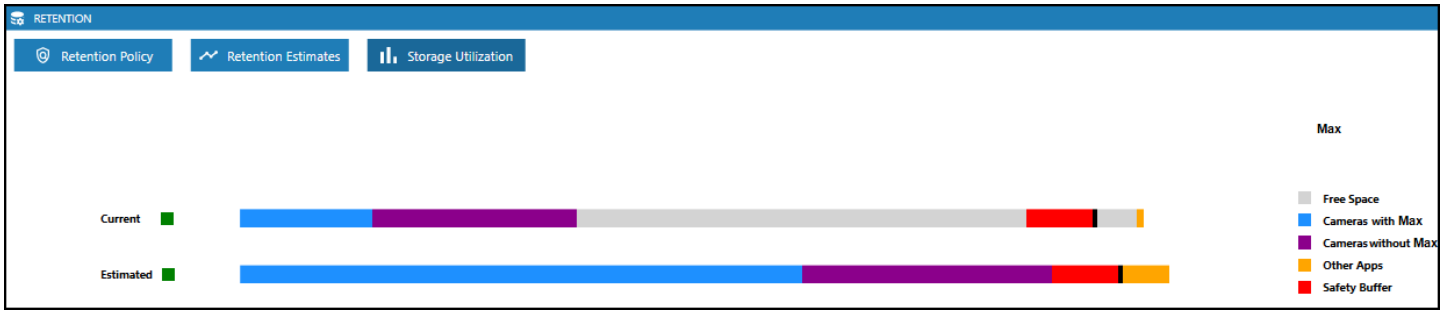
ID	CAMERA NAME	WRITE RATE (7D)	WRITE RATE (1D)	RATE STATUS	ACTUAL	EST (7D)	EST (1D)	ESTIMATED RETENTION REQ
1	Office-1	4.55 GB / Day	16.1 GB / Day		17.7 GB / 3 Days	41.3 GB	5.90 GB	
2	Office-2	4.87 GB / Day	17.8 GB / Day		19.2 GB / 3 Days	44.9 GB	6.41 GB	
3	Office-3	0.40 GB / Day	1.43 GB / Day		1.56 GB / 3 Days	3.65 GB	0.52 GB	
4	Office-4	1.90 GB / Day	6.68 GB / Day		7.32 GB / 3 Days	17.1 GB	2.44 GB	
5	Office-5	0.92 GB / Day	3.28 GB / Day		3.59 GB / 3 Days	8.37 GB	1.20 GB	
6	Office-6	0.91 GB / Day	3.21 GB / Day		3.52 GB / 3 Days	8.21 GB	1.17 GB	
7	Office-7	2.47 GB / Day	8.79 GB / Day		9.61 GB / 3 Days	22.4 GB	3.20 GB	
8	Office-8	1.85 GB / Day	6.67 GB / Day		7.28 GB / 3 Days	17.0 GB	2.43 GB	
9	PTZ	7.32 GB / Day	18.9 GB / Day		24.7 GB / 3 Days	57.6 GB	8.22 GB	

Storage Retention Estimates are intended to provide Administrators with historical and predictive data indicating whether or not adequate storage has been allocated to a given camera to meet the configured minimum retention requirements. Analysis is based on comparing historical averages with current write rates against currently allocated drive space. If the calculated required space is not available, a warning is issued once an hour until enough space is available by either freeing up existing drive space or adding more.

Heading	Data
Write Rate (7D)	The 7 day write rate is the exact amount of data written by the camera in the last 7 days.
Write Rate (1D)	The 1 day write rate is the exact amount of data written by the camera in the last day.
Rate Status	Indicates if the average consumption of storage space based on a camera's write rate falls within current norms. If the 1 day average exceeds the 7 day average, a warning status indicator will be displayed. A write rate increase of 20% will generate a yellow status, while a 40% increase will generate a red status. Note that the status will eventually return to green as the new average becomes the norm.
Actual	Indicates the amount of data written by that camera over the specified number of days.
Est (7D)	Estimated 7 day storage requirements based on historical write rate data, calculated by multiplying the Est (1D) by 7.
Est (1D)	Estimated 1 day storage requirements based on historical write rate data, calculated by divding the total bytes of storage written by the camera by the number of days the camera has been recording.
Estimated Retention Req	The top bar graphically represents the 1 day estimated retention requirements, and the bottom bar represents the 7 day estimated

Heading	Data
	requirements.

Backup Storage Utilization



Storage Utilization displays a graphical representation of current and estimated storage usage by data type. Rolling over the bars presents either a data type's current or predicted storage usage along with the its color's key information, also available on the right side of the pane. This data allows for a quick visual guide to what types of cameras or apps are utilizing the most and least space so that retention policies may be adjusted accordingly.

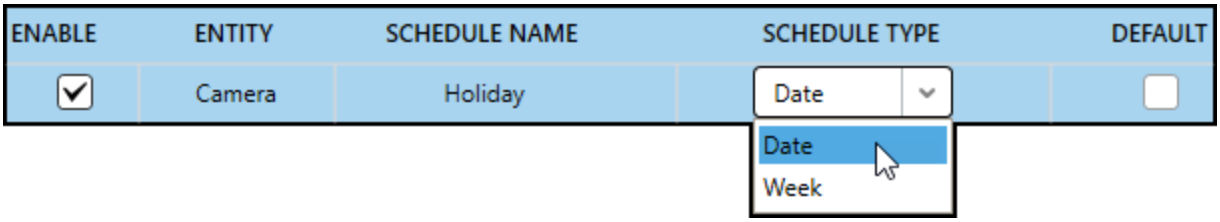
Storage Pool Notifications

Notification	Description
Insufficient Retention (warning)	Warns the user that there is not enough storage to meet the estimated retention requirements.
Write Failed	Indicates a failure to write a video clip or create video folder during write operation.
Delete Failed	Indicates a failure to delete a video clip or video folder during a FIFO, Expiration, or Archive process.
Free Pool Space Failed	Indicates that the FIFO was unable to clear enough space in the pool to continue to record. On a properly configured system, indicates a catastrophic failure.
Storage Threshold Met	Warns the user that the total free space of the pool has fallen below the user defined percentage.
Minimum Camera Retention Active	FIFO is deleting video from cameras with a minimum retention policy defined. This does not indicate that a minimum retention policy has been violated.
Minimum Retention Violation	FIFO is deleting video data from cameras with a minimum retention defined and the established policy of ‘n’ days has been violated.
Pool Drive Offline	Pool drive offline will be sent when an active drive in a pool goes off-line, indicating the Recording Server can no longer see the drive.
Pool Drive Online (normal)	Follows a Pool Drive Offline alert. Pool drive online will be sent when a previously offline pool drive becomes active, indicating the Recording Server can see the drive again.
Overflow Drive Active	Sent when any camera is writing to an overflow drive in the Regular pool.
Overflow Drive Inactive (normal)	Follows an Overflow Drive Active alert. Sent when the system stops writing to an Overflow drive to a Regular, non-overflow drive.

Recording Servers Schedules & Home Presets

The Schedules Panel is used to set up recording schedules for video and PTZ Home Presets. If the existing Client does not have any PTZ presets or PTZ cameras, then the Home Preset Schedule should remain blank.

Each Recording Server hosts its own schedule for recording video and Home Presets. Up to four Home Presets per camera can be configured to go to the home position at schedule times.



Schedule Types

There are two schedules types. The appearance and menu options of the schedules will change to match the selected type. All schedules begin at midnight (00:00).

Type	Description
Date	Sets a schedule for one day
Week	Schedule for any group of days in a given week, including Saturday and/or Sunday.

Schedule Visuals

The color on the timeline represents the intended action, and the duration of the colored timeline represents when the action is supposed to occur. The absence of color anywhere on the timeline indicates that no action is to be taken for the hours and minutes where the color is missing. The action could be video recording or a Home Preset. Recording of the video is identified by colors that are associated with four recording types. A quick visual inspection should allow easy understanding of the types and duration of the various schedules.

Recording Color Code

The colored schedule buttons are named to indicate the recording type they represent. Different situations will require different recording schedule configurations.

A Word About Pre-Alarm

Because motion events can be extremely short, Pre-Alarm helps to add enough information to each motion event so that the event can tell its story in full. Pre-recording is unique because it records continuously for a set period (in seconds) and adds the pre-recording to a motion or alarm recording as if it were part of the original motion or alarm event. Pre-Alarm shortens the total recording time when

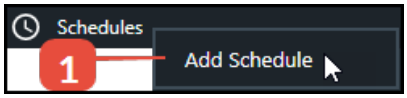
compared to continuous and motion or continuous and alarm. Pre-Alarm must be configured to work with each camera with which it's associated. Pre and Post-recording are found by selecting a camera, then selecting the Recording panel.

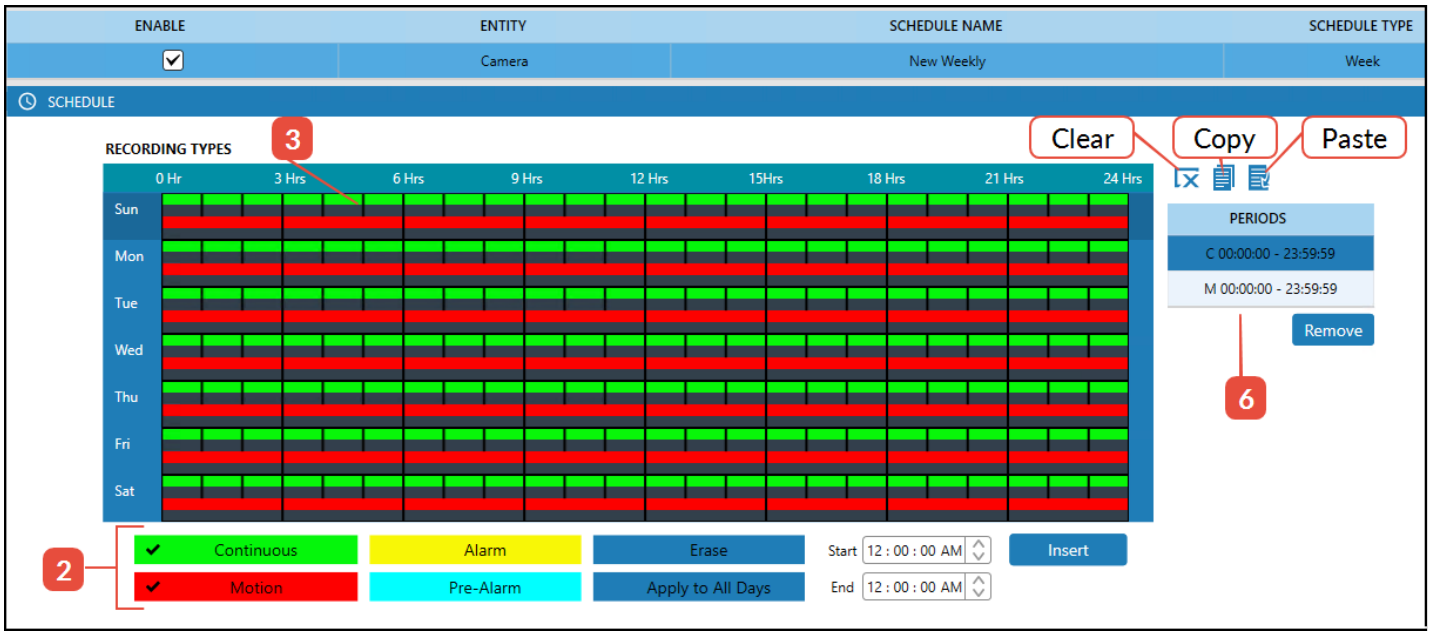
Configuring a camera with a (5) five-second Pre-Alarm and the camera captures a three (3) second Motion event would result in a total recording duration of nine (9) seconds for the entire motion event. CompleteView adds a default unchangeable post-motion recording of one (1) second to all motion events.

Pre-Alarm and Continuous Record may not be selected simultaneously for the same schedule. Continuous Recording may be set to record in parallel with alarm or motion, and during playback, the user may filter-out the continuously recorded video and review only motion or alarm recordings.

Add an Everyday Recording Schedule

Steps:





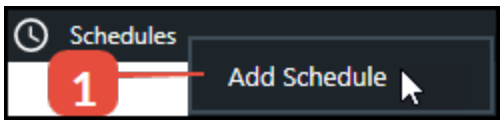
1. Right-click on Schedules and select Add Schedule (Week Schedule, if prompted)
2. Click on the desired recording type(s) or Home Preset, so they display a checkmark
3. Either use your mouse pointer and drag it from left to right across the timeline in order to enable the desired recording for the entire day **or** manually enter the Start and End times and click Insert. Manually entering the start and end times allows for more precise configuration.
4. **Alternatively**, different recording types may be placed at different hours of the day by selecting the recording type and dragging the mouse pointer across the desired time or manually entering the start and end times.
5. **Alternatively**, you may also copy a day's schedule and paste it to another day.
6. Configured recording periods are shown in the table to the right of the timeline and may be sorted and removed.
7. Check the boxes to associate cameras to the schedule. Variations in schedules for individual

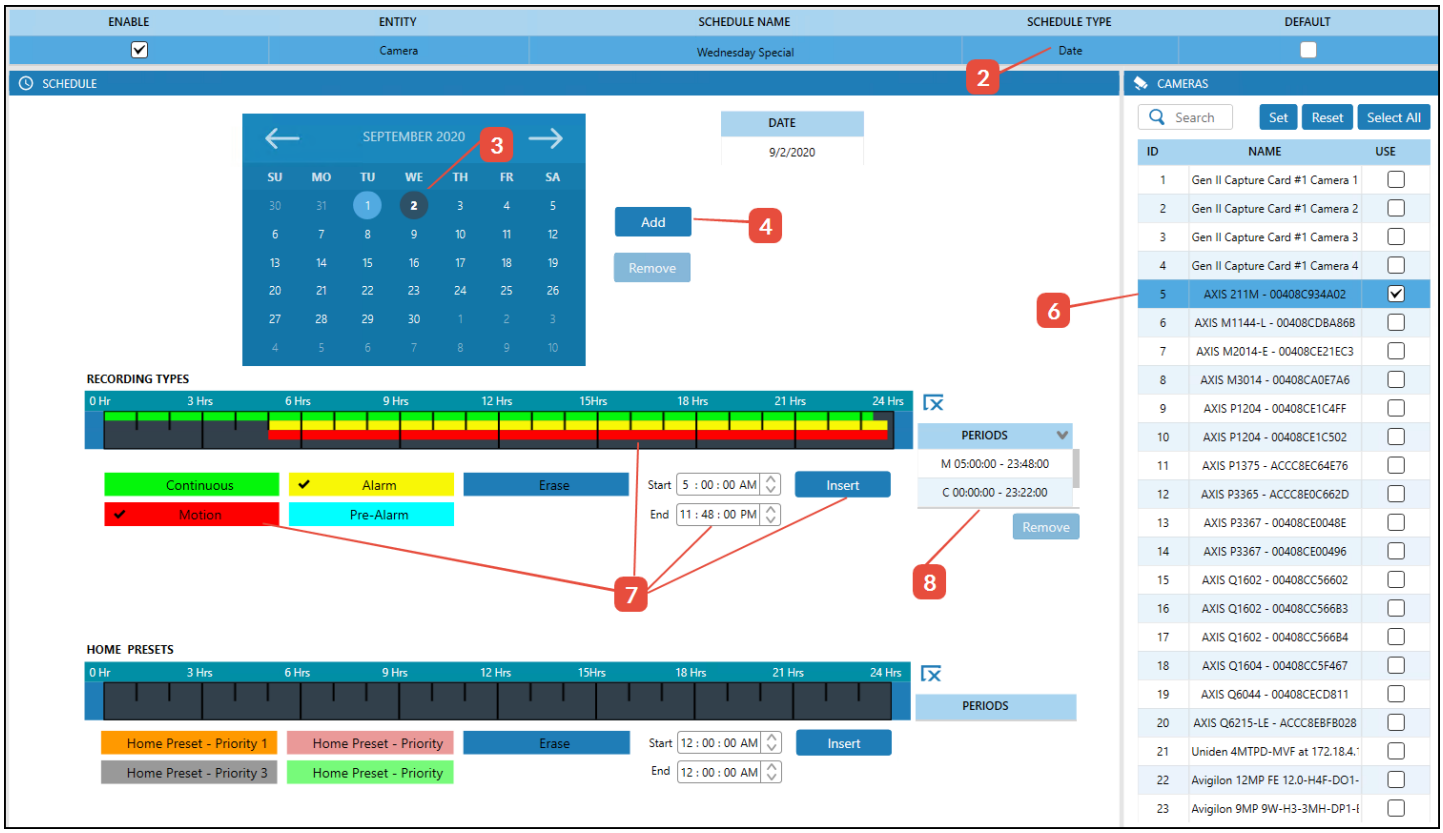
cameras will require the creation of separate schedules for the affected cameras.

8. Save the configuration

Remember If Pre-Alarm is selected, be sure to set the Pre-record time in the Camera's Record Panel for each affected camera and save the configuration when completed.

Create a Date Schedule





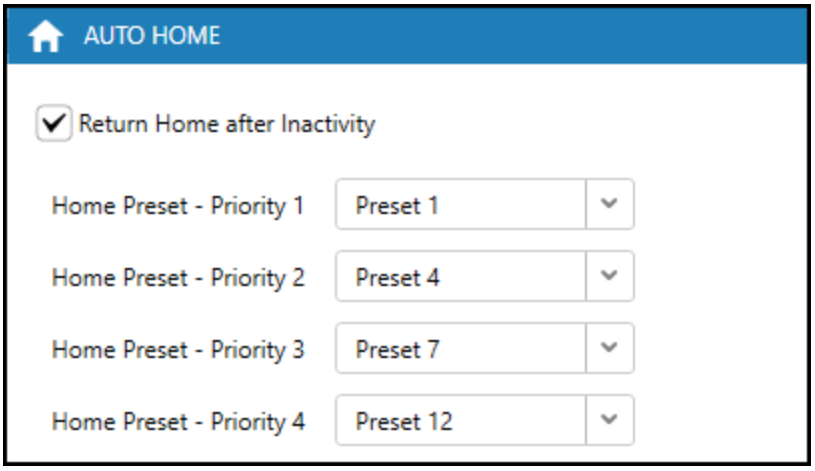
1. From the server pane, right click on Schedules, Select Add Schedule
2. Select Date from in the Schedule Type pull-down menu
3. When a calendar appears, select year, month, and day
4. Select Add
5. The date should appear in "Date" area, above and to the right of the Add button
6. Select the cameras for which the Date Schedule should apply
7. Add the desired recording type (color the timeline) with the mouse pointer
   a. Click on the colored bar(s) that represents the desired recording type
   b. Drag your mouse pointer from left (0 hrs.) to the right (24hrs) across the timeline to fill all 24 hrs. Mouse movement must be from left to right!
   c. Alternately, manually enter in the Start and End times, and click Insert. This method allows for greater precision when creating the schedule.

8. Recording periods are displayed to the right of the timeline, may be sorted, and removed.
9. Save the configuration when the schedule is complete

Home Presets

Home Presets enable the Administrator to send the same PTZ camera to as many as four different Home (Preset) Position at four different scheduled times. The feature sends a PTZ camera Home after the inactivity-time has expired.

Configure a Four (4) PTZ Home Presets Schedule



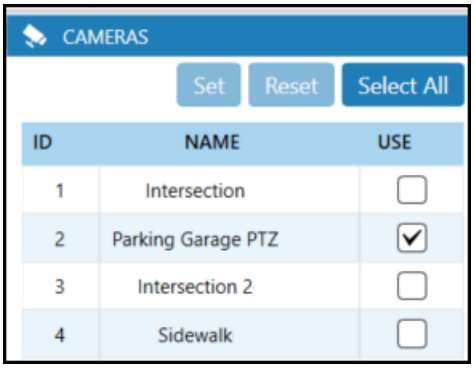
1. Select a Server
2. Select a PTZ camera
3. Select the PTZ panel
4. In the PTZ Settings Panel create up to four different PTZ positions. Up to four positions are supported as home positions.
5. Set the Inactivity Time in seconds
6. Use the menu to enter the desired PTZ positions in the four Home Preset locations
7. Save the configuration
8. Go to the same server's schedules configuration to configure a schedule for the home presets.

Set a Schedule for Home Positions

Note: Two home positions cannot occupy the same hours on the schedule.

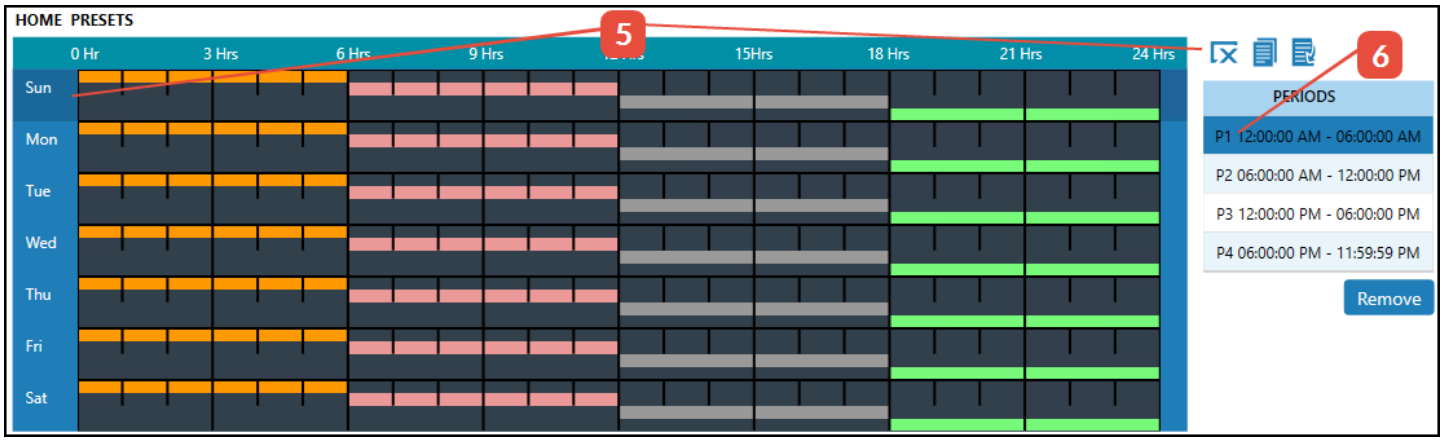
The illustration below shows how four different Home Presets should be scheduled for a single camera, with each Home Preset scheduled for a different period. If a second camera is required, then a second schedule should be configured for the second camera.

Start by selecting to which camera(s) the Home Preset schedule should be applied. Home Preset schedules are only applicable to PTZ cameras.



1. Schedule the hours of each day that the desired camera should return to Home 1
   a. Select the desired Home preset button with a checkmark
   b. Using your mouse, drag left to right to fill the timeline for Home 1 **or** manually enter the Start and End times, and click Insert
   c. As required, repeat step b as needed for Home 2-4
2. Ensure that Home Preset schedules do not overlap each other
3. Save the configuration when the schedule is complete

Delete a Home Preset Schedule



1. Select the Home Preset button so that a checkmark is on it
2. Select the erase button so that a checkmark is on it
3. Position your mouse pointer on the far left end of the home preset color you wish to erase in the timeline
4. Hold the left mouse button, and draw the pointer from left to right across the color to erase
5. Alternatively, select a day on the schedule, and select the clear icon to clear the presets for that day (select Apply to All Days to clear the entire preset schedule).
6. To delete just one preset period, select the day, the period from the table to the right of the timeline, and click remove.
7. Save the configuration

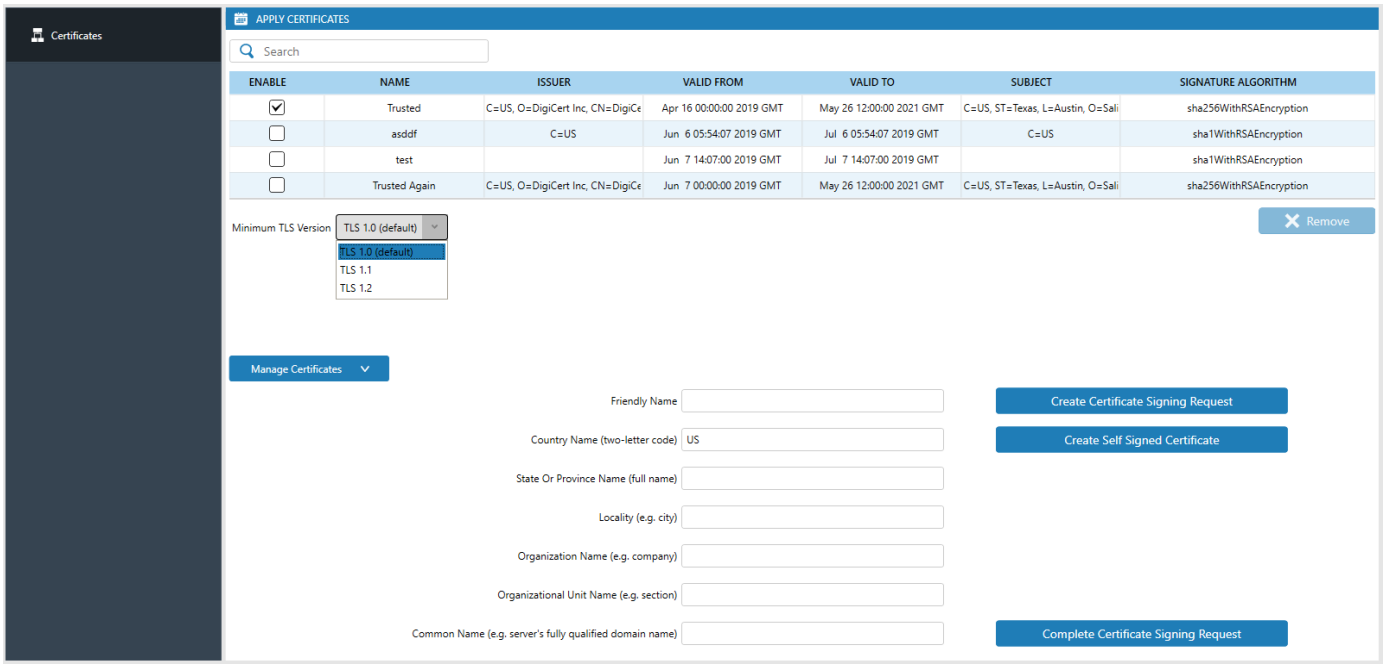
Security Settings

Security protocols may be implemented system-wide from the Common Settings Security screen, or per individual Recording Server. Recording Servers share similar settings with those located in Common Settings. Settings changed at the Common Settings level will be applied to all Recording Servers in the deployment, while Settings changed at the Recording Server level impact only that specific Recording Server.

Overview

CompleteView contains facilities for secure web-based communications via HTTPS. To be used properly these security facilities require local, per site management of digital certificates. This section of the manual deals with the practicalities of creating and configuring both self-signed certificates and certificates from a certificate authority. For more information, see **Digital Certificate Management and More.**

A digital certificate must be enabled on each Recording Server that will employ secure (HTTPS) web-based video streaming.



Note that the Minimum TLS version is selectable per Recording Server, but not from the Management Server.

Create Self Signed Certificate

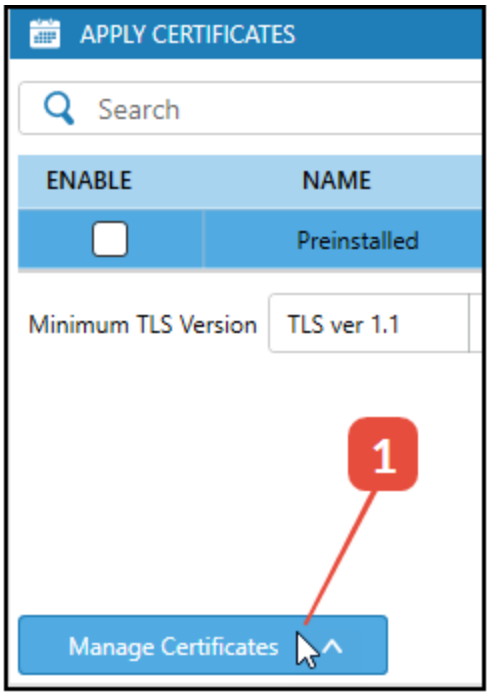
CompleteView comes with a pre-installed certificate, which has a number of limitations that should preclude its use in a production environment. First, it is formally associated with the CompleteView Recording Server, and not the site-specific server on which it resides and for which it is to serve as credentials. Second, it is self-signed as opposed to coming from a certificate authority.

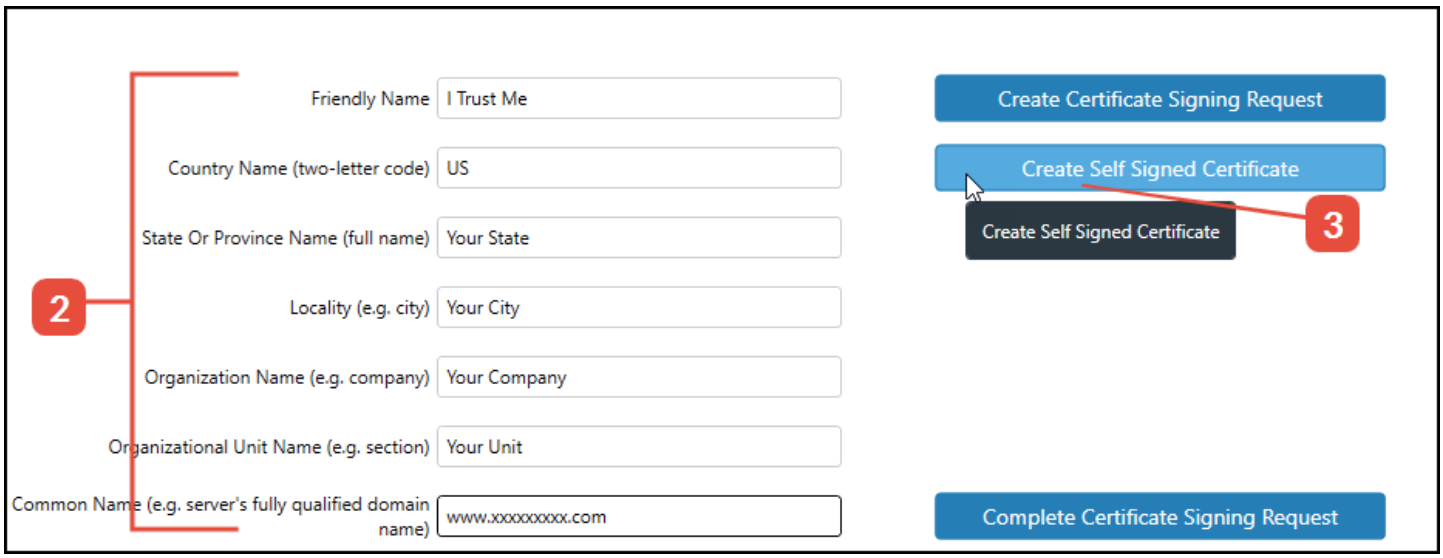
CompleteView supports the quick creation of a certificate that suffers only from the second of these limitations.

While logged into the Desktop Client, select the Configure module. Either select Common Settings or the desired Recording Server, select Security, then click the Manage Certificates button near the bottom of the window. It is recommended that you fill in all fields with reasonable values, except possibly the organizational unit name (which is commonly omitted in certificates). For the common name (the

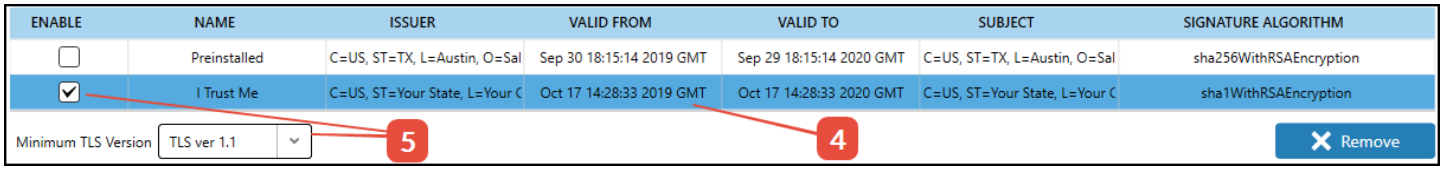
last field), it is important that you use the name by which the server will be accessed over the web. Enter a friendly name for the certificate. This value is used merely to distinguish among the certificates managed by CompleteView. Any string is legal, though it is recommended to avoid the empty string and to generally keep the friendly names distinct and recognizable. Click Create Self Signed Certificate when done, and Save the server configuration.

1. At the bottom of the Apply Certificates window, click on Manage Certificates.
2. Enter the proper information in the fields.
3. Click the button labeled Create Self Signed Certificate.





4. Your Self-Signed Certificate will be visible in the certificate list.
5. Select Enable and set your Minimum TLS version with the drop-down menu.
6. Save the Configuration.



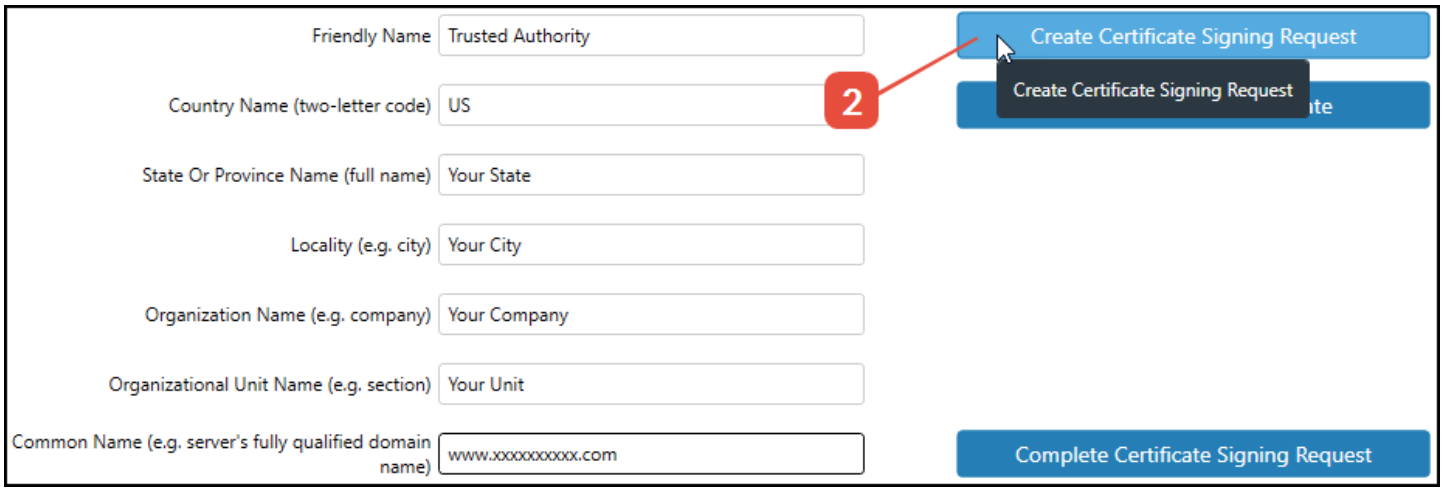
Create Certificate Signing Request for Certificate Authority

Note that Signing Requests may only be generated from within CompleteView for individual Recording Servers, and not via Common Settings.

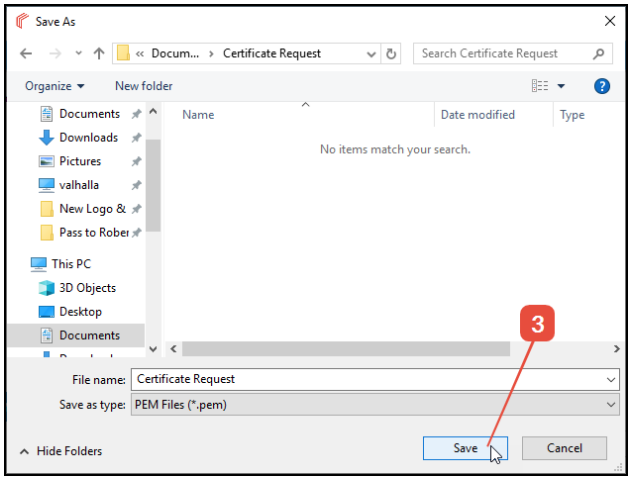
Self-signed certificates tend to scale poorly, and are deemed inadequate in most security-conscious environments. CompleteView provides support for creating and using a certificate signed by an external certificate authority.

While logged into the Desktop Client, select the Configure module. Select the desired Recording Server or Common Settings, select Security, then click the Manage Certificates button near the bottom of the window. It is recommended that you fill in all fields with reasonable values, except possibly the organizational unit name (which is commonly omitted in certificates). For the common name (the last field), it is important that you use the name by which the server will be accessed over the web. Enter a friendly name for the certificate. This value is used merely to distinguish among the certificates managed by CompleteView. Any string is legal, though it is recommended to avoid the empty string and to generally keep the friendly names distinct and recognizable.

1. Repeat steps 1-4 for Creating a Self-Signed Certificate.
2. Click the button labeled Create Certificate Signing Request.

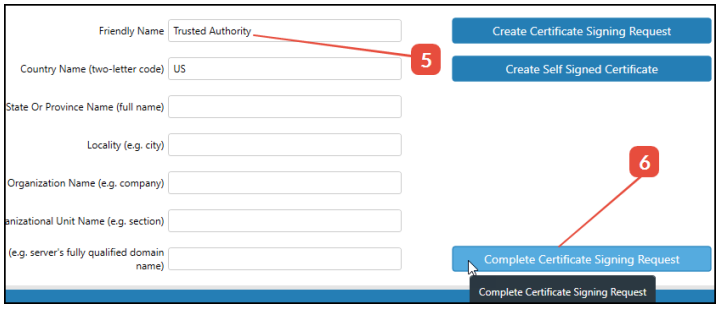


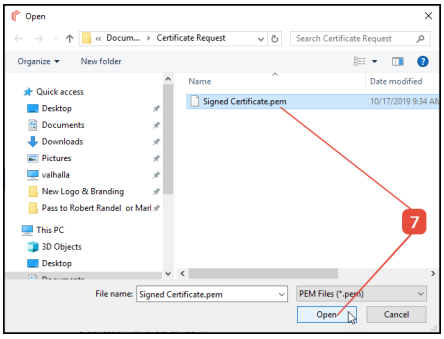
3. Specify a name and location to save the .PEM file.
4. Upload or e-mail the .PEM file you saved to the certificate signing authority.



After your certificate authority has returned the "PEM" file:

5. Enter the Friendly Name that you chose for your Certificate Signing Request.
6. Click on Complete Certificate Signing Request.

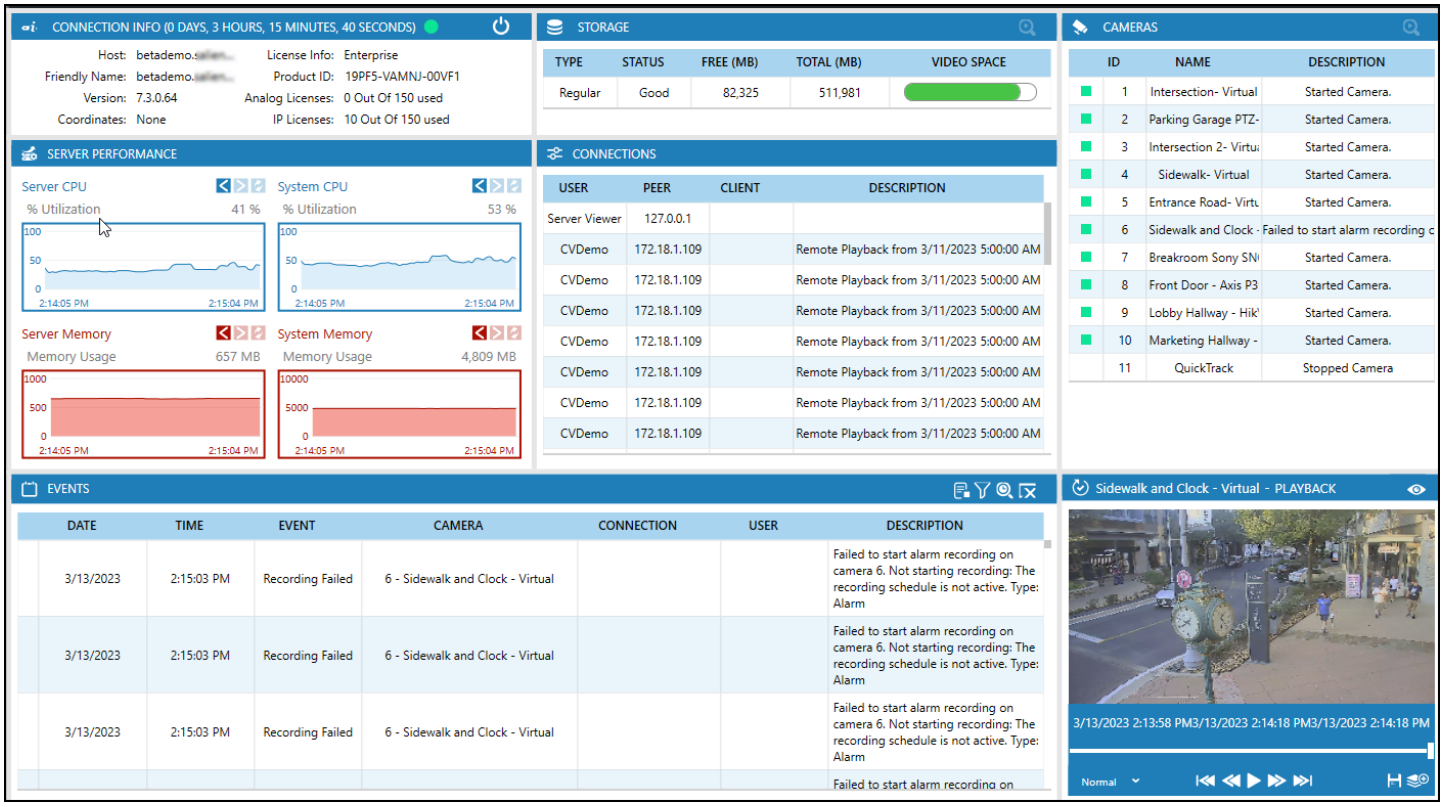




7. Navigate to the .PEM file returned by your signing authority and click open.
8. The certificate will populate in the certificates list.
9. Save the configuration.

Recording Servers Info Panels

Many of the informational panels for the Recording Server are identical to those found in the Dashboard.



For information about the Server Info/Title Bar, Click Connection Info Panel.

For information about the Storage Panel, Click Storage Pool Introduction.

For information about the Server Performance panel, Click Server Performance Panel.

For information about the Connections Panel, Click Connections Panel.

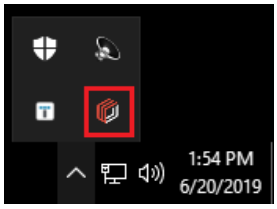
For information about the Events Panel, Click Events Panel.

For information about the Cameras Panel, Click Cameras Panel.

Recording Server Viewer

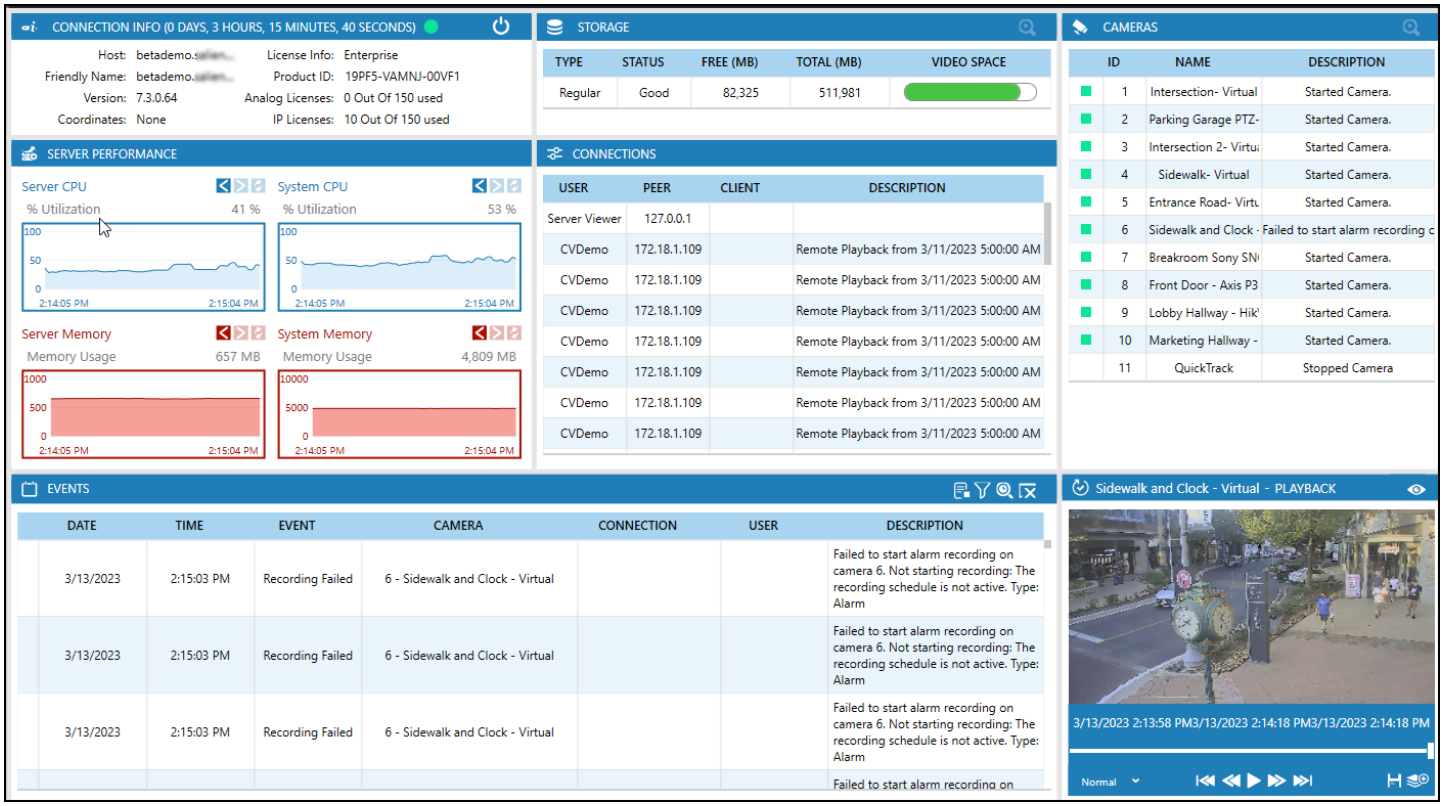
The Recording Server Viewer provides real-time monitoring of the local Recording Server's cameras, volumes, system, connections, and events. Its functionality is similar to Recording Servers Info Panels contained within Configuration.

The Recording Server Viewer is installed during the Recording Server installation process, and resides in the Windows System Tray.



The information displayed pertains only to the local Recording Server, and is refreshed per user session.

For more information about the individual panels, see the links below.



For information about the Server Info/Title Bar, Click Connection Info Panel.

For information about the Storage Panel, Click Storage Pool Introduction.

For information about the Server Performance panel, Click Server Performance Panel.

For information about the Connections Panel, Click Connections Panel.

For information about the Events Panel, Click Events Panel.

For information about the Cameras Panel, Click Cameras Panel.

NVR Introduction

CompleteView is capable of interfacing with select models of Hanwha (Samsung) and HikVision NVRs (Network Video Recorder) and DVRs (Digital Video Recorder)*. CompleteView can access both live and recorded NVR video. NVR support is available only in Pro, Enterprise and Trial editions. *Note: Hereafter, both devices will be referred to collectively as “NVRs”.

Currently Supported NVRs & Functionality Limitations

The list below reflects currently supported NVRs with their known functional limitations. Consult the latest Supported Hardware List, located at:

https://www.salientsys.com/support/supported-cameras/

Make/Series/Model	Limitation
HikVision DS-7716NI-SP/16	Currently limited to one (1) playback connection. No Export.
HikVision DS-76xx Series (DS-7604, DS-7608, DS-7616)	Currently limited to one (1) playback connection. No Export
HikVision DS-6700 Series (DS-6704, DS-6708, DS-6716)	No Export.
Samsung SRN-x73S Series (SRN-473S, SRN-873S, SRN-1673S)	SRN-x73S is limited to a maximum of three (3) users. Note: Samsung uses RTSP port 558 as opposed to CompleteView's port 554.

Search & Playback

The following apply only to video recorded to an NVR, and not to video recorded to a CompleteView server by a camera associated with an NVR. See the NVR Storage Option section for more detail.

Clip Search on NVRs is not filtered by events. All clips are returned within the time period specified by the search parameters regardless of what filters are selected.

Some lag may be evident seeking video.

Playback at any other speed than 1X is inconsistent at present.

Multi-channel playback is currently disabled for all NVRs.

Stressing the seek by holding down the left or right arrow (auto repeat) may hang Playback, and force the user to re-load the clip.

Smart Search is not supported.

There is no size information (file size) reported for clips stored on a NVR.

Thumbnail search is not currently supported.

NVR Licensing

Every 8 channels of an NVR count up to one IP license if the NVR Storage Option is set to Store on NVR.* If the Storage Option is set to VMS Volume, every channel will use an IP license.

*Does not apply to Hikvision encoders.

When adding a new camera/NVR channel to the server configuration, the IP license will be consumed based on the number of channels already configured. If cloning an NVR channel with storage option set to NVR and all IP licenses are consumed, cloning is allowed if all 8 channels haven't been added. This licensing applies to the following models:

Hikvision	Samsung
DS-7604NI-SE/P	SRN-1673S
DS-7608NI-SE/P	SRN-473S
DS-7616NI-SE/P	SRN-873S
DS-7716NI-SP/16	

Consult the current **Supported Cameras List** for the most updated information.

The license restriction is applied as follows:

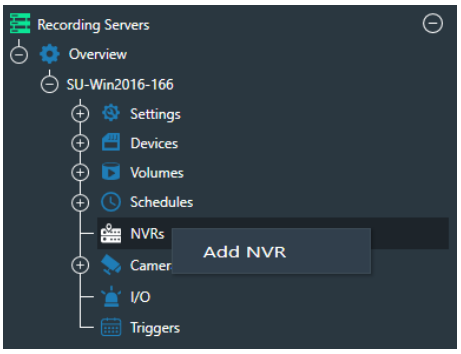
- An error message will be displayed when adding a new NVR if the license edition is Cloud or One.
- If a Recording Server configuration file that has NVRs already configured is loaded on to a Cloud or One server:
  - The server will not load the NVRs
  - An "Info" event with a warning message will be logged to the diagnostic logs (logging level must be Info or higher)
  - Cameras configured as NVR channels will no longer be associated with any NVRs. If the storage option was set to NVR only, it will be reset to VMS volume
  - Recording Server will not list any of the NVRs, and cameras will behave like regular IP cameras. IP model will remain unchanged
  - All of the above changes are made to the server's copy of the configuration in memory. The configuration file itself will not be modified unless a save configuration action takes place
- If an archived configuration file that includes NVRs is loaded in the Recording Server configuration, the NVRs will be listed, but when the configuration is saved and pushed to the server the server will perform the same actions as above. Reloading the configuration will remove the NVRs

NVR & CompleteView Setup

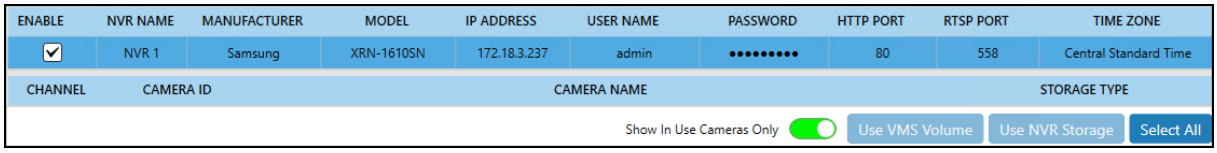
Configuration of recording schedule, settings, disk management, and backup are performed by the user using the NVR manufacturer's supplied interface.

Configuring CompleteView for use with the NVR

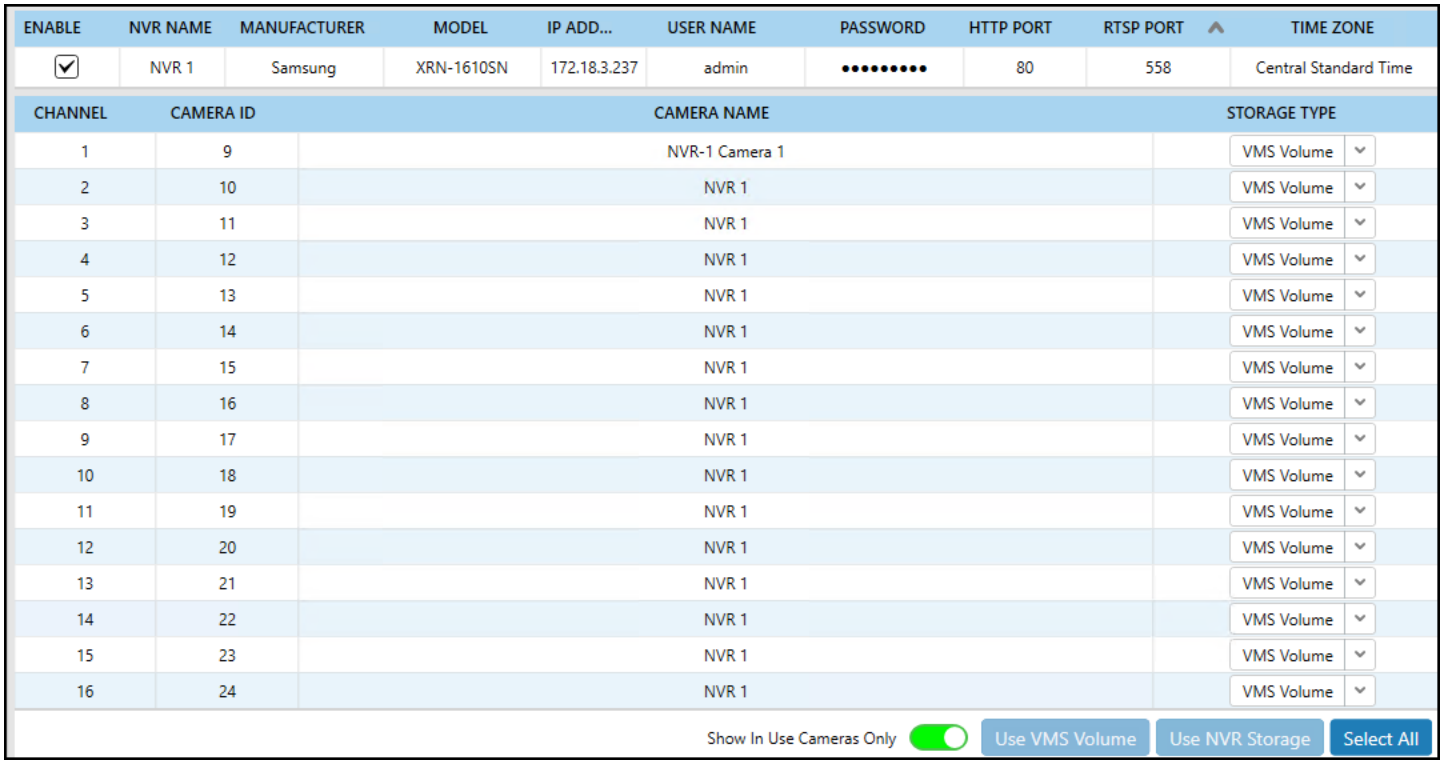
Initial configuration of the NVR and its associated cameras is to be done in accordance with the manufacturer's directions. Once configured, launch the CompleteView Desktop Client, log in, select the Configure Module, expand the Recording Server to which the NVR will connect, right click on the "NVRs" menu tree, and select "Add NVR".



Name the NVR if desired, select the Manufacturer, Model, enter IP Address, verify the HTTP and RTSP ports, then enter the appropriate credentials and select the NVR's time zone. Save the configuration when finished. Port settings configured on the NVR will be applied to its cameras.



Note that the number of channels for a given NVR are determined by that model's capabilities. A four channel NVR will have four accessible channels in CompleteView, a sixteen channel NVR will have 16, etcetera. Note that the screen below will appear after the NVR's cameras have been added to CompleteView, as detailed below.



ENABLE	NVR NAME	MANUFACTURER	MODEL	IP ADD...	USER NAME	PASSWORD	HTTP PORT	RTSP PORT	TIME ZONE
☑	NVR 1	Samsung	XRN-1610SN	172.18.3.237	admin	•••••••••	80	558	Central Standard Time

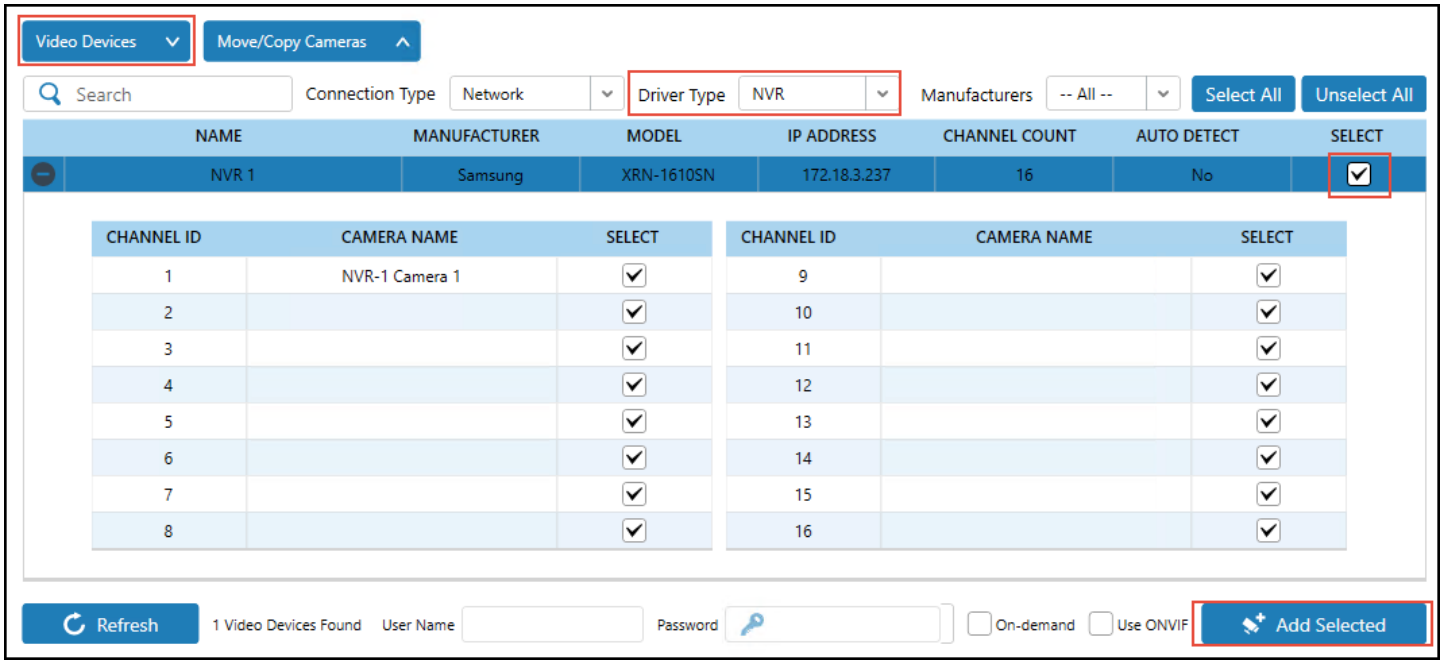
CHANNEL	CAMERA ID	CAMERA NAME	STORAGE TYPE
1	9	NVR-1 Camera 1	VMS Volume
2	10	NVR 1	VMS Volume
3	11	NVR 1	VMS Volume
4	12	NVR 1	VMS Volume
5	13	NVR 1	VMS Volume
6	14	NVR 1	VMS Volume
7	15	NVR 1	VMS Volume
8	16	NVR 1	VMS Volume
9	17	NVR 1	VMS Volume
10	18	NVR 1	VMS Volume
11	19	NVR 1	VMS Volume
12	20	NVR 1	VMS Volume
13	21	NVR 1	VMS Volume
14	22	NVR 1	VMS Volume
15	23	NVR 1	VMS Volume
16	24	NVR 1	VMS Volume

Show In Use Cameras Only | Use VMS Volume | Use NVR Storage | Select All

From this screen, all or specified cameras may be configured to use either VMS or NVR storage volumes, discussed below. Either use the “Select All” button and choose either “Use VMS” or “Use NVR Storage,” or select the desired volume camera by camera from the dropdown menu and save the configuration.

Adding the NVR’s Cameras to CompleteView

After successfully configuring and adding the NVR, adding cameras works similarly to adding non-NVR cameras in CompleteView. Still in the Configure module, click on “Cameras,” and select “Video Devices”. Select “NVR” as the Driver type, and click “Select” to select all cameras from the new NVR. Optionally, expand the NVR's camera list by clicking the + icon, and manually select which cameras to add. Enter a Camera Name, if desired. Finally, click “Add Selected.” The credentials from the added NVR should automatically grant access to the attached cameras.



NVR Storage Option

CompleteView presents two options for recording video from NVR cameras; VMS Volume or NVR Storage.

If VMS Volume is chosen, the video data is stored on the CompleteView server and behaves much like video data coming from any camera not associated with an NVR. The CompleteView server is capable of taking over stream processing as with other cameras whose on-camera capabilities are not natively supported by CompleteView. Scheduling for the video stream is configured on the CompleteView server as with any other camera.

If NVR Storage is chosen, the video data is stored on the NVR. Search filters within the Video Client such as motion or alarm event recording searches are not available, and the video can only be searched by a given time range. Currently, video stored on Hikvision NVRs is not available for export, while Samsung NVR video export is supported.

After selecting the Storage Option, save the CompleteView configuration. Note that the credentials, IP address, etcetera, auto populate from the configured NVR.

Changing NVR Parameters in CompleteView

Changes on the NVR to the NVR IP Address, HTTP port and RTSP port are echoed to cameras automatically via software, and are done within the NVR branch of the Recording Server, where the NVR was initially added.

Changes to credentials (username & password) are echoed to cameras automatically via software.

Changes to the storage options are echoed to cameras automatically via software.

Changing the Manufacturer of a configured NVR will sever the link between the cameras and the NVR instance. Only the Storage Type option of the associated camera(s) will change (to VMS Volume). The IP Address, HTTP & RTSP port and credentials will remain intact.

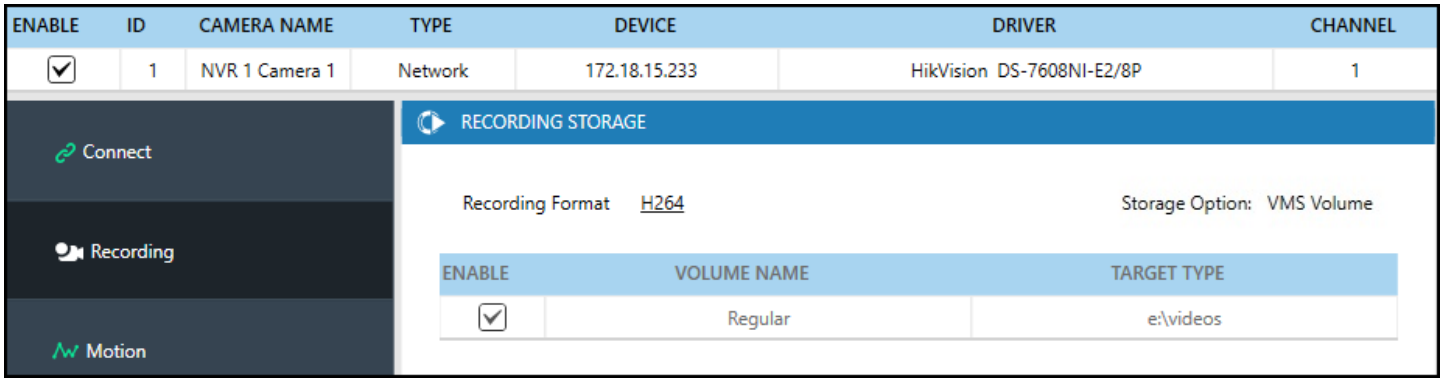
Changing the Model will sever the link of any camera that no longer falls in the range of channels. Otherwise, the existing configuration is maintained.

NVR Camera Recording Status

NVR camera recording status is reported similarly to other cameras in the Recording Server.

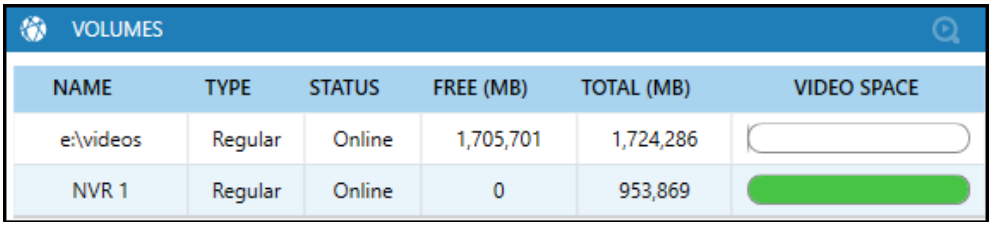
NVR Volume Recording NVR Volume Recording + Video Signal Lost VMS Volume Recording

The camera's storage setting and recording format may be viewed in the Recording pane of the selected camera.



NVR Volume Status

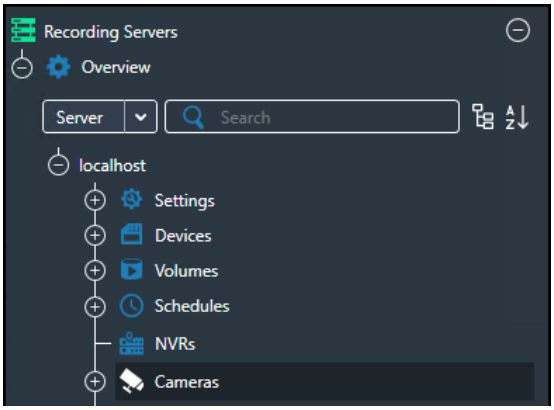
NVR Volume status is reported similarly to other video volumes in the Dashboard.



Recording Servers Cameras

Cameras Overview

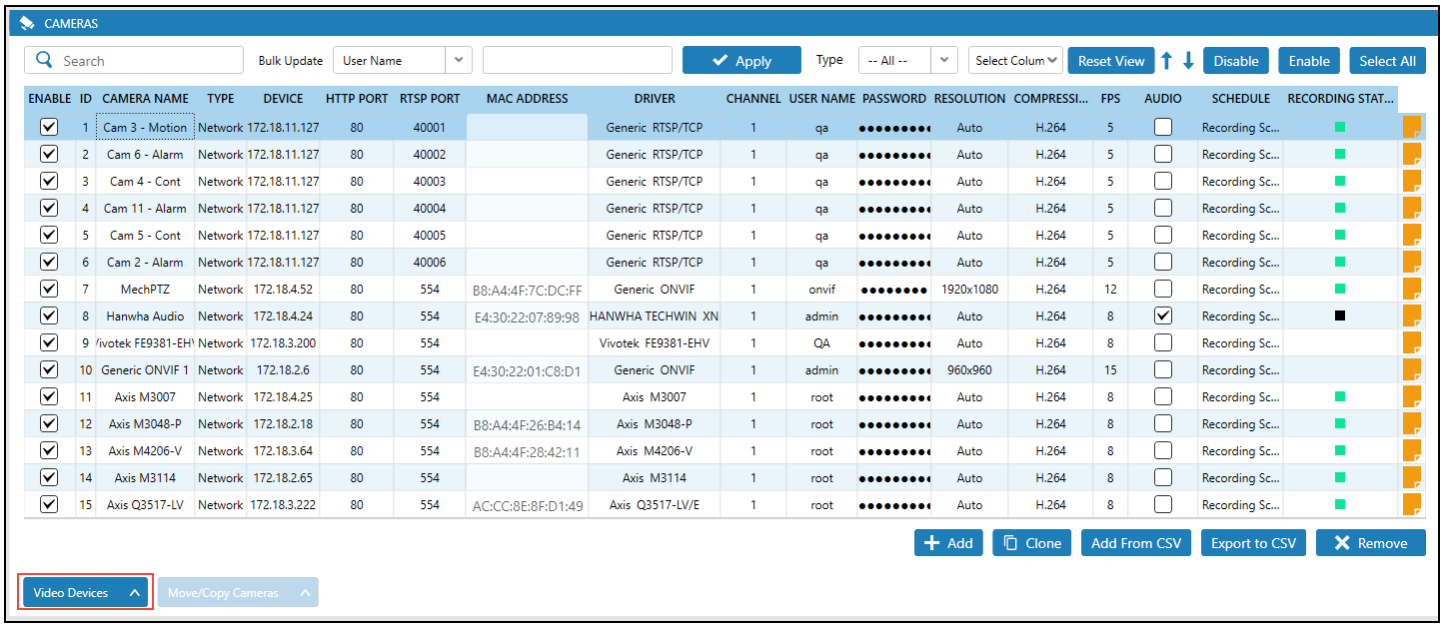
Cameras are installed on and recorded to a specific Recording Server. Some changes to device parameters may be made from the Camera Overview panel. Complete configuration may be done by selecting the specific camera from the Navigation Pane and using the camera configuration panels.



Discovering Video Devices

Clicking the Video Devices button outlined below launches a Camera Discovery sub-panel. The Video Devices panel displays cameras, capture cards and encoders that have been discovered, but are not yet added to a Recording Server. Discovery takes place using Universal Plug and Play or other protocols which must be active on the device.

When the discovery panel is closed, the Video Devices button is found at the bottom left corner of the Camera Settings Panel.



Cameras Overview Select Columns

Visibility of available data columns in the Cameras Overview pane may be selected or deselected via the Select Column dropdown menu.

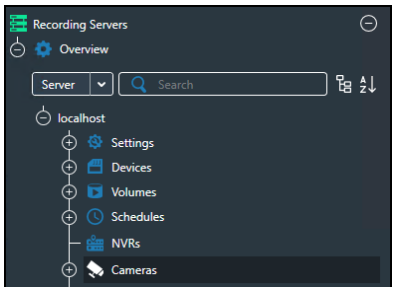
Adding a Camera (or other Video Device) Automatically

Note that any applications intended for use on a given camera should be installed and configured on the camera before adding it to CompleteView.

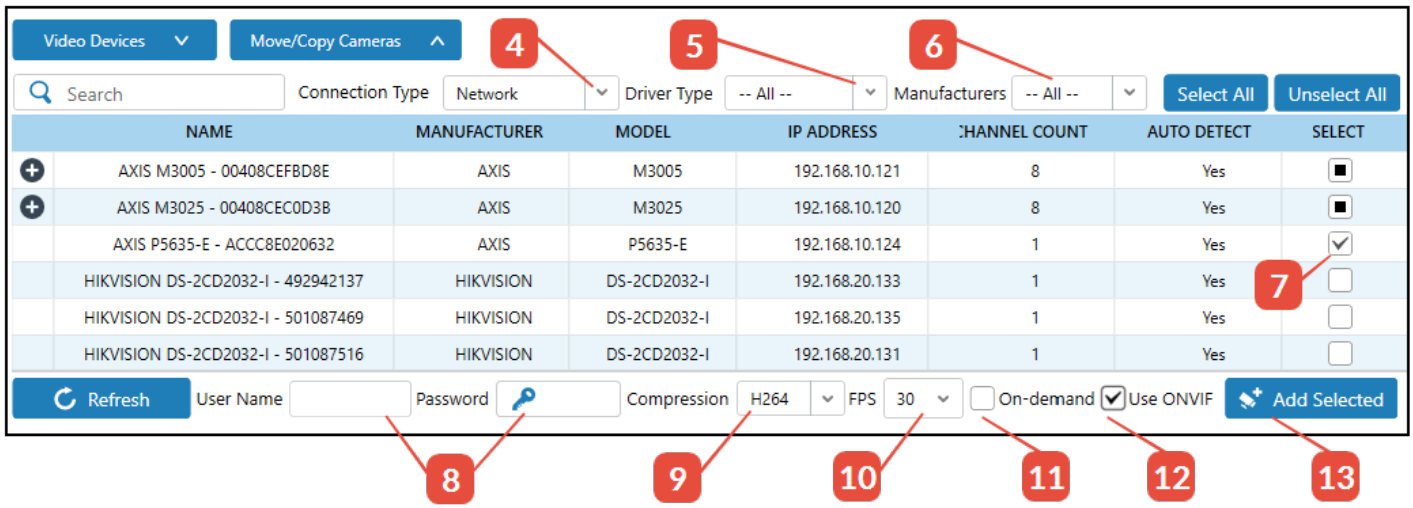
Steps:

Steps:

1. In the Recording Servers Panel, select the Recording Server that you wish to add cameras to.
2. On the Recording Server tree, select the Cameras Node
3. In the bottom left corner of the camera panel, select Video Devices. A pop up list will appear.



4. Select Network as the connection type, if necessary
5. Select the appropriate driver type, or leave as All



Note: For the Driver Type, IP single refers to a single CCD sensor, IP multi refers to multiple CCD sensors in a single camera (typically found in 360° or 180° cameras). IP NVR refers to Samsung, HIKVision and other NVR integrations.

6. Select device Manufacturer (scroll through the list)
7. Scroll through the list of devices and check the Select box
8. From the bottom toolbar, enter the device's credentials
9. Select the appropriate compression
10. Select the frame rate
11. Optionally, select On demand (On demand is useful for low bandwidth networks, but is not recommended in typical deployments. If selected, the video stream from the cameras will not be recorded.)
12. Select Use ONVIF to use that driver (preferred configuration). See the following ONVIF section for more detail.
13. Press the Add Selected button
14. Save the configuration

After addition, the camera name may be changed by clicking in the Camera Name field in either the Overview or individual camera's configuration page and entering in a new name. Camera names are limited to 80 characters.

Importing and Exporting .CSV Lists of Cameras

CompleteView has the ability to import and export groups of cameras to/from from a .csv file.

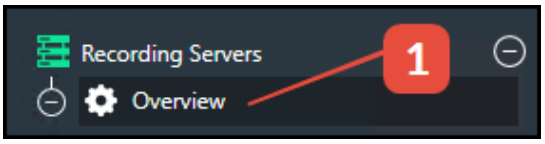
Name	IP Address	Manufacturer	Model	Channel Count	Channel	User Name	Password	Compression	FPS	On-Demand	RTSP Port	Image Path	Stream Processing	DVD	DFT
Camera 1	172.18.2.43	Axis	P3353	1	1	root	pass	H264	8	No	554		Yes	Yes	Yes

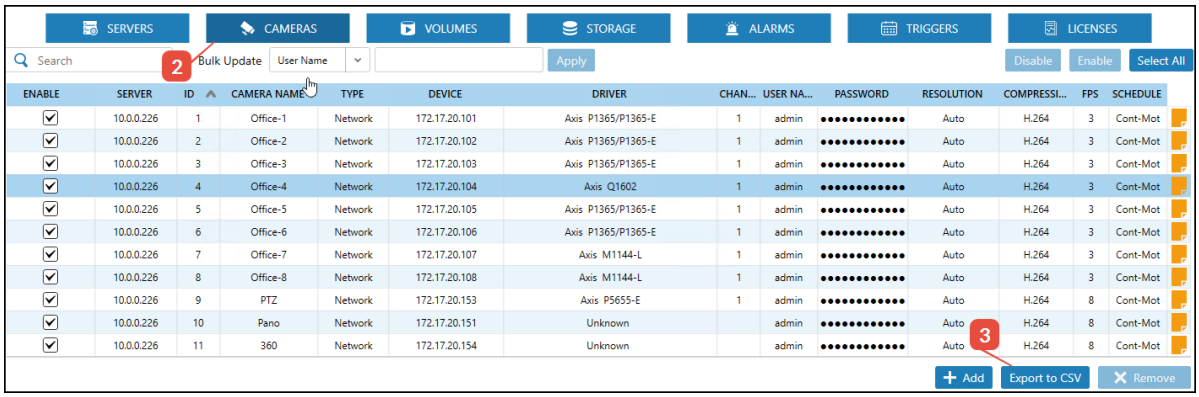
For more information, see the Creating a CSV Camera Import File Job Aid video at:
https://support.salientsys.com/knowledgebase/training-resources/

Exporting All Cameras in a Deployment

Use this method to generate a .csv file that lists all cameras connected to all Recording Servers in a deployment as well as information about the various Recording Servers. **Note:** Since this list contains Recording Server information along with the camera data, it cannot be imported back into CompleteView.

Steps:



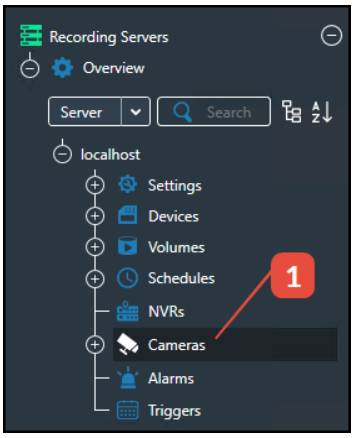


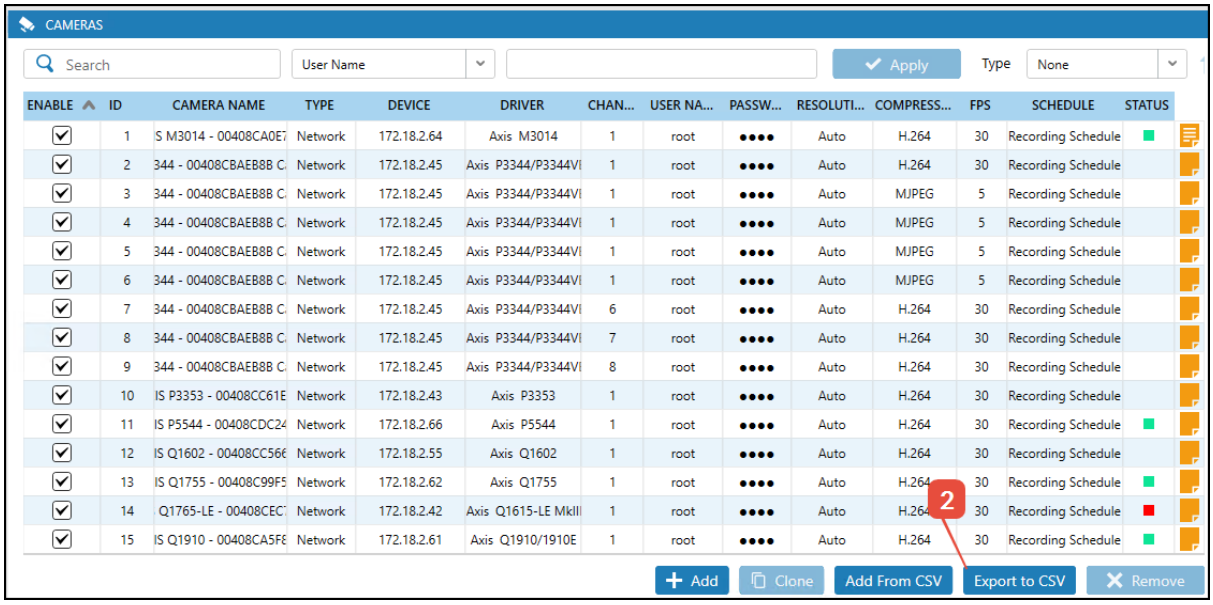
1. Select Overview under Recording Servers
2. Select the Cameras menu option
3. Select Export to CSV and save the file

Exporting a Single Recording Server's Cameras

Use this method to generate a .csv file listing all cameras attached to a single Recording Server. This file is valid for importation, and can be used as a backup or when setting up a new or replacement Recording Server.

Steps:





1. Select the Cameras node under a given Recording Server
2. Select Export to CSV and save the file
3. A confirmation prompt will appear asking "include password as plain text." Select Yes if the list is to be imported into a Recording Server, and either Yes or No if the list isn't meant to be used for importation. The plain text credentials will be sent to the cameras, alleviating the need for the administrator to manually type them in.

Importing a Single Recording Server's Cameras

Select the Cameras node from the Recording Server as above, select Add from CSV and select the file. The cameras will auto-populate after the file is finished loading.

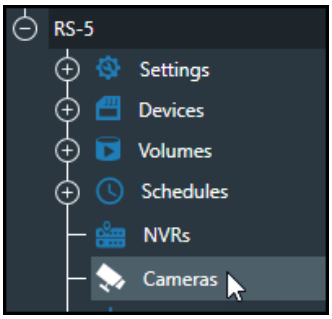
For more information, see the Adding Camera with CSV Job Aid video at:
https://support.salientsys.com/knowledgebase/training-resources/

Analog Capture Cards

CompleteView only supports Generation-Two (stretch) capture cards. Legacy servers (CompleteView 4.X and earlier) with first Generation capture cards will be supported if the Legacy server is added as a Legacy Server to the CV Client. First generation Capture Card drivers will reside on host Legacy Servers. Generation Two capture card drivers are added to the Client when the Recording Server is installed.

Analog Capture Card Discovery and Camera Addition

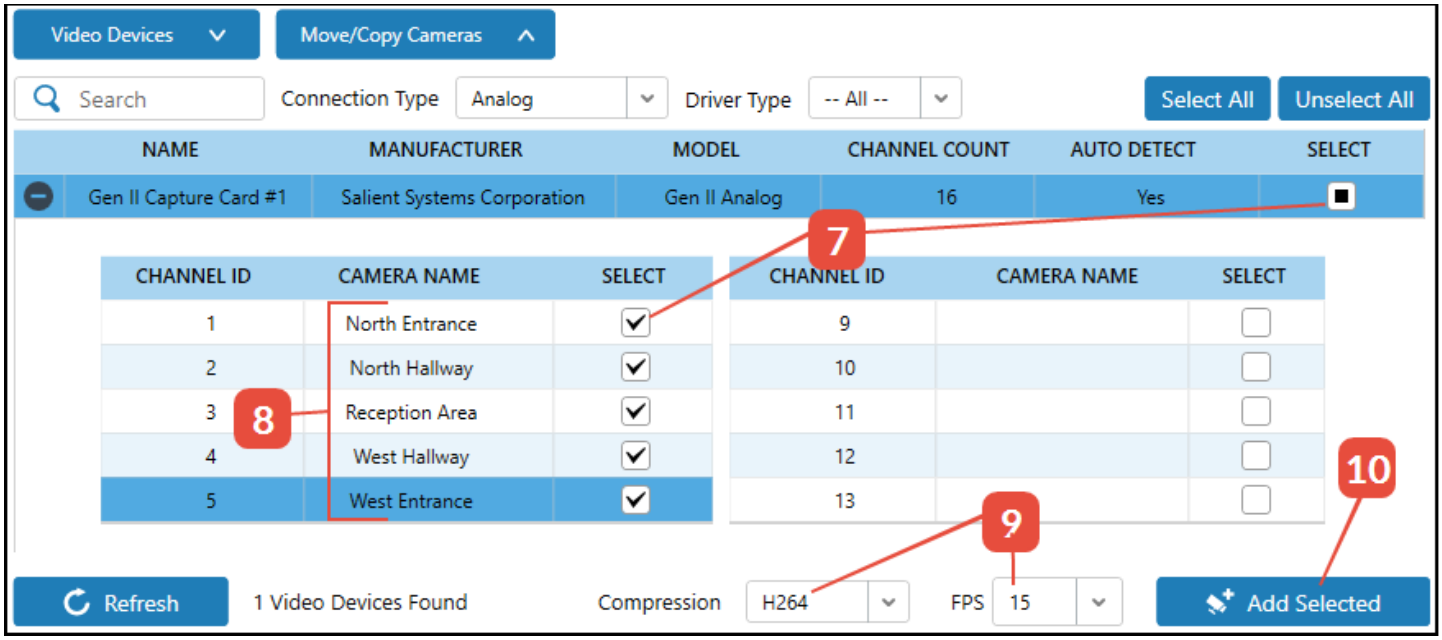
Steps:



1. In the Recording Servers Panel, select a Recording Server that contains a capture card
2. Select the Cameras Node
3. In the camera overview screen, look to the bottom left and select the Video Devices button

4. Select Analog as the connection type
5. In the devices to add list, locate the capture card
6. Select the ⊕ icon to view the capture card channels

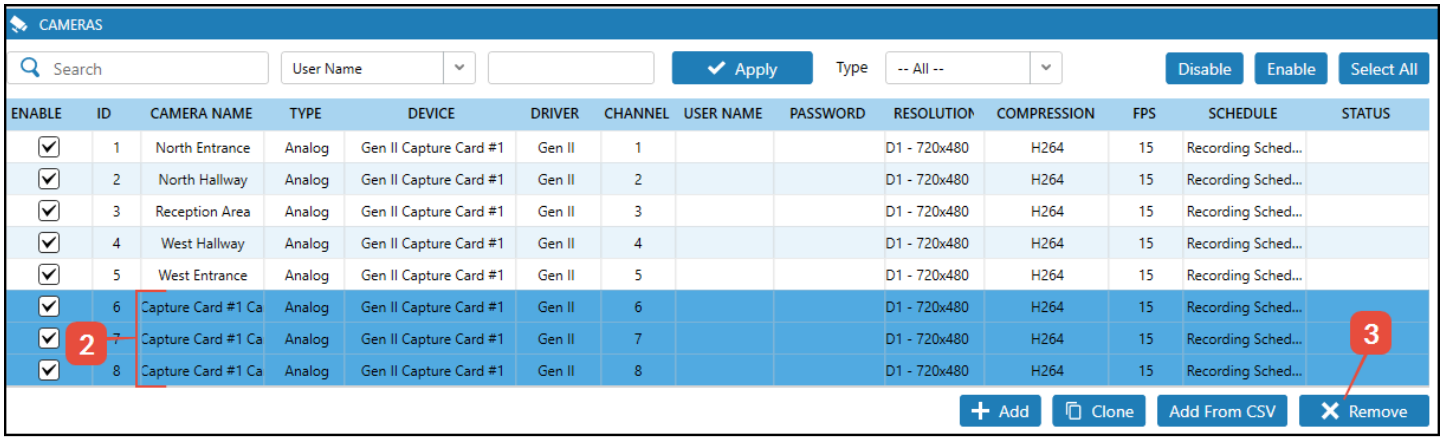
7. In the channel list, select the channels that are connected to cameras; alternatively, if all channels will be added, choose the select all button.
8. Recommended - select the camera name area and enter in a short, but meaningful name, for each camera
9. Select the capture card Compression and frames per second (FPS)
10. Press the Add Selected button
11. Save the configuration



Remove Unused Analog Channels

Unused capture card channels may be removed if they are not to be used.

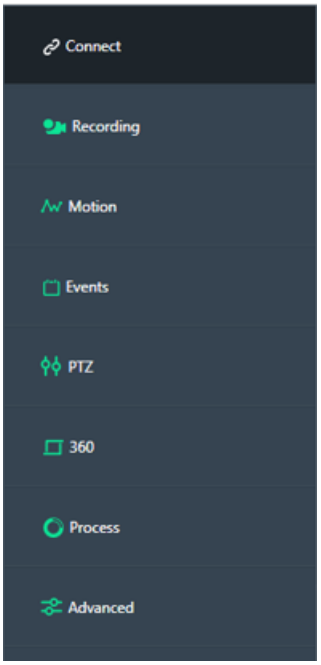
Steps:



1. Hold down the shift key on the keyboard
2. Select the unused capture card channels
3. Select Remove
4. Review your selection
5. Confirm the decision to remove the channels
6. Save the configuration

Camera Menu

After successfully adding a camera or other video device, it may be configured via the Camera Menu, shown below. Each menu will be discussed in its own subsequent section.

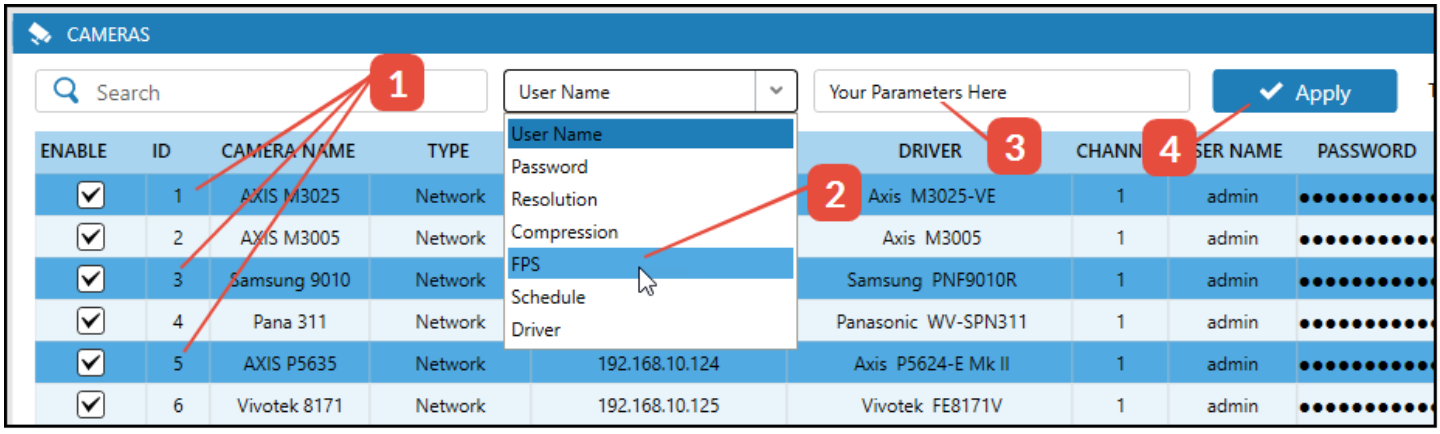


Changing Video Device Parameters

Frame rates, usernames, passwords, resolution, and compression for all cameras may be changed by:

1. Selecting the cameras - multiple cameras may be selected using shift+click or ctrl+click. Selection will be indicated by darker blue bars.

2. selecting the parameter from the drop-down
3. entering the desired information in the blank field
4. Select Spply
5. Save the configuration.



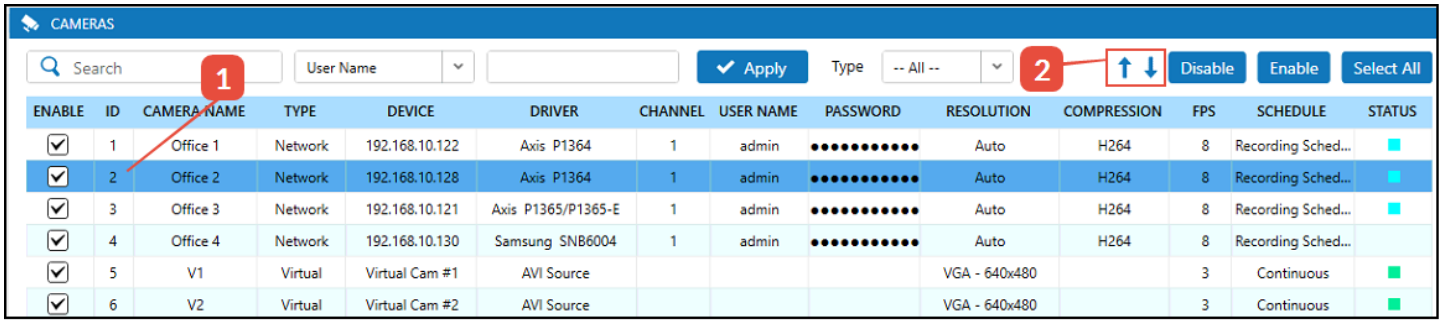
Refer to [Desktop Client Navigation and Functionality] for more information on Bulk Updates.

Reorder Cameras

If desired, cameras me be moved up or down in the list. Note that the Camera ID will change to reflect the camera's new position in the list. First, select the desired camera, next, select either the Move Up or Move Down arrow, then save the configuration.

Steps:

1. Select the desired camera from the cameras list
2. Select either the Move Up or Move Down arrow until the camera is in the correct position
3. Save the configuration.



Note: Reording cameras may disrupt 3rd party integrations such as access control systems which rely on specific camera IDs for functionality. In addtion, access to previously recorded video will be lost.

ONVIF Configuration

CompleteView conforms to the ONVIF media profile S standard, including configuration of video and audio streaming, PTZ, event handling, and device discovery. ONVIF is the preferred method of camera connectivity in CompleteView.

Before adding a camera to CompleteView using ONVIF, verify that the camera is ONVIF profile S compliant by visiting https://www.onvif.org/conformant-products/ and searching by profile, manufacturer, and model.

It is worth noting that while many ONVIF compatible cameras come pre-configured with ONVIF media profiles which are required for use with CompleteView, some do not. Those cameras will have to be configured with profiles and other options before use. Specifically, an ONVIF user must be created on the camera, and it is recommended that the camera's ONVIF user password be the same as the camera's administrator password. Axis cameras must have an ONVIF user created prior to use with CompleteView. Available existing profiles will be displayed after a successful connection.

Note: Although ONVIF compatible, use only the named driver for the Axis M3058-PLVE panoramic camera at this time. The M3058 driver should also be used for other M305X panoramic Axis cameras, as well.

For multi-channel cameras, configurations may need to be created for each channel. Consult the manufacturers' documentation for specific information.

ONVIF Profile S Feature Compatibility

Feature	CompleteView Support
General	
System Settings	
User Authentication (WS-Username Token)	Y
User Authentication (Digest Authentication)	Y
User Handling	
Query Services and Capabilities	Y
Device Discovery	Y
Default Access Policy	
Network Configuration	
Zero Configuration	
Firmware Upgrade	
Backup and Restore	
TLS Configuration	
IP Address Filtering	
NTP	
Automatic IP Assignment	
Media Profile Configuration	Y
Media Transport (RTP/UDP)	Y

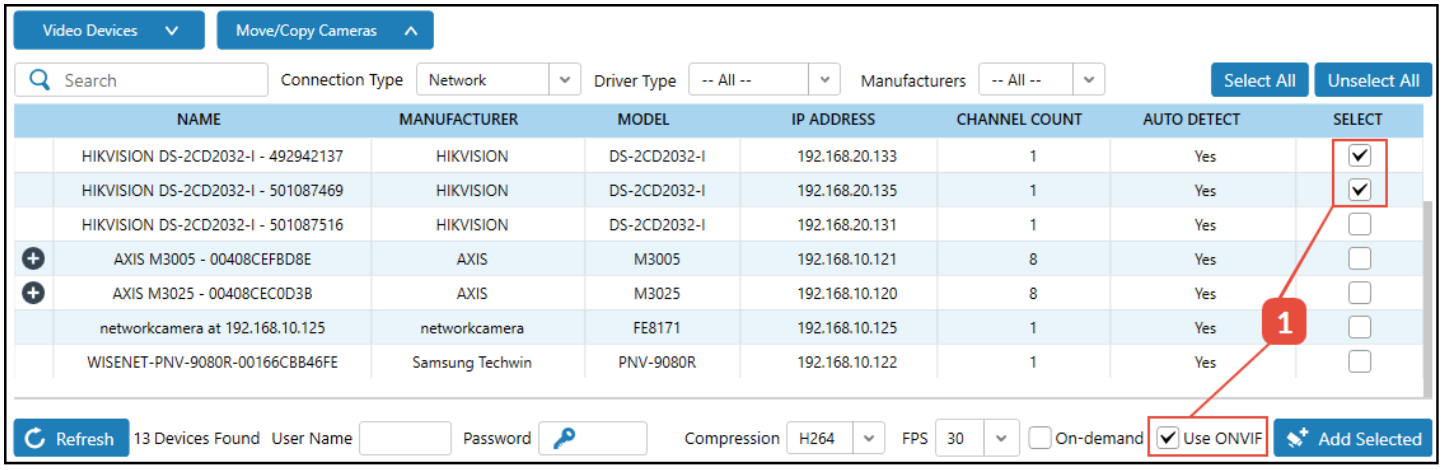
Feature	CompleteView Support
Media Transport (RTP/RTSP/HTTP/TCP)	Y
Media Transport (RTP/RTSP/HTTPS/TCP)	
Media Transport (RTP/RTSP/TCP/WebSocket)	
Media Transport (RTP/UDP Multicast)	
Video	
Video Streaming (MJPEG)	Y
Video Streaming (MPEG4)	Y
Video Streaming (H.264)	Y
Video Streaming (H.265)	
Video Encoder Configuration	Y
Video Source Configuration	Y
Media Profile for Streaming Ready out-of-the-box	
Video Source Mode	
Video Streaming (RTSP/RTP)	Y
Imaging Settings	
Recording Search	
Replay Control	
Recording Control	
Recording Control (Using an on-board media source)	
Recording Control (Using a Receiver as Source)	
Recording Control - Dynamic Recording (Recording)	
Recording Control – Dynamic Tracks (Tracks)	
Recording Source Configuration	
Events	
Event Handling (Pull-point)	Y
Event Handling (WS-Base-notification)	Y
Standard Monitoring Events for Devices	Y
Media Profile Configuration Events	
Access Control Events (Door)	
External Authorization Events	
Duress Events	
Access Profile Event (Changes on Profile)	
Credential Event (Changes on Credential)	

Feature	CompleteView Support
Schedule Event (Changes on schedule)	
Special Days Schedule Event	
Reset Antipassback Violation Event	
Stored Events (Seek)	
Motion Alarm Events	
Motion Region Detector Events	
Tampering Event	
Audio	
Audio Streaming (G.711)	Y
Audio Streaming (AAC)	
Audio Streaming (G.726)	
Audio Output Streaming (G.711)	
Audio Output Streaming (AAC)	
Audio Encoder Configuration	
PTZ	
PTZ Move (Absolute)	
PTZ Move (Continuous)	Y
PTZ Move (Relative)	
PTZ Presets	Y
PTZ – Home Position	
PTZ Configuration	
Additional	
Relay Outputs	
Auxiliary commands	
Focus Control	
Digital Inputs	
Configuration of On-Screen Display (OSD)	
JPEG Snapshot	
Motion Region Detector Configuration	
Metadata Configuration	
Metadata Streaming	
Recording	
Recording Search	

Feature	CompleteView Support
Replay Control	
Recording Control (Using an on-board media source)	
Recording Control (Using a Receiver as Source)	
Recording Control (Dynamic Tracks)	
Recording Source Configuration	
M = Mandatory compliance with the feature, C = Conditional compliance with the feature. For more information, refer to: https://www.onvif.org/profiles/profile-s/	

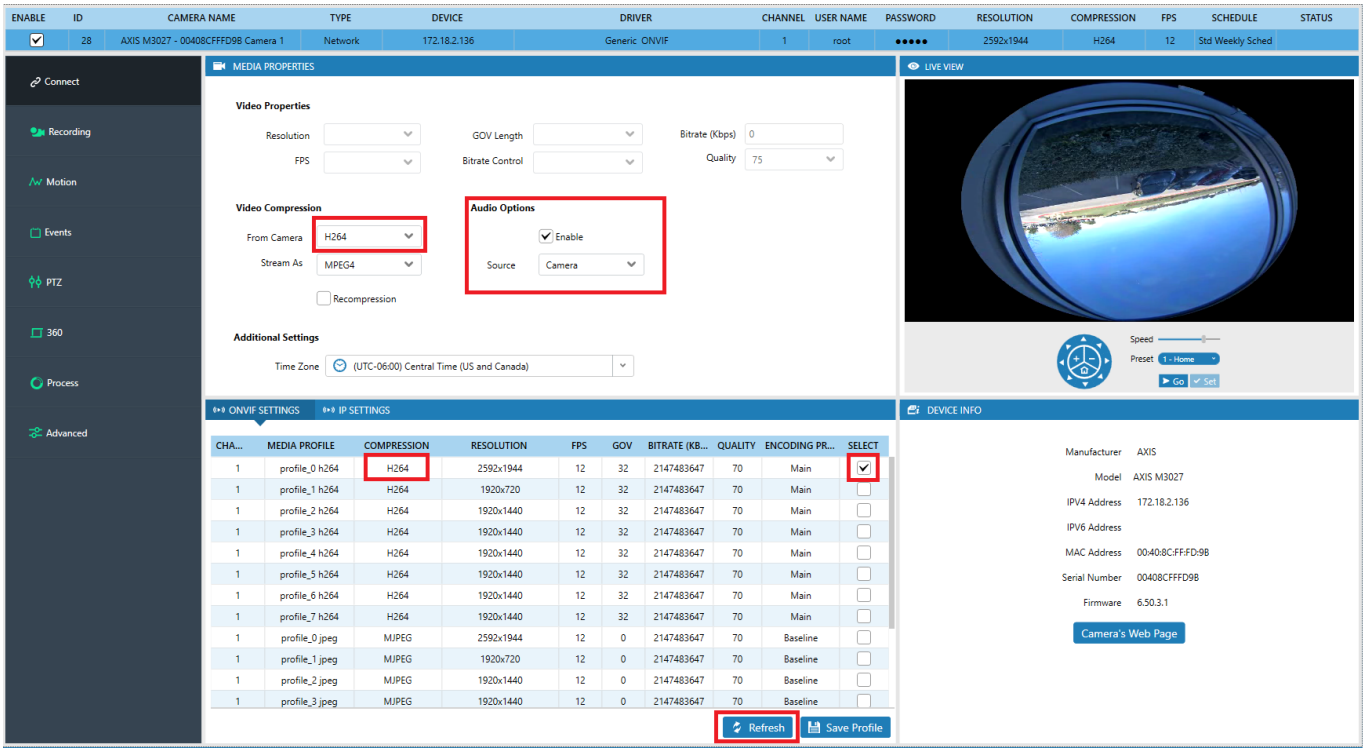
Adding ONVIF Cameras

Adding an ONVIF camera follows the same basic steps as any named driver camera, detailed in Recording Servers Cameras. To use ONVIF instead of using a named driver, check the Use ONVIF box during the Adding a Camera process. CompleteView Recording Server utilizes WS Discovery protocol for ONVIF camera discovery, consequently, UDP port 3702 must be open in Windows Firewall for discovery and other functionality. The example below shows a multi-channel camera added using the ONVIF driver, checked below.



ONVIF Configuration

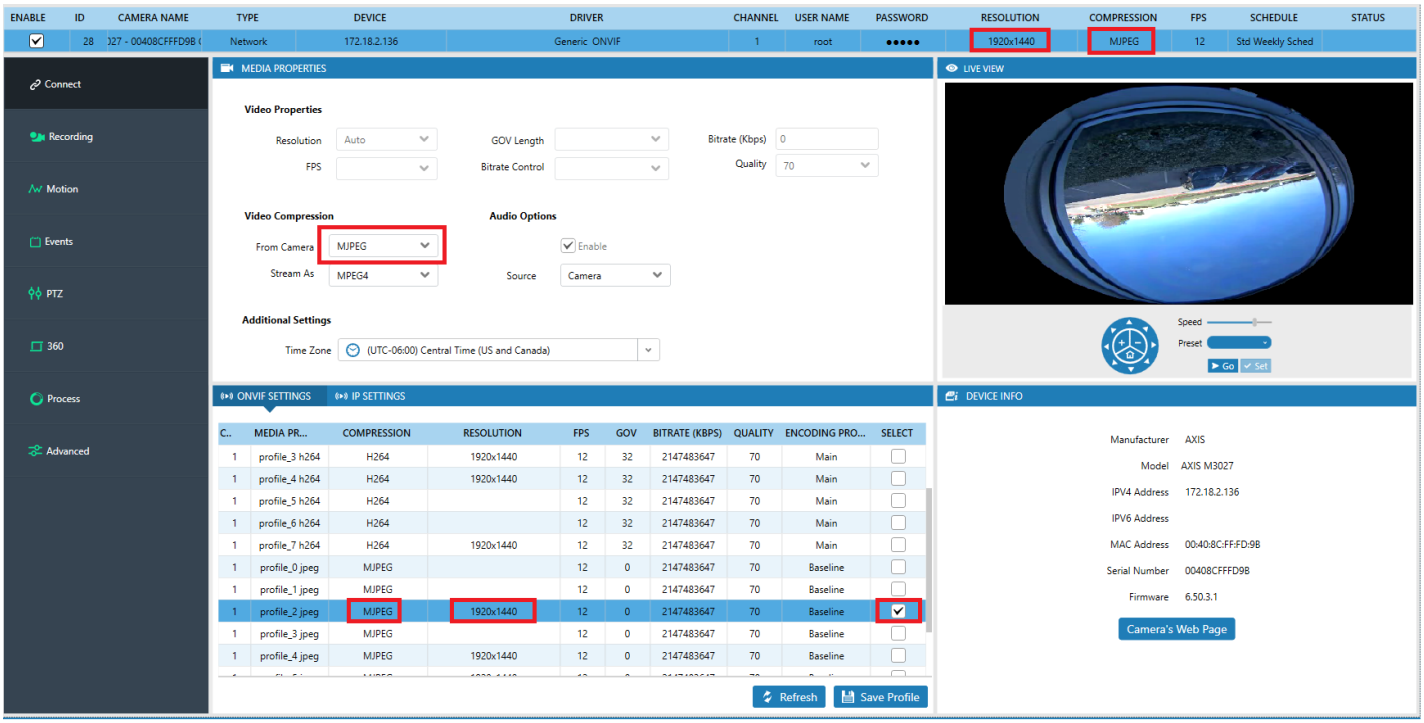
Once added, the first media profile in the video device's supported profiles that matches the selected compression and channel ID will be selected by default. If the compression selected by the user is not supported by the profiles, the first profile in the list will be selected. If the selected profile supports audio, the audio options will be enabled, or else will be disabled.



In certain cases, the media profile information might not be available immediately after adding the camera to the Recording Server. If not entered manually during the Adding a Camera process, the Recording Server uses default credentials to retrieve profile information during discovery, which may not work for all cameras. Once the correct credentials have been entered and saved, the Recording Server queries the camera for the profile details. It may be necessary to click Refresh to populate the list of media profiles.

Selecting ONVIF Media Profiles

To select a media profile, check the checkbox for the desired profile and save the configuration. Depending on the profile selected, the values are updated in the top camera grid row and Video Compression pane. The example below (using profile_2 jpeg) shows the change in compression and resolution from the example above (profile_0 h264).



If the camera supports multiple channels, changing the channel ID from the top camera grid row will update the profile selection and vice-versa. For a single channel camera with multiple profiles, the channel ID column will remain the same. **Note:** It is recommended to change and apply only one profile at a time.

Modifying Existing ONVIF Profiles

Some media profile settings may be changed and saved to the camera, depending on make and model. Change the desired settings for one or more profiles and click the Save Profile button. If the operation was unsuccessful, an "Invalid Profile Data" error will be reported and the changes will not be applied. For more information, consult Desktop Client and Recording Server diagnostic logs.

Configuring ONVIF Events

Configuration of ONVIF events is nearly identical to named driver events. See Recording Servers Camera Events for more information. Note that port 7775 needs to be open in Windows Firewall to allow ONVIF based event handling.

ONVIF PTZ

An ONVIF PTZ driver has been added to the IP PTZ driver list. This can be set for any network camera, regardless of the camera driver selected. Select the Show All PTZ Drivers to view the driver. The driver supports pan, tilt, zoom, presets, focus near/far, auto focus and auto iris operations.

Multi-Stream Camera Functionality

CompleteView is able to pull up to 3 separate video streams from cameras conforming to the ONVIF Profile-S standard capable of multiple streaming profiles. The streams may be assigned to specific recording types (Continuous, Alarm, and Motion) as appropriate for the application. At this time, CompleteView does not support multi-stream functionality on analog, NVR, or encoder based cameras.

For example, CompleteView can be configured to pull a low resolution, low bandwidth stream from a camera for Continuous recording, but upon either a Motion or Alarm event, automatically begin recording a higher resolution stream from the same camera. This "bump on alarm or motion" functionality allows for greater camera density, maximum conservation of storage space, and reduction of network bandwidth usage while providing a higher resolution stream when necessary.

CompleteView automatically selects the appropriate stream for Live View based on the size of the viewing tile. Digital zooming takes place on the stream currently being viewed. For maximum resolution and detail, maximize the video tile or switch to full screen viewing before zooming in.

Multi-Stream Specifications

One primary and up to two secondary streams may be handled by CompleteView. Only one IP license is required for the camera for multi-stream functionality. As mentioned in the previous section on ONVIF, some cameras come preconfigured with ONVIF users and profiles while some do not. In the latter case, an ONVIF user and ONVIF streaming profiles must be manually created on the camera before CompleteView can be configured to pull multiple streams. Consult your camera's documentation for configuration information. Once the profiles have been set up on the camera, they can be modified within the CompleteView interface.

One or more recording types may be assigned to each stream, but a given recording type may only be assigned once to that camera. For example, the primary stream may have both Continuous and Motion recording types assigned to it, but the secondary stream may only be assigned Alarm recording, as the other two recording types are taken up by the primary stream.

Recordings from all streams will be stored in the same camera directory and will be accessible via normal search functionality and the Playback module within CompleteView. Motion detection, subscription to on-camera events, PTZ operations and other CompleteView functions will take place only on the primary stream. When viewing a live stream, taking a snapshot will capture the actively viewed stream's frame to match the requested resolution.

Note: If an ONVIF camera configured for multi-streaming is later switched over to its named driver in CompleteView, some Recording Types checkboxes may remain visible, but be grayed out and non-functional.

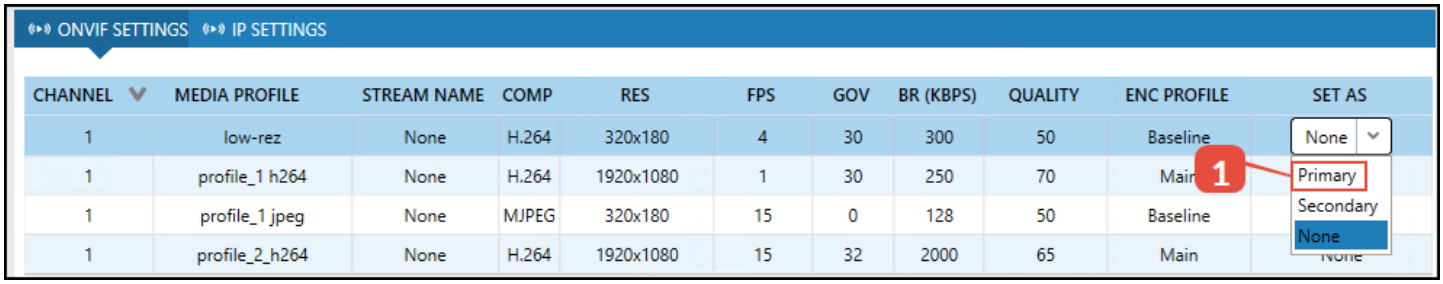
Configuring a Multi-Stream Camera

First verify that an ONVIF user and profiles exist on the camera as described in its documentation. Next, either add the camera as an ONVIF camera as described in the previous section, or change its driver in CompleteView to Generic ONVIF.

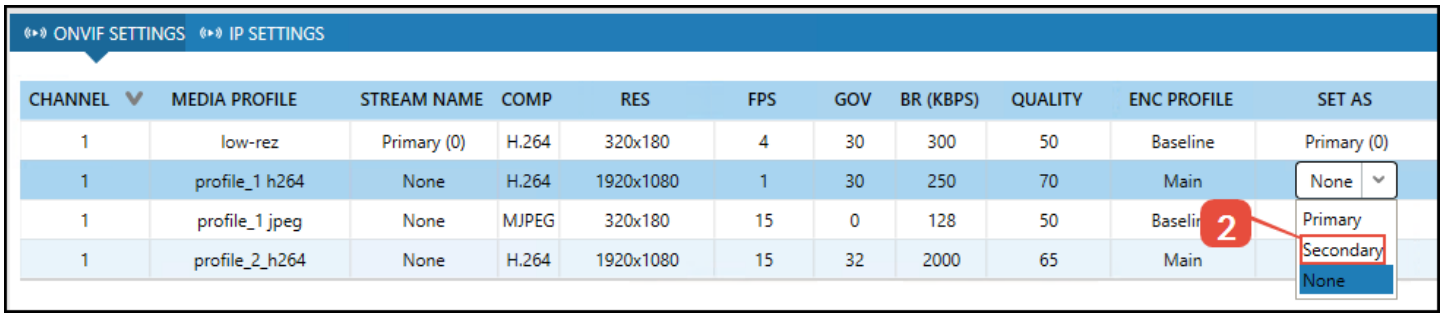
Add Primary and Secondary Streams

Once the camera is added, perform the following steps to create primary and secondary streams.

Steps:



1. Select primary stream by clicking the Set As dropdown menu and selecting Primary.

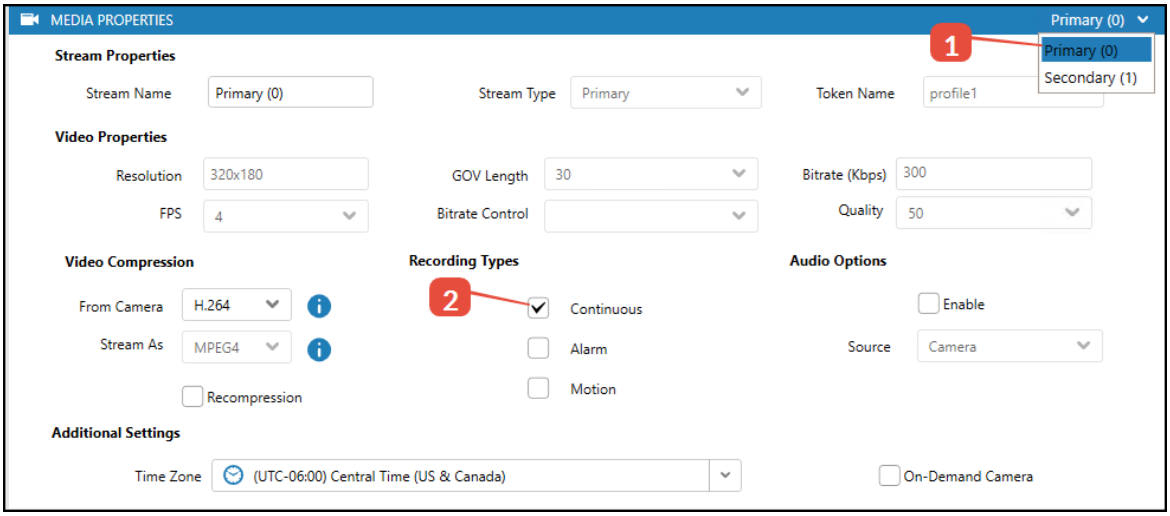


2. Select secondary stream by clicking the Set As dropdown menu and selecting Secondary. One primary and up to two secondary streams are supported.
3. If desired, change the Stream Name and adjust the compression, resolution, FPS, GOV, bitrate, Quality, and encoder profile by clicking in the respective cells.
4. Save the profile

Assign Recording Types to Streams

Once the primary and secondary streams have been added and configured, follow the steps below to assign the recording types.

Steps:



1. Select the Stream from the dropdown menu
2. Select the Recording Type(s)
3. Save the Configuration

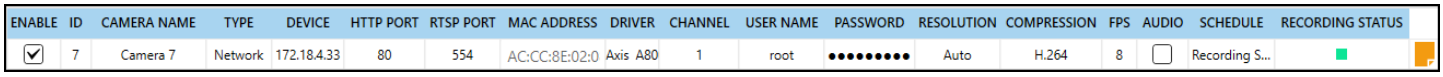
Repeat the steps above for the secondary stream(s).

Recording Servers Camera Connect Panel

CompleteView is designed to automatically configure and add video devices using their optimal settings. However, the connection parameters may be changed manually and saved for individual devices from the Connect Panel. Some menu options contained in the panel are camera-specific and not available for all cameras.

Connect Panel Device Parameters

The top of the Connect Panel displays connection status and basic information about the attached device.



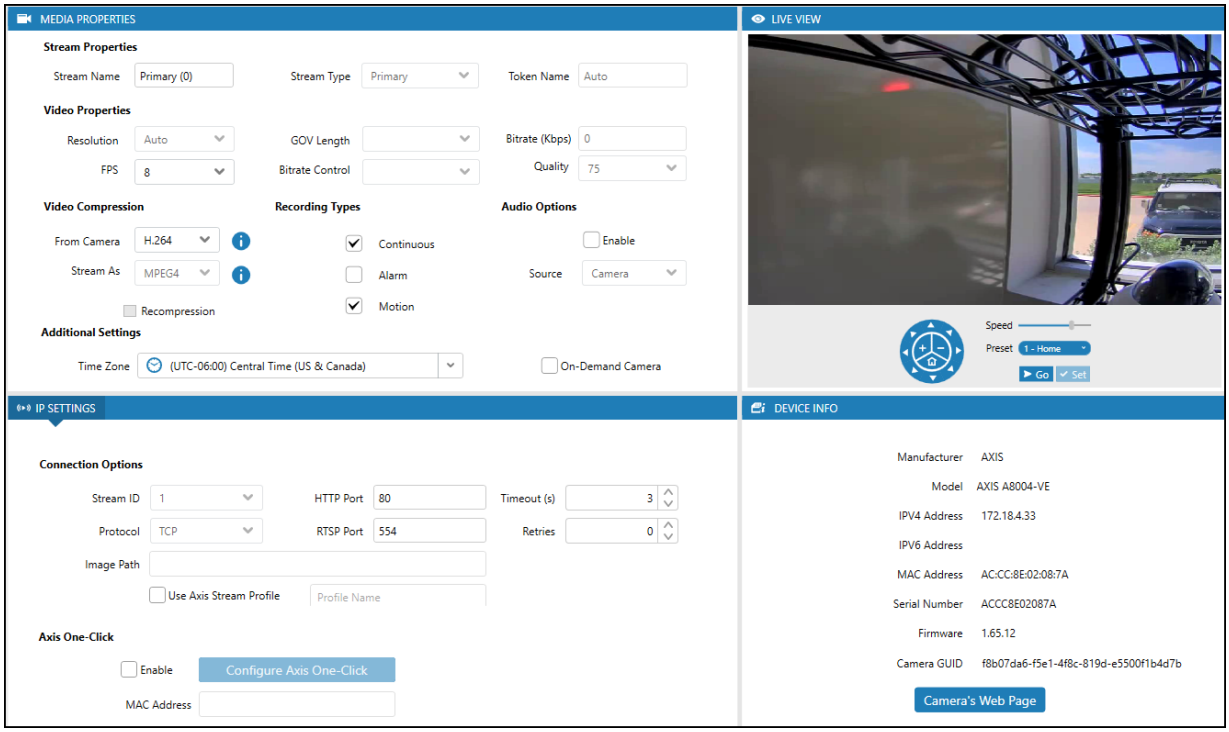
Device Parameters

Title	Description
Enable	Enables or disables the video device connected to the Recording Server
ID	Numerical position in the Recording Server's list of devices
Camera Name	The friendly name of the camera or video device
Type	Analog or Network
Device	IP address or Capture Card Number
HTTP Port	The HTTP port used to communicate with the camera
RTSP Port	The RTSP port over which the camera streams video
MAC Address	The MAC address of the selected camera
Driver	Used to connect to your devices. Select manufacturer and model from drop-down lists to match your device. For ONVIF supported devices, select Generic for the manufacturer and ONVIF for the model. Basic RTSP, MJPEG drivers are also available under Generic. ONVIF is the preferred driver for all new devices starting with CompleteView 7.0 and newer versions.
Channel	Channel in use (applies to multi-channel cameras only)
User Name	The device's user credential
Password	The device's user account password
Resolution	Resolution setting for the camera, contains a pull-down menu; Auto will display for most network cameras. For ONVIF supported cameras, the resolution will be in the ONVIF settings panel.
Compression	MJPEG, MPEG4, H.264, H.265
FPS	Selectable Frames Per Second. For ONVIF supported cameras, the frame rate will

Title	Description
	be in the ONVIF settings panel.
Audio	Enables incoming audio for audio capable cameras
Schedule	Displays the schedule the camera is being recorded to
Recording Status	Displays the status of the recording state for the device

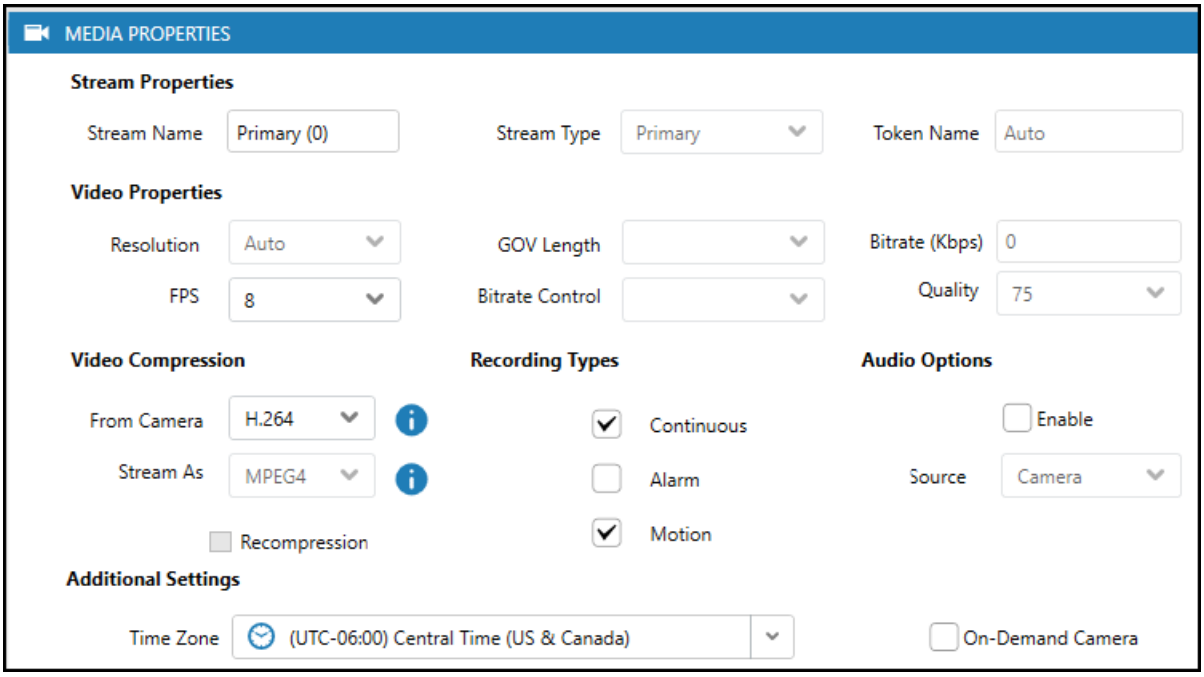
Connect Panel for IP (Network) Cameras

The Connect Panel may be used to change video settings for both Analog and Network devices manually. The Connect Panel is divided into the Media Properties, Live View, IP (or Analog) Settings, ONVIF Settings (when using an ONVIF driver), and Device Info sub-panels. Its purpose is to confirm Recording Server connection information and enable access to the network video device's web interface.



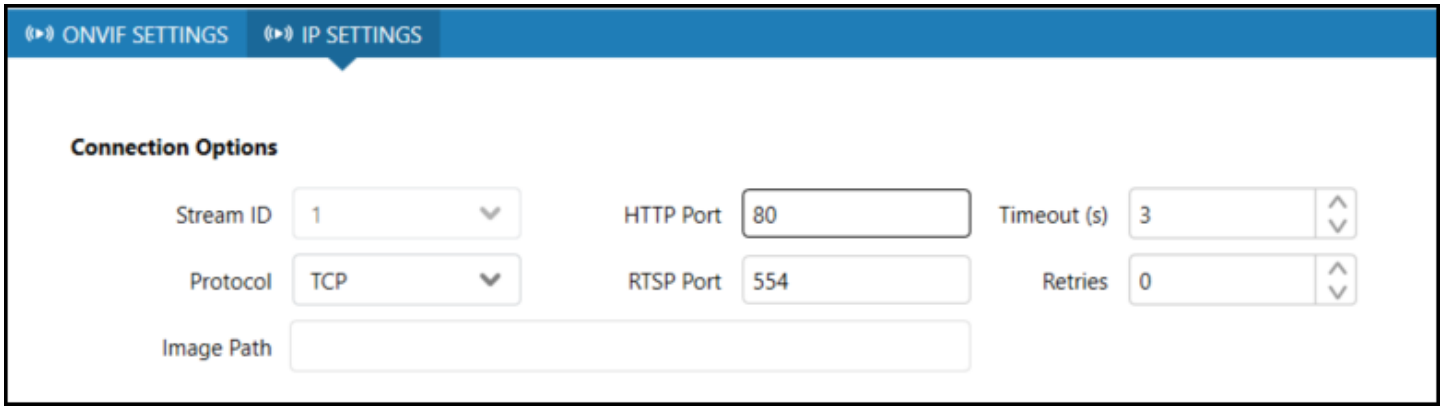
Media Properties for IP Cameras

Media Properties contains resolution, frame rate, audio, compression type, and other configurable elements of the selected camera. For multistream cameras, the stream name and type may be selected and configured here. Recording types are assignable per camera here, as well. On Demand is useful for customers in constricted bandwidth environments, but is not recommended for use in typical deployments. If On-demand is enabled, the camera connects to the Recording Server only when live video is requested by the client, but does not otherwise connect and record the video. On-demand supports all H.264 streaming profiles.



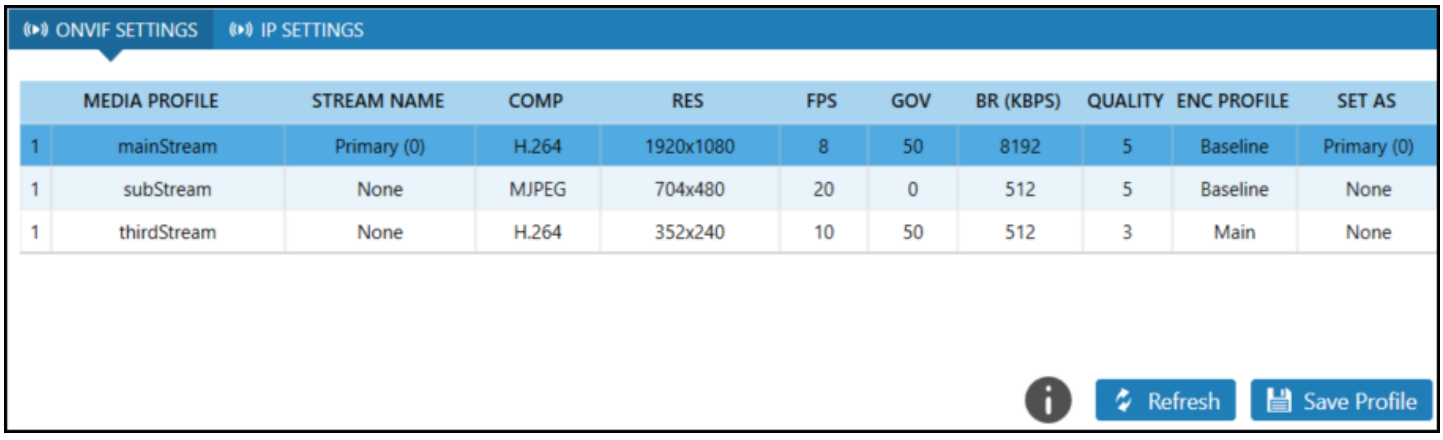
IP Settings

IP settings contains port, protocol, and other settings for IP configuration.



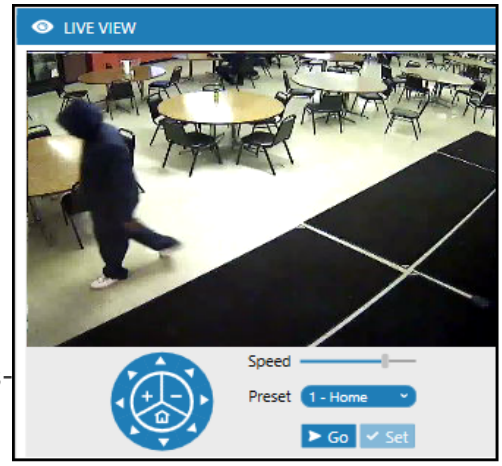
ONVIF Settings

For cameras using the ONVIF driver, configuration of their various, on board media profiles can be viewed and configured here. For more information, see [ONVIF Configuration](#).



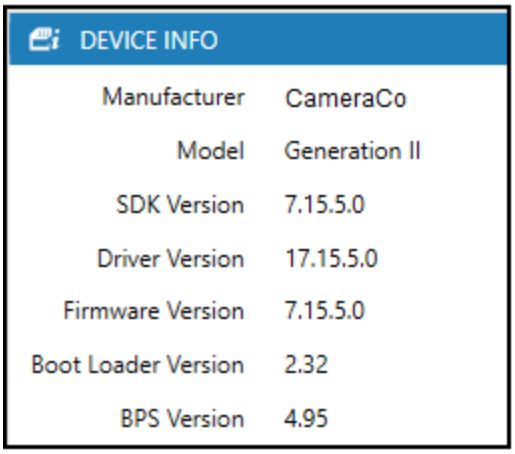
Live View Panel

The Live View panel displays video from the currently selected camera, and includes basic PTZ and preset functionality. Live View is the same for both Network and Analog cameras.



Device Info

Device Info displays the video device's specific information. The network device's web page, illustrated on the left, can be launched from this panel and is where changes such as analytics, date/time, streaming properties, and any other camera specific settings should be made. When an analog camera is selected, capture card information, illustrated on the right, is displayed.



Analog Settings

Analog Settings is exclusive to Analog cameras, and replaces the Connect IP Settings when an Analog camera is selected. Its settings are used to set image quality for the selected analog camera. Each section will be detailed below. The Live View subpanel displays real-time results when image quality settings are changed.

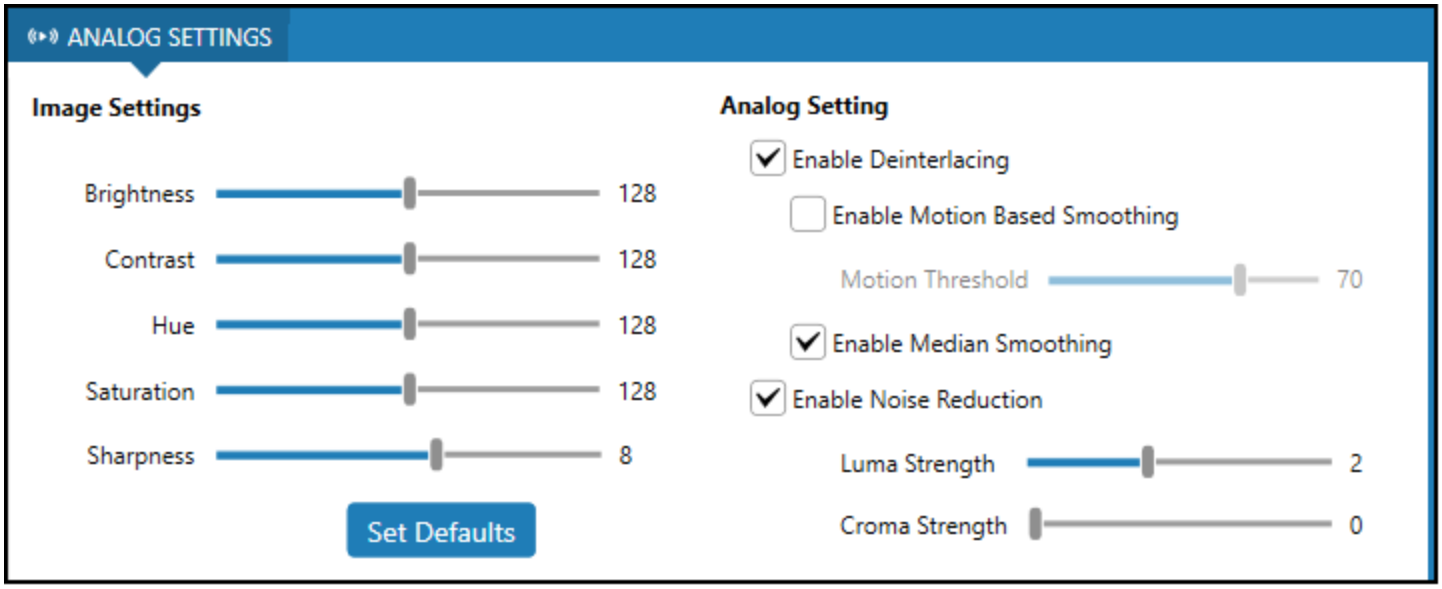


Image Settings

Each adjustment slider has a range from 0-100. Moving the slider to the left reduces brightness, contrast, etc. Selecting “Set Defaults” resets default image settings for the selected analog channel. The results are immediate and visible in the Live View Panel as it is being adjusted. The various settings adhere to their traditional roles (e.g. brightness, contrast, etc.).

A Word About Deinterlacing

Analog video produces a picture (or frame) by drawing two separate, interlaced visual fields. When Enable Deinterlacing is selected, CV digitally combines both fields and presents them as one cohesive image, which is useful for video processing purposes. In the process of digitizing and combining the interlaced fields, some video artifacts and motion-blurring may arise from the time delay intrinsic to the separate field renderings in the original interlaced video. CV includes smoothing functionality to address the potential anomalies. Generally speaking, Enable Deinterlacing should be enabled, unless there is known deinterlacing of the video stream before it reaches the CompleteView Recording Server. Enable Deinterlacing is defaulted to the “On” position and should remain so to accommodate newer display technologies.

Motion Based Smoothing

Motion Based Smoothing applies to deinterlaced video, based on detected motion in the camera’s field of view. If no motion is detected, no smoothing is applied. Use the slider to increase or decrease motion sensitivity.

Median Smoothing

If checked, smoothing is always on.

Enable Noise Reduction

When selected, Enable Noise Reduction will apply an algorithm to “clean up” analog video, reducing grain and video artifacts. The Luma Strength slider enhances or decreases the achromatic (black and white) elements of the video picture. The Chroma Strength slider enhances or decreases the color elements of the video picture.

Video Standard

CompleteView supports the two most common video standards; National Television Standards Committee (NTSC) and Phase Alternating Line (PAL).

All video capture cards in a Recording Server or within the same CompleteView must be set to NTSC or PAL. Combining NTSC and PAL in the same Recording Servers or in the same CV is not supported.

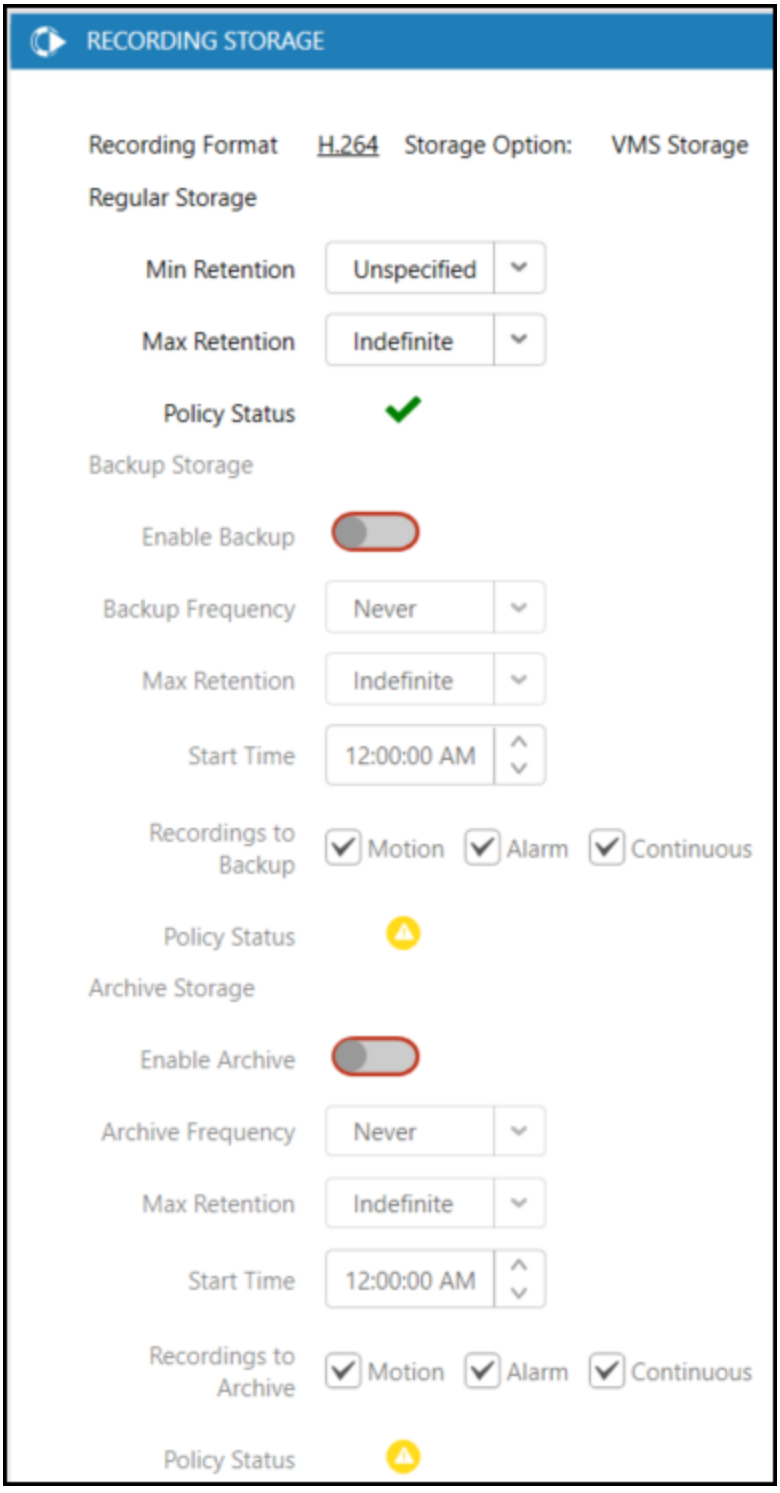
Recording Servers Cameras Recording

Recording enables the Administrator to select a camera and configure specific recording volume and edge storage parameters if not using pools, if available.

Recording Storage

Recording Storage displays a camera's pool or volume and recording compression information, and allows a user to enable or disable a specific volume, if using volumes and not pools.

In addition, Regular, Backup, and Archive storage information pertaining to retention policies, policy status, etc., will be displayed and is configurable here. For more information, see Storage Pool Introduction.

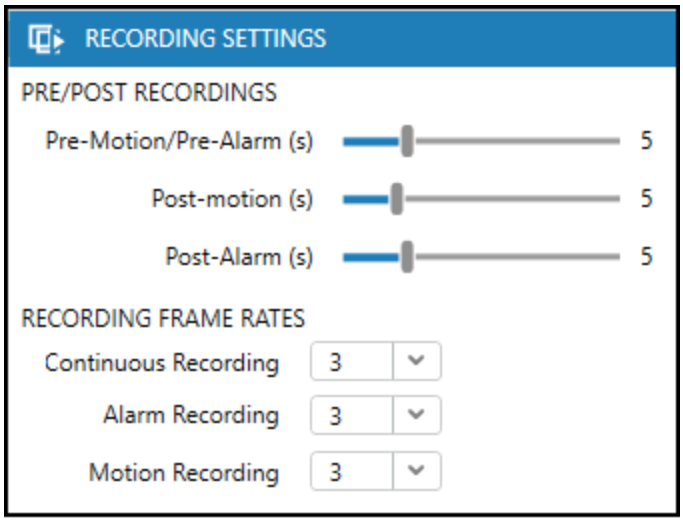


Store on NVR

NVRs may be added and configured in the same way one would configure a camera. Currently, CompleteView integrates with Hanwha/Samsung and HIKVision NVRs. The integration allows the NVR's video to be stored on either CV Recording Server, or on the NVR. If Store on NVR is enabled, the NVR will store the recorded video. If disabled (default), the video is stored on the CompleteView Recording Server. For more information, see **NVR Introduction**.

Recording Settings - Pre/Post Recording & Recording Frame Rates

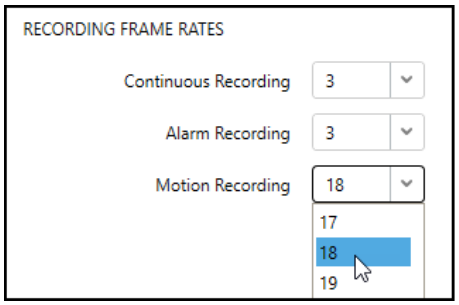
Pre and post motion alarm settings are intended to add time to the beginning and ending of recorded video motion or alarm video events. Pre and Post times should be configured exclusively when the Recording Server's recording schedule includes motion or alarm recording for the selected camera. A pre-motion Recording Schedule needs to be created and applied to the camera for Pre to function. Cameras that record continuously do not require Pre and Post Recording to be configured.



Pre-motion/Pre-Alarm determines the number of seconds to record video prior to the start of a video motion detection or an external alarm event. Pre-motion recording can be adjusted from zero (0) seconds to sixty (60) seconds. Pre-motion and post-motion recording are added to the motion event and played back as a unified video clip. Post-motion determines the number of seconds to record video after the video motion event has stopped. The default setting is three (3) seconds and cannot be less than one (1) second. Post-motion may be extended from one (1) to sixty (60) seconds. Post-Alarm determines the number of seconds to record video after the alarm event has ceased. Post-Alarm recording can be adjusted from zero (0) seconds to sixty (60) seconds. Pre-alarm and post-alarm recording are added to the alarm event and played back as one video clip.

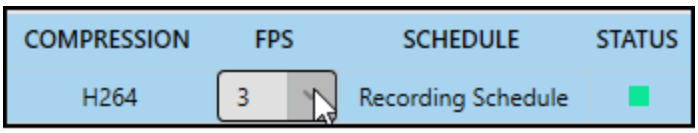
Recording Frame Rates

Recording Frames Rates in the Recording Settings panel permits frame rate customization. Customization is the process wherein a camera's FPS rate is set to increase upon motion or alarm recording, and return to a normal when the motion or alarm event has ceased. Customization is set for individual cameras, and the conditions must be configured as prescribed.



Set FPS Without Customizing

Frames should be set during initial camera installation on the Recording Server, but may be modified by making a change to the frame rate in the Camera Install Parameters located in the top right portion of the Connect or Recording Panels.



For more information, Click Recording Servers Camera Connect Panel.

Customization may be applied:

1. If the camera, capture card, or encoder recording is uncompressed
2. If the camera, capture card, or encoder compression is MJPEG
3. If the Recording Server's recompression is enabled for the selected camera

If one of the above three conditions are not set, the FPS will be received and continually recorded at the same frame rate.

Very Important Note: The frame rate customization applies exclusively to individual cameras.

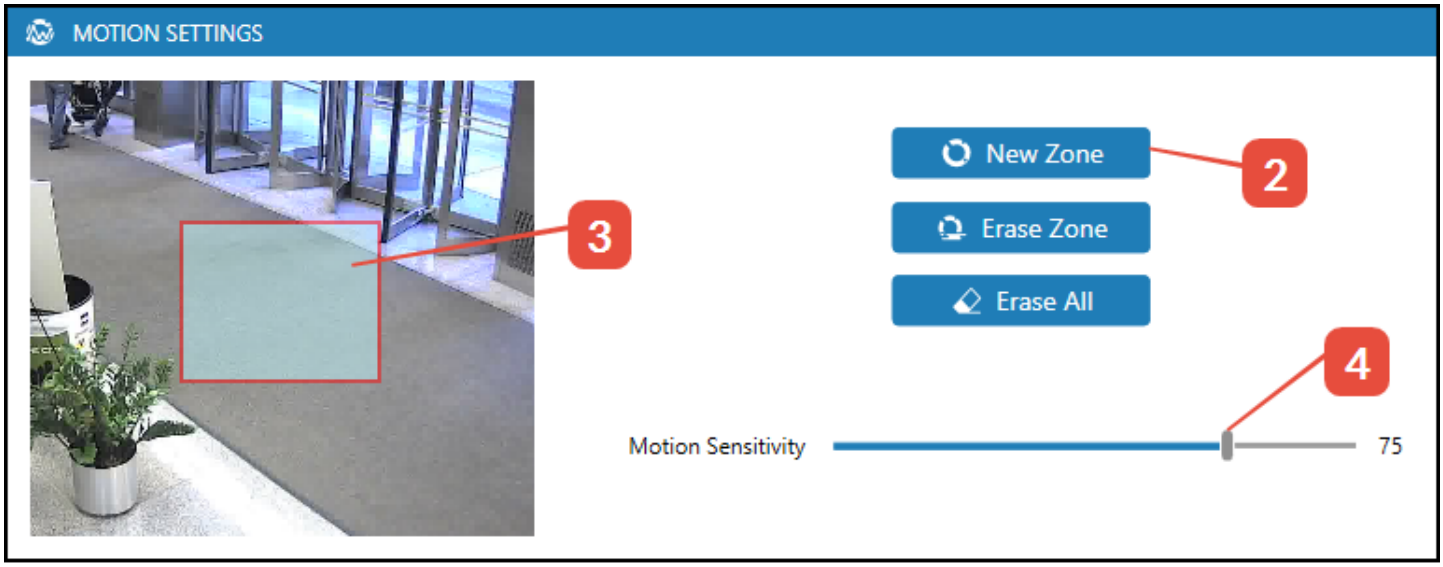
Recording Servers Camera Motion Panel

The Motion Panel is used to configure the Recording Server for motion detection on either analog or network cameras. This feature is commonly referred to as Server-based motion detection. Motion Zones are areas in the field of view where motion is detected. A still shot from the selected camera will appear to assist with the placement of the motion zone. Motion detection may be configured from network cameras in the Camera/Events Tab. Motion areas must be configured for motion recording to occur, and to be reported by the Recording Server as motion in the client's Alarm View.

For information about both utilizing a camera's native motion processing functionality and setting up Recording Server motion, see the related Job Aid videos at:
https://support.salientsys.com/knowledgebase/training-resources/

Create a Motion Zone

Steps:

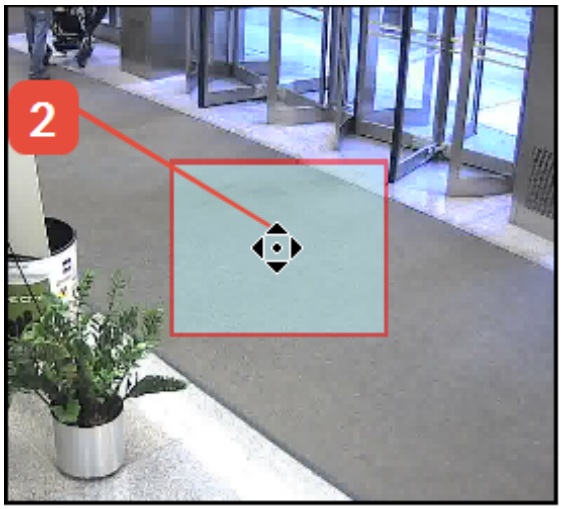


1. Select a network or analog camera.
2. Select New Zone.
3. Draw a motion zone over the desired motion area with the mouse pointer:
   a. Place your mouse pointer at any corner of the area of interest (AOI).
   b. Hold the left mouse button down and move the mouse pointer diagonally across the desired motion area.
   c. Release the mouse button
4. Set Motion Sensitivity. Some trial and error will be required to achieve the appropriate level for the selected scene. See Adjust Motion Sensitivity below.
5. Save the configuration

Move a Motion Zone

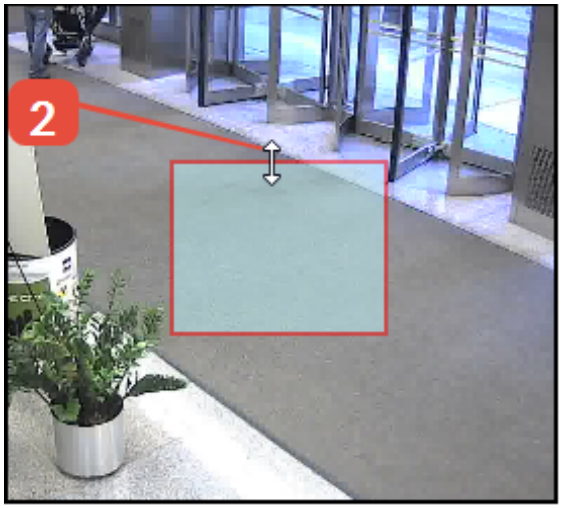
1. Place the mouse pointer in the center of the motion zone
2. Look for the arrow cursor to appear
3. Press and hold the left mouse button
4. Drag the motion area to the new location
5. Release the mouse pointer
6. Save the configuration

Note: Motion zones may be created and moved to any area of the video with the mouse pointer.



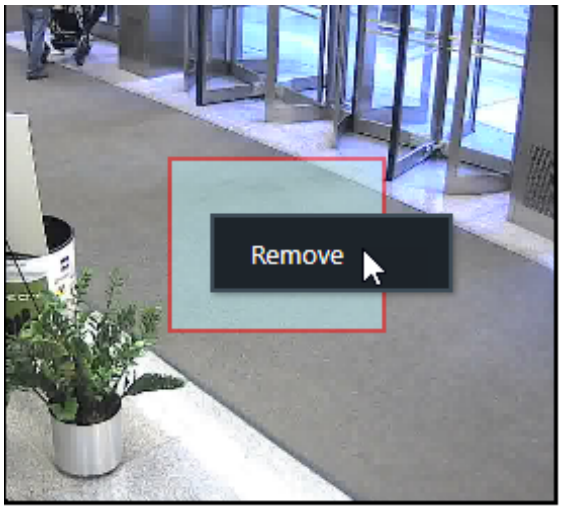
Resize a Motion Zone

1. Place the mouse pointer at an edge of the motion zone
2. Look for the arrow cursor to appear
3. Press and hold the left mouse button
4. Resize the motion area
5. Release the mouse pointer
6. Save the configuration



Remove (Delete) a Motion Zone

1. Right-click on the motion zone
2. Select Remove
3. Save the configuration



Adjust Motion Sensitivity

Sensitivity range is 0-100 from least to most sensitive; the default is 75.

Steps:

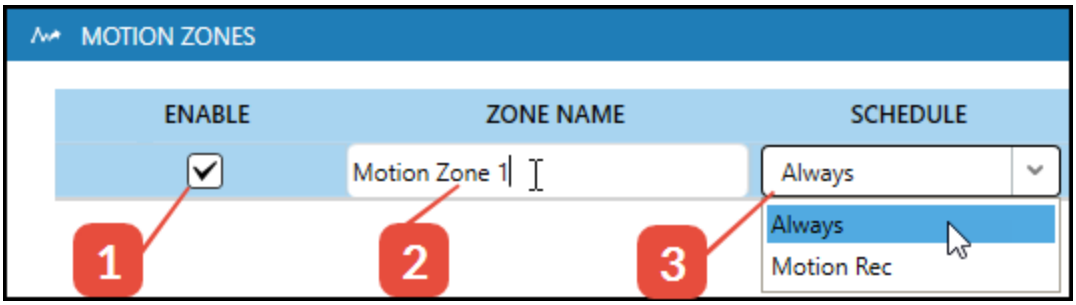
1. Set up a motion zone
2. Monitor motion activity in the Client Alarm View
3. Lower or increase the sensitivity if a motion event appears for no reason; increase the sensitivity if, motion activity occurs in the motion zone, but no motion event results
4. Remember to save the configuration each time motion sensitivity is adjusted

Motion Zones and Action

A motion zone entry is created in the Motion Zone subpanel and enabled when a motion zone is created. From this subpanel, the administrator can disable an existing motion zone without removing it. Actions can be enabled to respond when the recording schedule is recording continuously or only when motion recording is scheduled.

Configuring Motion Zone Action

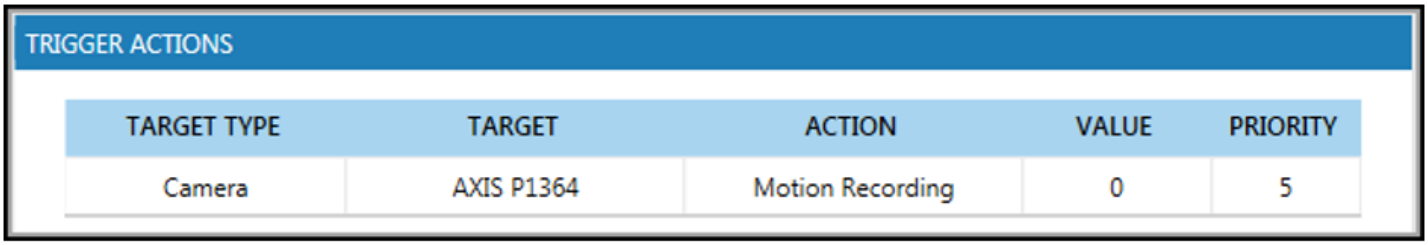
Steps:



1. Ensure the motion zone to be recorded is enabled
2. Optional: re-name the motion zone; (click on & type over the existing name)
3. Select when the Target Actions should respond
   a. Always–anytime recording is scheduled
   b. Motion Rec -only when motion recording is scheduled
4. Save the configuration

Trigger Actions-Motion

Trigger Actions allows the Administrator to configure an optional triggered action based on a motion event from a camera. After creating a motion zone, the Add Action button allows users to create a trigger based on a detected motion event. The chart below explains each part of the Trigger Actions Panel.



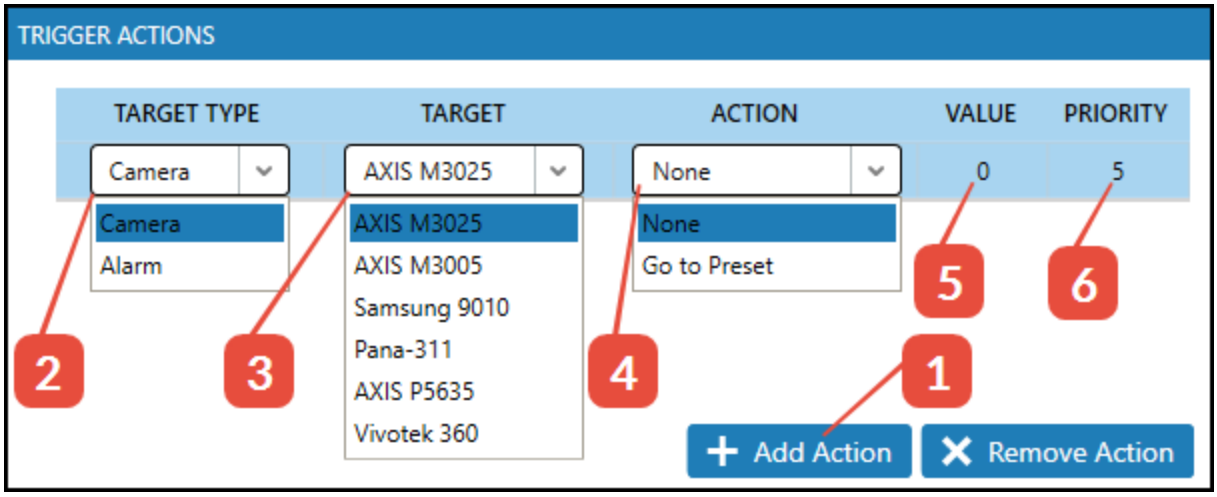
Trigger Actions

Name	Description/Option
Target Type	Camera or Alarm
Target	The object of the targeted action: • If the target type is a Camera, select a specific camera. • If Target Type is Alarm, use the pulldown menu to select the specific Alarm
Action	The Action that is taken by a Camera or an Alarm in response to the event: • If Target Type is a Camera, select Go to Preset, Alarm Recording, or Motion Recording. • If Target Type is Alarm, select Activate Output or Deactivate Output
Value	Select the PTZ location if a camera is the Target. Select the desired output if using an Alarm.
Action Priority	Resolves conflict by determining Action priority for the same Target that may be configured to serve two Events that occur simultaneously Priority ranges: 0 (lowest) through and including 10 (highest)

Add a Trigger Action

Trigger Actions are created when a Motion Zone or an Event is originated in the CV client for a camera or an I/O device.

Steps:

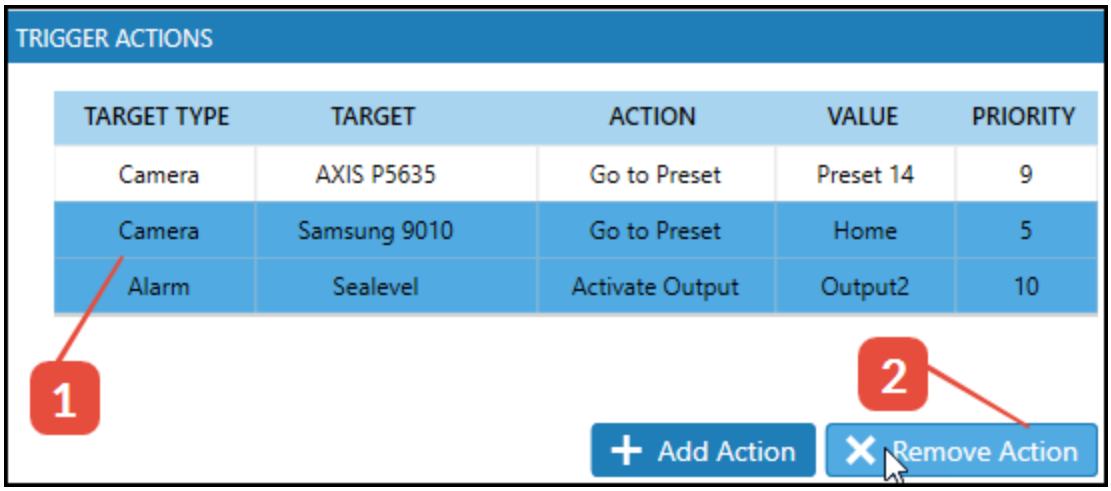


1. Press Add Action
2. Target Type: Use the drop-down menu to select the Target Type
   a. Camera
   b. Alarm
3. Target: Select the Target
   a. Cameras: select the camera for the intended Target Action
   b. Alarms: select the alarm for the intended Target Action
4. Action: Select the desired Action for the Camera Options:
   a. Go to Preset
5. Value: send a PTZ camera to a Preset Position #, when motion is detected in a fixed camera
6. Priority: Set the priority; the range is 1(lowest) to 10 (highest). The priority value defines the Action priority for multiple actions by the same Targets
7. Save the configuration

Remove One or More Trigger Action(s)

Trigger Actions may be removed. Removing a Trigger Action that is associated with a motion zone will not remove the associated motion zone.

Steps:



1. Highlight the Target Action(s) to be removed; (multiples may be removed simultaneously by holding down the shift key and selecting each Target Action to be deleted)
2. Select Remove Action
3. Save the configuration

Recording Servers Camera Events

From the Events Panel, the Administrator can configure CompleteView to register, record, and notify about a variety of camera-based events. The list of events will change to match the selected camera and its available, on-board analytic capabilities. Cameras using named drivers will usually present a different list of events than those using the ONVIF driver. When an ONVIF profile S conformant camera is added, CompleteView queries the camera for all its available events and makes those events available for use. For named-driver cameras, CompleteView uses a basic set of predefined events. Consequently, it's advisable to use the ONVIF driver whenever possible for maximum flexibility and compatibility.

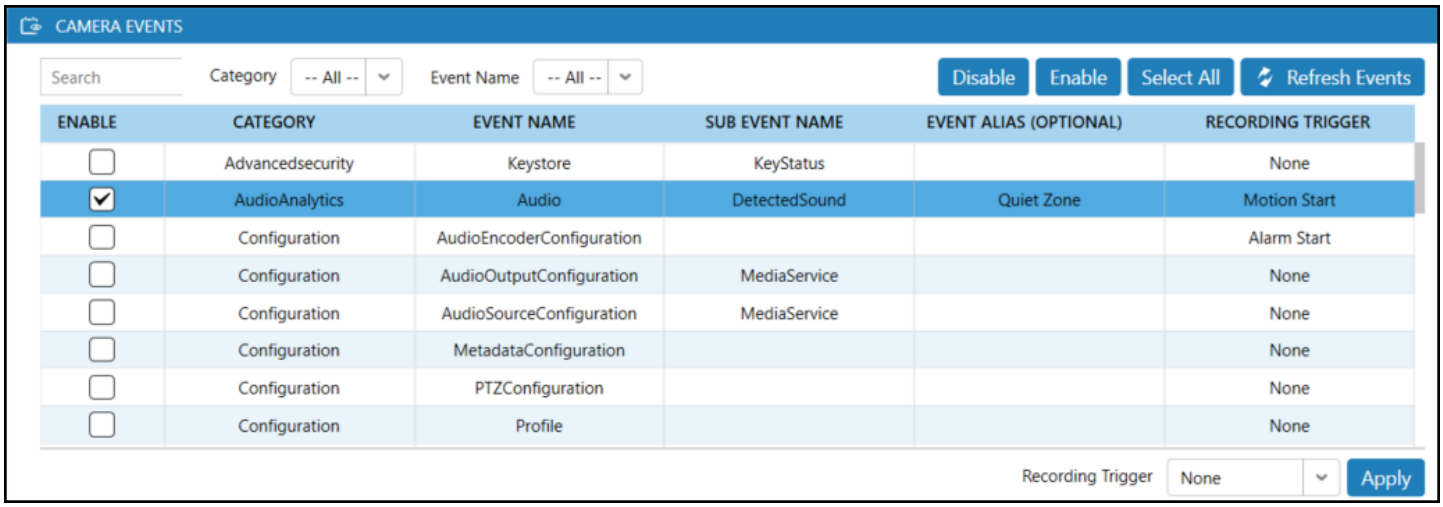
A word about Camera Events

Configuring camera events is a multi-step process that involves both internal camera settings and CV server configuration. The process of enabling events as outlined below, configures the CompleteView Recording Server to listen for events that are generated and reported to the Recording Server by a connected and properly configured network camera. Additionally, the Events to Generate and Trigger Action sub-panels may be used to configure specific alarm or camera actions that are tied to motion or alarm for each camera generated event.

CompleteView handles stateless events such as a virtual line cross, gunshot, etc., by recording 20 seconds of video plus any pre- and post- event recording time, as configured. Stateful events are recorded for their duration, plus any pre- and post recording time, as configured.

Example: HikVision® DS2CD4165F-IZ

This example shows the event capabilities of a HikVision DS2CD4165F-IZ, and how to access and configure those events in CompleteView.



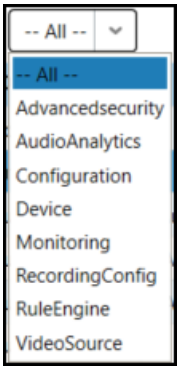
Camera Events

Enable	Configures CompleteView to listen for the selected event from the camera. It's advisable to enable only required events in the interests of clarity and ease of configuration. **Note:** If a camera is not configured for continuous recording and an enabled camera event is received for which a Recording Trigger is not turned on, CompleteView will display a “no video found” message if you try to play back the event.
Category	Describes the general type of the event. If using a named driver, CompleteView

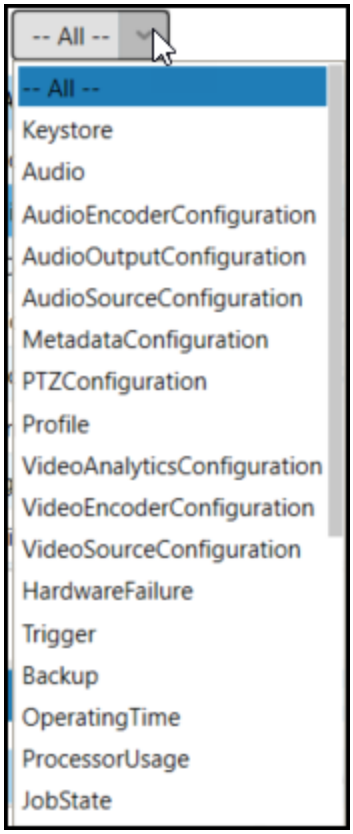
	generates the list of available categories. If using the ONVIF driver, the categories are both provided by the camera upon adding it to the Recording Server and generated by CompleteView.
Event Name	As above, the list comes from either CompleteView or the camera, depending on the driver.
Sub Event Name	Comes from the camera, and is not always populated. Further describes the event.
Event Alias	Aliases allow users to provide meaningful descriptions of camera events. Event aliases are searchable, where applicable, and appear first in description fields. Only the following characters may be used for event aliases: • a-z • A-Z • 0-9 • '!', '@', '#', '$', '%', '^', '&', '*', '(', ')', '-', '.', '_', '+', '[', ']', '{', '}', '?', ' ' • Max length: 128 characters
Recording Trigger	Selectable between None, Alarm Start, and Motion Start. In the event a particular event is detected, designates what kind of recording CompleteView generates. Note: If a camera is not configured for continuous recording and an enabled camera event is received for which a Recording Trigger is not turned on,CompleteView will display a “no video found” message if you try to play back the event.

HikVision DS2CD4165F-IZ Category, Event Name, and Recording Trigger menus

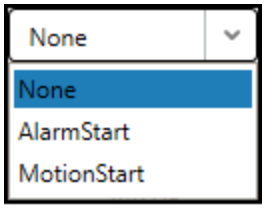
Category Menu



Event Name Menu



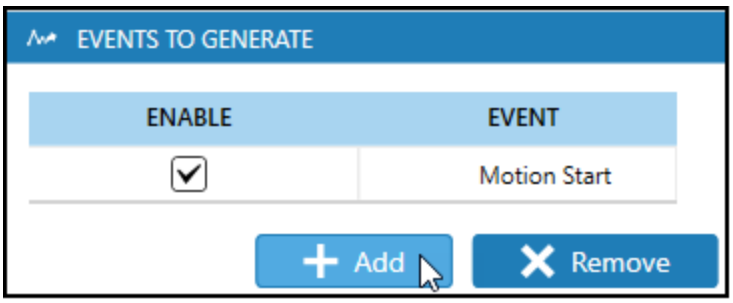
Recording Trigger Menu



The Category Menu enables users to filter the available events by either all or a single category. At the top of the panel, the Administrator may also use the Event Name menu to filter for a specific event for monitoring. Not all devices or cameras are capable of on-board analytic capabilities. Cameras using named drivers that do not host internal analytic capablities will not display details in the Camera Events panel. CompleteView displays what is available on a given camera. If a named driver camera should be displaying specific features, check the camera's firmware to ensure it is current and that the camera is supported for onboard analytic capabilities before calling technical support.

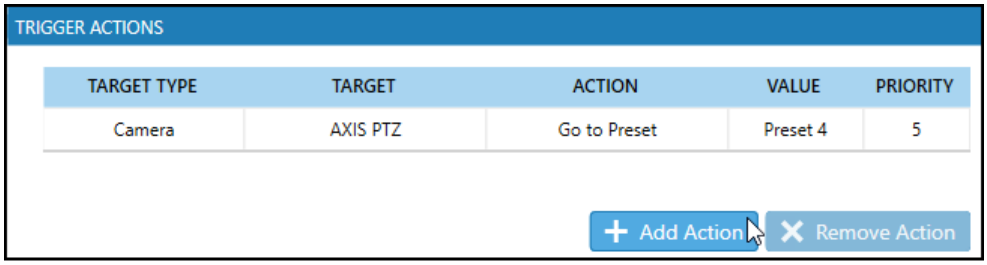
Events to Generate

When camera events have been configured with one or more Recording Triggers, users can add those events into the Events to Generate monitoring panel by selecting the add button. Once added, the events can be enabled/disabled as necessary, and linked to available trigger actions.



Trigger Actions

Any event can be linked to any available action. Trigger Actions make it possible for the Administrator to configure a triggered response based on any camera analytic or camera hardware event.



Triggers can act on either cameras or alarms. See table below for more information.

Trigger Actions

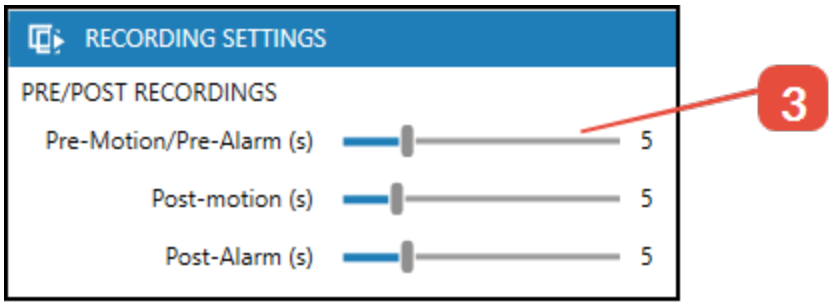
Name	Description/Option
Target Type	Camera or Alarm
Target	The object of the targeted action: • If the target type is a Camera, select a specific camera. • If Target Type is Alarm, use the pulldown menu to select the specific Alarm
Action	The Action that is taken by a Camera or an Alarm in response to the event: • If Target Type is a Camera, select Go to Preset, Alarm Recording, or Motion Recording. • If Target Type is Alarm, select Activate Output or Deactivate Output
Value	Select the PTZ location if a camera is the Target. Select the desired output if using an Alarm.
Action Priority	Resolves conflict by determining Action priority for the same Target that may be configured to serve two Events that occur simultaneously Priority ranges: 0 (lowest) through and including 10 (highest)

Configure On-Camera Motion Detection

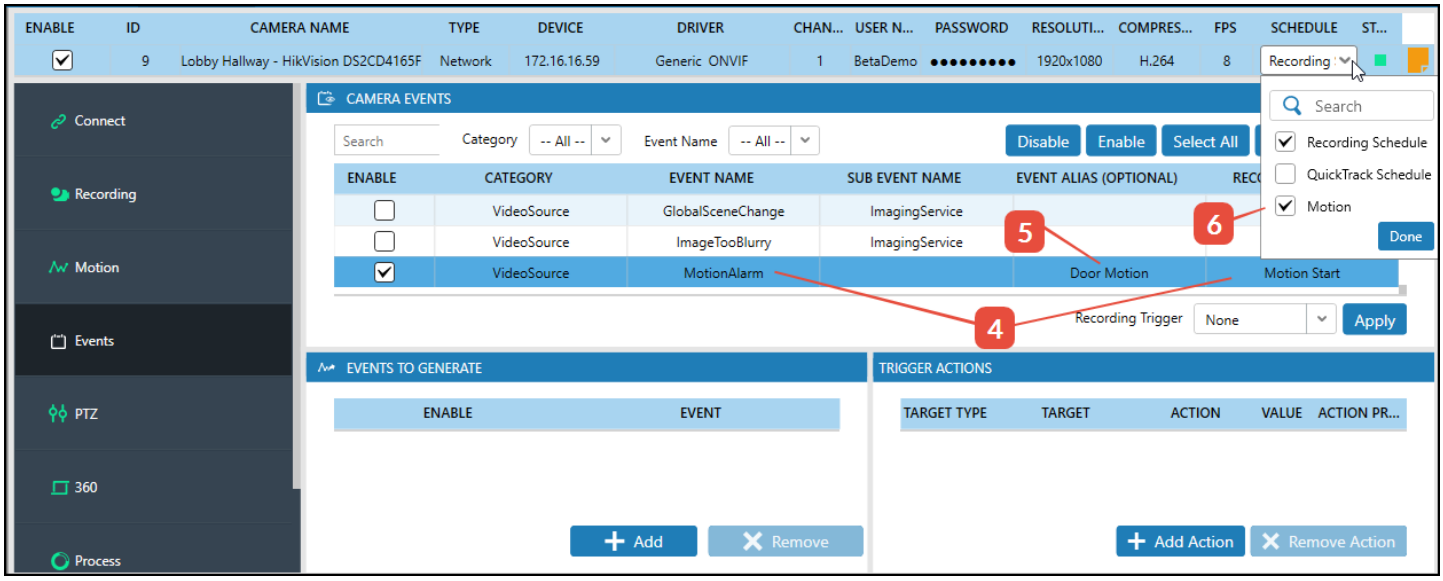
Trigger actions specific to server-based motion detection are configurable in the Motion Panel. The following information pertains to camera-based motion detection.

Steps:

1. Select the camera to be configured for motion detection from the cameras list.
2. From the camera Connect panel, enter the camera's web interface, and configure the camera for "motion detection" (or similar verbiage), per the manufacturer's instructions.
3. Select the camera Recording tab and adjust recording settings as needed.



4. in the Camera Events tab, under display name, locate "Motion Detection" (or similar verbiage) and set the Event to Generate to Motion Start
5. Optionally add an alias
6. In the Camera Title Bar, use the dropdown schedule menu to select a motion record schedule, if created
7. Save the configuration



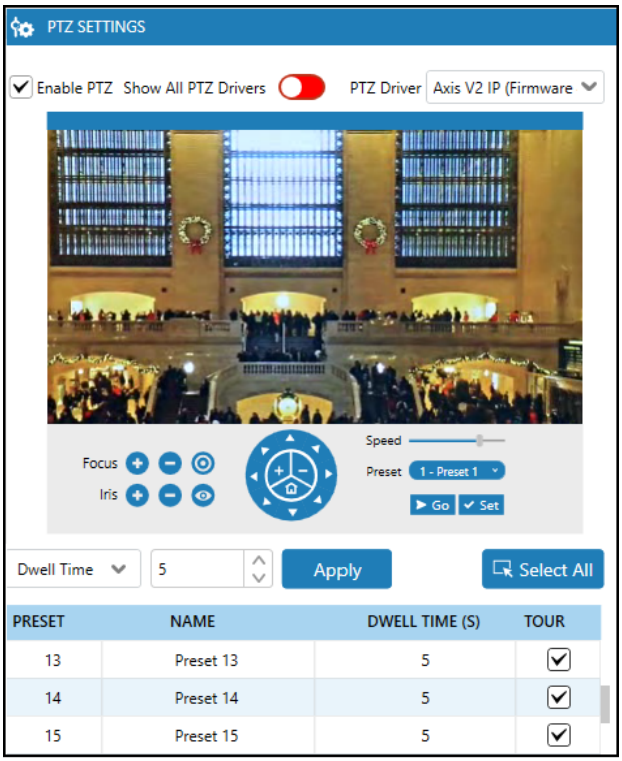
Recording Configuration for On-Camera Motion

Selecting Motion Start requires that the camera must be configured for motion recording in the recording schedule. If Alarm Start is selected, then the camera must be configured for alarm recording in the recording schedule.

Recording Servers Camera PTZ

The PTZ subpanel is used to enable/disable digital PTZ or to enable/disable and configure mechanical PTZ cameras. The Camera PTZ subpanel is divided into four parts, and provides a live image of the camera being configured. From this panel, PTZ presets may be configured, enabled, and combined to create PTZ camera tours.

CompleteView supports many different PTZ camera manufacturers and provides a digital PTZ driver to enable digital Pan Tilt and Zoom for fixed analog and IP cameras. Digital PTZ is defaulted on for all fixed cameras.



PTZ Functionality

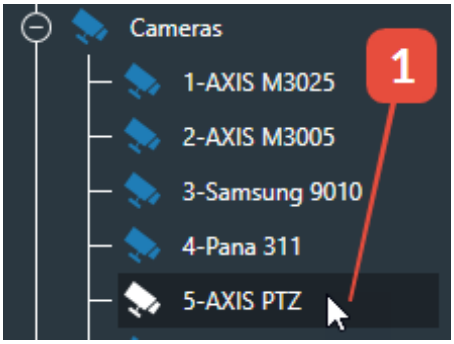
Function	Description
Enable PTZ	Enables/PTZ camera control functions for the selected camera
Show All PTZ Drivers	Displays current list of available PTZ drivers
PTZ Driver	Selects and enables the control protocol that CV should use to communicate with the selected camera
Focus	Focuses the camera
Iris	Adjusts the camera iris
Speed	Adjust PTZ control reaction speed
Preset	Preset position selection
Go	Go to a preset position that is displayed in Preset
Set	Sets current video position and view as a preset position
Select All	Starts PTZ camera tour through all existing presets for the selected camera

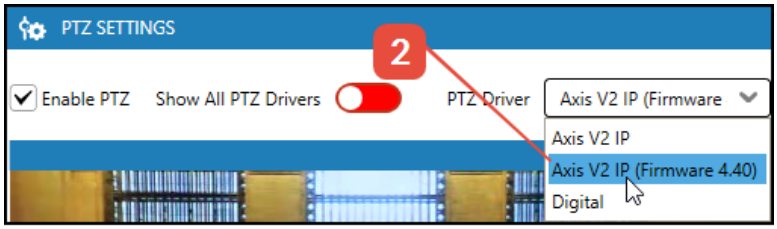
Selecting the Correct PTZ Driver

When added to CompleteView, all cameras are enabled and defaulted to the digital driver. If necessary, change the driver to the correct make and model.

Steps:

1. Select the desired PTZ camera
2. Select the driver from the pulldown menu
3. Save the configuration



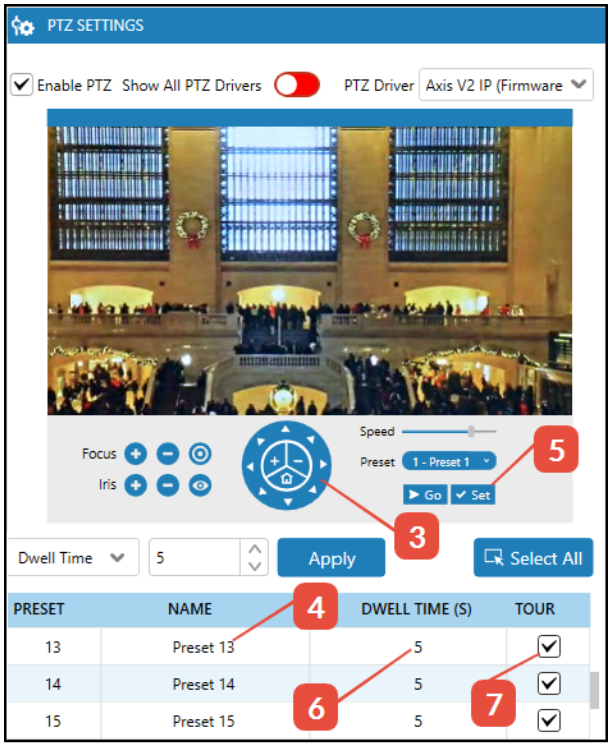


Set PTZ Camera Preset Position(s)

These steps assume the PTZ camera is enabled and has been assigned the correct manufacture driver.

Steps:

1. Select a PTZ camera
2. Select the PTZ subpanel
3. Use your mouse pointer and the PTZ controls to pan, tilt, and zoom the video image to the desired preset position
4. Enter the position name in the box provided
5. Select Set Preset
6. Option: If the PTZ preset is part of a tour, click on the Dwell Time and set the dwell time
7. Option: If the PTZ preset is part of a tour, check the Tour Box
8. Repeat steps 1-9 as necessary to create additional preset positions
9. Save the configuration

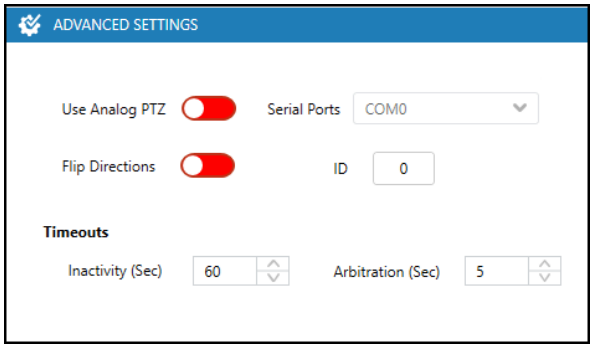


Click to Center PTZ

Users may point and click on the image with the mouse pointer and roller ball to PTZ to the correct preset position. This is called Click to Center. The image pans/tilts toward the mouse pointer. The roller ball zooms the image in and out. This is often a more precise method to PTZ a camera and avoids joystick or other image controls from overshooting the desired PTZ preset position.

Advanced Settings

The Advanced Settings panel allows configuration of elements specific to analog and mechanical PTZ cameras.



1. Use Analog PTZ - allows for the use of an analog PTZ driver on an IP camera. After activating, select the desired PTZ driver from the PTZ Settings pane, as described in Selecting the Correct PTZ Driver above.
2. Flip Directions - inverts left/right movement commands. This may apply to any PTZ camera
3. Serial Port - Specifies which RS-232C serial port on the recording server is used.
4. ID - the serial bus ID of an analog camera that is attached to an analog matrix switch
5. Inactivity (Sec) - is the period, measured in seconds, CompleteView waits in order to detect an idle camera. If no communication has been received during the Inactivity Timeout, the camera is treated as idle. See below for a list of behaviors resulting from the idle condition.
6. Arbitration (Sec) - specifies the back off period that expires when contention occurs between users attempting to control the same camera. See below for more information.

PTZ Inactivity

If the inactivity threshold has been reached:

1. If a preset tour is defined and active, then CV will restart the tour from the beginning.
2. If a preset tour is defined but inactive (a user turned off the preset tour in the CompleteView Desktop Client), and the Return Home after Inactivity timeout has been enabled (see Auto Home below), then CV will show the Home Preset location.
3. If no preset tour is defined, and the Return Home after Inactivity timeout has been enabled, then CompleteView will show the Auto-Home Preset location.
4. If neither a preset tour nor auto-home after inactivity timeout is enabled, CompleteView will do nothing.

PTZ Arbitration

User access to camera PTZ controls is prioritized. The user with the highest priority always gains immediate PTZ control. When users having the same or lower priority contend for access to a camera already under user control, CompleteView initiates the Arbitration.

If the Arbitration expires without any control activity from the user currently granted PTZ access, PTZ control passes to the contending user with the highest priority.

If PTZ activity occurs during the Arbitration, the timeout resets and continues to run.

The arbitration timer continues to run in this manner until PTZ control passes due either to timer expiration or contention from a higher priority user.

Analog to Digital PTZ Communications

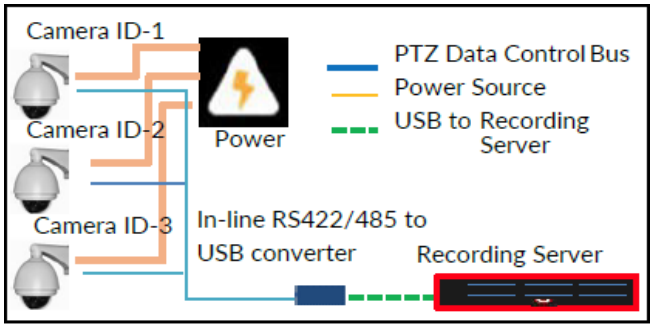
The most common method of PTZ operation is through RS485 serial communications. To enable digital control of analog PTZ cameras that are hosted on an analog matrix switch, a RS232-to-RS485 inline signal converter must be installed.

It is possible to utilize Coaxitron if a serial port (COM-B) on the CM-6700 is configured for RS232 and CompleteView is configured to use the Pelco ASCII PTZ protocol. The CM-6700 converts RS232 to Coaxitron signaling and from Pelco ASCII to Pelco P control protocols.

Analog PTZ cameras may be locally controlled by standard analog MUX and matrix switch/joystick combination or converted to enable digital control if the control data is fed into the recording server via an RS422 or an RS485 to USB inline serial to digital converter.

In-line USB to Serial Converter

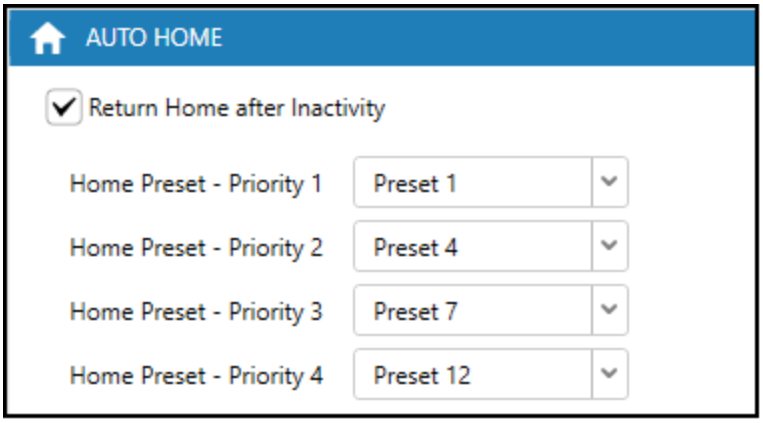
Digital PTZ control requires the installation of an inline USB RS232 to RS485/RS422 serial to digital converter. Analog PTZ cameras that are connected to the Recording Server by USB inline converter should have their unique ID placed into the camera PTZ ID box in Advanced Settings during camera installation.



Auto Home

This panel is used to configure the parameters for returning a PTZ camera to its home position. This panel supports four PTZ cameras' home positions.

Each of the four positions can be associated with a Home Preset schedule located in the schedules panel. The schedule optionally allows a single PTZ camera to be positioned at four Home Priority positions at different times of the day and week.



Return Home after Inactivity - enabled if checked. Returns the PTZ camera to the home position after the designated amount of seconds.

Circumstantial Operation

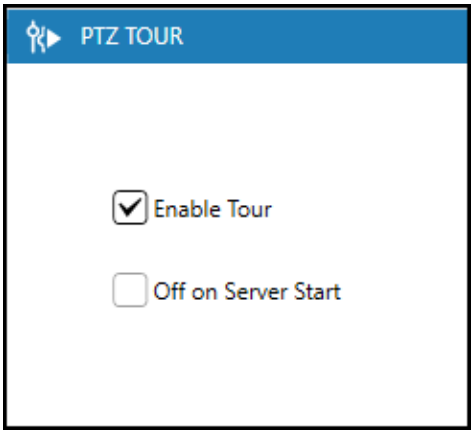
- If a preset tour is defined and active, then CV will restart the tour from the beginning.
- If a tour is inactive, CV will return to the Auto-Home Preset location.
- If a preset tour has not been defined, CV will return to the Auto-Home preset location.

PTZ Tour

The purpose of this panel is to enable a PTZ Tour, set time between PTZ preset positions, and define the time delay after a PTZ tour has been interrupted.

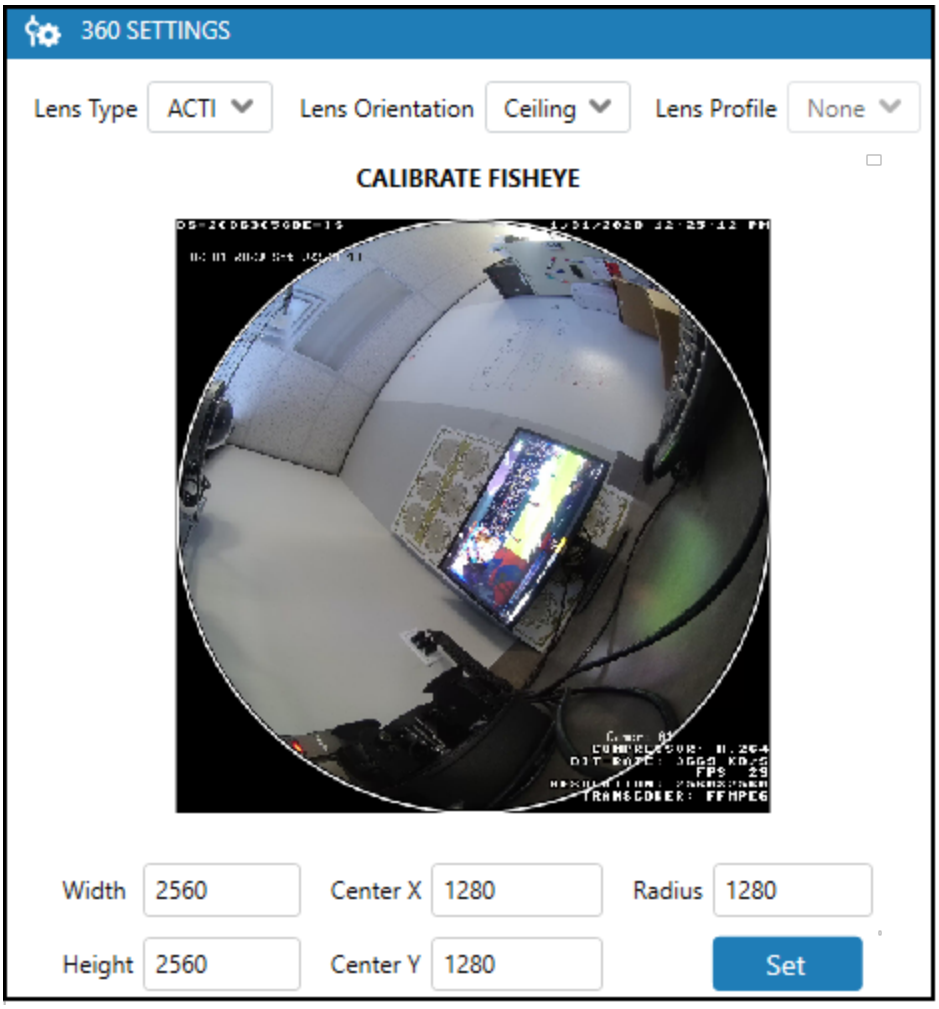
The purpose of this panel is to enable a PTZ Tour, set time between PTZ preset positions, and define the time delay after a PTZ tour has been interrupted.

1. Enable Tour - enables configured PTZ tours
2. Off on Server Start - Tour requires manual startup from Live View: tour will not start when the server reboots



Recording Servers Camera 360 Cameras

Use the 360 Panel to configure a 360° camera. Lens type, orientation, and profile are selected using the pulldown menus, and fields provided. 360° camera X-Y orientation is based upon the camera's API and drivers.

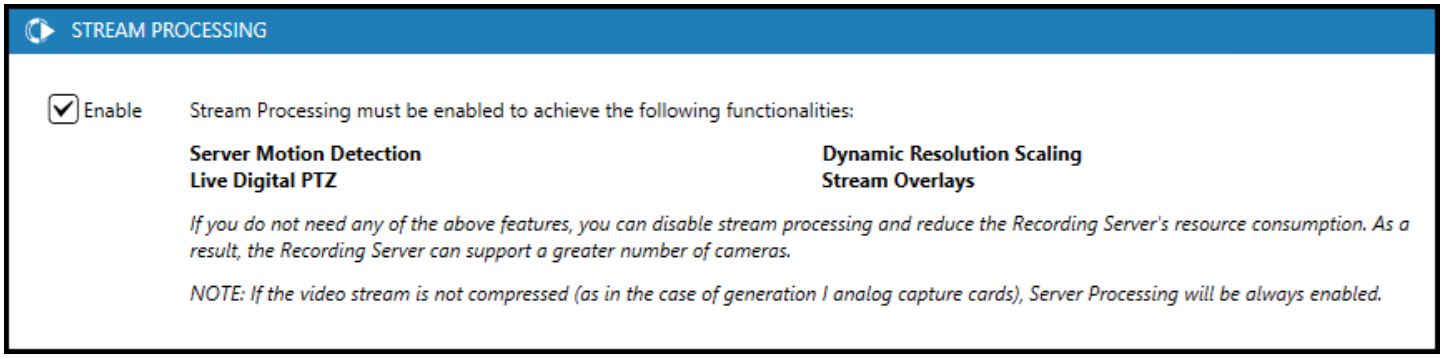


Recording Servers Camera Process

The Process Panel allows access to ancillary camera features. The panel is divided into four parts, Stream Processing, Stream Overlays, Dynamic Video Decoding, and Dynamic Frame Throttling. These settings are grouped together because they allow the Administrator to adjust some of CompleteView's back-end performance settings. Unless necessary, it's best practice to leave settings set to the defaults.

Stream Processing

CompleteView performs Stream Processing on the incoming video stream to provide advanced functionality, including Dynamic Resolution Scaling, Live Digital PTZ, Server Motion Detection, and Stream Overlays. Again, it is strongly recommended to leave Stream Processing enabled.

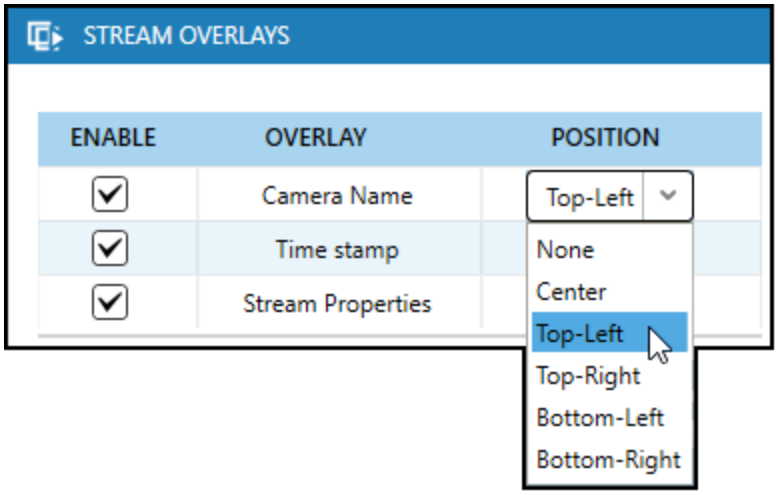


Stream Overlay

Camera name, Time Stamp and (Video) Stream Properties overlays can be enabled/disabled from the Stream Overlay panel. The placement of Camera name, Time Stamp and (Video) Stream Properties may also be changed here.

To change overlay placement:

1. Ensure the Overlay selection is enabled
2. Select the desired position for the overlay
3. Save the configuration



Note: Stream Overlay is on by default and must be configured for each camera.

Stream Overlay: Analog Cameras

Analog cameras must have Stream Overlay enabled with the desired position in the client for camera name and timestamp to be included in live video and recorded video. This is an individual camera setting, and it is highly recommended to have the Stream Overlay enabled and set for each camera for evidential purposes.

Stream Overlay: Network Cameras

Generally, network cameras should have the camera name and time stamp turned on in the network camera's interface, and disabled in the Client's Stream Overlay panel. This is an individual camera setting.

Dynamic Video Decoding (DVD)

DVD monitors which camera feeds are currently being viewed. Feeds that are not being actively viewed are not processed for live viewing by the server, significantly reducing CPU load. It should be noted that feeds configured for Server Motion Detection, Server Video Analytics, and video feeds pushed to Immix (which is typically a server wide setting) will not enjoy the benefits of DVD, as those functions require constant video stream processing. Some cameras are capable of On-Camera Motion Detection which does not rely on the CV server for processing, hence they are able to take advantage of DVD. DVD is compatible with approximately 80% of current camera drivers supported by CompleteView, including Generic RTSP drivers.

DVD Trigger Events

- One or more live video streams is being viewed from any CV video application that permits live viewing
- Any analog or network camera is configured to enable server-based motion detection. Camera-based motion detection does not require server stream processing
- Agent VI analytics is used and requires support from the Recording Server. Only those cameras requiring support for Agent VI are affected
- When Immix Protect is enabled, DVD is disabled for all cameras
- When a camera's stream is transcoded by the server from one compression type to another prior to recording
- Video dewarping is required for a fisheye lens or multi-stream camera
- **Important Note:** DVD applies exclusively to Recording Server performance during live video streaming to the client

Dynamic Frame Throttling (DFT)

When Dynamic Frame Throttling (DFT) is enabled, CompleteView monitors incoming video queue length. When queue length exceeds a certain threshold set in Server Configuration Advanced panel, DFT engages and processes only key video frames until the queue length is restored to normal levels. This helps reduce video latency, maintain video quality, and reduce CPU load. The frame throttling only affects live video to CV clients. Playback is unaffected, and all video data is available for review. When DFT is applied to a video stream, a start/stop log entry is created, and an overlay is displayed indicating DFT activity. Analog cameras are not impacted by DFT.

By default, DFT is "Enabled." In almost all cases, DFT should remain enabled, unless directed by Technical Support or a Field Systems Engineer to disable it. DFT does not affect recorded video, and if activated generally lasts only for a few seconds before CV returns to normal operation.

Advanced

Advanced options include video quality, port, and other settings. The defaults are configured to provide optimal performance, and making changes should only be done by a qualified individual who understands the impact of the changes, or by direction of Salient Technical Support.

Camera Ports

Camera ports allows for certain commands and data to be sent and received over specified ports for certain ACTi and others cameras.

Control Port

Enter the port over which commands to/from the camera will be sent.

Stream Port

Enter the port over which the video stream to the camera will be sent.

Connection Settings

Connection Settings is intended to give the end user options that affect video quality and use of HTTP for PTZ joystick command and control.

Favor Continuous Video Over Image Quality

This option allows the user to choose between image quality and continuously streaming video. It relates to cameras that employ User Datagram Protocol (UDP) as their favored IP transport protocol. Some camera manufacturers prefer UDP as their primary video transport protocol because it may provide slightly quicker streaming.

User Persistent HTTP Connection for PTZ (Joystick or mouse control)

Persistent HTTP employs a single TCP connection to send and receive multiple HTTP request-s/responses, as opposed to opening a new connection for every single request/response pair. The benefit of enabling Persistent HTTP is generally quicker PTZ responses.

Keep Alive Method

Keep-Alive configuration is available on select Axis cameras streaming MPEG4 or H.264 only. When “Auto” is selected, the server will determine the optimal means of sending and receiving keep-alive messages to the camera, and is the preferred method of configuration. For the purposes of troubleshooting and addressing camera connectivity issues, the user may force CompleteView to util-ize RTCP Receiver Report or RTSP OPTIONS, based on the camera’s firmware version.

Auto

Auto automatically selects the optimal method for the circumstances, and is the default option.

RTCP Receiver Report

The primary function of RTCP is to provide feedback on the quality of service (QoS) of video and audio distribution by periodically sending statistics information (reports), such as transmitted octet and

packet counts, packet loss, packet delay variation, and round-trip delay time to the server. Administrators may use this information to control the quality of service parameters, perhaps by limiting flow or using a different codec.

RTSP Options

Like HTTP, RTSP uses TCP to maintain an end-to-end connection and, while most RTSP control messages are sent by the client to the server, some commands travel from the server to the client. While similar in some ways to HTTP, RTSP defines control sequences that are useful in controlling multimedia.

Recording Servers Alarms

CompleteView is capable of integrating with third party digital I/O devices. Digital inputs detect and digital outputs assert external alarm conditions.

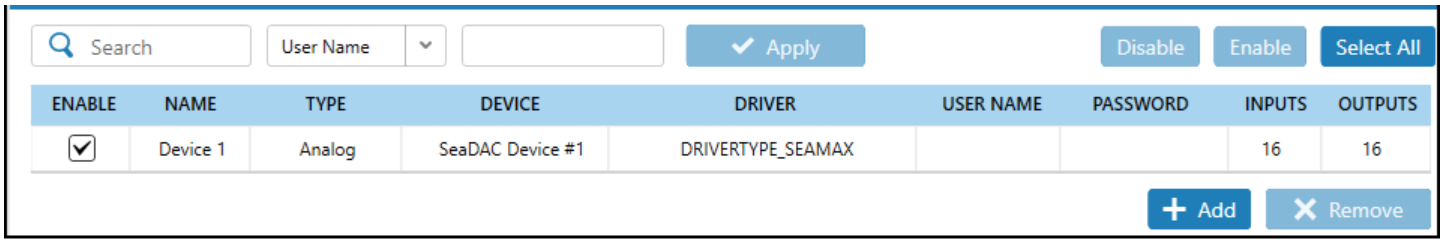
Alarm inputs can be used to trigger a number of actions including recording from specified cameras, moving a camera to a preset, or activating an alarm output.

Alarm outputs from CV indicate the occurrence of camera events such as camera sync loss or other external events.

Alarm devices can be associated with IP or analog cameras. It is possible to add a single device or any combination of alarm devices to a Recording Server, contingent upon hardware configuration.

Alarm Panel

The Alarm panel is similar to the Cameras Panel. The top portion of the panel displays added devices and their information.



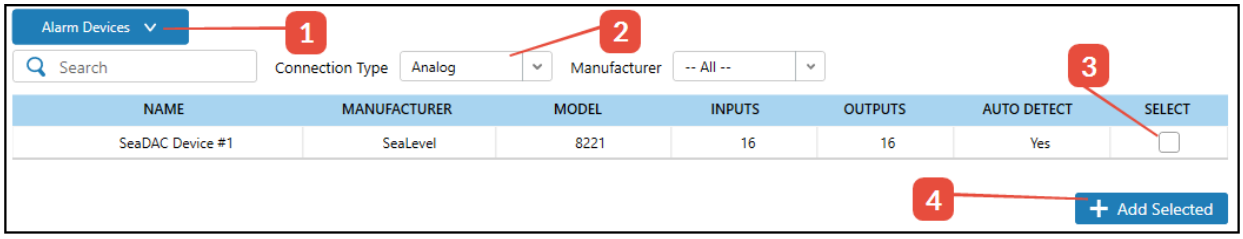
Alarm Device Discovery

The bottom of the panel hosts an Alarm Device button. When pressed, the button produces a panel that displays discovered Alarm devices that are ready to be added to the Recording Server. Any device that was previously added will be displayed above the new devices.

Discover and Add an Alarm Device

Important: Third-party I/O devices that require Windows drivers for operation will need the drivers to be installed prior to adding the Alarm device into CompleteView.

Steps:



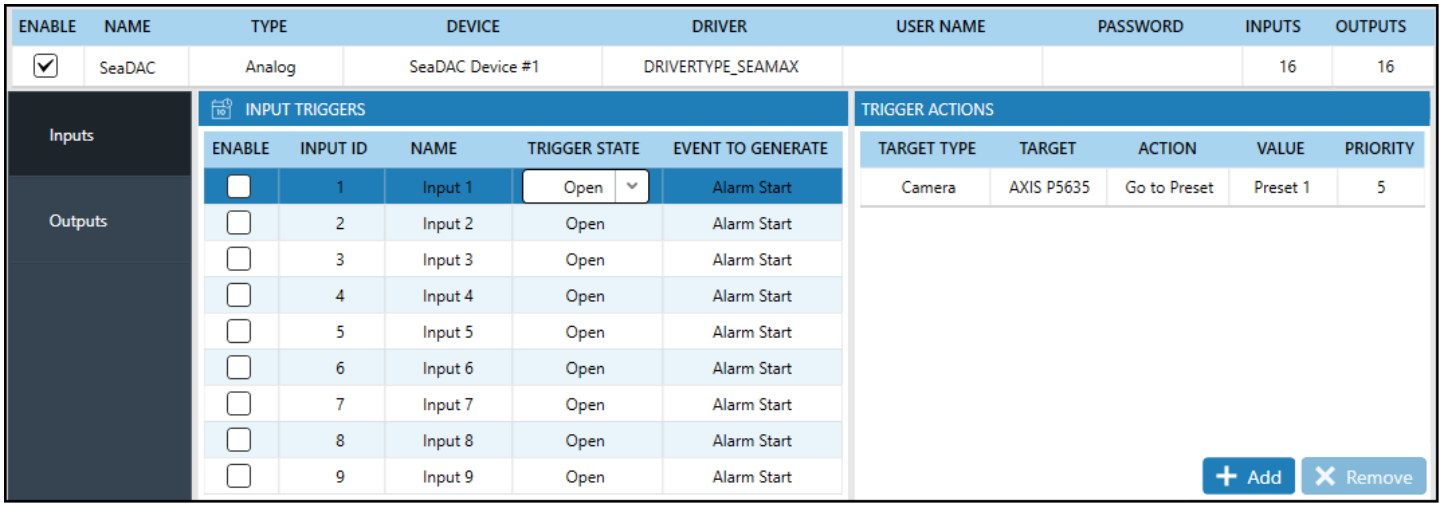
1. Select the Alarm Devices button to display discovered I/O devices
2. Connection Type must be Analog
3. Select the desired I/O device for installation by selecting the devices checkbox

4. Press Add Selected
5. Save the configuration

The name of the device may be changed, but all other device information is predetermined by the device driver, and cannot be altered.

Input-Output Triggers

Selecting the I/O device presents options for configuration. Individual Input and Output panels can be selected from the left. Above the panels resides the device's specific information.



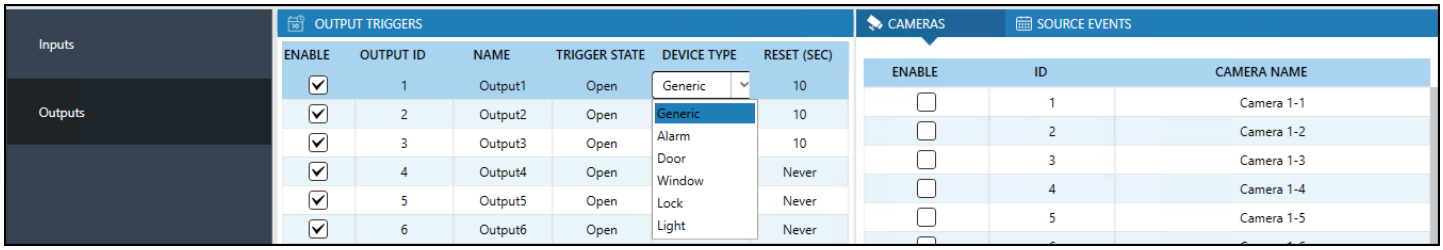
Input Triggers

Name	Description
Enable	Checked box enables the input channel
Input ID	Channel number, which is a fixed value
Name	Initially "Output Number, Input Number" but may be manually changed
Trigger State	Open, Closed, Unknown
Event to Generate	Input Activated

Trigger Actions

Name	Description
Target Type	Lists target device type
Target	Name of target device
Action	Action to be taken upon trigger

Name	Description
Value	Device-specific result of action
Priority	Priority of action

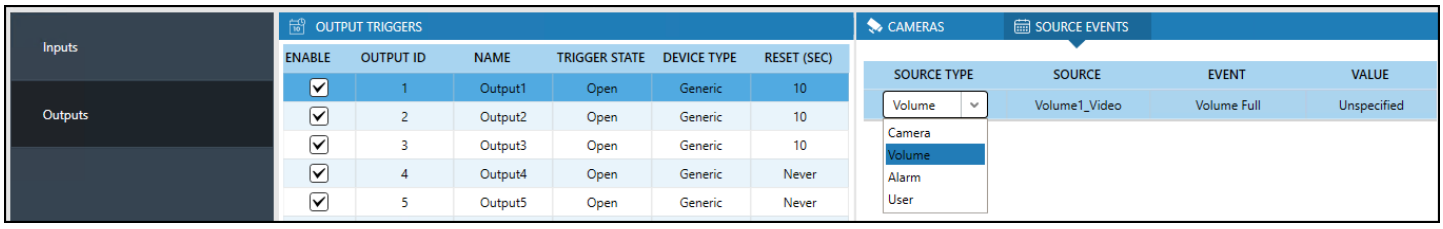


Output Triggers

Name	Description
Enable	Checked box enables the output channel
Output ID	Channel number-fixed
Name	Initially “Output Number, Input Number” but may be changed
Trigger State	Open, Closed
Device Type	Generic, Alarm, Door, Window, Lock, or Light
Reset (Sec)	Resets the Output to default: Never, 1-100 seconds

Cameras

Name	Description
Enable	Checked box enables the Camera
ID	Channel number-fixed
Camera Name	Name from Camera Configuration



Source Events

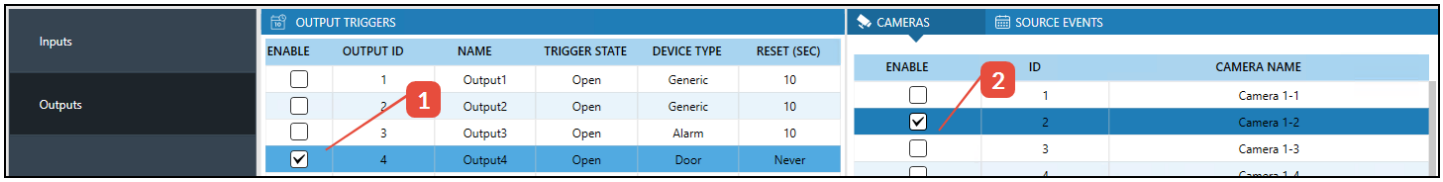
Name	Input Description
Source Type	Camera, Volume, Storage Pool, Alarm, User
Source	Name of event source
Event	Name of event, dependent upon device
Value	Outcome, dependent upon device

Associating Alarm Device Outputs with Cameras

After adding and configuring the device, its outputs may be associated with a camera to allow for manual triggering by a user. In the example below, the device's Output4 may be triggered by the user while viewing Camera 1-2.

Steps:

1. Select the device's outputs to be associated with a given camera.
2. Select the camera.
3. Save the configuration.



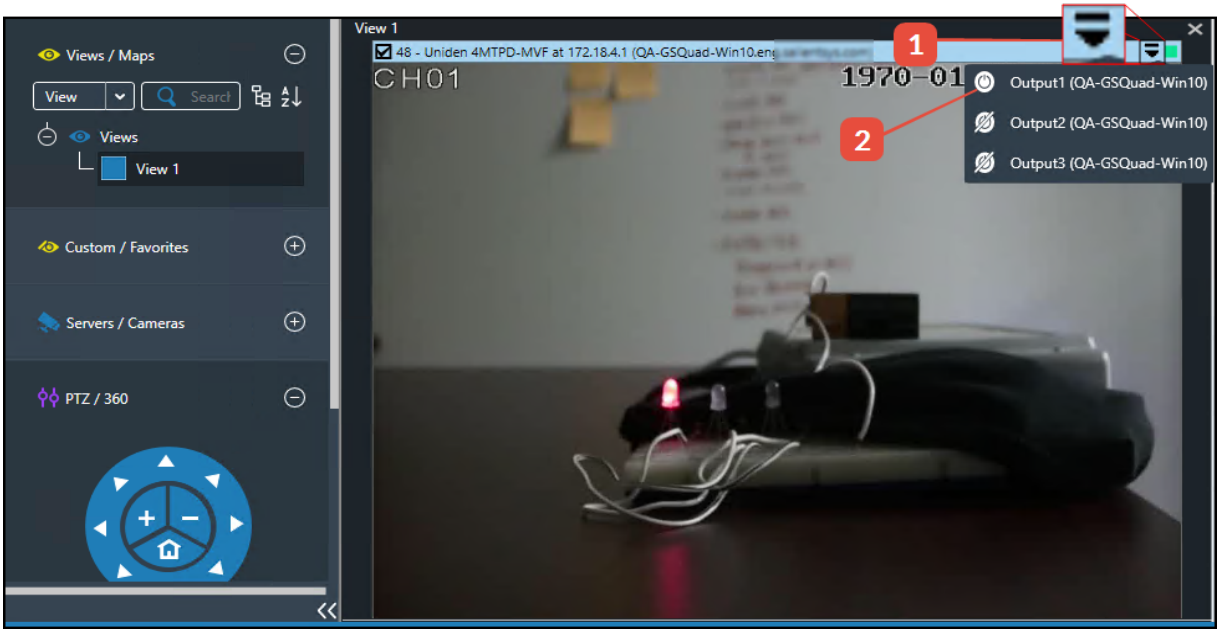
To associate Alarm Device Outputs to cameras within a View, see Views & Maps Creating Views and Templates .

Triggering Output Manually

Outputs may be manually triggered within Live View (cameras in view layout, camera being viewed live in the Video Player pane), Dashboard (camera being viewed live in Video Player pane), and Alarm View (camera pop-up and camera being displayed in Video Player).

Steps:

1. Select the Output Triggers icon in the upper right corner of the camera window.
2. Select the desired Output.



Different output types are represented by different icons.

Alarm Device Icons

Icon	Description
	Alarm Device
	Door Alarm Device
	Generic Alarm Device
	Lock Device
	Window Device
	Indicates multiple alarm devices

Recording Servers Triggers

Triggers provides the ability to create event based trigger actions from one place, also known as "Event Linking," where an event generated by resources (such as cameras, volumes, storage pools, etc.) can be linked (or configured) to trigger one or more actions on resources (such as cameras, volumes, storage pools, etc.).

Triggers can be created for the following sources and the events they generate:

Trigger Sources and Events

Camera	Storage	Volume	Alarm	User
Alarm start/end	Insufficient Retention	Offline	Input activated/deactivated	Login/logout
Motion start/end	Minimum Retention Violation	Online	Output activated/deactivated	Failed login
Sync loss/gain	Pool Drive Offline/Online	Full		Start live view/-playback
DFT start/end	Delete Failed	Recording Failed		Export
Recording Started After Failed	Free Pool Space Failed	Video Export		
Recording Failed	Overflow Drive Active/Inactive	Min Storage Violated		
	Minimum Camera Retention Active			
	Storage Threshold Met			
	Storage Write Failed			

Currently, the following types of actions can be created as triggers:

- Trigger a camera action: motion recording, alarm recording or sending to a preset
- Trigger an alarm action: trigger an alarm output (I/O device)

Trigger Actions/Source Events Panels

If an input is configured, a matching Trigger Action must also be configured for the Action resulting from the input. If an output is configured, then a Source Event must be configured for an event and desired event action. There are several input and output variables that can be configured.

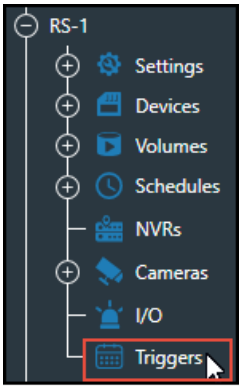
Triggers

The purpose of the Triggers Panel is to centralize all the Triggered Actions across a Recording Server's alarms and cameras. Changes to Trigger Actions that were originated in the Motion, Events, or Alarms can be modified from the Trigger Actions Panel. Additionally, new Trigger may be created and configured from this panel, associated with actions.

Summary View

Selecting Triggers at the top of the triggers list opens the overview screen which will display a summary with all of the triggers that have been created on the recording server.

The source event in the illustration below was established for a camera in the Motion Panel. When a Source Event is selected, the information for the event is displayed at the top of the panel.



The source event in the illustration below was established for a camera in the Motion Panel. When a Source Event is selected, the information for the event is displayed at the top of the panel.

ENABLE	NAME	SOURCE TYPE	SOURCE	EVENT	VALUE	TARGET TYPE	TARGET	ACTION	VALUE	PRIORITY
☑	Trigger 1	Alarm	Device 1	Input Activated	Input 1	Camera	AXIS P5635	Go to Preset	Preset 1	5

SOURCE EVENTS

SOURCE TYPE	SOURCE	EVENT	VALUE
Alarm	Device 1	Input Activated	Input 1

TRIGGER ACTIONS

TARGET TYPE	TARGET	ACTION	VALUE	PRIORITY
Camera	AXIS P5635	Go to Preset	Preset 1	5

Add Remove

The Trigger may be disabled but retained by unchecking Enable on the top left corner. Other changes can be made from the top of the panel or from the Trigger Actions panel with pull-down menus. Changes that are made here will also be reflected in their originating location.

Alarm Device Example Implementation

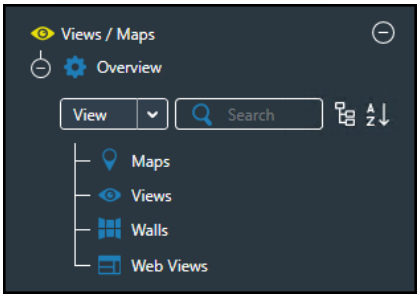
The information below is intended to outline the general work flow of adding and configuring an external Alarm Device in CompleteView.

Steps:

1. Add an Alarm Device either by either selecting the Alarm Devices list, described in **Recording Servers Devices Summary**, or by manually adding it via the method described in **Recording Servers Alarms**.
2. Enable the desired inputs and optionally set names and triggers for each one, as described in **Recording Servers Alarms**. Triggers can include, but aren't limited to initiating recording on a camera, sending a camera to a preset, or activating an alarm output.
3. Enable the desired outputs and optionally set names, device types, and reset times for each one, also described in **Recording Servers Alarms**.
4. Associate the output triggers to a camera in order to allow the user to manually activate and deactivate the output. Events may be also configured to automatically trigger the output. Events can be from a camera, alarm, user, volume, or storage pool. Associating the output triggers to an individual camera is discussed in **Recording Servers Alarms**. Note that using this method requires the cameras to reside on the same server as the device. To add the output triggers to a camera in a View, see **Views & Maps Creating Views and Templates**. This method has the advantage of allowing the camera and device to reside on different servers.
5. Administrators can set user and group level permissions to access the outputs, described in **Users & Groups Configuration**. If the user has access to a camera but not the output trigger associated with it, only the camera will be visible, not the output trigger.
6. Finally, trigger outputs from Live View, Dashboard and Alarm View, described in **Live View Overview**.

Views / Maps Introduction

Views are collections of cameras and video devices available to users when they log into CompleteView. There are two types of Views: Universal and Desktop. Universal Views are generally created by an administrator and universally available to any user, while Desktop Views are created by individual users, and are also available to other users. Both view types may be created by end users as custom views. In addition, Universal Views maintain selected cameras' aspect ratios, and are the optimal choice for 4:3 and 16:9 camera layout, while Desktop Views maintain the viewing tiles' aspect ratios, and is the better choice for panoramic and corridor cameras.

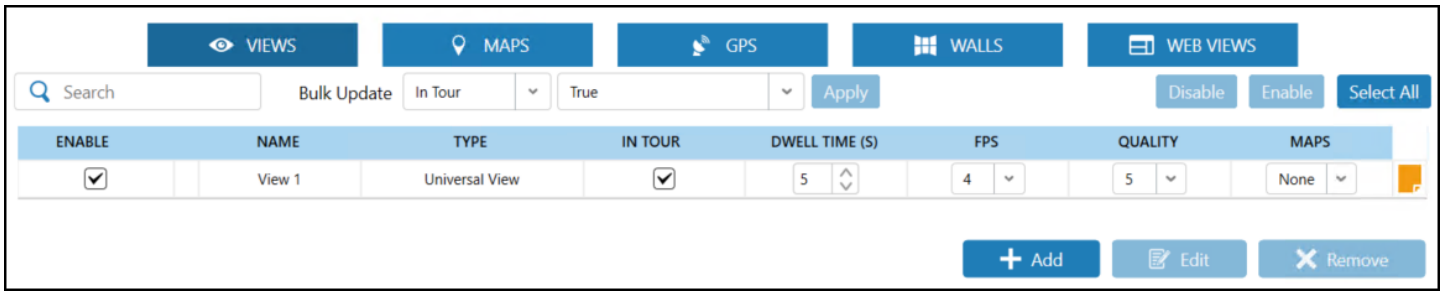


Within Views, Maps, Video Walls and Web Views may also be added and configured. Refer to Video Wall Introduction and Web Views for more information.

Note that non-administrator users may need to be granted access to Views. For more information on View permissions, see Users & Groups Configuration.

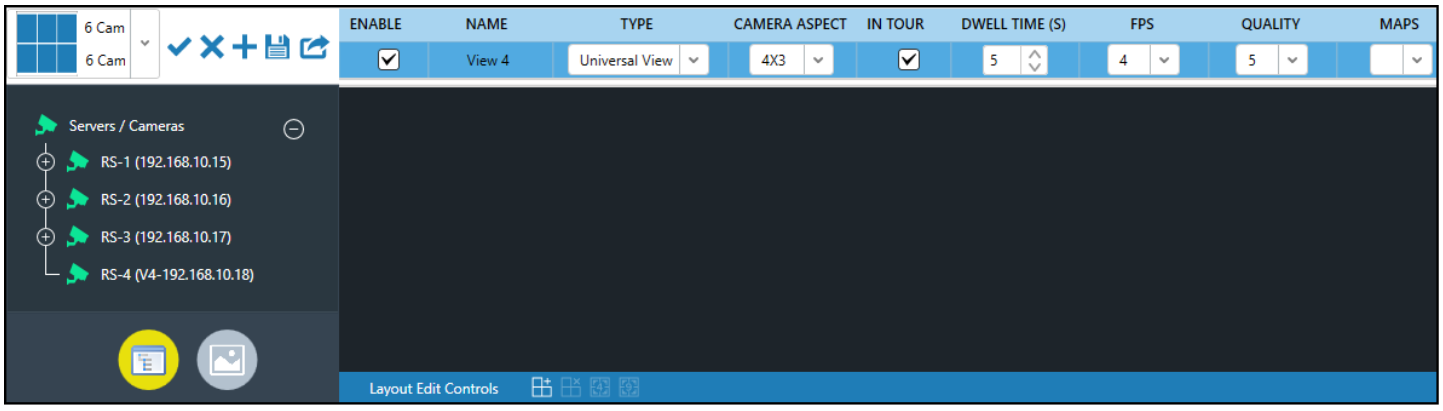
Views / Maps Overview

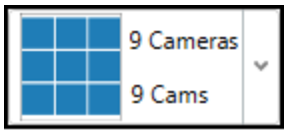
Selecting Overview will produce the following menu from which Views / Maps features may be accessed. A dynamic list of Bulk Update options will be displayed, whose functionality will depend on which feature is selected. Details for the various functionalities will be described in the following sections.



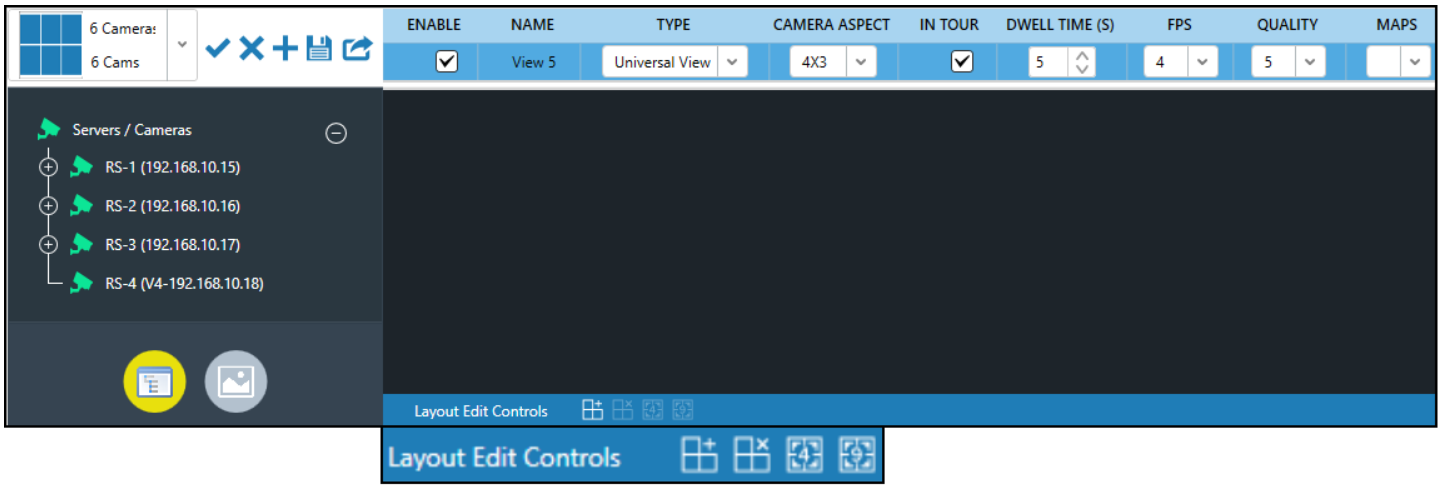
Video View Creation Tools

Client Views provides practical tools and processes to create live view templates, views, and maps for all Recording Servers.



Icon	Purpose
	Pulldown menu of saved templates.
	Apply the template that is presently displayed in the menu.
	Delete the template that is presently displayed in the menu.
	Add the existing view layout as a new template.
	save the presently displayed view layout to the template menu.
	Exports the selected template
	Display servers and their cameras in a heirarchical view by name.
	Display servers and their cameras in a thumbnail view with names.

View layout editing controls are at the bottom of the view layout panel, immediately below the video layout.



Icon	Description
	Add video cell

 Delete a video cell

 Split a single existing cell into a 2x2 in the same original cell

 Split an existing cell into a 3x3 in the same original cell

 In the *View Title Bar*, clears the current layout

 In the *View Title Bar*, saves the view for use without saving it as a template

 In the *View Title Bar*, opens a menu to create new views, new auto-views, and new maps

 In the *View Title Bar*, opens a quick-link menu for all overview panels

View Construction Parameters

Above each view is an Information Title Bar. Changing the information in the Title Bar affects the view's structure, name, maximum FPS, and defines its association with a map.

View Parameters

Menu Item	Description
Enable	Enables the currently displayed view in Live View
Name	View name; defaults to view and next number in order. The name may be changed by clicking in the box and typing in the new name
Type	Desktop or Universal. Both are available to all users. Universal

Menu Item	Description
	Views maintain cameras' original aspect ratios, and are preferred for use with 4:3 and 16:9 cameras. Desktop Views maintain selected viewing tiles' aspect ratios, making them the better choice for panoramic or corridor cameras.
Camera Aspect	Administrator sets the cell size when configuring the view. Choices are: 4:3, 16:9, and 9:16. The ratio selection applies to all cells within the view.
In Tour	When checked, places the View in a “View-Tour.”
Dwell Time	The length of time between each view is presented before the next is displayed in a View-Tour, in seconds.
FPS	Allows users to set the frame rate for the current camera from among the following choices: 1, 4, 8,15, 30; The maximum number of frames-per-second delivered while viewing live video will never exceed the rate configured by the administrator on the Recording Server.
Quality	Sets the video compression visual quality (low, medium, high) for all currently selected cameras.
Maps	Permits the Administrator to associate the view under construction with the maps that are listed in the pull-down menu

Views & Maps Creating Views and Templates

There are two methods for creating views and templates. Drag and Drop permits the creator to drag the video from servers into the video display area. The Client allocates equal space for the placement of each camera as its dropped into the area. The resulting view can be saved as a template, which may be used for future use for other views.

The second method requires the creator to use Template and Layout Edit controls, naming and saving the template. Video may be added to the template after it is created. An unlimited number of templates can be created and saved. Using the template tools, a template-cell can be subdivided into 2x2 or 3x3 cells.

For clarity, some UI elements may be omitted from the following information.

Manual Creation

The following methods of creating views and templates lend themselves to custom configuration, requiring manual selection of specific cameras for specific views.

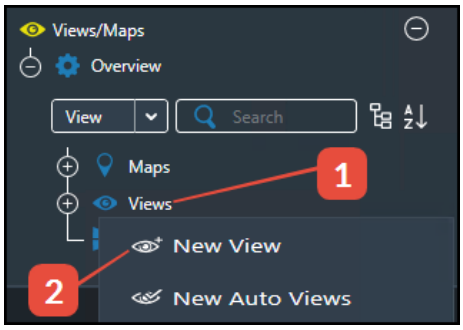
Drag and Drop

The drag and drop process can be used to name and save the view as a template. Views do not have to be saved as a template.

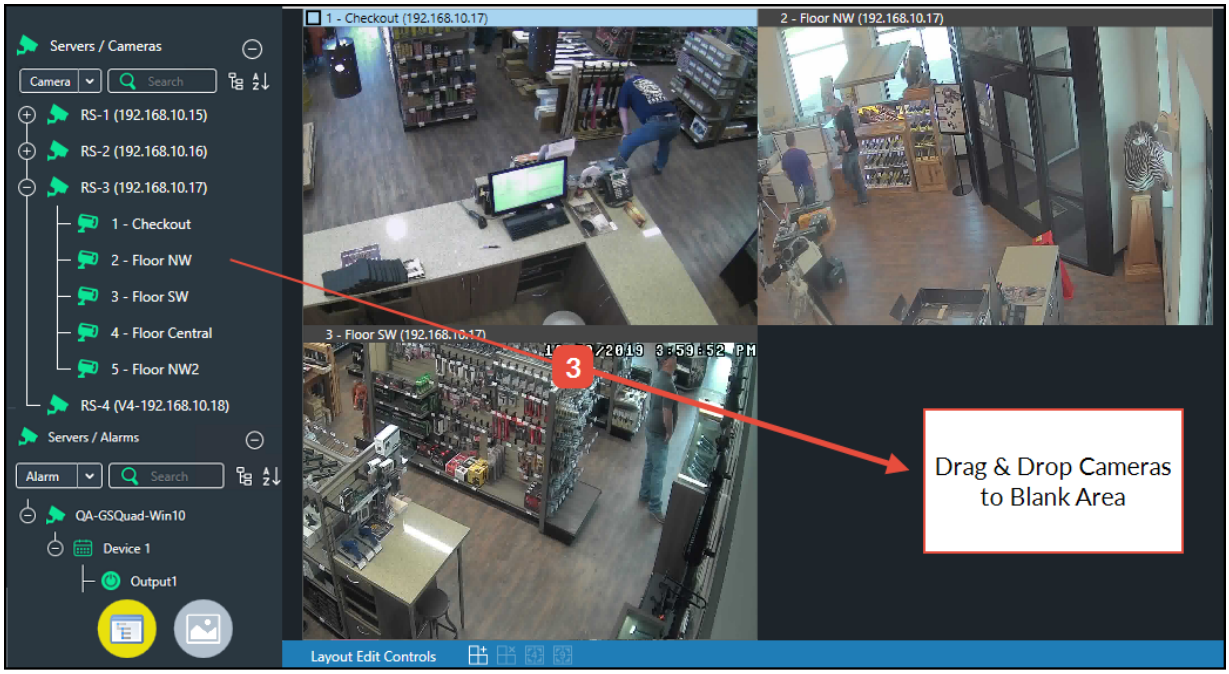
Steps:

1. Right-click on Views
2. From the menu that appears, select New View

Note: Wait for the View Creation Panel to appear with the list of Recording Servers displayed to the left

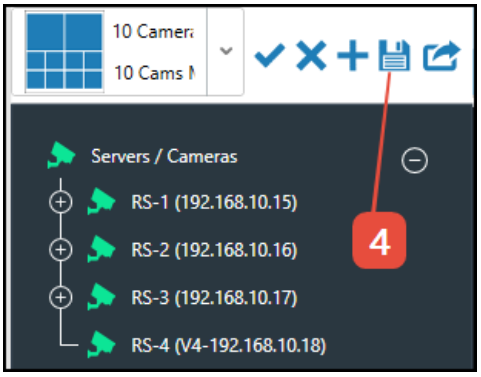


3. Drag video cameras from list of the available Recording Servers onto the large blank area to the right.



Important Note: to build the template, drop the desired video onto some portion of the blank area beside the presently existing video camera feeds.

4. **Optional:** save the view as a template
5. Save the configuration

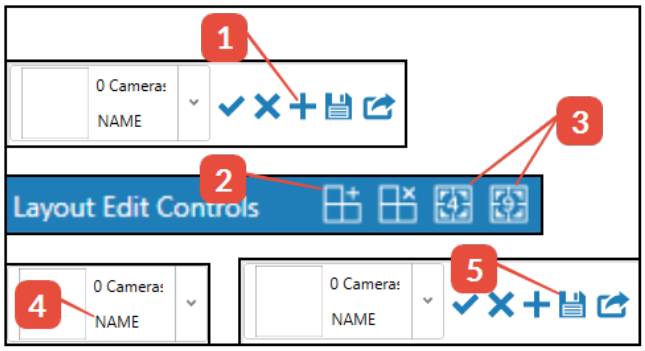


Create View Templates

Client Views must be open to proceed. View templates may be saved and repeatedly used for quick, flexible, and customized view creation.

Steps:

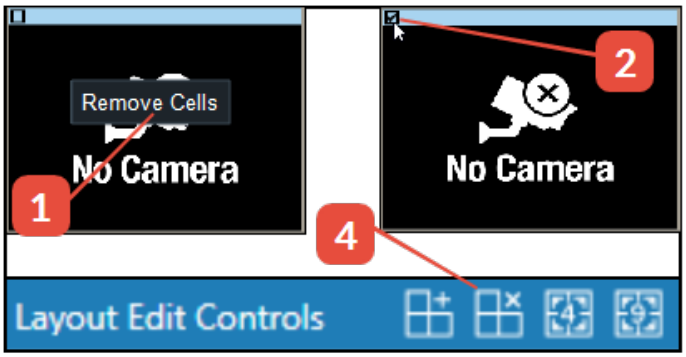
1. Select Add Template (+)
2. Repeatedly click on Add Cell until the desired number of video cells are displayed
3. **Optional:**use the Layout Edit Controls to split cells
4. To name the template, select and type over the existing name
5. Save the template



6. Save the configuration

Delete a Template Cell

Steps:



1. Right-click on the cell to be removed and select remove cell

   **Method 2

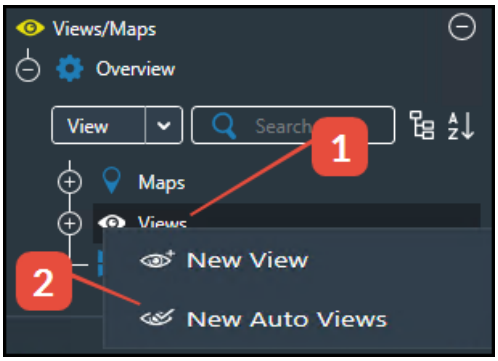
2. Select the checkbox in the top left of the camera tile
3. **Multiple Cell Removal:** multiple cells may be simultaneously removed by checking the checkboxes of the cells to be removed before proceeding to the next step
4. Use the Layout Edit Controls; select remove cell
5. Save the template
6. Save the configuration

Automatic Creation

Auto Views create a series of views based on camera count per view (choices: 1,4, 9,16,25,36,49,64,81, and 100) camera aspect ratio (choices: 4x3, 16x9, 9x16) and permit the inclusion of Site Name, Server Name, and the replication of the Server Hierarchy into the overall view construct. During Auto View construction, the Administrator selects the server and the options. Note that if creating an Auto View for a Region a Recording Server must be associated with that Region.

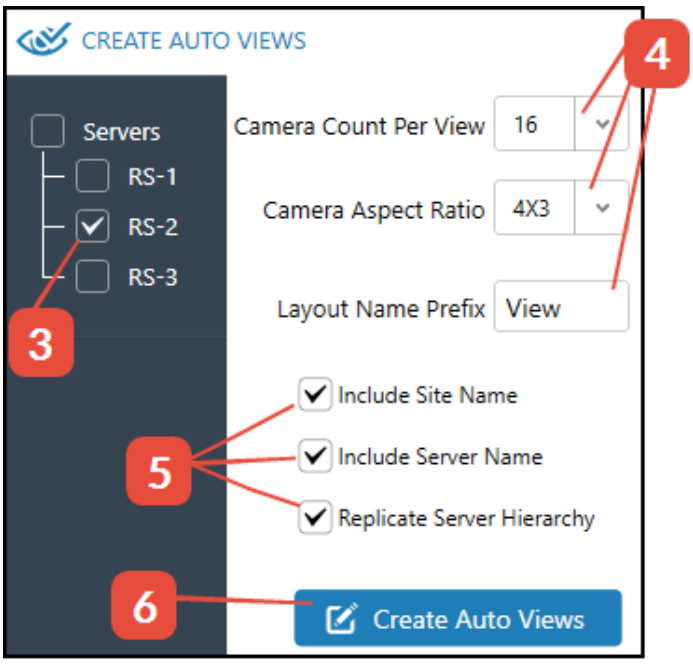
Universal Auto View

Steps:



1. Right-click on Views
2. Select New Auto View; wait for the screen to change Note: The new screen will display the Recording Servers with checkboxes to the left of the Recording Server names.
3. Check the box of a single Recording Server for which the AutoView is to be constructed

4. Select:
   a. Camera Count per view
   b. Camera Aspect Ratio
   c. Layout Name Prefix
5. Check the desired boxes:
   a. Include Site Name
   b. Include Server Name
   c. Replicate Server Hierarchy
6. Select the Create Auto Views button
7. Save the configuration



Desktop Views

Desktop Views are customized views created by individual users, and are available to other clients, as well.

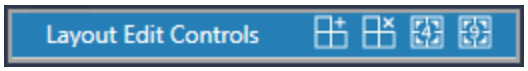
Desktop Templates - Layout Edit Controls

Desktop Views have their own template creation process; Universal View templates are not available when Desktop View is selected. The layout toolbar resides below and to the left of the large blank video template creation area. The icons are dynamic. Roll over an icon to reveal its function in the context of the view being created.

Desktop Layout Edit

Icon	Function/Description
	Add row to the top
	Add row to the bottom
	Add column to the left
	Add column to the right
	Delete selected row
	Delete selected column
	Split selected cell horizontally

Universal Layout Edit

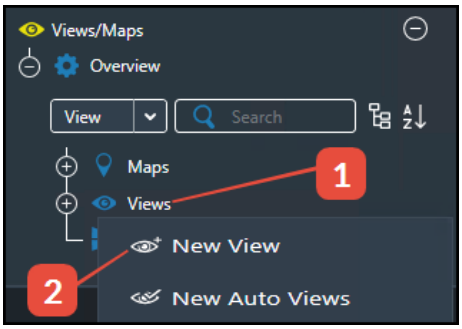


Icon	Function/Description
	add cell
	Remove cell
	Split cell 2x2
	Split cell 3x3

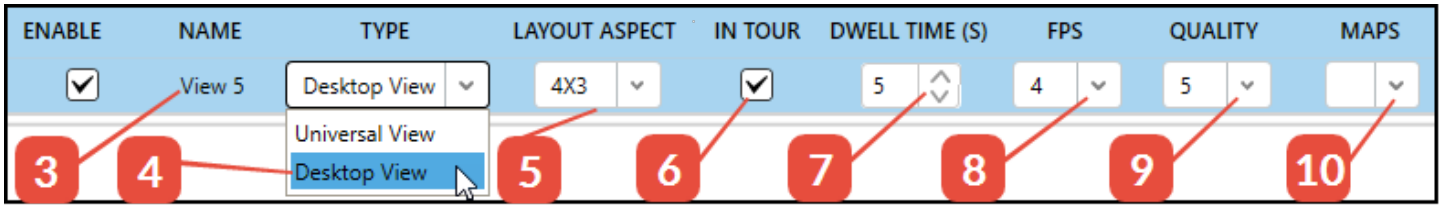
Desktop Layout Edit	Universal Layout Edit
 Split selected cell vertically	
 Merge cells	

Create a Desktop View

Steps:



1. Select Views
2. Select New View
3. Name the view (click in the box and type over the default)
4. Select Desktop View (from the pull-down menu)
5. Select the desired Aspect Ratio (4:3, 16:9, 9:16)
6. If desired, include the view into a sequential video view tour
7. If the view is part of a sequential video tour, set the dwell time
8. Set the maximum Frames Per Second (FPS)



Note: FPS defines Live Viewing video stream fluidity. Higher FPS creates a more fluid video presentation. This setting is a general setting for live viewing video and is regulated not to exceed the FPS set for cameras in the Recording Server.

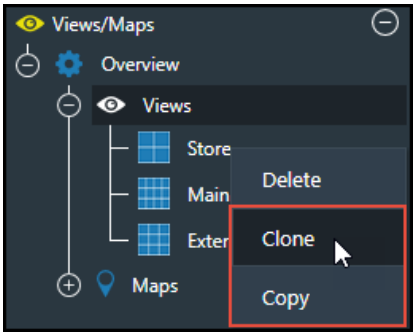
9. Set Quality (range is 1-10; ten is the highest quality and lowest compression)

Note: Quality is setting a general video client, live view, quality setting. It cannot be increased above the settings of the Recording Server.

10. Associate a map, which should be presented as the default view when the desktop view is selected in Live View
11. Use the Layout tools to create a template
12. Drag and drop the video into the template
13. Save the Configuration

Views Clone/Copy

Once created, a View may be cloned or copied by right clicking on the view's name, and selecting either Clone or Copy.

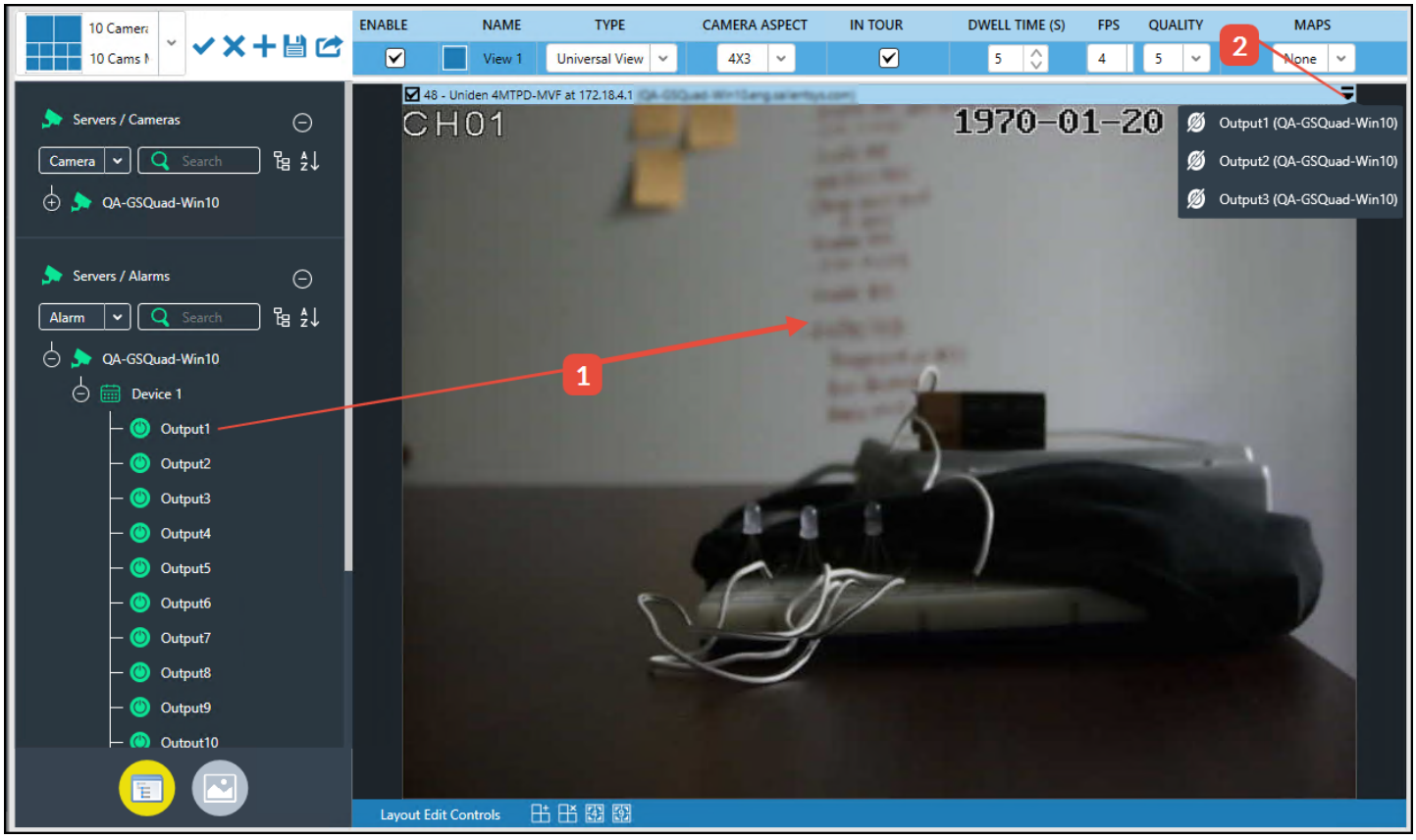


Adding Alarm Output Triggers to a View

Once a camera has been added to a view, outputs from a preconfigured Alarm device may be associated with it, and triggered from within Live View.

Steps:

1. Drag the desired output to the camera
2. Click the icon in the upper right corner to view added outputs



To remove outputs, right click on the camera, and select Remove All Output(s).

Maps

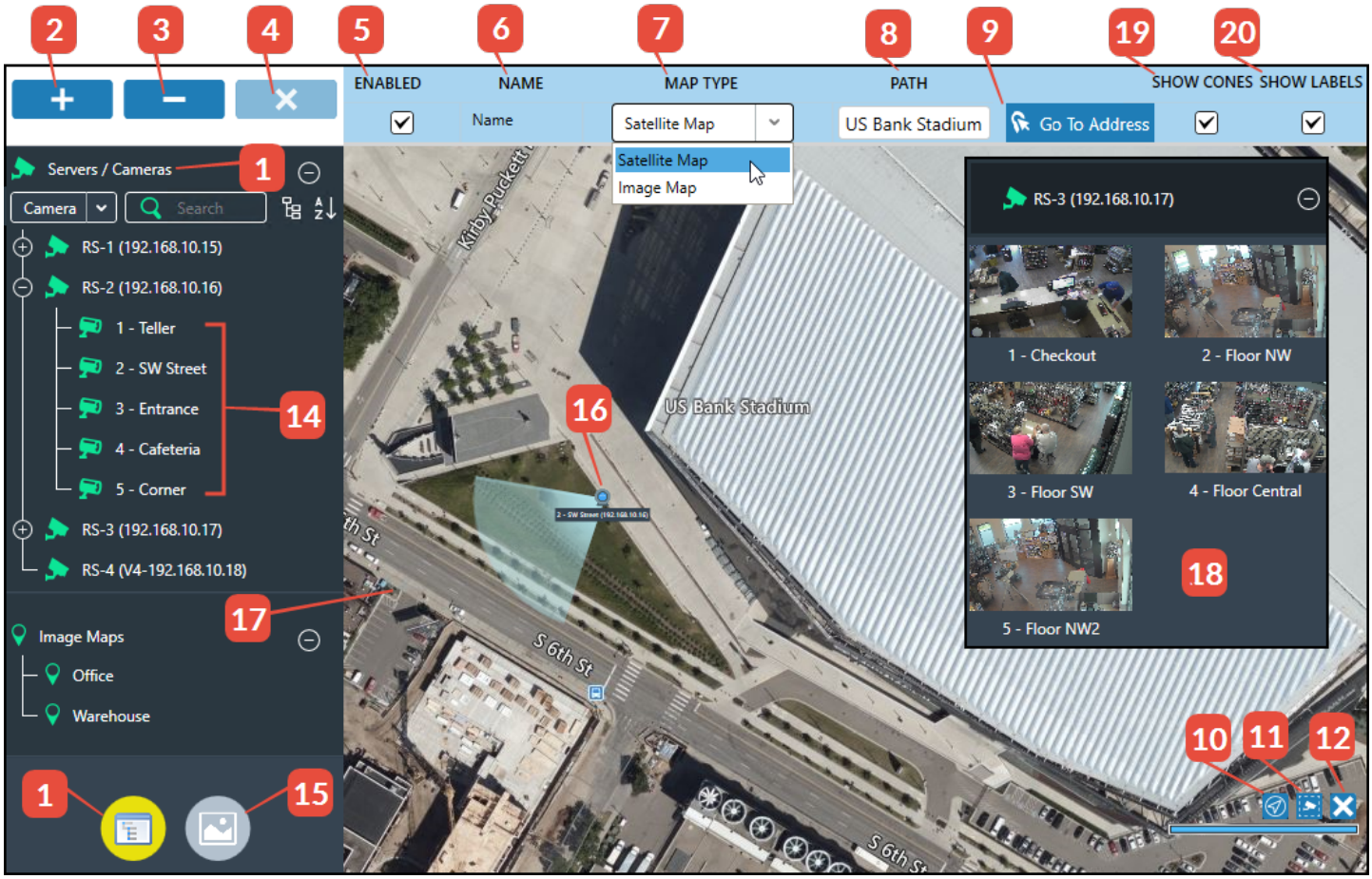
Maps with video are an intuitive, geographical means to present an installation's security camera infrastructure. Image maps may be hyperlinked to each other.

Maps may be constructed with still image maps. But, for a system that is connected to the Internet, real-time satellite images may be selected by using Satellite Map as the Map Type, illustrated below. Supported still image formats include PNG, JPG, GIF, and BMP. Both still images and Satellite images may be used by the Client for maps.

For clarity, some UI elements may be omitted from the following information.

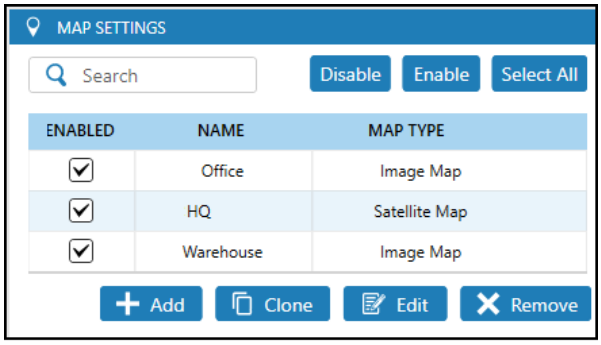
Map Configuration Overview

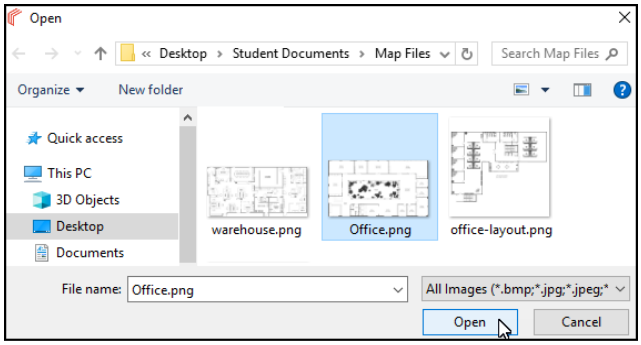
1. Server - Cam/Maps Panel
2. Zoom In
3. Zoom Out
4. Clear Map
5. Enable (for viewing)
6. Map name
7. Map Type: Includes Satellite and Image
8. Path of Image, landmark, address, or GPS Coordinates
9. Import or browse to GPS Location
10. Go to current location
11. Select camera
12. Remove camera
13. Select Hierarchical View
14. Hierarchical View
15. Select Thumbnail View
16. Camera Icon
17. Image Area
18. Thumbnail View
19. Toggle Show/Hide Camera Cones
20. Toggle Show/Hide Camera Labels



Map Settings

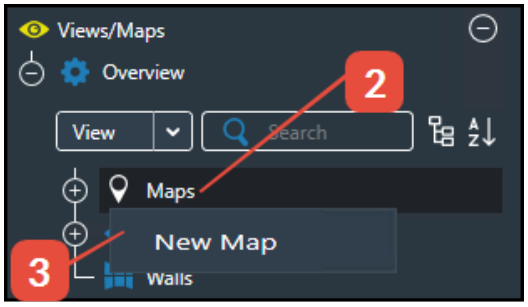
The Administrator can add, delete, disable, select and edit maps from the Map Setting list of existing maps. Disabling a map leaves the map in place, but makes it inactive so that it does not show.





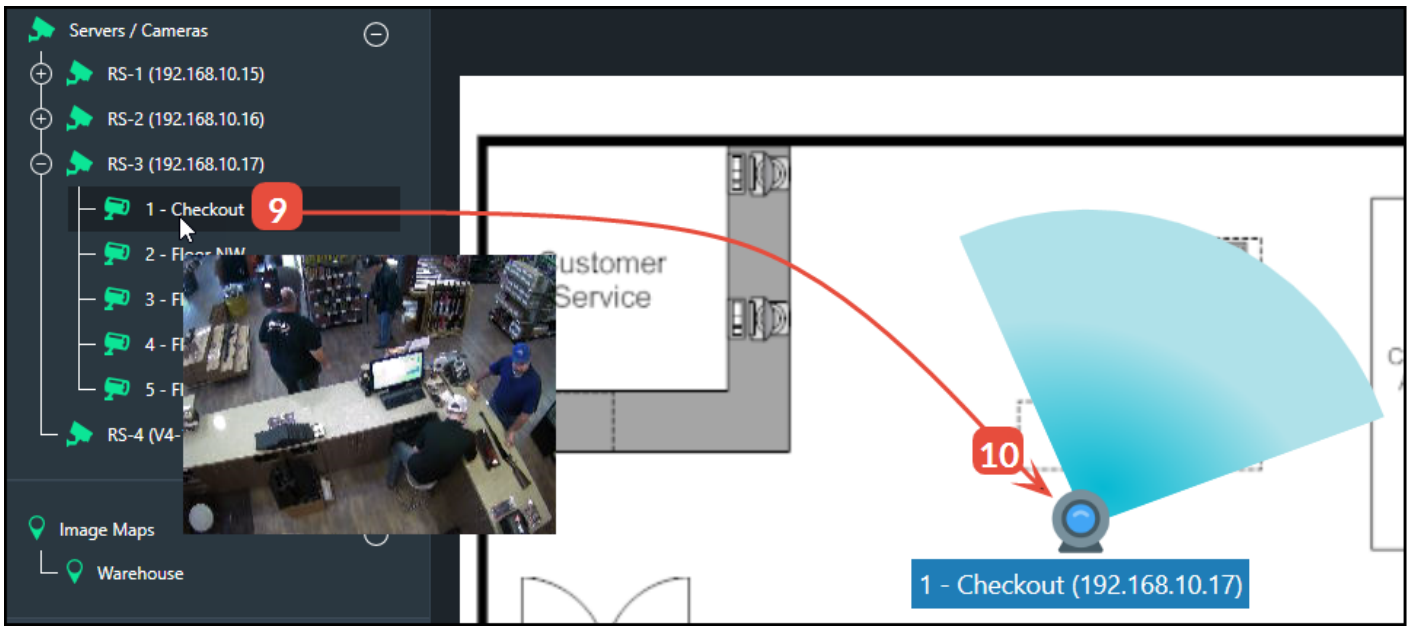
Add an Image Map

Steps:



1. Create and save the desired map still images to an accessible folder
2. In the Client, Right-click on Maps
3. Select New Map
4. Select Image Map as the map type
5. Select Import Image (See illustration above) **Note:** users will be redirected to find the map still-images

6. Select the desired still image (from the desktop folder)
7. The still-image name will appear in the Path
8. Type the new name over the exiting-default map name
9. Drag cameras from the Recording Server list on the left of the map panel
10. Drop the cameras on the still image to the location that best matches the camera's actual physical location
11. Save the configuration

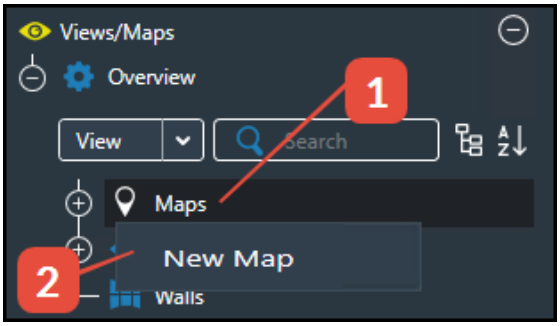


Repeat the steps above as required to add additional maps.

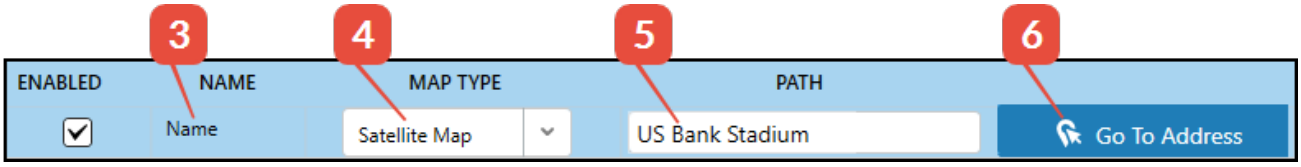
Add a Satellite Map

Note: CompleteView must be online with Internet access to permit search and retrieval of satellite map images. Satellite maps may not be hyperlinked to each other.

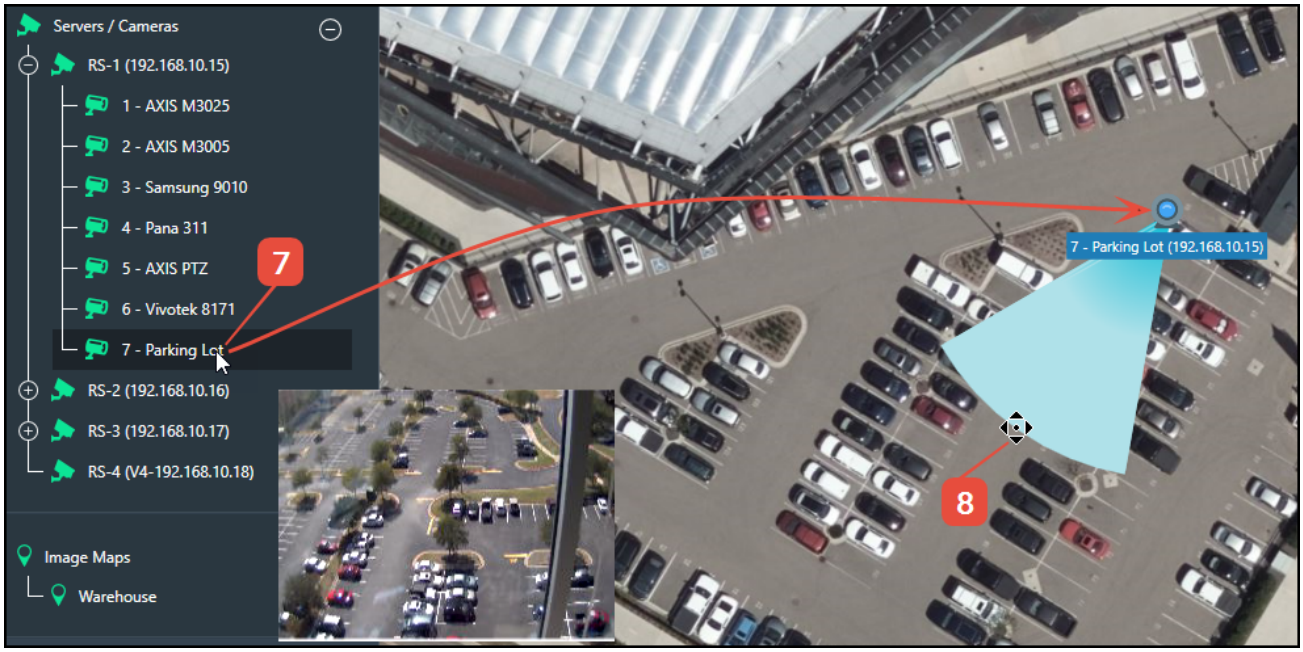
Steps:



1. Right-click on Maps
2. Select New Map
3. Type the new name over the existing-default map name
4. Use the pulldown menu and select Satellite Map
5. Enter the street address, GPS Latitude-Longitude coordinates, or landmark name in the location (Ex: US Bank Stadium)
6. Select Go to Address



7. Drag cameras from the Recording Server list the camera(s) and drop them on the map image
   Note: Cameras may be pulled from different Recording Servers onto the same map.
8. Use the four-sided arrow to size and rotated to identify the field of view.



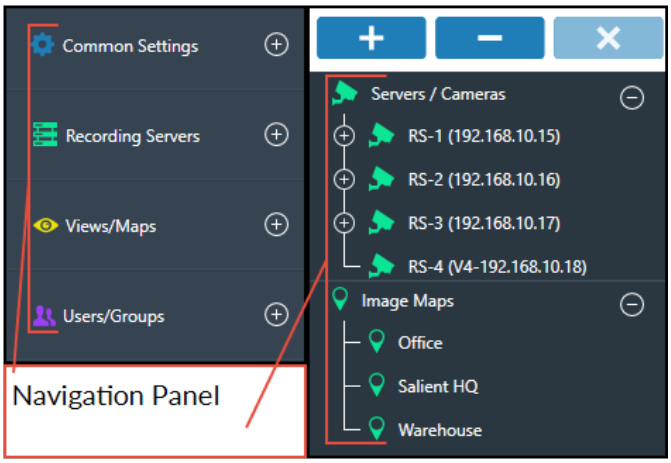
9. Save the configuration

Note: Be sure to save the configuration before selecting some other part of the Client to avoid starting the map creation process from the start.

- Map images may be enlarged (zoom in) or reduced (zoom out)
- Camera Icons are not intended to be changeable
- Images are saved to the Management Server's database

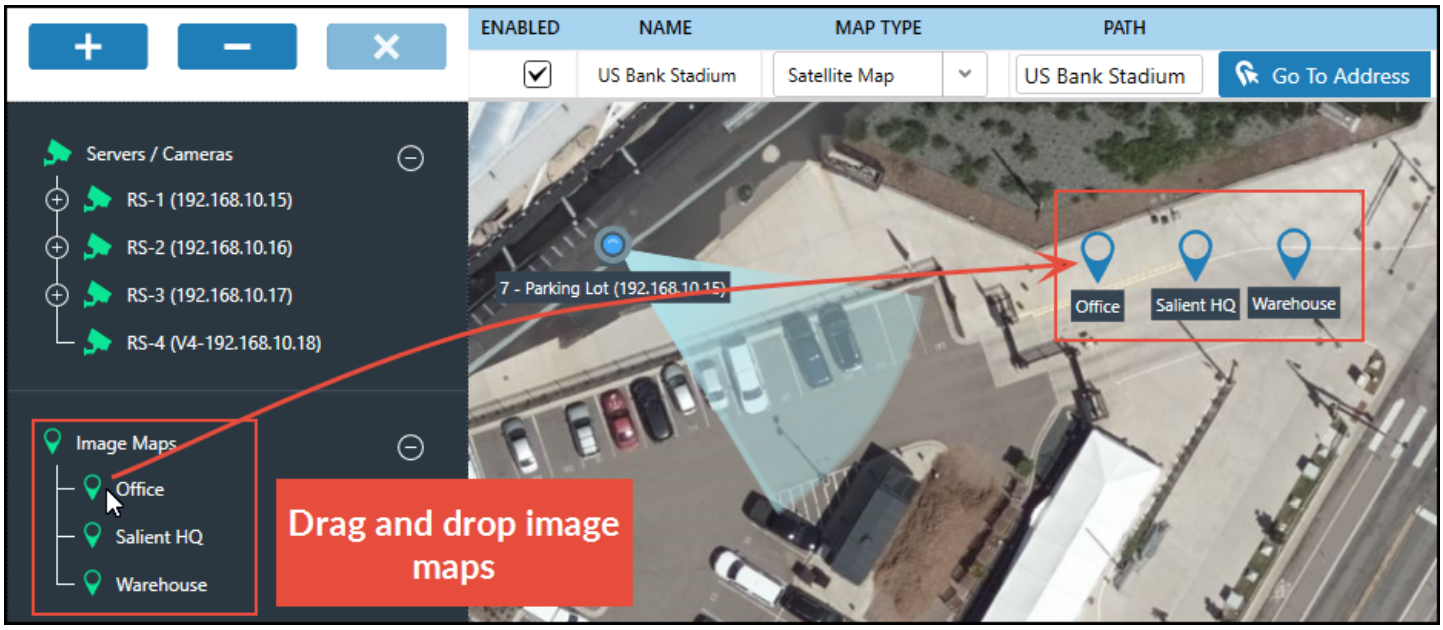
Map Hyperlinks

Map hyperlinking provides a quick method to move from one map to another without searching through the list of maps in the Navigation Panel. Hyperlinking is exclusive to Image Maps. Collect multiple hyperlinks in the same general area on the image for ease of location.



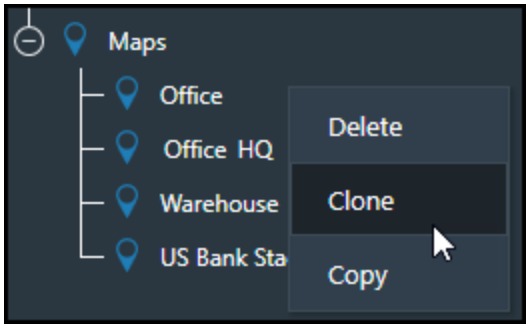
Hyperlink Methodology

Map 1 is displayed, and maps 2,3,4, and 5 are related to Map 1. To configure Map 1 with hyperlinks to all other listed maps, the Administrator must drag and drop the list of Image Maps 2,3,4, and 5 onto Map 1's image. While doing so, the Administrator must ensure that the hyperlinks are on top of Map 1's image and in the same general area of Map 1's image.



Maps Clone/Copy

Once created, Maps may be cloned or copied by right clicking on the map's name, and selecting either Clone or Copy.



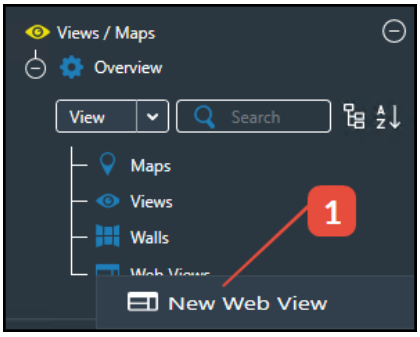
Web Views

CompleteView allows for the display of web and HTML content within the Playback and Live View modules. After creation of a Web View, administrators may use the Users / Groups section of the Configure module to configure functionality of and access to the Web View.

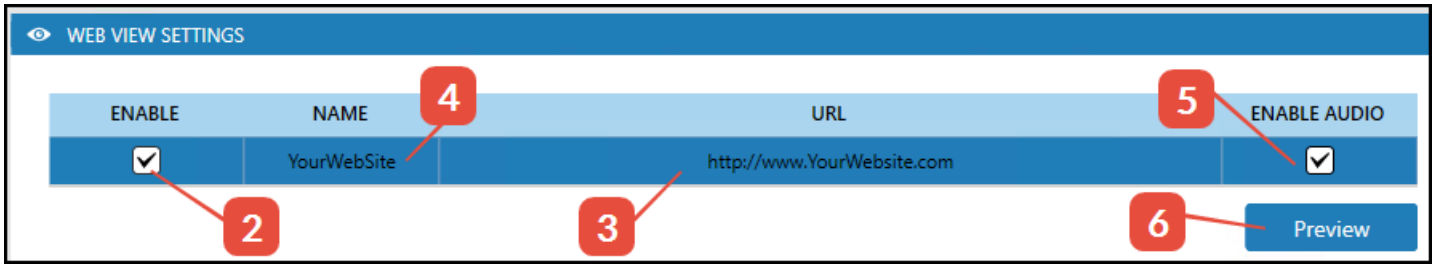
Create a Web View

From within the Views / Maps section of the Configure module:

1. Either right click on Web Views and select New Web View, or select Add from the Web Views overview screen.



Note that a Web View may be deleted by right clicking its name in the left pane and selecting Delete or by using the Remove button in the overview screen.



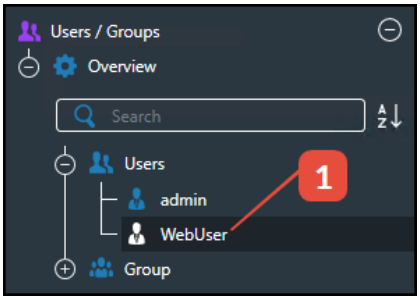
2. Verify the view is enabled
3. Enter the URL
4. Enter in a meaningful Name
5. Select or deselect Enable Audio
6. Optionally Preview the content

Grant Web View Access & Permissions

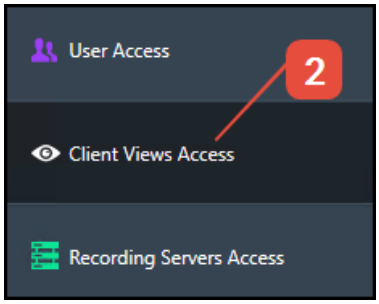
After creation, an administrator must grant non-administrator users or groups both access to and define the functionality of a Web View. Users or groups with administrator privileges are automatically granted access to Web Views.

From within the Users / Groups section of the Configure module:

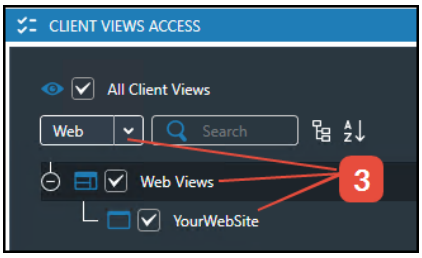
1. Select desired User or Group



2. Select Client Views Access



3. Grant access to the Web View



4. Select the Web Views Resource Type
5. Assign Permissions to the Web View

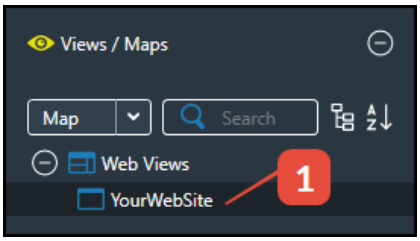
Web View Permissions

Permission	Function
Navigation	Hides or displays the browse backward, forward, reload, and home controls for the Web View. 
Show URL	Displays or hides the Web View's URL. **Note:** The URL is not editable within either the Live View or Playback modules.
Live View	Grants or denies access to the Web View within the Live View module.
Playback	Grants or denies access to the Web View within the Playback module.

Viewing a Web View in Live View

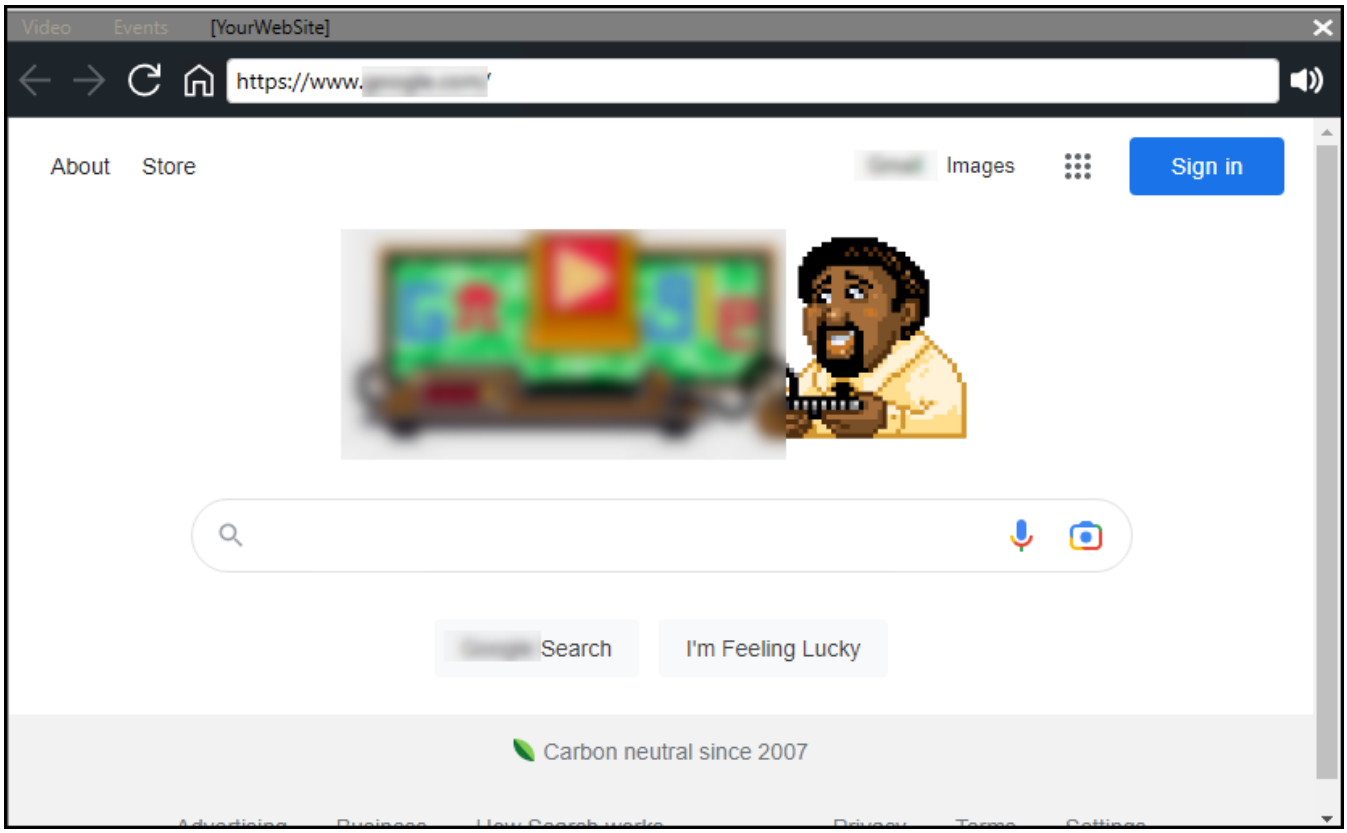
Method 1

From within the Views / Maps section of the Live View module:



1. Expand Web Views and select the desired Web View

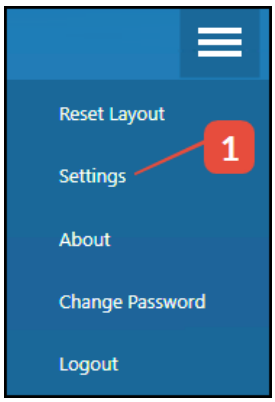
Note that after selecting the desired Web View, right clicking in the same menu area will produce a New Tab option.



2. The content will be displayed in the Video and Events panel with the permissions configured in Users / Groups.

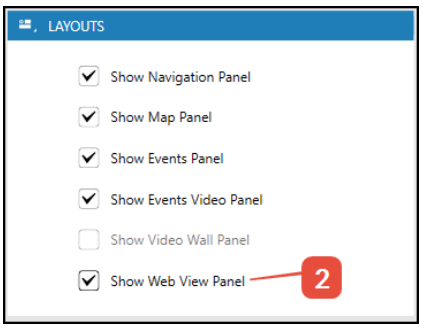
Method 2

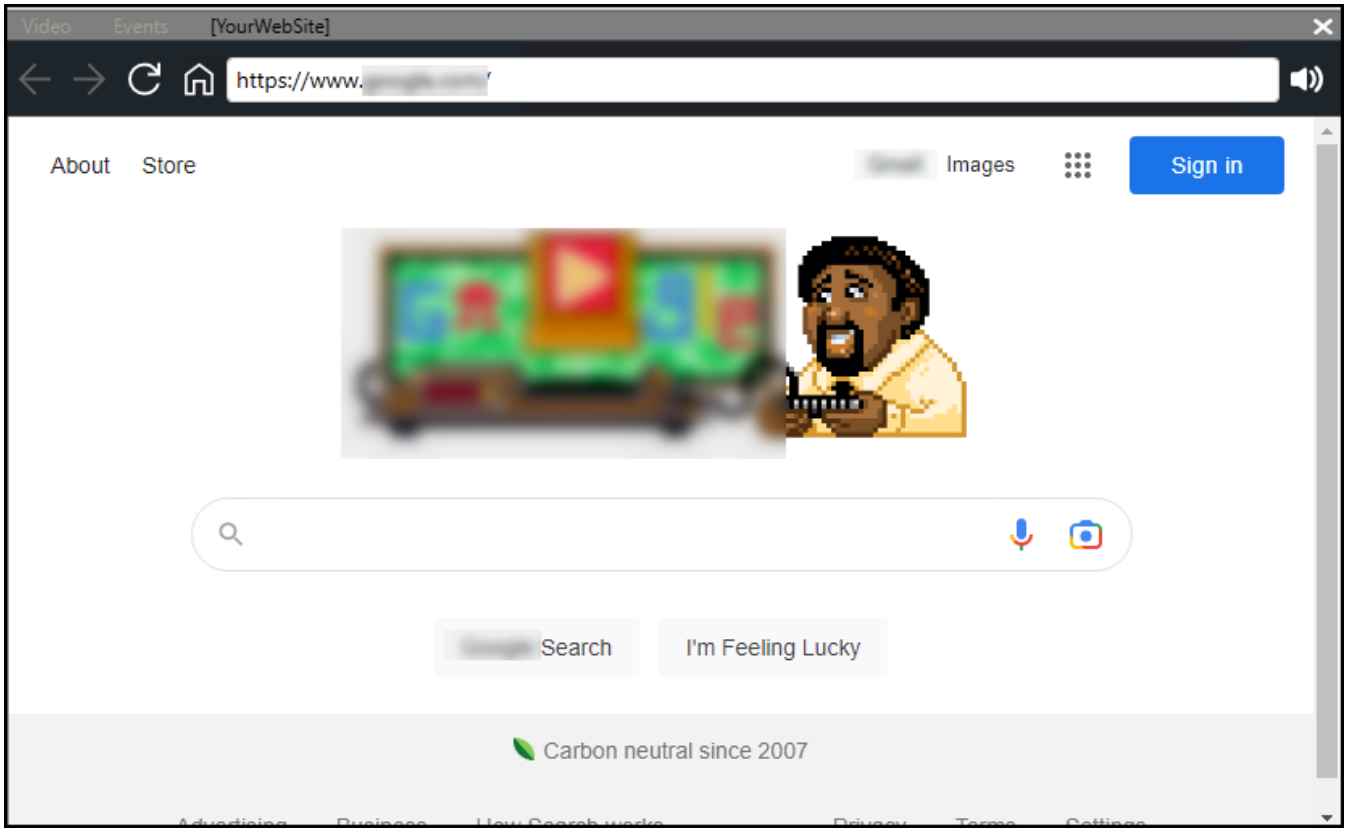
From within the Live View module:



1. Open the Main Menu and select Settings.

2. From the Layout panel, select Show Web View Panel.





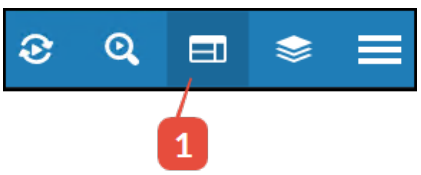
3. The content will automatically be displayed in the Video and Events panel with the permissions configured in Users / Groups.

If multiple Web Views are available, the one that was created first will be displayed. Selecting subsequent views will replace the initial view in the Video and Events panel. Right clicking on one of the Web Views will produce a New Tab option which can then be populated by another existing Web Views.

Note that Web Views may be floated out of CompleteView and redocked. Selecting Reset Layout from the Main Menu will close docked and undocked Web Views.

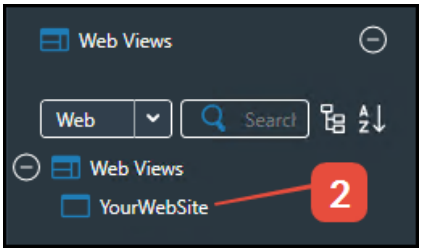
Viewing a Web View in Playback

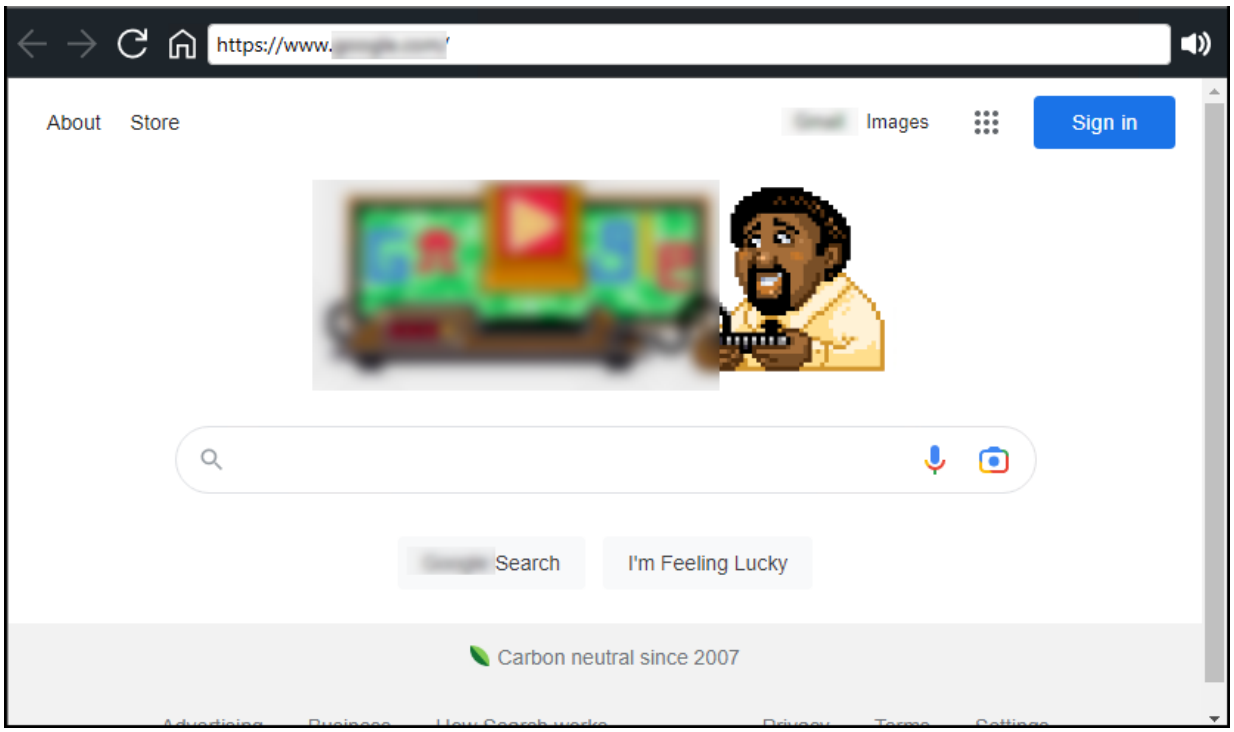
From within the Playback module:



1. Select the Web Views icon from the toolbar. Note that the icon will only be visible if the user has permissions to access the Web View.

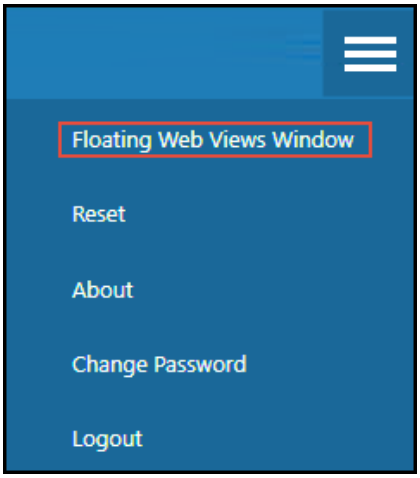
2. Expand the menu and select the desired Web View in the left pane





3. The content will be displayed in the right pane with the permissions configured in Users / Groups.

Note that the Web View may be floated from the Playback module by opening the Main Menu and selecting Floating Web Views Window. The floated window will initially appear behind the Desktop Client. Use either the Windows taskbar or select the Floating Web Views Window menu option again to view the window. The floating window will remain until the user either closes it, or navigates to the Home module.



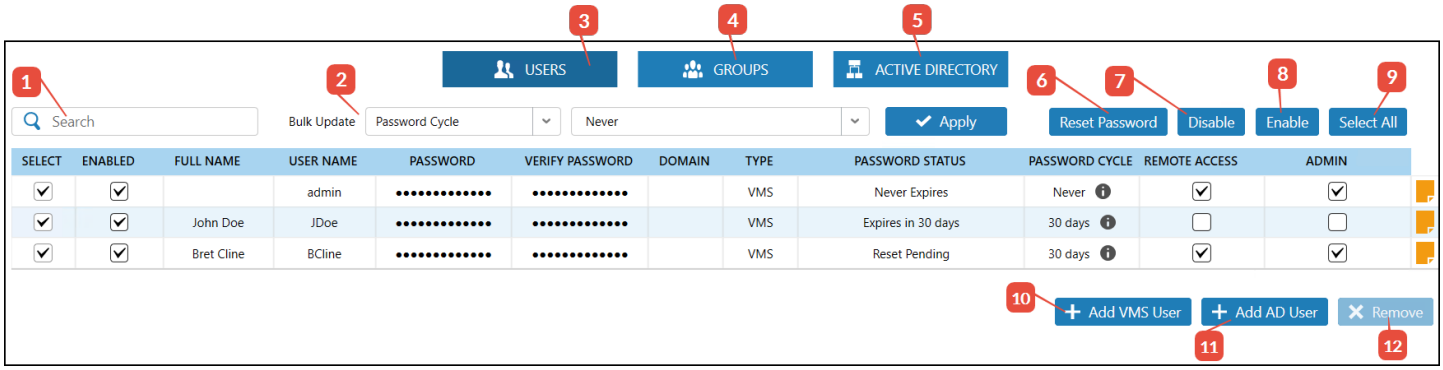
Users & Groups Introduction

From the Users/Groups Panel, Administrators can configure who and how cameras, Recording Servers, and their related features are used. The panel also enables the Administrator to add new users and groups to the Client. Users' and groups' camera permissions and exceptions are set for all Recording Servers from this panel.

Overview

User/Group Overview provides a quick review of CompleteView users and groups, and provides convenient access to Users, Groups, and importation of users and groups from Active Directory.

The default display is set to Users. From this panel, a user or group may be disabled but kept in the configuration for possible future re-activation.



1. **Search**—permits searches for names or groups
2. **Bulk Update**—see below for details
3. **Users**—presents the User Overview panel
4. **Groups**—presents the Group Overview panel
5. **Active Directory**—present the Active Directory Information and Search panel
6. **Reset Password** — forces reset of the selected user(s) password on next login
7. **Disable**—disables the selected user or group
8. **Enable**—enables the selected user or group
9. **Select All**—selects all the users or groups in the Overview panel
10. **Add VMS User**—adds a VMS user to the Client
11. **Add AD User**—adds an Active Directory user to the Users overview panel
12. **Remove**—the selected user or group is removed after a confirmation is approved by the person making the selection

Administrators may click inside a full name, username, password, or domain box and type over the existing information to make changes. Boxes that are checked are included or enabled.

Note that if a password is changed, it must also be verified in the VERIFY PASSWORD column. In addition, the Password Status and Password Cycle columns only appear when the global Password Policy is enabled. See Common Settings Operations for more information.

Bulk Update

Bulk update provides administrators with the ability to change specified attributes for selected users en-masse. Check the Select box for the users to be configured, then select the Bulk Update attribute

from the dropdown menu. Finally, select the desired option. Click Apply when done. The table below displays the configurable attributes and their respective options.

Password Cycle	Admin	Remote Access	Password	Verify Password
Never	True	True	Manually enter	Manually enter
# of days	False	False		

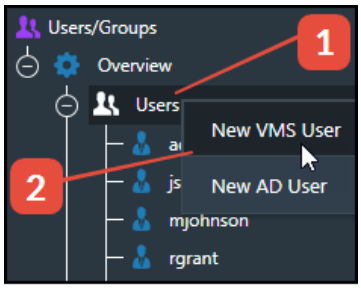
Users & Groups Configuration

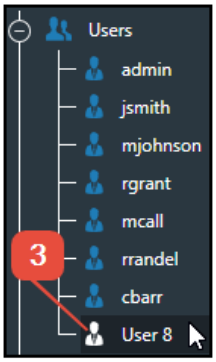
The following section describes configuring user and group access.

Add a User

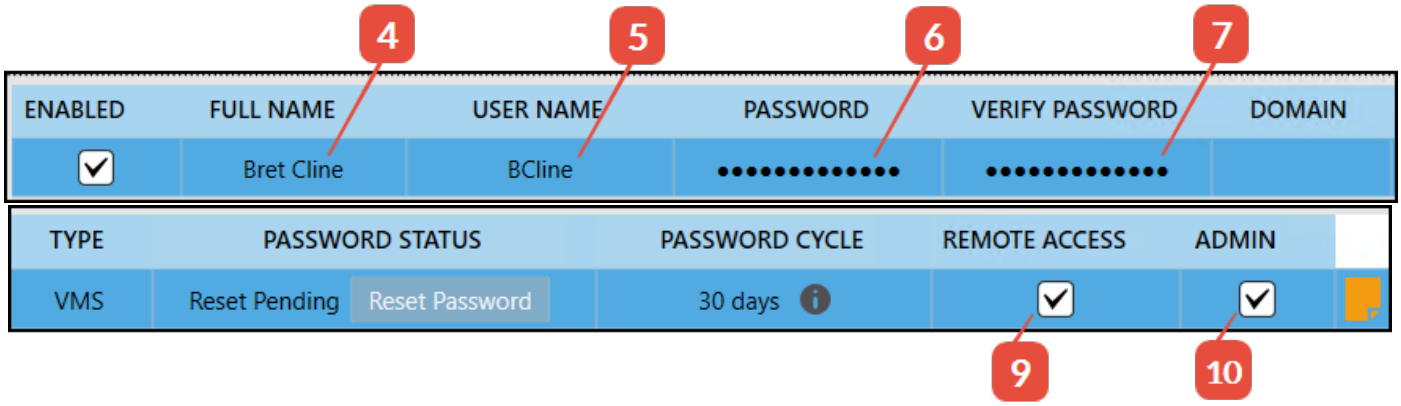
Steps:

1. Right-click on Users
2. Select New VMS or New AD User
3. The default user (example: User 8) will appear in the list of users
4. Optional: add a full name
5. Change the username
6. Add a user password (click in the box and type)
7. Verify the password
8. Optional: if AD is utilized, enter the domain name
9. Optional: When Remote Access is selected, the user will have access to the deployment via Salient Cloud Services.
10. Optional: if the user is to be an Admin, select the Admin checkbox
11. Save the configuration





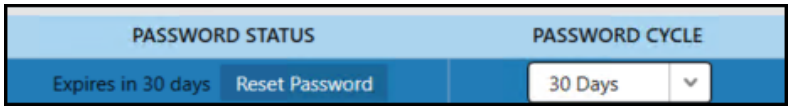
Note: If Password Policy has been enabled, administrators must set a password for new users that complies with the policy. If adding multiple users, it's advisable create the users and use Bulk Update in the Overview section, described in [Users & Groups Introduction]. Also see the Password Policy section below.



Password Policy

CompleteView provides administrators with the ability to enforce password policies, which includes password complexity and password cycle time. By default, password policies are disabled. See [Common Settings Operations] to enable and configure the policy and for a description of CompleteView's behaviors when the policy is enabled.

Password Status & Cycle



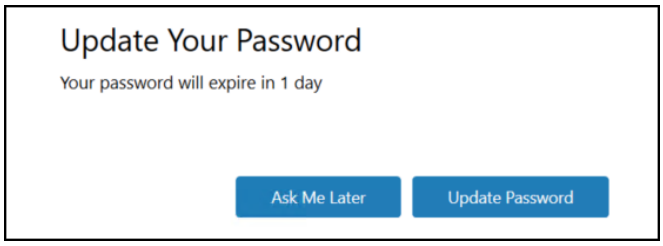
The Password Status and Cycle columns will only appear if Password Policy has been enabled. The Password Status column indicates the state of the user's password. The table below describes the various password states and their meanings. The Reset Password button located within the column may be used to force a password change the next time a user logs in.

The Password Cycle column displays either Never or the total duration of the user's password cycle, usually set by the Global Password Cycle located in Common Settings Operations. Users' password cycles may be individually configured by clicking in the column, which produces a drop down menu. From there, either change the day value with the arrow keys or select Never. Rolling over the "i" informational icon will display the user's password expiration date.

Password State	Meaning
Never Expire	CompleteView will not force a password change for that user. The original Admin user is automatically configured this way. The Reset Password button cannot be used to force a password reset for the Admin user, but may be used for other users set to Never Expire.
Reset Pending	The password must be changed the next time the user logs in. This status is displayed for newly created users, users with insufficiently complex passwords after password policy has been enabled, or after the Reset Password button has been clicked.
Expires in X days	Indicates the number of days a user's password is valid.
Expired	The user's password has expired, and must be changed on next log in.

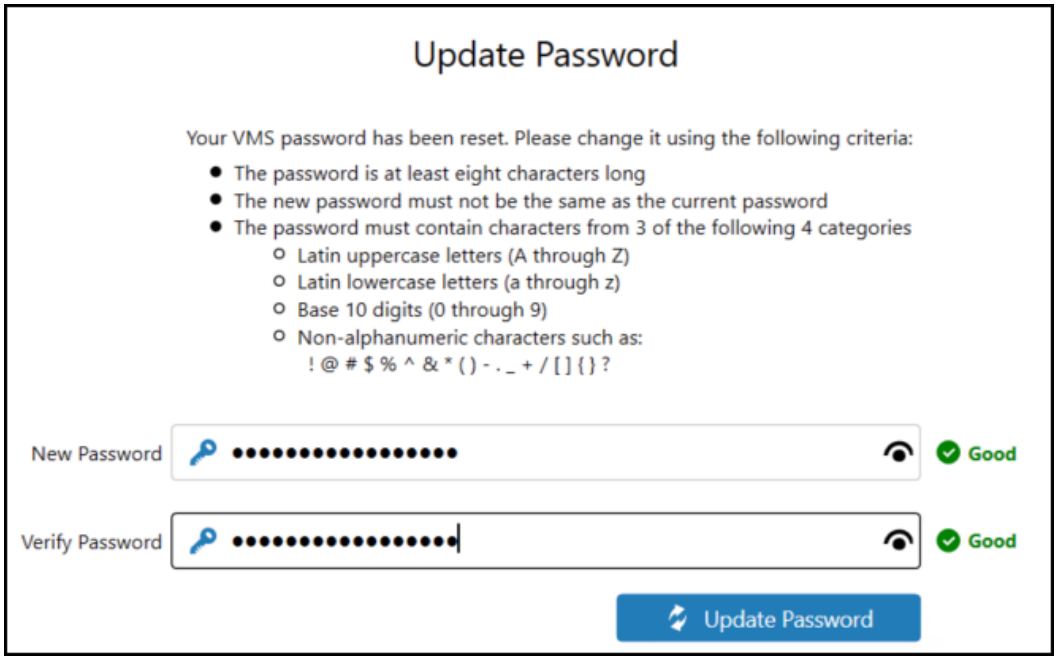
Password Expiration

CompleteView will notify users when their password is about to expire. From the prompt, users may choose to delay changing their password or update it at that time. If they choose to update it then, they will be taken to an Update Password screen, similar to the one described below.



Update Password

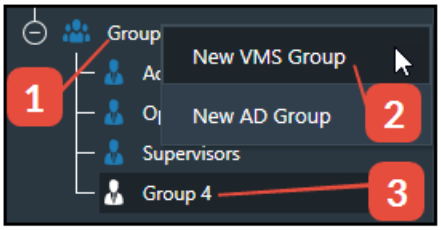
Upon log in, a new user, a user with an insufficiently complex password, or a user with an expired password will be presented with the following Update Password screen.



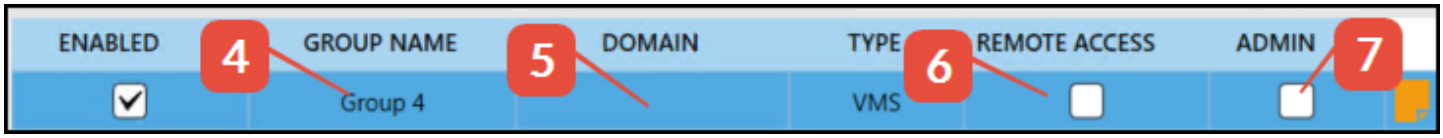
CompleteView will verify adequate password complexity before allowing the user to select Update Password.

Add a Group

Steps:



1. Right-click on Groups
2. Select New VMS/AD Group
3. The default user (example: Group 4) will appear in the list of users
4. Change the Group Name
5. Optional: if the group is an Active Directory Group, add the Domain Name*
6. Optional: if the group is to be allowed Remote Access, check the box
7. Optional: if the group is to be an Administrator group, check the Admin box
8. From "Users in this Group Panel," check the boxes to include the users for the group
9. Save the configuration



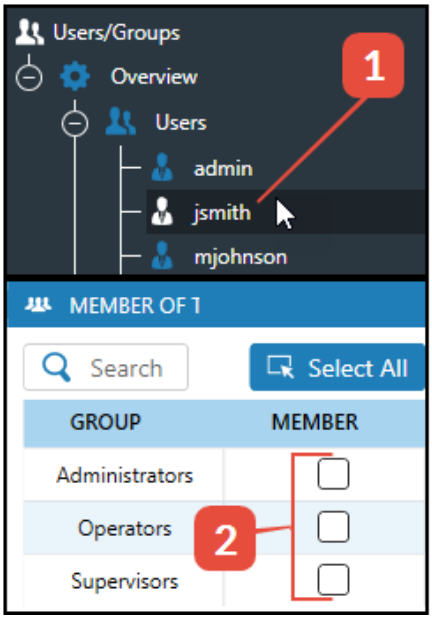
*Note that if a user belongs to multiple groups and the groups have differing options, the options inherited by the user depend on the order in which the groups are added in CompleteView, with the first group added taking precedence.

Add a User to a Previously Created Group

Steps:

1. Select the username*
2. In “Members of These Groups,” check the box to the right of the desired group to set group membership
3. Save the configuration

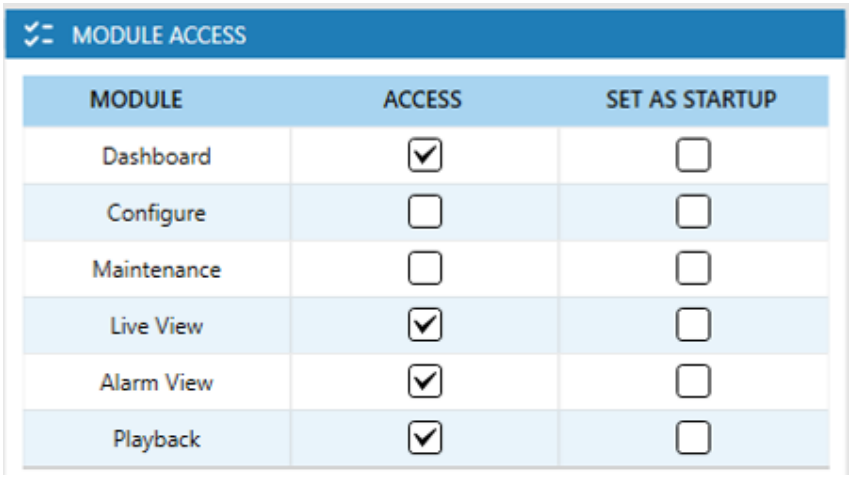
*Note that AD users may be added to VMS groups.



Users and Groups Access & Permissions

Users/Groups hosts three (3) panels. User Access, Client Views Access and Recording Servers Access. Using the navigation tabs allows an administrator to configure individual or group access and permissions for the CV modules, views, maps, and recording servers.

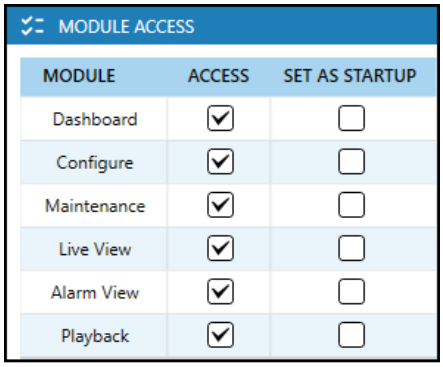
Module Access



Users/Groups host three panels. Each panel defines some aspect of CompleteView access. Module Access allows the Administrator to define which of the six functions (Dashboard, Configure, Maintenance, Live View, Alarm View and Playback) users may access. Access is granted by checking the box to the right of the module name.

Set as Startup

Set as startup defines the one default module to open for the group or user at login. If a user is a member of a group, the group module will take precedence. If all boxes are left unchecked, the Client will default to the Home screen. Only one “Set at Startup” module can be checked. Remember to save the configuration when selections are completed.

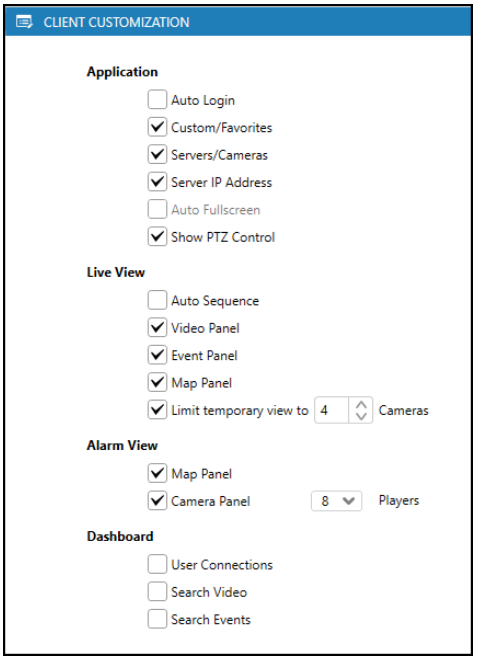


Client Customization

From Client Customization, the administrator grants access to different features and functions that exist in the Recording Server and Client Applications. Features with their boxes checked are accessible to the selected user or group.

Application Module

Feature	Purpose
Auto Login Auto Login	Allows the user to bypass the normal login process by double-clicking on the CV desktop icon. Credentials that are used when first selecting Auto Login are saved, reused and logged. When selected, an Auto Login option is displayed on the Desktop Client homepage. Check to enable.
Custom/Favorites	Allows the user to access and create custom and favorite views
Servers/Cameras	Allows access to servers for creating custom views
Server IP Address	If checked, the Recording Server’s IP address is displayed when viewing live video
Auto Full Screen	Live View application displays full-screen upon login
Show PTZ Control	Toggles user access to PTZ controls. Applies to navigation panels in Live View and Play-back modules.



Live View Module

Feature	Purpose
Auto Sequence	Causes Live View application to defer to view sequencing upon login. Sequencing must be configured
Video Panel	Allows the user or group to access the Live View video panel and its contents
Event Panel	Allows the user or group to access Live View's Event panel and its contents
Map Panel	Allows the user or group to access the Live View's Map Panel and its contents
Limit temporary view to	Allows the administrator to limit the number of cameras a user can drag into a temporary view or GeoView in Live View (default value 4, maximum 100, and this feature is deactivated by default)

Alarm View Module

Feature	Purpose
Map Panel	Allows the user or group to access the Alarm View's Map panel and its contents
Camera Panel	Allows the user or group to access the Alarm View's Camera panel and its contents
Players 0-64	Defines and limits the number of Alarm Players to the selected value. Default is 8

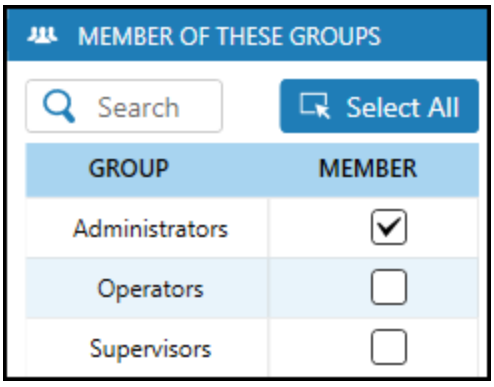
Dashboard Module

Feature	Purpose
User Connections	Allows the user or group to access the Dashboard's User Connection panel and its contents
Search Video	Allows the user or group to access the Dashboard Search Video feature
Search Events	Allows the user or group to search events from the Dashboard

*For more information about Bandwidth settings, see Bandwidth Control.

Group Membership

Highlighting a user in the Navigation Panel and looking in the Members of These Groups panel will display the selected user's group membership.



Admin Group Access

The Administrator Group defaults to all access of the applications, but does not default the following features in the applications.

- Auto Login

- Auto Full Screen
- Auto Sequence

Difference between Access and Permissions

It's important to understand the difference between access and permissions. Access allows users to use the various applications of the Client. Access is determined by group and user status.

Permission relates specifically to cameras; it prescribes who uses them and what the user is permitted to do with the video. Viewing live video is a "permission."

Admin Group Access

The Administrator Group defaults to all access of the applications, but does not default the following features in the applications.

- Auto Login
- Auto Full Screen
- Auto Sequence

Operator & Supervisor Group Access

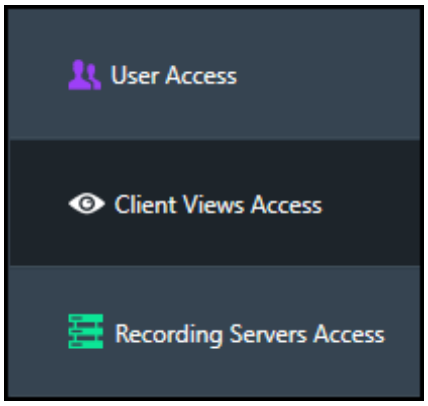
The Operator and Supervisor Group members receive default access to Dashboard, Live View, Alarm View, and Playback applications. By default, there is no configured access for Client Views or Recording Servers; these must be configured by the administrator.

New Users Access

When created, new users are granted limited individual access and permissions. New users must be given permission to view created views and maps, and access to recording servers and cameras must be granted. New users may be assigned to a group, and will inherit the permissions of that group.

Client Views Access

From the Client Views Panel, the Administrator can grant or deny access to a specific client view, map, event, PTZ preset, trigger, web view, input and/or output. Additionally, the Administrator has control over user and group camera permissions. Checked boxes grant camera permissions to a user or group and permit access to views and features such as an alarm or event. In addition, administrators can grant new users and groups retroactive access to video recorded prior to account creation via the Time Limit setting, discussed in the table below.



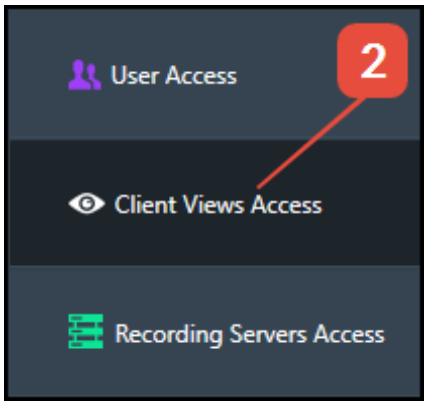
User-Camera Permissions

Permission Name	Description
Live	View live video
Playback	Playback recorded video
Playback Time Limit	For specific cameras, select a numeric value and unit (minutes, hours, days) prior to the current date to which the new user or group should have access. If there is a Time Limit conflict between a given user account and its group, the shorter limit will take precedence.
Audio	Listen to live and recorded video with audio
Export	Export recorded video
Snapshot	Take snapshots of the live video and recorded video
PTZ	Control Joystick and digital PTZ cameras

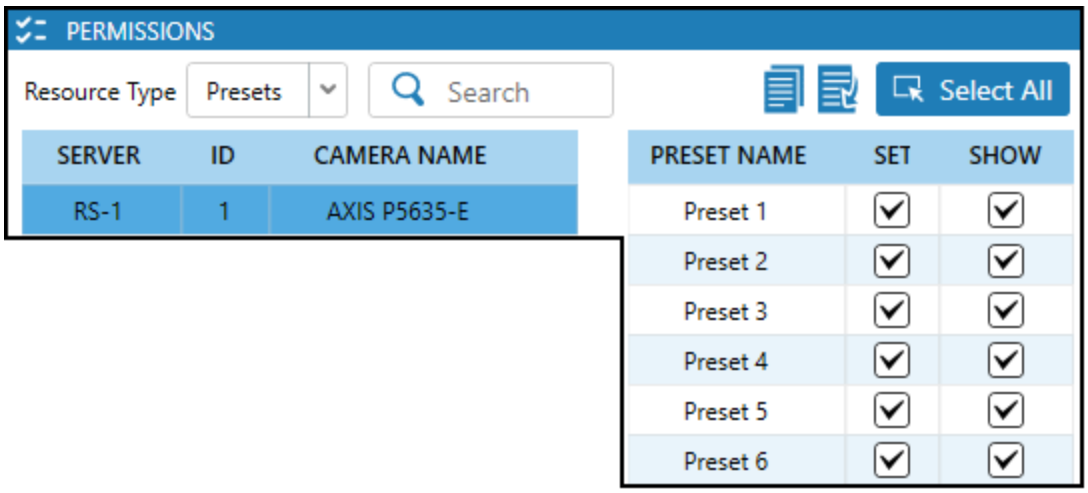
Change PTZ Set and Show Permissions

By default, the Operators Group (all newly created users) have all Set and Show permissions.

Steps:



1. Select a user or group
2. Select Client Views Access
3. Use the resource Type pull-down menu, select Presets
4. Select the camera(s) for which the preset permission change is intended
5. Look at the list and change any desired preset
   a. **Set** - permits the selected user or group to set a pre-set position from Live View
   b. **Show** - permits the selected user or group to select and show a preset position from Live View.
6. Save the configuration



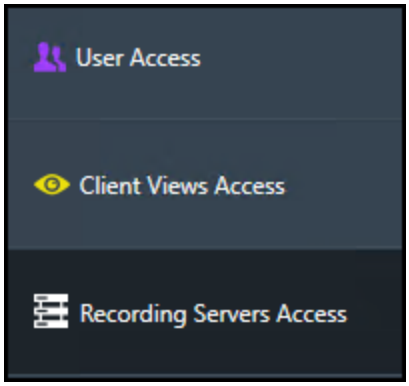
Note: The first ten (10) camera-presets are set to display the digital preset positions for all cameras.

Recording Servers Access

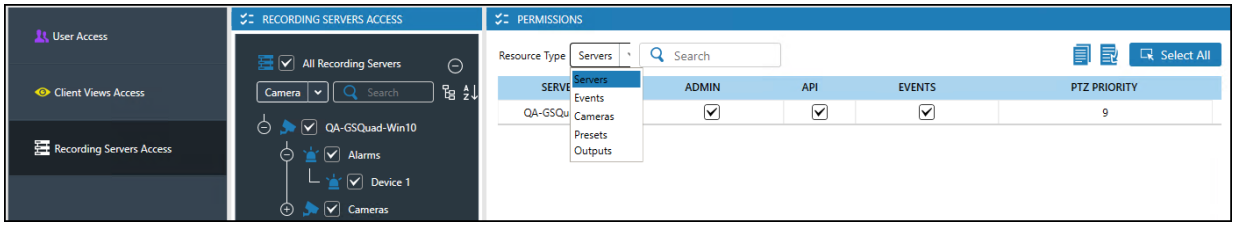
When a new user or group is added to CompleteView it is assumed that the user or group has access to all of CV's Recording Servers, events, cameras, presets, triggers, and inputs by default, unless exceptions are configured. Access to Alarm device outputs must be configured by the Administrator.

If desired, the Recording Server Panel and the Resource Type's menu permit the Administrator to select users or groups in order to set exceptions for one or all of CV's features.

Resource Type selections are duplicated in both Client Views and Recording Server Panels, causing a restriction that is set in the Client View Panel to be applied in the Recording Server Panel. The difference may be restrictions of Maps, which is exclusive to the Client View Panel.



Note: Checked boxes enable and unchecked boxes disable the selection.



Servers

The Resource Type selection of Recording Servers allows exceptions to be set for the following:

1. Configure API access for access control and other partner products
2. Define PTZ (control) Priority (priority is set for the selected user or group)

3. Set the selected user or group as an Administrator for a selected server. The user or group must be selected in the Navigation Panel prior to selecting the admin checkbox

Events

By default, when users or groups are added, they are given access to review all CompleteView events. The Events Selection for events allows the administrator to give access to or to limit a user or groups search and review all or some events in the Dashboard application.

Cameras

By default, when users or groups are added, they are given access to all Recording Servers and their cameras. Selecting Cameras from the Entity Selection allows the Administrator to set camera use permission exceptions for a specific Recording Server's camera.

Presets

When users or groups are added, they are given access to all Recording Servers, and they may Set and Show PTZ camera preset positions, by default. The Administrator may restrict the use of the Set and Show permissions for one or more cameras for a user or group.

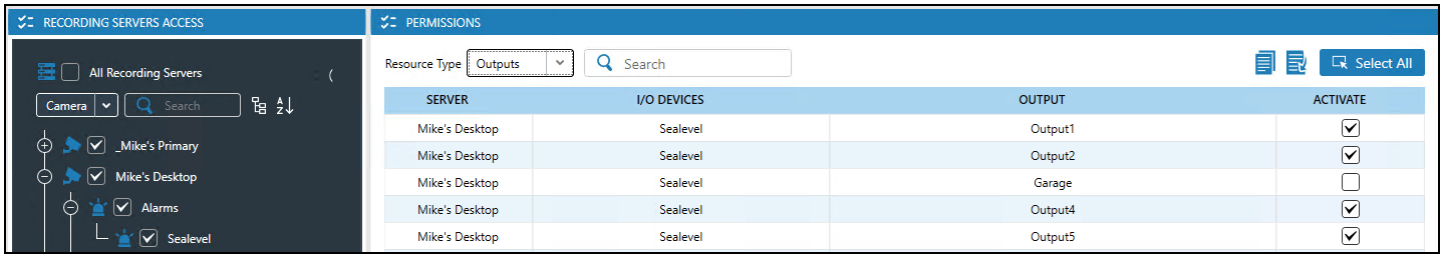
Set - allows the selected user or group to define a PTZ camera preset

Show -allows the selected user or group to select and display a PTZ camera preset. Show also applies to digital PTZ

Note: Checked boxes enable and unchecked boxes disable the selection.

Outputs

Access to Alarm device outputs must be configured by the Administrator. Once permission has been granted, outputs may be manually triggered within Live View (cameras in view layout, camera being viewed live in the Video Player pane), Dashboard (camera being viewed live in Video Player pane), and Alarm View (camera pop-up and camera being displayed in Video Player).

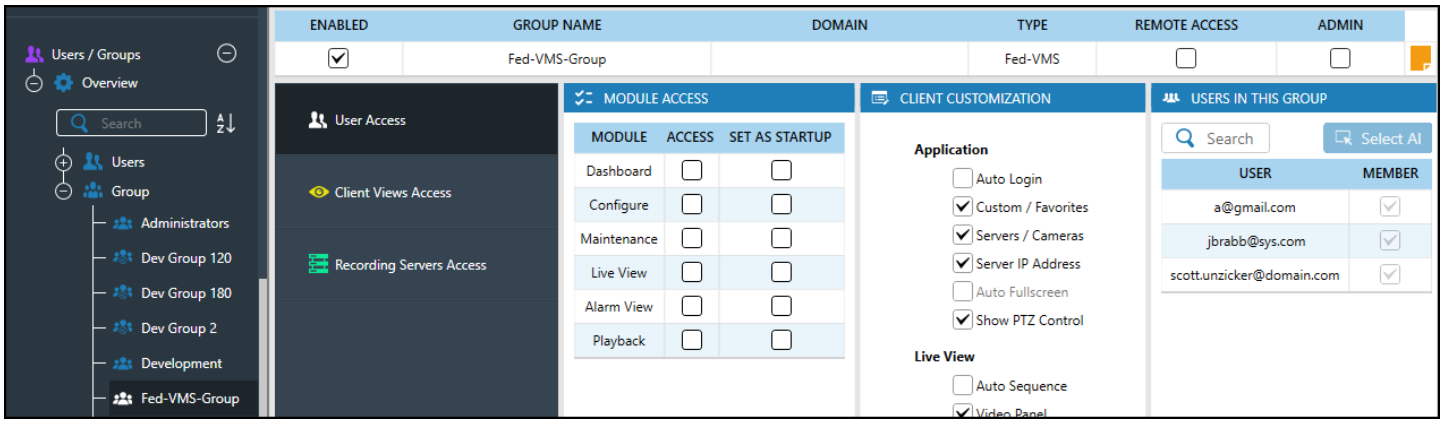


Outputs

Setting	Description
Server	Shows the server the device is attached to
I/O Devices	Displays the name of the device
Output	Lists the output channels
Activate	Select or deselect to configure user/group access to view and activate the output

Federation Groups and Users Permissions

The configuration of permissions for Federation Groups is similar to configuring any other group described above. Permissions for Federation Users cannot be configured individually but are instead set at the Group level. In addition, a Federation User cannot be added or removed from a Federation Group at the Child Management Server level. Group membership is handled by the Parent Management Server as is site access. However, access by Federation Users and Groups to the site may be disabled by the Child Management Server. See the Federation Overview and Federation Implementation sections for more information.



Users & Groups Active Directory Configuration

Active Directory is leveraged to quickly import multiple users/groups at once to the CompleteView deployment via the Management Server, thereby saving the time required to add each user or group individually. Groups and users are created in the Active Directory Domain Controller and imported via the Client. Permissions and access to Recording Servers and cameras are then granted as required, and Windows login credentials are used to access CompleteView.

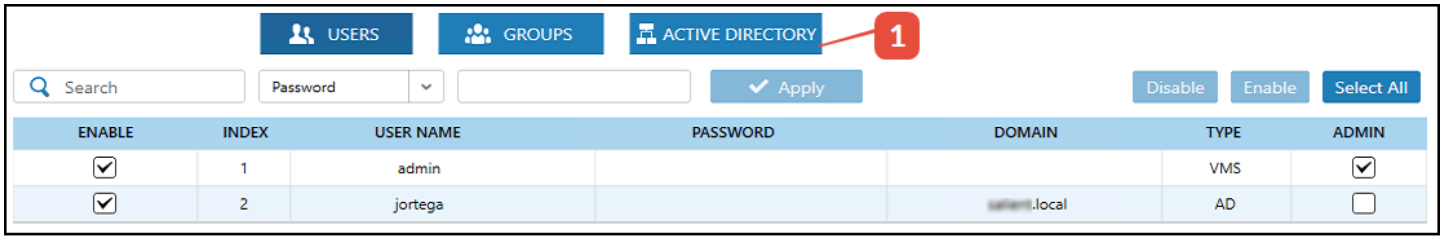
Active Directory Initial Connection

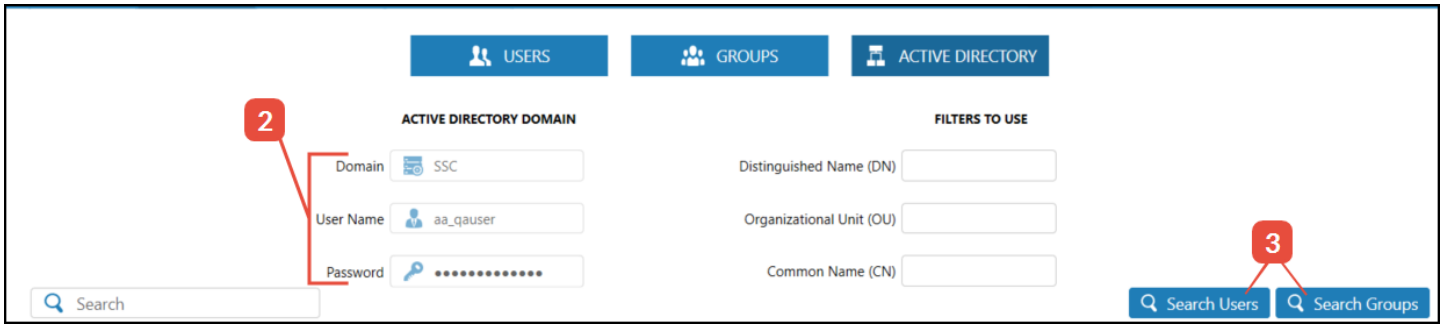
The connection to the Active Directory domain controller is completed in the Management Server's Common Settings/Services pane, which is applied to all Recording Servers. See the Common Settings Services section of this document for more information. If the site is to be part of a Federation and using AD users and Groups, it is critical that it can authenticate the AD users to the same domain that the Parent Management Server is associated with. See the Federation Overview and Federation Implementation sections for more information.

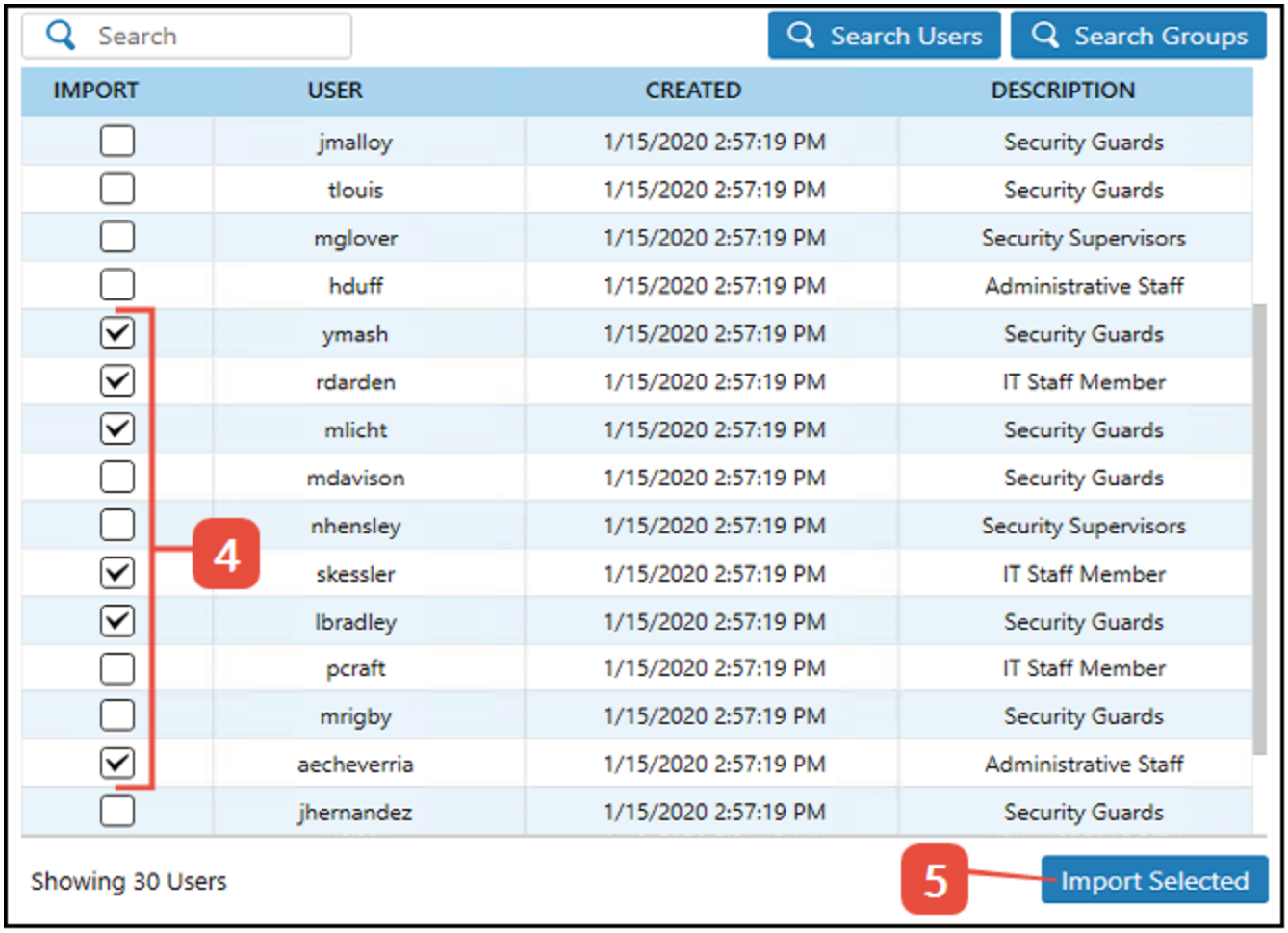
Adding Active Directory User and Group

Note: Before proceeding, ensure that the Domain Controller's initial connection in Services is completed, and Active Directory (AD) is available for the user and group import.

Steps from Users/Groups Overview:







1. Select Active Directory
2. The Domain name, user name, and password should be populated with the AD domain info from Common Settings/Services.
3. Select Search Users or Search Groups as appropriate **Note:** User/Group names for import will appear below
4. Select the users or groups by checking the box next to their name
5. Press Import Selected

Note that imported AD users can be added to one or more VMS groups. If a user belongs to multiple groups and the groups have differing options, the options inherited by the user depend on the order in which the groups were added in CompleteView, with the first added group taking precedence.

Failover Introduction

CompleteView implements an N+1 failover model to support redundancy of Recording Servers. Multiple Standby Servers can be defined to support multiple Primary Recording Servers. When a Primary Recording Server fails, its functionality will be transferred to the first available associated standby server so that all server operations continue without interruption. All video and event data are captured by the standby server during the downtime and are available for user access. All live and event monitoring will continue to take place without requiring any manual intervention.

Once a Primary Recording Server is restored and online, the acting Standby Server will transfer all configuration and functionality back to the Primary Server. The Standby Server will return to the available pool of standby servers. Failover is only available in Enterprise and Trial editions of CompleteView.

Failover Terminology

Primary Recording Server – Recording Server designated to record video and events under normal operating conditions.

Standby Recording Server – Recording Server designated to assume the activities of the Primary Recording Server in the event the Primary Recording Server becomes unreachable by the Management Server.

Failover Mode – The Primary Recording Server becomes unreachable by the Management Server which has transferred the Primary Recording Server's configuration and functionality to the Standby Recording Server.

Normal Operations – Primary Recording Server is reachable by the Management Server and is recording video and events. The Standby Server is online and available but not recording video or events.

Failover General Operation

The Management Server will monitor all Primary Recording Servers configured for failover for any unexpected shutdowns. If a Primary Recording Server unexpectedly shuts down, the Management Server will roll over its configuration to the first available Standby Server associated with that Recording Server after a configured wait time. All network cameras will continue to stream video to the Standby Server (locally attached analog cameras will not be failed over), and all clients will continue to access live video and events from the Standby Server after being refreshed. If in Live View, refresh the Desktop Client by either clicking Live View on the top tool bar or switching to another module and then clicking back into Live View.

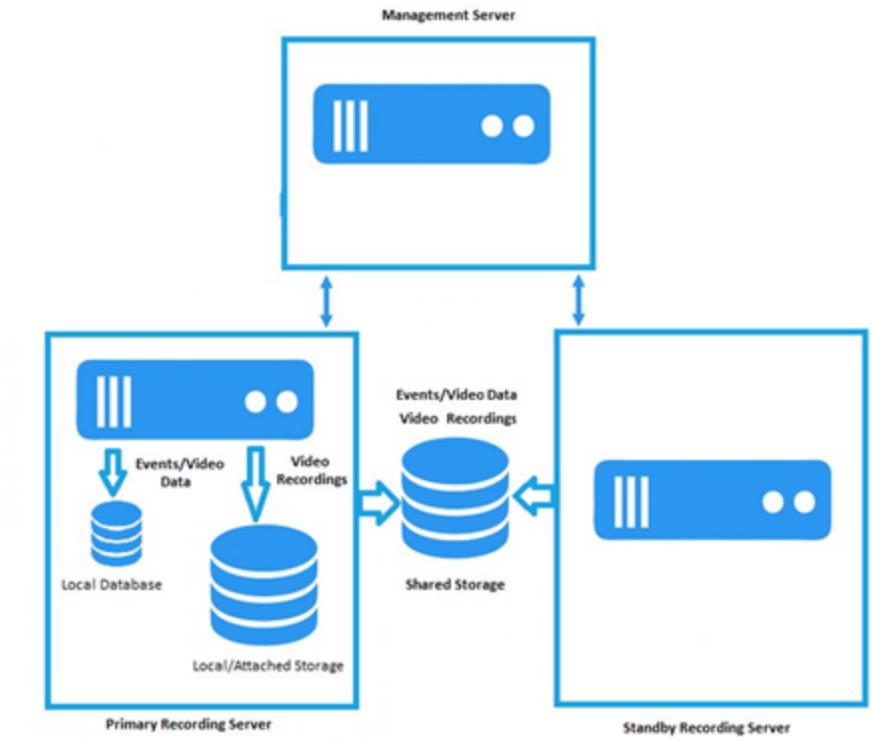
Failover Video & Events Storage

The Standby Server will store all video and event data in a shared Failover Storage Pool that can also be accessed by the Primary Server. The Failover Storage Pool is automatically created by the Management Server on the shared storage drive(s) allocated during configuration, but will be neither visible nor accessible until a failover event has occurred. Once the Primary Server is restored, the video on the shared pool will be synced with its internal database, but video will remain on the shared directory. Events on the shared directory will be merged into the database of the Primary Recording Server. Events recorded on the Standby Server will be searchable and viewable during the failover event.

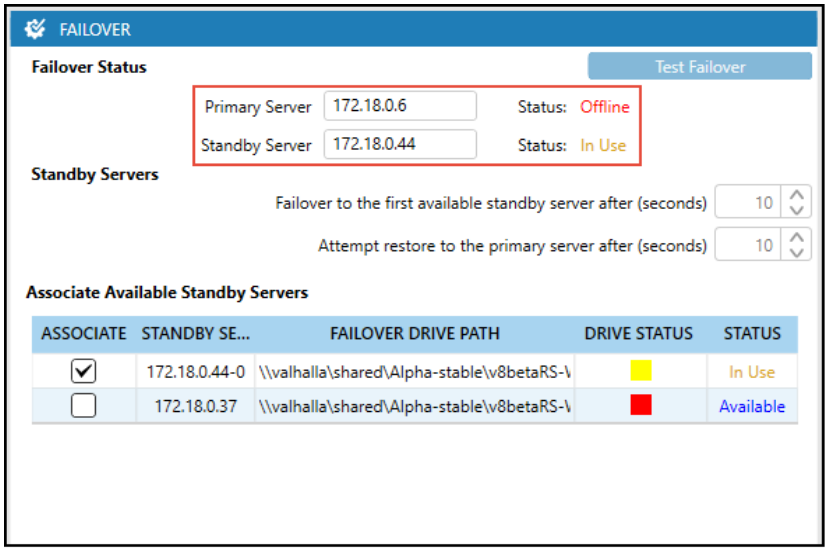
Retention policies configured on the Primary Server will carry over to the Standby Server, but will not be configurable. Retention Estimates will also be unavailable on the Standby Server, but disk utilization information for the Failover Storage Pool will be displayed. Normal FIFO operation will take place if the failover pool reaches capacity. Neither scheduled archiving nor backup will take place during the

failover event, but continuous backup will, if that storage pool is available and visible to the Standby Server.

Once the Primary Recording Server is restored, normal functionality will automatically be transferred back to it from the Standby Recording Server. The diagram below illustrates the general topology of the failover solution.



The Failover pane below, located in the Edit Server screen of the Configure module, shows a deployment in a failed over state, indicating the Primary Recording Server is offline, and the Standby Recording Server is in use.



Failover Configuration

Utilize the following information to configure CompleteView for failover functionality.

Failover Requirements

Failover is available in CompleteView Enterprise versions 7.4.0 and newer. To implement the failover solution, an Administrator must license at least one Standby Server. The Standby Server must have CompleteView Recording Server installed with a brand new configuration that's never been added to a Management Server, and it must be licensed for the maximum number of potential cameras that would record to it in a failed over state. The Standby Server must have access to a storage path shared with the Primary Recording Server, and both must have Storage Pools enabled and configured. The shared storage must be accessible via a standard UNC path. Associated Standby Servers must be set to the same time zone as the Primary. For systems using TLS, communications between the CompleteView clients, Management Server, and Recording Servers will be secured. In v7.4.0, Standby Recording Servers do not support TLS and during a failover, communication from the Management Server and CompleteView clients to the Standby Recording Server will not be secured. The system will support a mixed mode to maintain secure connection between any components supporting TLS without operator interaction. Finally, v7.4.0 and later does not support failover configurations from any previous version of CompleteView.

Upgrade Instructions

If needed, instructions on migrating from CompleteView 6.X to 7.X, including Storage Pool migration, may be found in the following locations:

https://support.salientsys.com/download/migration-guide/

https://support.salientsys.com/download/completeview-v7-migration/

https://www.salientsys.com/download/database-migration-utility/

Note that software installers are located in the Software Downloads section of the Salient Portal:

https://mysalient.com/

Migration video documentation may be found on Training Resources site:

https://support.salientsys.com/knowledgebase/training-resources/

Information regarding the reindexing of camera IDs to camera GUIDs may be found in the link below. The process happens automatically after upgrading from 6.X, but can take a significant amount of time, depending on the number of cameras, Recording Servers, etc.

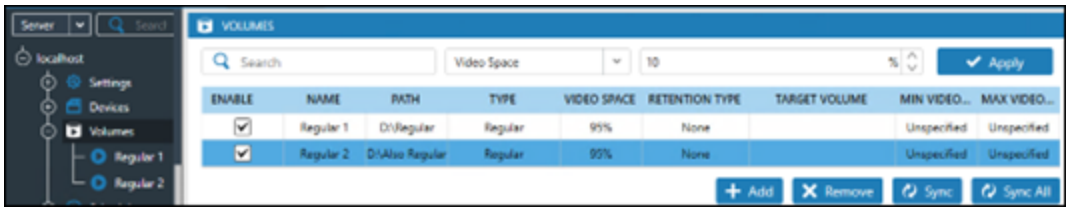
https://support.salientsys.com/download/completeview-v7-2-recording-server-upgrade-information/

Retaining Video from a Failover Volume

Previous versions of CompleteView with failover capability stored video taken during a failover event on a Failover Volume (as opposed to a Failover Storage Pool used in 7.4 or newer). That video needs to be moved from the Failover Volume before migrating to Storage Pools, as happens during an upgrade to 7.4 or newer. The following steps illustrate best practices for the process to be done before upgrading to 7.4 or newer.

1. Create a new Regular Volume
2. Manually copy video folders from Failover volumes to new Regular Volume

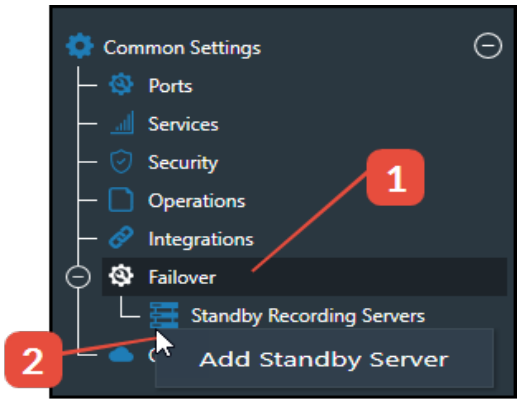
3. Sync the volumes by selecting the Volumes node under the Recording Server and selecting Sync All.



4. Delete the Failover Volume
5. Upgrade the deployment to 7.4 or newer
6. Migrate to Storage Pools
7. Proceed with the following steps

Adding a Failover Server

Within Common Settings, expand the Failover node, right click Standby Recording Servers, and select Add Standby Server. Provision the new server with the required information, licensing, feature keys, etc.



Standby Server Licensing

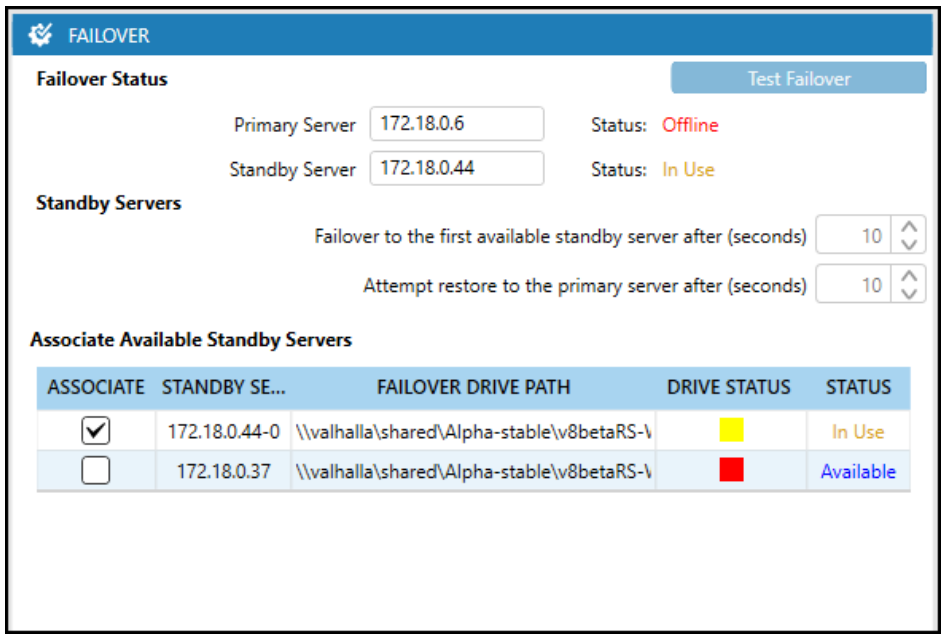
Note that all Standby Servers should have the same number of camera licenses as the Primary Server with the most camera licenses that might fail over to them. In a deployment of three Recording Servers, for example, if one Recording Server has 100 camera licenses, one has 50, and one has 25, all Standby Servers to which any of the three Recording Servers may fail over must have 100 camera licenses available in the event that the first Recording Server with 100 cameras fails.

Associating Standby Recording Servers to a Primary Recording Server

Once the Standby Server is licensed and has access to the shared storage path, the Administrator can configure failover options by selecting the Configure Module and selecting the name of the Primary Recording Server.

Presuming they are implemented correctly, an Administrator can associate any number of Standby Servers with the selected Primary Recording Server. The available Standby Servers will be displayed in the Failover pane, shown below. A Standby Server can only have a single shared drive per Standby Server at a time. The path can be changed when the Standby Server not actively in Failover mode. Once defined with a path, that same path must be used by any Primary Server associated to it. The configuration supports the ability for different Standby servers with a different drive path to be associated

to the same Primary. The same Standby Server list will be available across any Recording Server, and a Standby Server may be associated with multiple Primary servers.



Failover Panel

This panel provides several different status indicators to help the administrator understand the current state of failover for a given Primary Server. This section provides information relative to failover for the selected Primary Recording Server.

Failover Status

Failover Status displays the IP addresses of the Primary Server and Standby Server and their statuses. While the Primary Server is offline, the IP address of the active Standby Server will be displayed. The status indicators to the right of the IP addresses display the states of the servers. When the Primary Server is active, there will not be any value listed for the Standby. Valid statuses are:

- Online
- In Use
- Offline

Standby Servers

This section provides the ability to define how long the system should wait to execute the failover process. The Management Server monitors the Recording Servers involved in the failover configuration. When it detects that either a Primary Recording Server has gone offline or it has been restored, the Management Server will refer to the values configured here before executing the failover process. Both settings have a minimum value of 10 seconds, and a maximum value of 300 seconds (5 minutes).

Failover Time Values

Failover to the first available Standby server after (seconds)	Defines the value the MS will use before marking the Primary Recording Server down and executing the failover process.
Attempt restore to the Primary after (seconds)	Defines the value the MS will use before marking

a Primary Recording Server online and executing the recovery process.

Associate Available Standby Servers

This table represents all available Standby servers in the system. The administrator is able to associate any number of Standbys to the select Primary Server via the Associate column, as described above. Once a Standby Server has been associated, the administrator must provide a UNC path to a Failover Storage Pool in the “Failover Drive Path” column to enable saving data. Upon saving, CompleteView verifies both the Primary Server and the Standby Server have write access to the drive path before the configuration can be saved . Failure of write access will prevent the configuration from being saved.

Associate Available Standby Servers Values

Associate	This provides the admin the ability to establish the relationship between the Primary and available Standby servers.
Standby Server	Lists the friendly name of the Standby servers.
Failover Drive path	Text entry for UNC path to a directory that both Primary and Standby servers have write access to and has been configured as a Failover Storage Pool.
Drive Status	Provides a color icon and tool tip to represent the current write access status of the Primary and Standby servers to the provided failover drive path. The states are: • Green - both Primary and Standby servers have been validated to have access to the directory • Yellow - one of the Primary or Standby servers does not have write access to the directory • Red - neither the Primary nor the Standby server has write access to the directory • Black – Indicates an unknown status. Refresh the page by either clicking on the Configure module or clicking Save to update the status if stale
Status	Provides a color text status of the status of the Standby server relative to being to the Management Servers list of know status. As the MS is the orchestrator of failover, it keeps track of each Standby server. The possible values are: • Available - the Standby server has been defined, and is not currently participating in an active failover. • In Use - the Standby server is currently acting on behalf of a Primary server and is not available for other Primary servers to failover to. • Unavailable - The Standby server is offline. The status is only updated upon loading of the Edit Server screen.

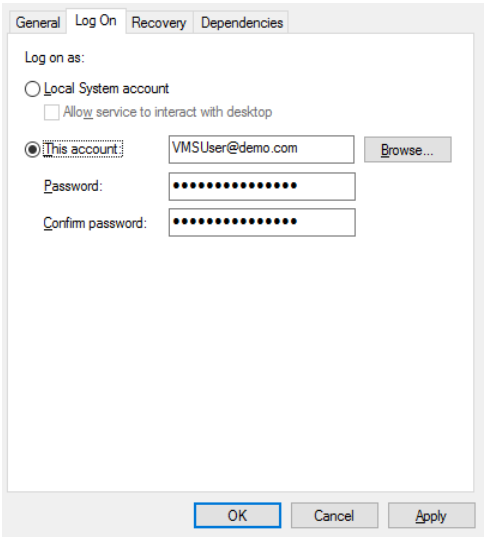
Failover User Permissions

The user account utilized for log on of the service must have administrative access to the local machine and full access to any share being utilized by the Primary and Standby Recording Servers. The following configurations may or may not be necessary, depending on network configuration.

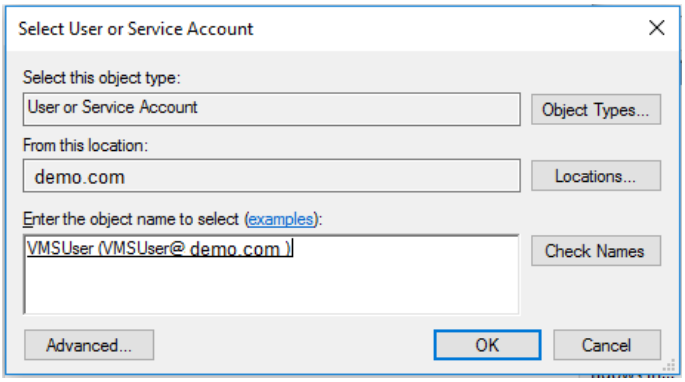
Permissions Configuration

After installation, launch services.msc, and stop the CompleteView Recording Server service. Right-click on the service and select Properties.

In the Log On tab, the Log on as: value will need to be changed by an administrator to This Account (from Local System account), shown below.

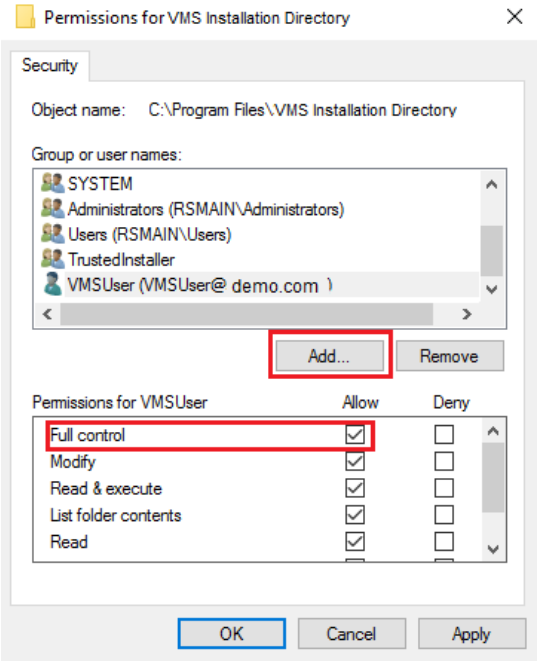


Select Browse and use the Windows user selection tool to select the admin user. After exiting the Windows user selection tool, enter the user's password and click OK to exit the Properties window.



Recording Server Application and Shared Folder Permissions

As stated above, the logged on user must have administrative access to the local machine and full control of the shared Failover drive. Navigate to the CompleteView installation directory, right-click on Salient Security Platform folder and select Properties. In the Security tab, the admin user may be added by clicking Edit... then Add.... Use the Windows user selection tool to add the admin user and select Full Control for the admin user. Repeat for the Shared failover drive.



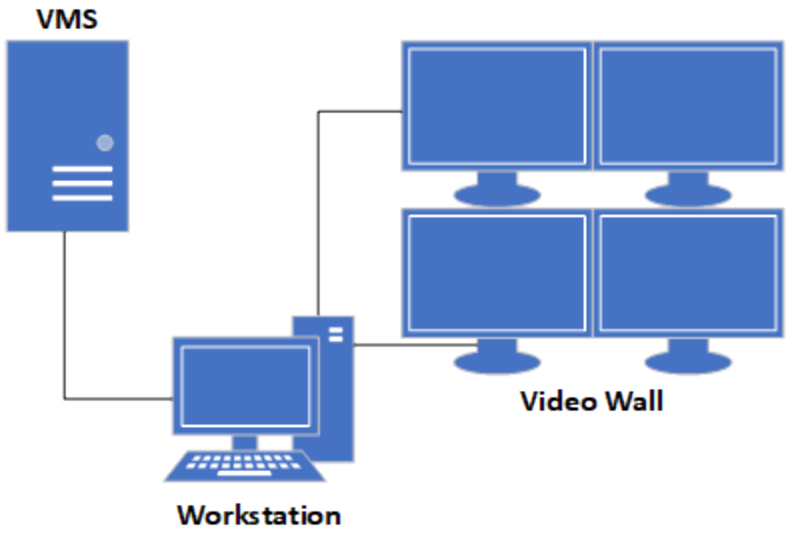
Once complete, click OK and exit out of the folder properties.

Restart the CompleteView Recording Server service. Failover configuration is now complete.

Video Wall Introduction

Using the Video Wall feature, users can push and display cameras, Views, and Maps to remote video monitors so that the content may be seen by others in a monitoring facility or elsewhere. The Video Wall setup consists of collections of video monitors connected to one or more host workstations. Each host workstation will be connected to one or more monitors, depending on the number of installed display adapters and supported video outputs. A video wall view layout is created to represent the organization of the monitors, and users and groups are given access. Using the Desktop Client's Live View module, users can drag and drop cameras, Views, and Maps onto one of the display tiles within the layout and push the content to the corresponding monitor.

Note: Video Wall configuration takes place first via the Video Wall Agent, optionally installed during the Desktop Client installation, then within Views/Maps, then finally in Live View. If the Video Wall Agent was not installed initially, uninstall the Desktop Client, then re-run the Desktop Client installer, selecting the Video Wall Agent option during re-installation. The Video Wall Agent needs to be configured prior to configuration within Views/Maps and Live View. In addition, it is strongly advised to run the Video Wall Agent on a workstation not hosting either recording or management servers.



Video Wall Configuration - Video Wall Agent

The Video Wall Agent (VWA), optionally installed along with the Desktop Client, allows the local workstation to display full screen Views, cameras, and Maps across all or selected connected monitors. It should be noted that the Video Wall is best run on a computer not hosting any other component of CompleteView other than the Desktop Client. If the Video Wall Agent is desired but was not installed, simply uninstall the Desktop Client, reinstall it, and select the Video Wall Agent check box.

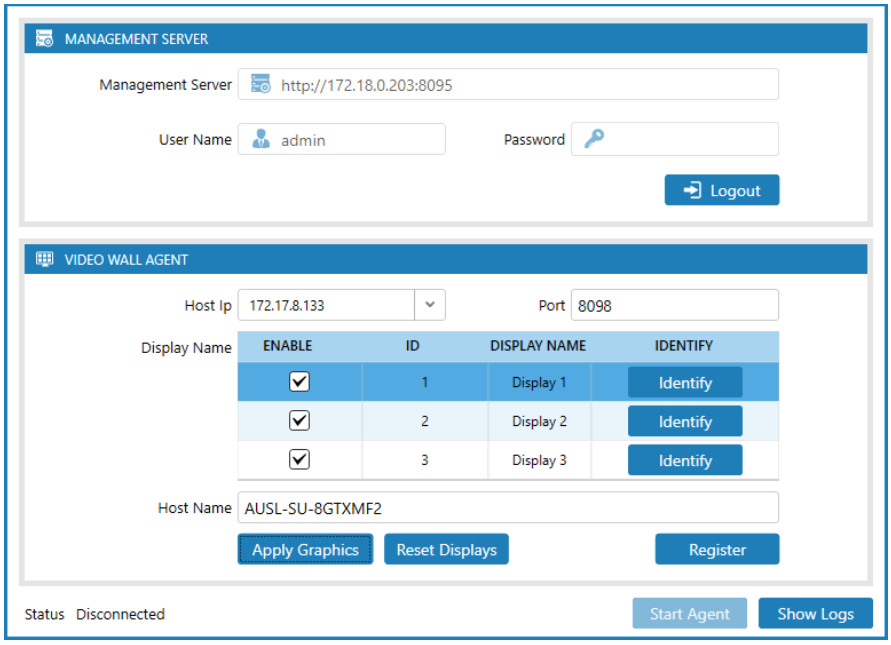
Note that the Video Wall Agent must be configured before configuration of Views/Maps and Live View.

Video Wall Agent Configuration

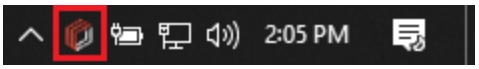
Follow the steps below to configure the Video Wall Agent.

Login

Upon initial launch of the Desktop Client, the Video Wall Agent will also launch. Enter a valid address and credentials for the Management Server, and click Login. If the VWA is not visible, launch it from the system tray, as described below.

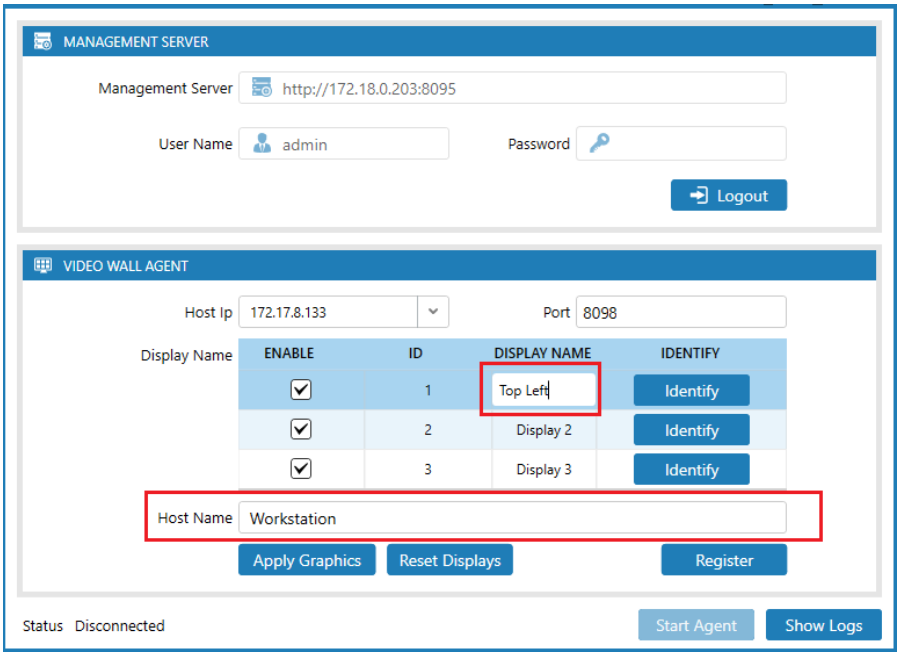


After the Video Wall Agent has been launched once, it will reside in your system tray. Right click and select Video Wall Agent to bring it up. Note that the Desktop Client must be launched for the Video Wall Agent to be functional unless configured to launch automatically as described below.



Identify & Name the Displays & Host Name

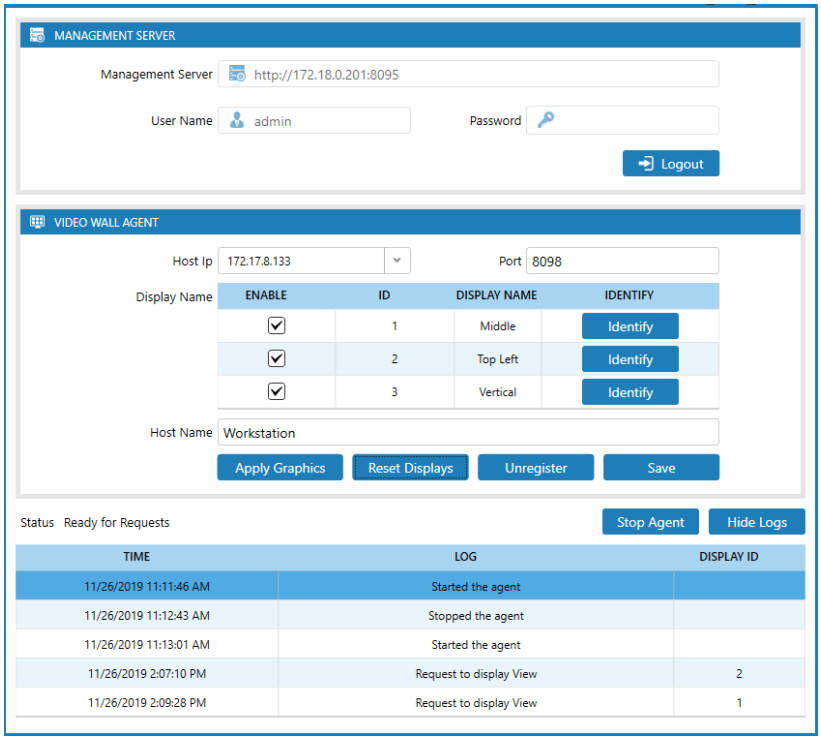
Clicking the Identify button will display a number on the corresponding monitor. Change the Display Name to meaningfully describe the monitors by clicking in the field and entering the new name. It is strongly suggested the names of the displays reflect their relative positions and/or characteristics in the real world. Doing so will greatly assist the configuration process in Views/Maps and the Live View module.



After naming the monitors connected to the Video Wall Agent workstation, rename the Host Name something meaningful. Finally, click Register, then Start Agent. This process identifies the current machine as an available VWA to the deployment's Management and Recording servers.

Views/Maps is now ready for configuration. After configuring Views/Maps, use Live View to push the selected streams to the Video Wall Agent. Both procedures are detailed in following sections.

Note: In the event of a workstation shut down, the Video Wall Agent must be restarted unless the agent is configured to automatically start (see below). First launch the Desktop Client, then log into the Video Wall Agent, then click Start Agent. The workstation is now ready to have the video feeds pushed to it from the server via Live View.



Apply Graphics

Clicking Apply Graphics will display the preconfigured logo screen on all connected monitors. Click the x in the upper right hand corner to clear the graphics one at a time.

Reset Displays

Click Reset Displays to clear all video feeds and graphics from all connected monitors. Video Wall agent may be accessed via the system tray, or Alt+Tab, if running in the background.

Unregister

Click Unregister to remove the workstation from the list of available Video Walls in Views/Maps.

Save

Clicking Save will save any changes made to the VWA configuration.

Start/Stop Agent

Clicking this button will start and stop the Video Wall Agent. If stopped, the workstation will not accept video feeds from the Recording Server.

Show/Hide Logs

Clicking this button will display or hide the agent's log entries.

Configure Video Wall Agent for Automatic Launch

The Video Wall Agent can be configured to automatically launch on system startup. The configuration process presumes Windows administrative access and knowledge as the required tasks will not be detailed here.

CompleteView Configuration

1. Complete all the required configuration steps above.
2. Grant the CompleteView user logging into the VWA Desktop Client machine Auto Login permissions in the Client Customization section of the User Access screen in Users/Groups.
3. Log out of the Desktop Client and either select or verify that Remember Me is checked.
4. Log back into Desktop Client.

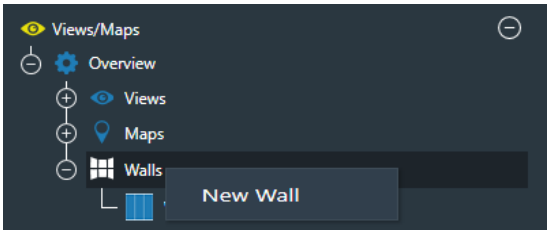
Windows Configuration

1. Configure the Windows user used on the Video Wall Agent PC to automatically log in upon system startup:
   https://learn.microsoft.com/en-us/troubleshoot/windows-server/user-profiles-and-logon/turn-on-automatic-logon
2. Create a batch file or equivalent startup script for the user in step 1 containing the following:
   cd C:\Program Files\Salient Security Platform\CompleteView\Desktop Client VideoWallAgent.exe /loginAndStartup
   https://www.windowscentral.com/how-create-and-run-batch-file-windows-10

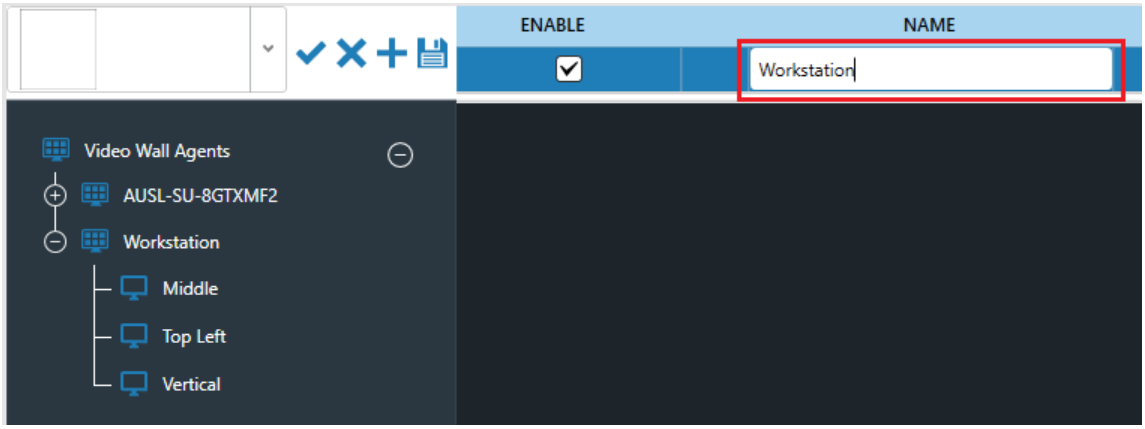
Video Wall Configuration - Views/Maps

Using the Configure module, administrators can configure Video Wall view layouts referred to as Walls, similar in concept to creating and editing Views. Once the wall layout is created, permissions for users and groups can be given similar to Views and Maps.

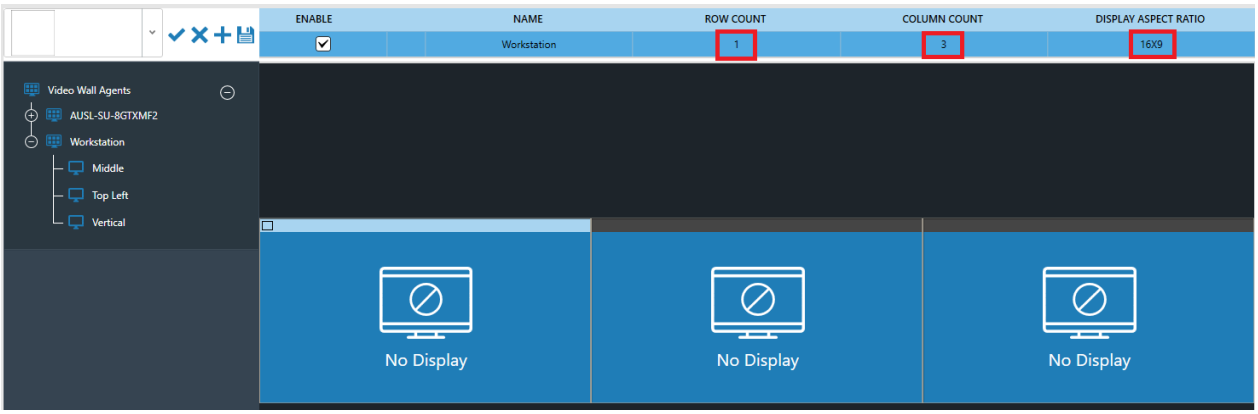
Within the Configure module, select Views/Maps, right click on Walls, and select New Wall.



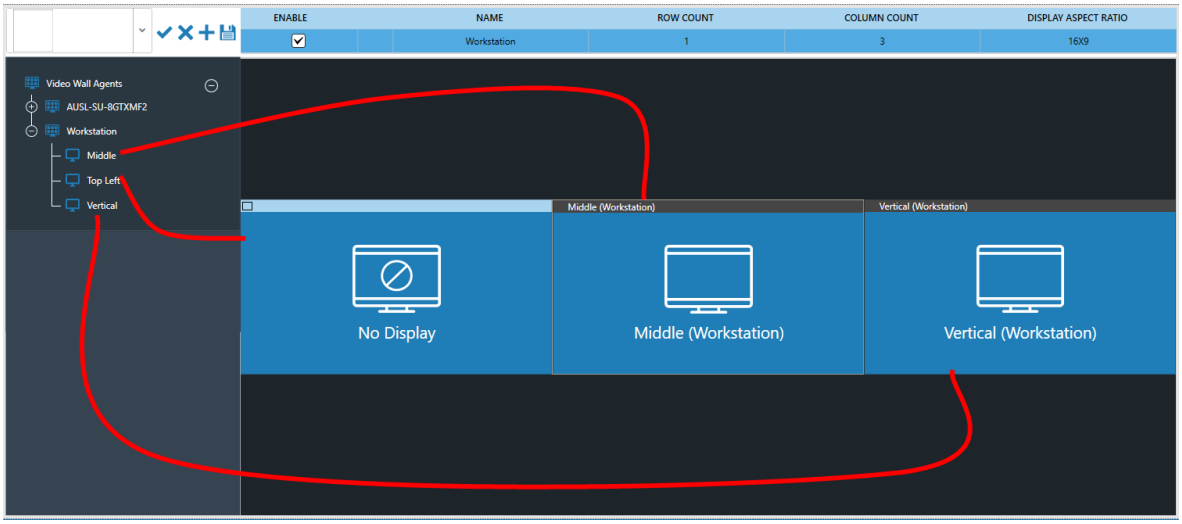
A list of available Video Wall Agents will be displayed in the left pane. Name the new wall something meaningful in the info bar above, either reflecting the nature of the video feeds to be displayed, or the destination of the video wall (in this case, "Workstation"). Note that the Wall is organized by the Host Name (Workstation), and the names of the monitors attached to it, as configured in the Video Wall Agent, described in the previous section.



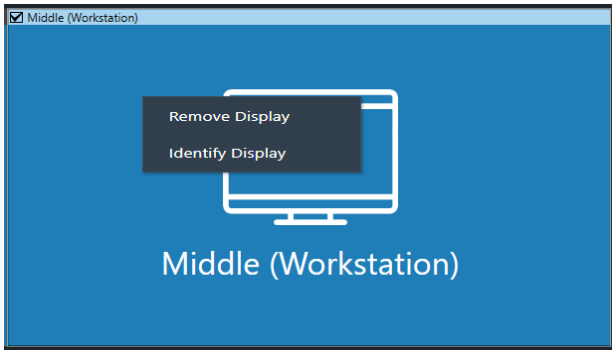
Next, create a row and column count that reflects the physical layout of the monitors to which you will be displaying video. For example, if you've 4 monitors in 2 rows, create a 2 row, 2 column layout. This example will use a 1 x 3 layout. Select the aspect ratio, then save.



Next, drag the display to its appropriate position in the new layout. In this example, the Middle display was dragged to the middle, the Top Left will be dragged to the left position, and Vertical to the right, reflecting their real-world relative positions.



Right clicking on a tile within the layout will present options to Identify Display and Remove Display. When Identify Display is picked, the remote display associated with the current Video Wall Agent will show its monitor ID. This feature allows the user to verify the physical location of monitor within the layout. Remove Display removes the selected display from the Video Wall configuration, and may be re-added from the Video Wall Agent on the workstation.



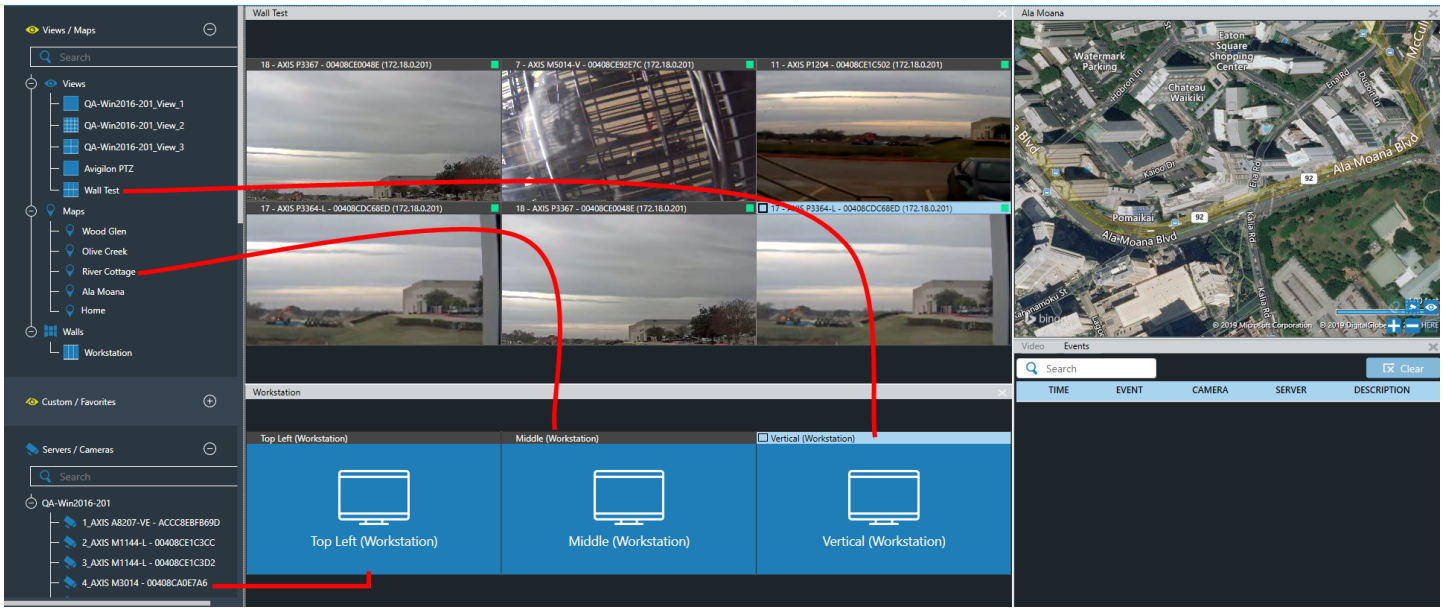
Templates can be created, saved, and applied onto a new wall layout similar to Views. See **Views & Maps Creating Views and Templates** for detailed information.

Finally, the Video Wall may have Views, cameras, and Maps pushed to it in Live View, described in the next section.

Video Wall Configuration - Live View

After first configuring the Video Wall Agent then Views/Maps, select the Live View Module.

From the Live View module, select and drag the View, Map, or camera to the desired Wall's Agent's monitor. The View, Map, or camera will automatically begin displaying on the targeted monitor, obscuring applications behind it, but not obscuring the system tray, allowing access to the Video Wall Agent. Once again, launch the Video Wall Agent and select Reset Displays to clear all monitors of the workstation of the streaming feeds.



In the example above, the Wall Test View will be displayed on the Vertical monitor, the River Cottage Map will be displayed on the Middle monitor, and the 4_AXIS M3014... camera will be displayed on the Top Left monitor.

Note: If the function of the workstation is interrupted as would happen in a power outage or other system shutdown, the Video Wall Agent must be relaunched by first launching the Desktop Client, then clicking Start on the Video Wall Agent. Then the streams must be dragged to their respective monitors once more to start displaying again.

Cameras and Integrations Overview

CompleteView integrates with an ever-expanding list of cameras, camera protocols, NVR/DVRs, and third party access control and alarm systems. The following sections detail many of those integrations, but the latest information may be found on Salient's website **https://www.salientsys.com** .

Analog Camera Control Protocols

The following analog camera protocols adhere to EIA Standards RS-422/485.

AD ASCII Continuous	American Dynamics ASCII; Continuous commands
AD ASCII Make/Break	American Dynamics ASCII; Start/Stop commands
AD Pelco P	
Canon VC-C4	
Kalatel	
Digital	CompleteView PTZ control for fixed analog or IP cameras
Panasonic WV-CS850 Conv	Panasonic Conventional
Panasonic WV-CS850 New	Panasonic New
Pelco ASCII	For CM6x00 video matrix switch and CM9760
Pelco D	
Pelco P	
Philips Biphase	
RVision	
SAE	
Samsung	
Sensormatic	For Sensormatic and American Dynamics cameras
Sony EVI-D30/D31	Sony Visca protocol
Ultrak KD6 (Diamond)	Ultrak; formerly known as the Diamond protocol
VCL	
Vicon	

IP Camera Control Protocols

The following IP camera protocols adhere to EIA Standards RS-422/485.

ACTi HTTP IP	ACTi IP camera driver
ACTi Pelco D IP	ACTi IP camera driver
ACTi Pelco P IP	ACTi IP camera driver
AD Illustra	
AD	
Axis V2 IP	Axis Communications V2 API
Axis V2 IP version 4.0	Axis Communications V2 API; Use for camera/encoder firmware
Bosch BiCom	
Bosch OSRD	
Bosch Pelco-D	
Brickcom	
Canon	
Cisco IP	V 1.0
CohuHD RISE	
Dahua IP	
Digital	CompleteView Digital PTZ control for fixed analog or IP cameras
FLIR	Nexus (DLTV) IP, Nexus (IR) IP, IP
Generic-D	Generic Dynacolor IP PTZ Protocol
Hikvision Speed Dome	
Milesight PTZ	
Mobotix IP	Mobotix 360 degree IP cameras
ONVIF	
Panasonic IP	All Panasonic cameras
Pelco API	
Pelco	
Samsung	
Samsung IP (v2)	
Sentry360 IP	
Sentry Railway	
Sony IP Continuous Move	
Sony IP-Move	Sony IP-Move
Sony Visca IP	All other Sony cameras
Speco IP	
Symmetry ENVS IP	
Toshiba IK-WB IP	Toshiba IK-WB01A/11A

Toshiba IK-WB21A Toshiba IK-WB21A
Vivotek

Generic IP Camera Drivers

CompleteView has been designed as a flexible platform for supporting IP imaging devices. Accordingly, a generic driver model is available that supports a basic functionality for most IP cameras.

Generic IP Camera for MJPEG

Repetitive HTTP requests for a JPEG image:

Enter the path* for a JPEG image on the camera. Examples include "image", "jpeg", and "axis-cgi/jpg/image.cgi?camera=2".

Generic IP MJPEG Streaming Camera for MJPEG

An HTTP request for streaming JPEG images:

Enter the path* for an MJPEG stream on the camera. Examples include "image", "nphMotionJpeg", and "axis-cgi/mjpg/video.cgi".

Generic IP RTSP Streaming Camera for MPEG-4

RTSP control of MPEG-4 video over RTP, both tunneled through HTTP. Enter the path* for an MPEG-4 stream on the camera.

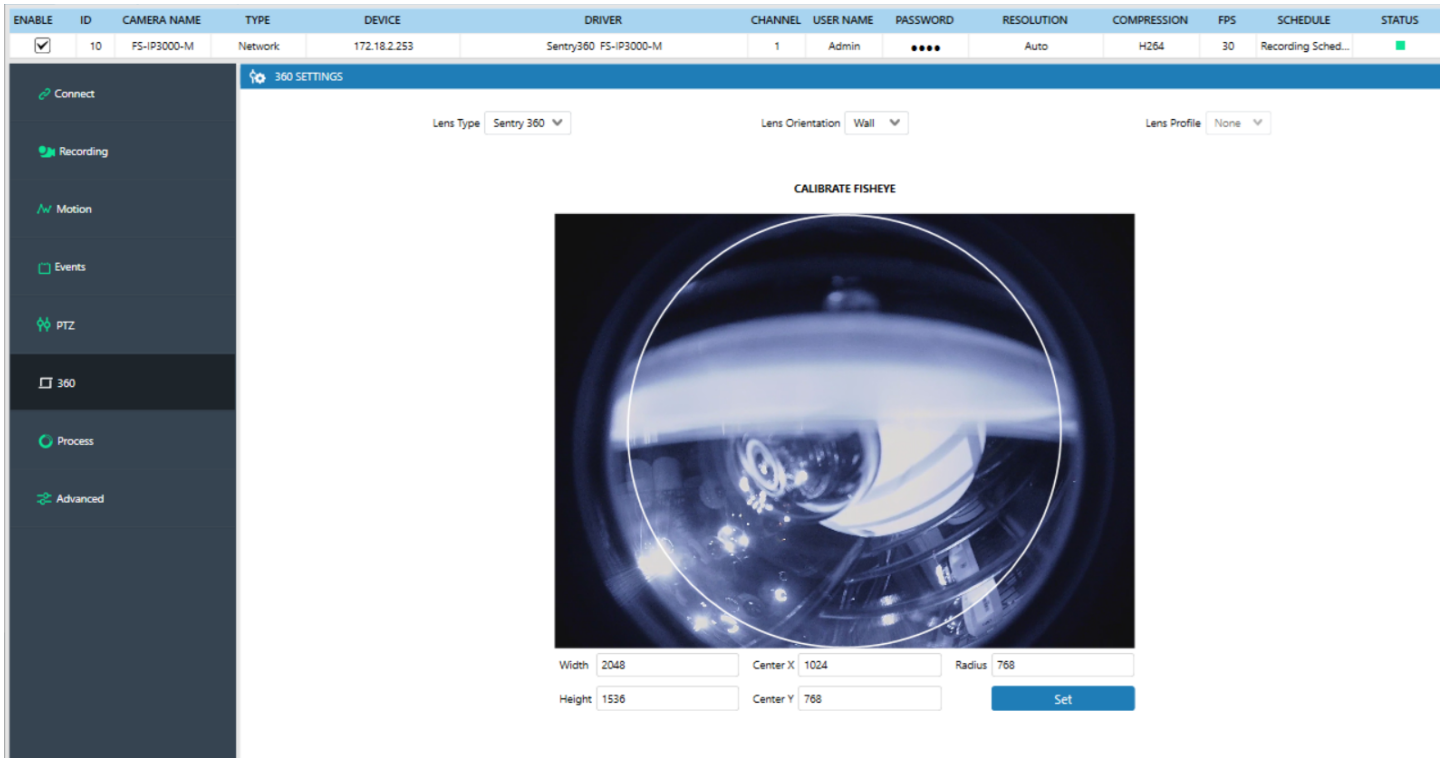
Note: A URL path follows the domain name (and optional port number) and precedes the query string. For example, in the URL, "http://192.168.1.100:80/image?speed=10", "image" is the path. However, CV's use of "path" includes everything after the domain name (and optional port number), which also includes the query string, if present. Therefore, from the example URL, one may enter "image?speed-d=10" as the path. If one does not enter the path beginning with a slash character ("/"), as in our example, CV provides one. For those rare cases where the camera does not allow a path, enter a single slash character instead of leaving the path field blank.

Fisheye Calibration

CompleteView allows for calibrating the area of focus on many Sentry360 and ACTi fisheye cameras. Select the appropriate camera from the Cameras list in CV Configure/360. From the Lens Type drop-down menu, select Sentry360 or ACTi.

Acknowledge the notification that Dynamic Resolution Scaling will be disabled for the camera to be adjusted, if presented.

Click and drag the field of view circle (in white) to encompass the desired area. Alternately, the axis coordinates and circle radius can be set manually by entering the desired values in the corresponding fields.



Click Set when done.

The field of view has now been set.

Active Directory Connector

This appendix assumes that you already have a live Active Directory implementation on your network and that you are familiar with the concepts, terms and tools surrounding it.

Key Benefits of Integration with AD (Enterprise feature)

1. Active Directory can be leveraged for resolving issues related to the management of multiple passwords and accounts and greatly alleviates the account administration burden of the IT staff.
2. End-users in Windows environments typically already employ Active Directory for their Windows login, thus options for achieving reduced or single sign-on are expanded.
3. Authentication against a central directory such as Active Directory allows end-users to have only one password to remember or change, eliminating the downtime and lost productivity associated with maintaining multiple passwords.
4. With end-users employing only the Active Directory password, administrators' account management functions are streamlined and they realize a dramatic reduction in Help Desk calls, as end-users no longer require them to perform password resets for forgotten passwords.
5. Coordinating disparate password policies is no longer an issue for administrators as Active Directory controls password quality, expiration, etc.
6. Authentication redirection to Active Directory provides strength and flexibility for optimizing compliance related activities, such as enforcing password policies that require passwords to be strong and changed regularly.

Prerequisites

The following conditions should be met for each video server on which you wish to enable the AD connector.

1. The computer should be a member of the domain for which you have configured the AD connector. However, non domain joined servers connecting to AD are supported.
2. An Enterprise feature key must be installed.

Limitations

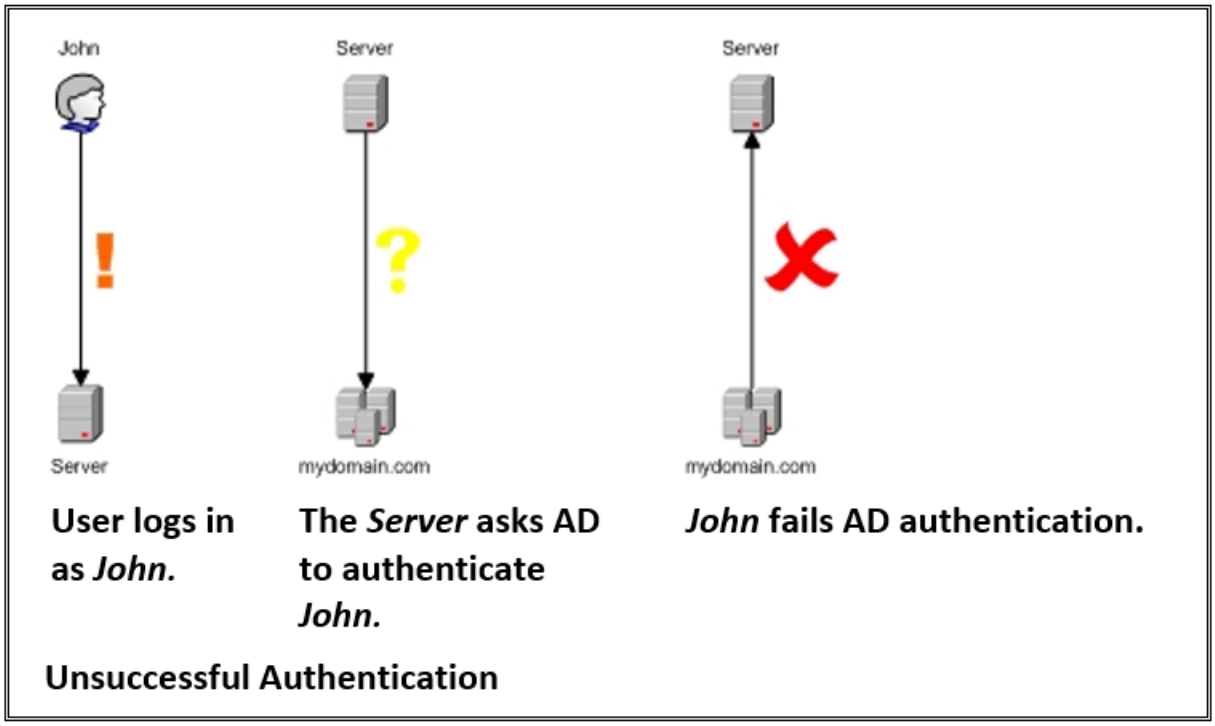
The following limitations exist in the current implementation of the AD connector.

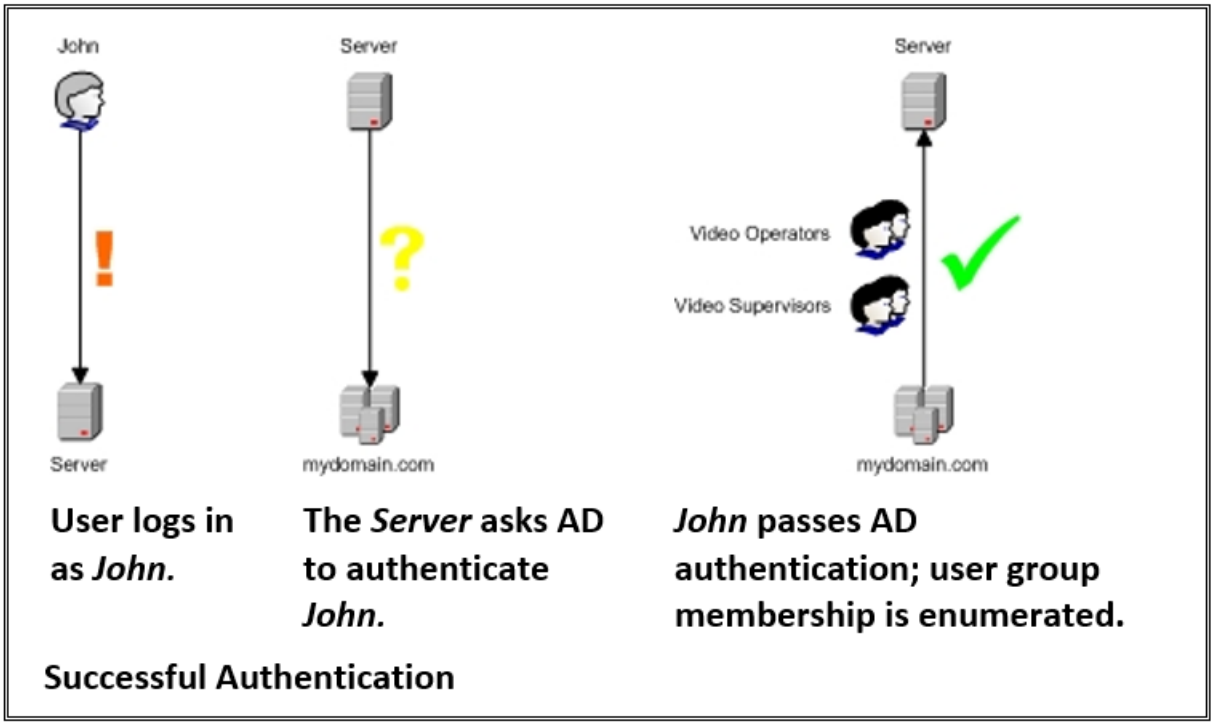
1. Dynamic selection of domains is unavailable.
2. Supports only User and User Group objects.

Implementation

- Performs dynamic authentication of users against the configured AD domain.
- Enumerates a user's group membership within the configured AD domain.
- Access control remains within CompleteView.
- The Active Directory database schema is not extended.

Dynamic User Authentication



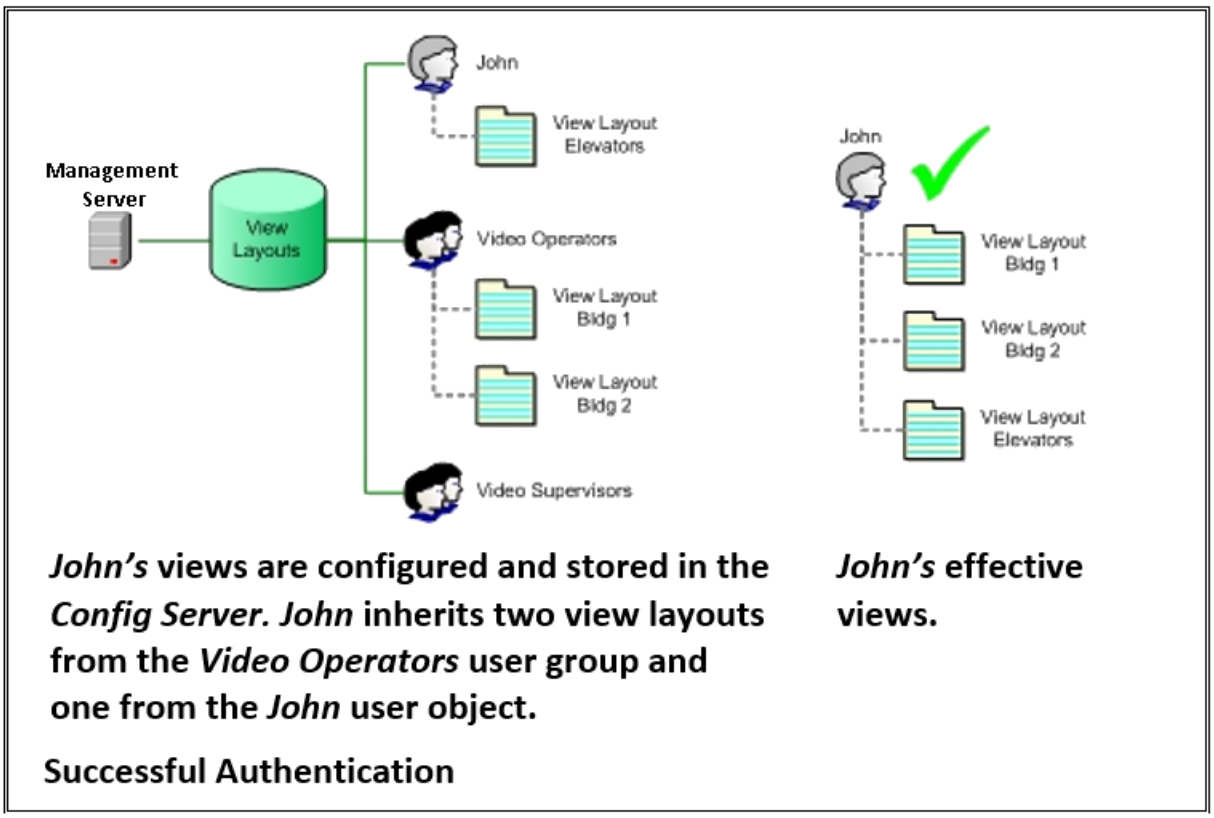


CompleteView Management Server

When the AD Connector for the Management Server has been enabled, dynamic authentication against AD is performed as users' login to CV. User credentials pass through the Management Server to each CV Server that the user attempts to access.

***John's* effective views.**

Unsuccessful Authentication



***John's* views are configured and stored in the *Config Server*. *John* inherits two view layouts from the *Video Operators* user group and one from the *John* user object.**

***John's* effective views.**

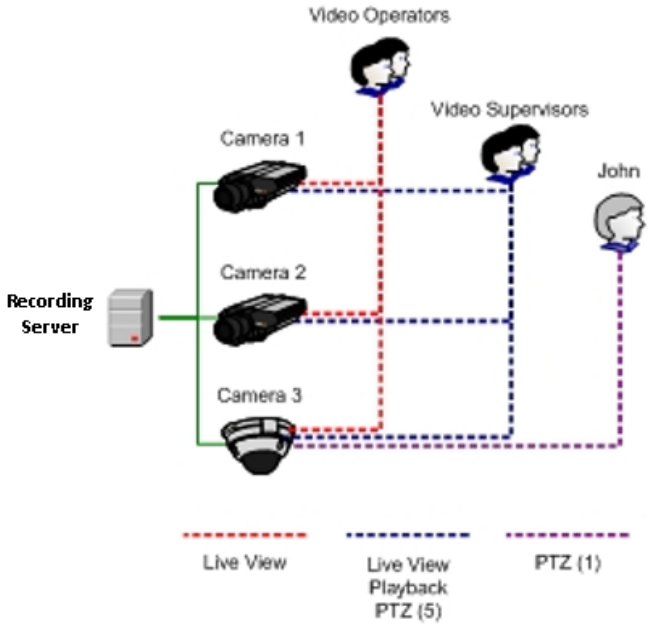
Successful Authentication

CompleteView Server

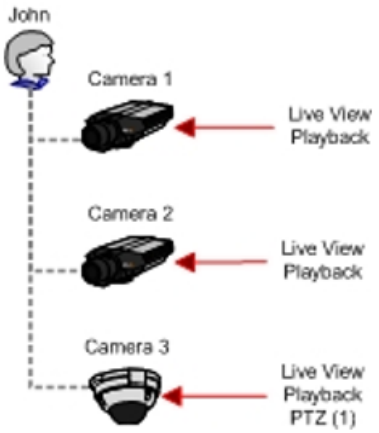
When the AD Connector for the Management Server has been enabled, dynamic authentication against AD is performed as users' login to the CV application. User credentials pass through the Management Server to each CompleteView Server that the user attempts to access.

***John's* effective camera permissions.**

Unsuccessful Authentication



Camera permissions are configured in the *CVSP Server. John* inherits live view permission from the *Video Operators* and *Video Supervisors* user groups, playback permission from the *Video Supervisors* user group, and a PTZ priority level of '1' from the *John* user object.



***John's* effective camera permissions.**

Successful Authentication

FLIR Camera Configuration

About the FLIR A310pt

The FLIR A310pt unit typically consists of two video sensors mounted on a single pan/tilt base. Consequently, the sensors always share the same elevation and bearing. One sensor provides a television (TV) image with zoom, focus, and iris control. The second sensor provides an infrared (IR) image with zoom and focus control.

The FLIR A310pt and CompleteView

Add the sensors on the A310pt as you would any other camera in CV. When adding different sensors from a single A310pt, each sensor is individually treated as a unique camera model. The TV sensor is added as the FLIR camera model A310pt DLTV and the IR sensor is added as model A310pt IR. This configuration allows the CV software to issue the proper camera control commands to each sensor.

In the event an A310pt unit consists of two or more of the same sensor types, the ID field on the PTZ cameras tab in CompleteView will provide the unique instance ID for sensor control commands (zoom, focus, iris).

Command Control Conflicts and Tour Considerations

The FLIR A310pt is a shared network device. When multiple users are connected to the A310pt, only one user at a time can issue commands to the unit. When a control command is requested by a VMS client station without the control token, CV automatically issues a request for camera control. After receipt of the unit control token, the client station is able control the unit. There may be a noticeable delay between each command as the interface waits for a response from the unit.

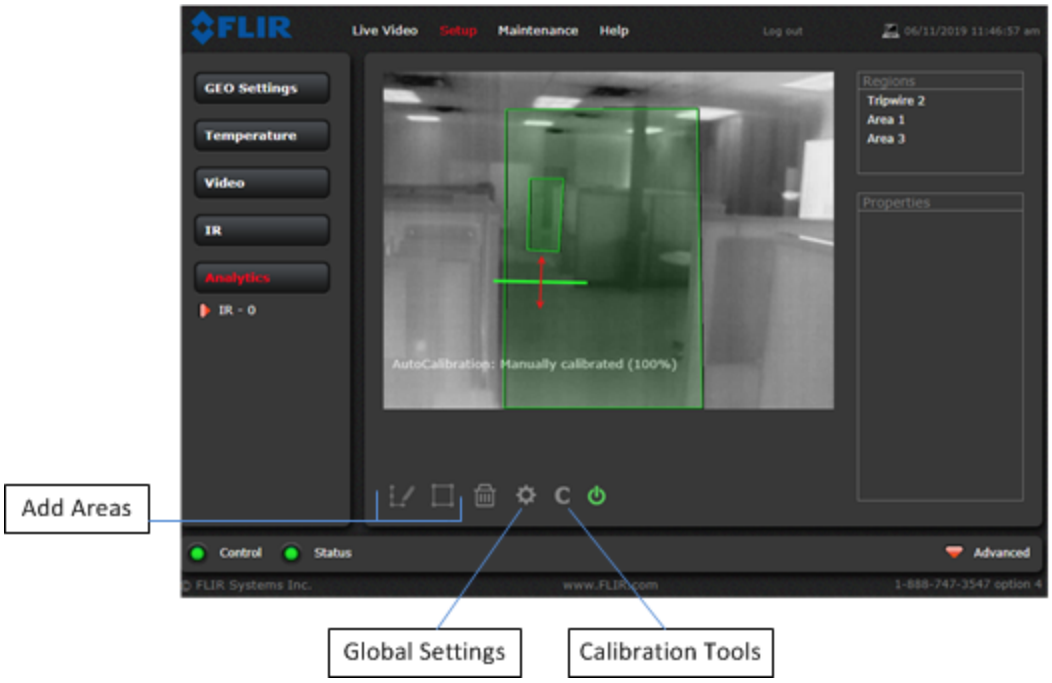
When setting up a CompleteView Tour, it is important to remember that both sensors (TV & IR) are mounted on the same pan/tilt arm of the FLIR unit, and share the same set of preset point coordinates. While each sensor tour may specify a different set of preset times, the preset points are the same because they are stored in the Pan/Tilt module of the FLIR unit. If you have a large number of named presets you want to share between sensors in CV, best practice is to install and configure one sensor (camera) first, clone that camera, and make the appropriate changes to the IP model and PTZ driver.

For more information on the FLIR A310pt unit, please consult the FLIR Nexus IP Camera Configuration Guide available on the FLIR website.

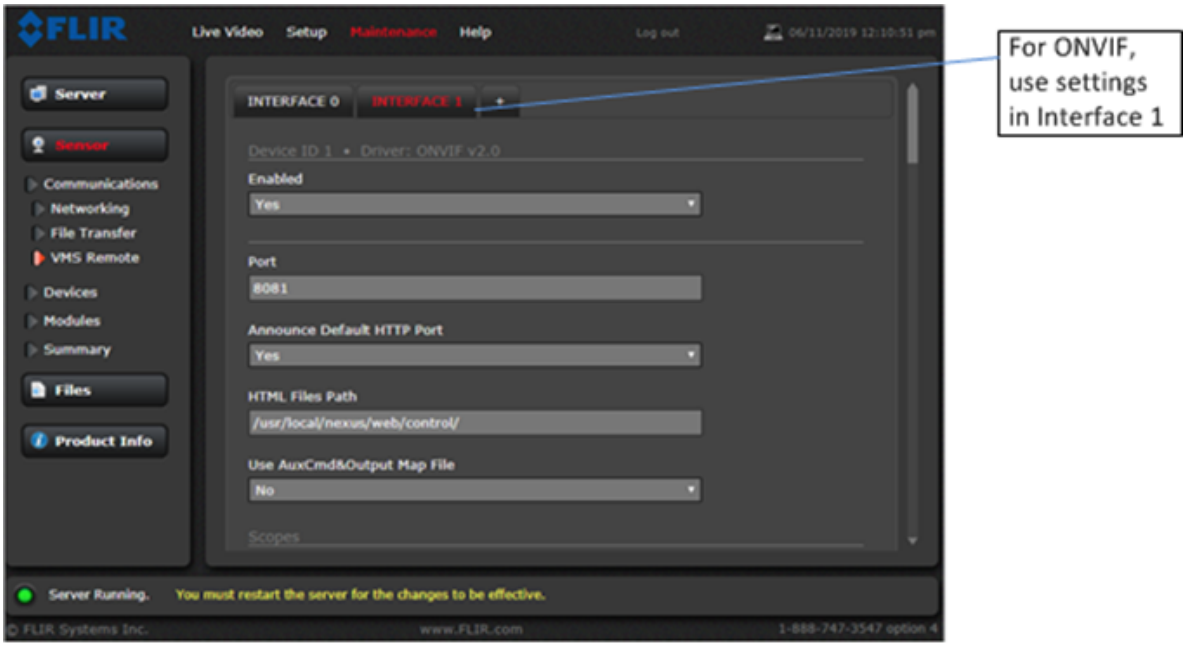
FLIR FC-Series Event Support

FC-Series Camera Setup

Use the Analytics page of the FLIR camera to configure areas and tripwires, exclude areas, and calibrate (auto or manual) for human, vehicle, or objects of interest. While an example configuration is shown below, Refer to the FLIR Installation Manual FC-Series ID for detailed instructions.


FLIR
Live Video
Setup
Maintenance
Help
Log out
06/11/2019 11:46:57 am
GEO Settings
Temperature
Video
IR
Analytics
IR - 0
AutoCalibration: Manually calibrated (100%)
Regions
Tripwire 2
Area 1
Area 3
Properties
Control
Status
Advanced
© FLIR Systems Inc.
www.FLIR.com
1-888-747-3547 option 4
Add Areas
Global Settings
Calibration Tools

Use the VMS Remote page of the FLIR camera to enable ONVIF (used only to pass event information to CompleteView). By default, the camera is configured with a VMS Remote interface with ONVIF 2.0 parameters (Profile S). Use the settings in Interface 1.

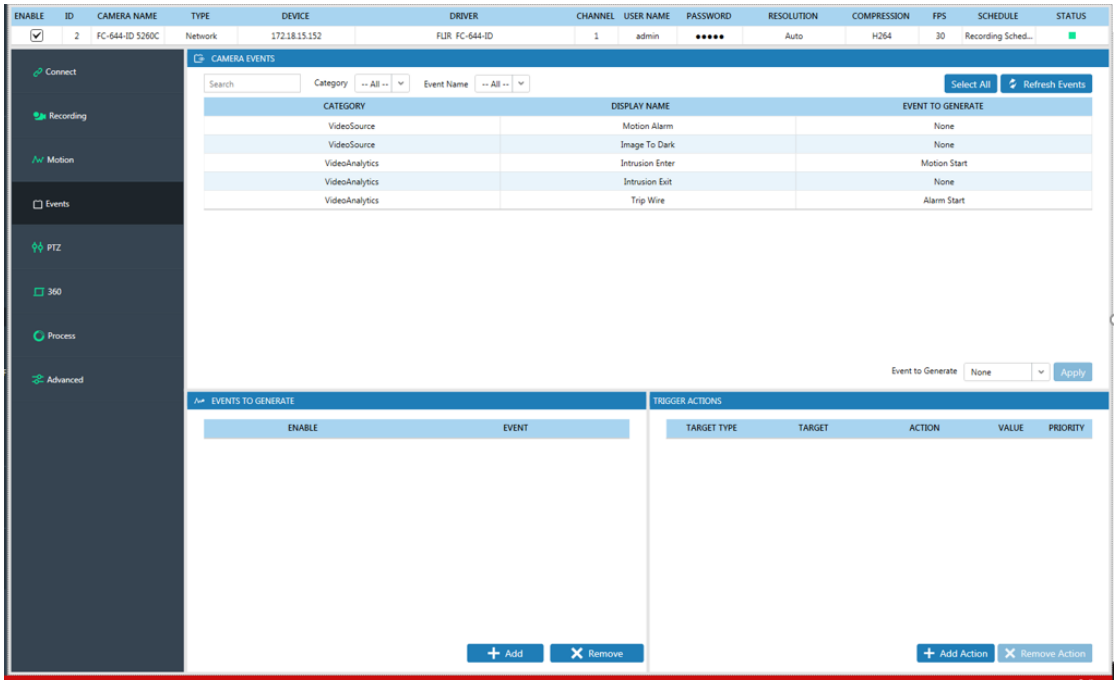


FC-Series CompleteView Configuration

CompleteView integrates with FLIR FC-Series cameras, and supports the following events/analytics. Configure the events as normal.

FLIR FC-Series Events

Motion Detection	On/Off
Intrusion Enter	Trigger
Intrusion Exit	Trigger
Trip Wire	Trigger
Image Too Dark	Trigger


ENABLE
ID
CAMERA NAME
TYPE
DEVICE
DRIVER
CHANNEL
USER NAME
PASSWORD
RESOLUTION
COMPRESSION
FPS
SCHEDULE
STATUS
2
FC-644-ID 5260C
Network
172.18.15.152
FLIR FC-644-ID
1
admin
Auto
H264
30
Recording Sched...
Connect
Recording
Motion
Events
PTZ
360
Process
Advanced
CAMERA EVENTS
Search
Category
-- All --
Event Name
-- All --
Select All
Refresh Events
CATEGORY
DISPLAY NAME
EVENT TO GENERATE
VideoSource
Motion Alarm
None
VideoSource
Image To Dark
None
VideoAnalytics
Intrusion Enter
Motion Start
VideoAnalytics
Intrusion Exit
None
VideoAnalytics
Trip Wire
Alarm Start
Event to Generate
None
Apply
EVENTS TO GENERATE
ENABLE
EVENT
Add
Remove
TRIGGER ACTIONS
TARGET TYPE
TARGET
ACTION
VALUE
PRIORITY
Add Action
Remove Action

ImmerVision Panomorph Lens Profiles

The following ImmerVision lens profiles are compatible with CompleteView.

ImmerVision Panomorph Lens Profiles

Manufacturer	Model	RPL
ImmerVision	IMV1-1/3	A0IFV
Fujifilm	YF360A-2	A0NKV
Fujifilm	YF360A-SA2	A0NKV
Fujifilm	DF360SR4A-SA2	A1UST
H.Q.O.	PL-M01-V08	A8TRT
Kolen	KL04Z	B0QQV
CBC Computar	H1328KP	B4QQV
CBC Computar	L1028KRW/ L1028KDRW	B5SST
CBC Computar	L1028KRW-180	B6SST
C360	6K	B72YV
CBC Computar	T0928-KRW	B8QQT
Xiamen Leading Optics Co., LTD	F117B12924IRM12	B9VVT
Kolen	KL16618	C1ZZV
Vantrix		C322V
Hanwha Techwin	SNF-8010/ SNF-8010VM	C7SST
Hanwha Techwin	PNF-9010R/RV/RVM	C8WWT
CBC Computar	E1222KRY	C9VVT

Pelco Optera

Overview

CompleteView includes basic Pelco Optera integration. While CV supports all three Optera Compatibility Modes, Salient recommends using the Tiled H.264 mode, which, at this time, provides the best viewing experience.

NOTE: While both UDP and TCP protocols are supported, Salient recommends using TCP when possible due to the size of the images and the potential for bit-errors during transmission.

Optera Compatibility Mode Selection

The Pelco model selection for the Optera camera MUST match the current compatibility mode selected for the camera. CV provides three model selections for the Optera:

- Optera IMM12018 (Tiled).
- Optera IMM12018 (Panomersive).
- Optera IMM12018 (Unistream).

Tiled H.264 Compatibility Mode

Optera IMM12018 (Tiled) must be selected when the Optera is in the Tiled H.264 Compatibility mode. This CV model selection provides for an additional four selections under the Camera ID:

a. Left – Includes the left 60° of the 180° panoramic view
b. Front – Includes the middle 60° of the 180° panoramic view
c. Right – Includes the right 60° of the 180° panoramic view
d. Mosaic – Left, Front, and Right views stacked on top of each other

The following images indicate the Pelco Optera and CV settings for operation in the Tiled H.264 compatibility mode. Note the Pelco Model selection is Optera IMM12018 (Tiled).

Panomersive H.264 Mode

The CV Pelco model selection Optera IMM12018 (Panomersive) must be selected when the Optera is in the Panomersive H.264 Compatibility mode. This model selection provides for an additional three selections under the Camera ID:

a. Left – Includes the left 60° of the 180° panoramic view
b. Right – Includes the right 60° of the 180° panoramic view
c. Mosaic – Left and Right views stacked on top each other

The following images show the Pelco Optera and CV settings for operation in the Panomersive H.264 compatibility mode setting. Note the Pelco Model selection is Optera IMM12018 (Panomersive).

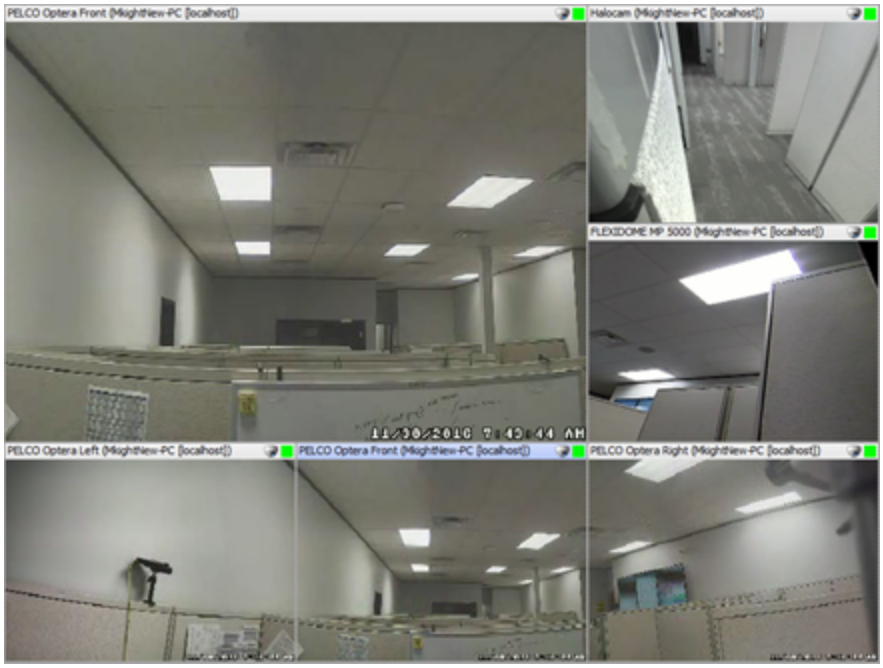
Panomersive Uni-stream

The Pelco model selection Optera IMM12018 (Unistream) must be selected when the Optera is in the Panomersive Uni-Stream Compatibility mode. There are no Camera ID selections for this model.

The following images show the Pelco Optera and CV settings for operation in the Panomersive Uni-stream compatibility mode setting. Note the Pelco Model selection is Optera IMM12018 (Unistream).

Optera Tiled H.264 Sample Display

The image below is an example of the Pelco Optera operating in Tiled H.264 Compatibility Mode with the tiled images being displayed along the bottom of the image pane and the enlarged Front view displayed in the largest video pane.



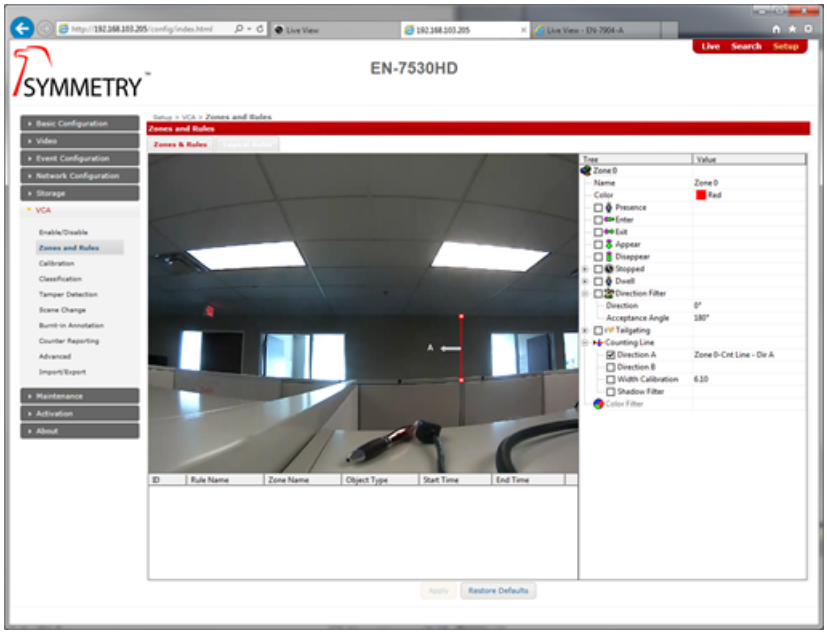
Symmetry Analytics Setup

1. Enabling VCA events from Symmetry Cameras.

a. From the Web interface, select VCA, then Enable/Disable.

b. Check the Enable VCA checkbox and the desired features. Only the features selected will activate. Read the text describing how selecting events will affect performance.

Apply the settings then move on to defining each event (setting lines and zones, etc.).



2. Enabling VCA events for Symmetry cameras from CompleteView. Enabling VCA events in CV is done in the CompleteView Configuration application.

a. Select the Cameras branch from the desired sever root, then select the Symmetry camera of interest.

b. Select the IP tab and check the Use On-Camera Alerting checkbox. Next, click on the <Configure Alerts...> button.

c. Enable / disable the Events of choice and select the recording level (Alarm or Motion).

d. Make sure the schedule for the Symmetry camera of interest is enabled for Alarm and/or Motion based on the settings in the On-Camera Alerting.

e. The Post motion and Post alarm timings on the Motion/Alarm tab are used when recording the triggered on-camera events.

3. Enabling DI events from Symmetry Cameras. Unlike the VCA events, interface setup beyond simply enabling the events is required.

a. From the Web interface, select the IO Configuration then DI/DO.

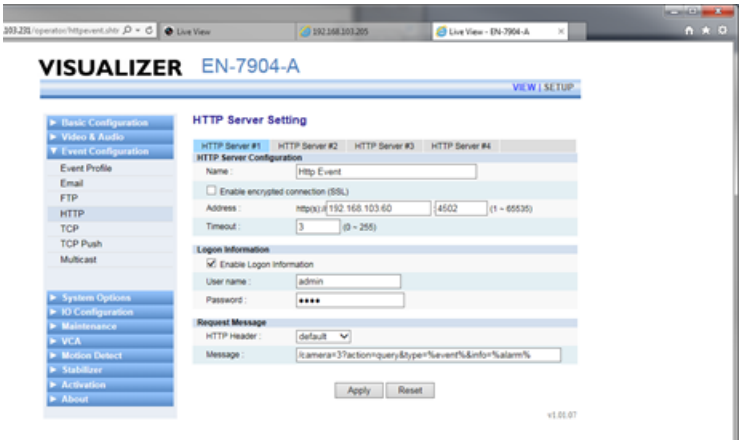
b. Select the DI Resource Type.

c. Select the DI Trigger Type.

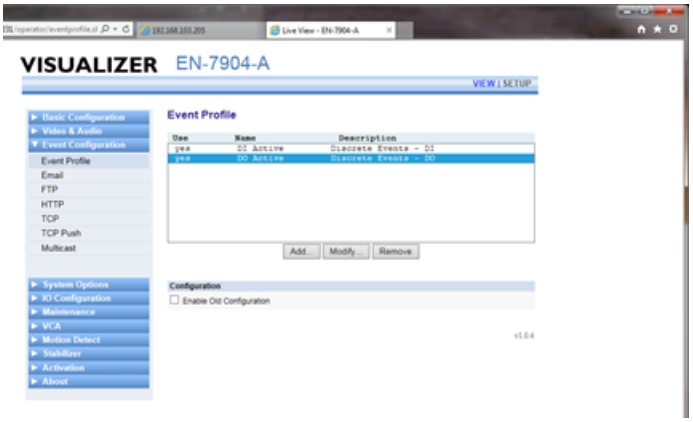
d. Select Event Configuration from the Web interface then HTTP.
e. Under HTTP Server Configuration, enter the address of your server (e.g., 192.168.103.60) and the port number (e.g., 4052)
f. Select to Enable Logon information. Fill in the user name and password of your server. NOTE: Reentering the password may be required.
g. The Request Message format depends on the device model.

For all NVC series models, enter: /camera=3?action=query&type=%event%&info=%alarm%

For all IPX/IPN series models, enter: /camera=3?action=query&type=<eventtype>&info=Alarm (where <eventtype> is di or do). The important part is the /camera=#, where # is the camera number in CV.



h. Apply the changes.
i. Select Event Profile and add a profile (or modify an existing one).
j. Select Enable Profile then, under Configuration, select DI, the Channel (e.g., DI #1) and Active status.



k. Click on the <OK> button to exit.

4. Enabling DI events for Symmetry Cameras from CompleteView. There are two main steps involved in enabling DI events: 1) Enable Discrete Inputs triggers in the On-Camera Alert configuration, and 2) Enable the Web Server HTTP interface.

a. Select the Cameras branch from the desired sever root then select the Symmetry camera of interest.
b. Select the IP tab and check the Use On-Camera Alerting checkbox then click on the <Configure Alerts...> button.
c. Enable / disable the Discrete Inputs event and select the recording level (Alarm or Motion).
d. Select the desired server root node then the Web Server tab.
e. Check the Enable Web Server (HTTP) check box.
f. Enter the same port number as in the Camera DI setup (e.g., 4502).

Symmetry ENVS Setup

The Edge Network Video Server (ENVS) is used for recording and transferring video in MPEG-4 format. Four-channel (four camera) and single-channel (single camera) versions of the ENVS are available. The ENVS has ports for two auxiliary outputs, four inputs, a PTZ controller and external (e.g. security system) controller. Local storage of video is provided by an internal 80GB or 160GB hard disk. For further details about initial hardware setup and configuration for the ENVS, consult the manufacturer's documentation. The information below is offered as a guide for integrating an ENVS with CompleteView.

ENVS Factory Reset

The ENVS may require a factory reset so it can be configured. The reset can be accomplished as follows.

NOTE: you will need the original factory assigned IP address to access the ENVS once the reset is complete.

1. Open up ENVS BOX (unscrew) and locate RED Deep switch with 4 pins.
2. Turn on ENVS. Once it has finished its boot-up and stabilized, indicated by the Diagnostic light blinking slowly…
3. Turn Red Deep switch's PIN-2 ON.
4. Press Rest button. It will restart the ENVS, and return all configuration data to default.

Once Restart is completed, turn the Red Deep switch's PIN-2 OFF in order to set new static IP address and other parameters as required.

ENVS IP Address Setup

For the purposes of ENVS integration with CV, only the DHCP, IP, and HTTP settings (highlighted in yellow) need to be configured for functionality. While other XML nodes are shown in the example below, they do not need to be modified.

DHCP Node

- enable = false (disable DHCP)

Ip Node

- address attribute = network IP address assigned to this ENVS.
- netmask attribute = network subnet mask
- gateway = the default gateway address

HTTP Node

- portNo = HTTP port number

```
<Configuration>
        <Network>
                <Dhcp enable="false"/>
                <Ip address="172.18.2.192" netmask="255.255.240.0" gateway="172.18.1.1" hostname=""
                domain="" dns=""/>
                <Http htmlInterfaceEnable="true" xmlInterfaceEnable="true" portNo="80"
                securityEnabled="true"/>
                <Rtp enable="true">
                        <Aes enableAes="false" mode="ecb" encryptionKey="" encryptionKeyLength="128"
                        iv="" ivLength="0"/>
                </Rtp>
                <Ftp directoryPath="" autoSetArchive="true">
                        <Server url="" userName="" password=""/>
                </Ftp>
                <Sntp enable="false" queryInterval="60">
                        <Server serverName=""/>
                </Sntp>
                <Snmp enable="true" trapAddress="255.255.255.255" readCommunityName=""
                writeCommunityName=""/>
        </Network>
</Configuration>
```

ENVS Pan/Tilt/Zoom

The following attributes detail the ENVS configuration file settings required for PTZ control of cameras supporting Pelco-D or Pelco-P serial protocol.

- The ptzAddress attribute under <Configuration><VideoAcquisition><Channel> should match the cameras PELCO address. Remember that you add one (1) to the camera address when using PELCO-P protocol.
- The panAndTilt, zoom, and focus attributes under <Configuration><PTZ><Channel> should reflect the capabilities of the PTZ camera attached to the ENVS. (One camera entry for each PTZ camera)
- The baud, parity, bits, stop, handshake, and physical attributes under <Configuration><Serial><Port> should reflect the serial settings required by the PTZ camera attached to the ENVS.

```
<Configuration>
        <VideoAcquisition>
                <Channel port = “1” ptzAddress=”2” . . .
                <Channel port = “2” ptzAddress=”4” . . .
                <Channel port = “3” ptzAddress=”6” . . .
                <Channel port = “4” ptzAddress=”11” . . .
        </ VideoAcquisition >
        <PTZ scriptName="Pelco (P)">
                <Channel port="1" panAndTilt="true" zoom="true" focus="true"/>
                . . . . Other channels as required
         </PTZ>
        <Serial controllerPort="1" ptzPort="2" hisecPort="0">
                <Port port="1" baud="9600" parity="none" bits="8" stop="1" handshake="none"
        physical="rs232"/>
                <Port port="2" baud="9600" parity="none" bits="8" stop="1" handshake="none"
        physical="rs422"/>
        </Serial>
</Configuration>
```

ENVS Monitor Point Events

```
<Configuration>
        <GPInput>
                <Channel enable="true" port="1" channelId="0" description="Input 1"/>
                <Channel enable="true" port="2" channelId="0" description="Input 2"/>
                <Channel enable="true" port="3" channelId="0" description="Input 3"/>
                <Channel enable="true" port="4" channelId="0" description="Input 4"/>
        </GPInput>
        <Events>
                <Server url="http://172.18.1.15:4502/CvHttp" userName="YWRtaW4=" password=""/>
                 <Transaction txnType="MonitorPointAlarm" reportEvent="true" runScript="false"
                functionName=""/>
                <Transaction txnType="MonitorPointNormal" reportEvent="true" runScript="false"
                functionName=""/>
        </Events>
</Configuration>
```

- The <Events><Server> url attribute is “http://[vms server ip]:[port]/VMSHttp”. (e.g., http://172.18.1.15:4502/VMSHttp)
- The <Events><Server> username attribute is the Base64 encode of the VMS server username. (e.g., the password admin Base64 encode value is ‘YWRtaW4=’)
- The <Events><Server> password attribute is the Base64 encode of the VMS server password.

VideoIQ Analytics Camera Configuration

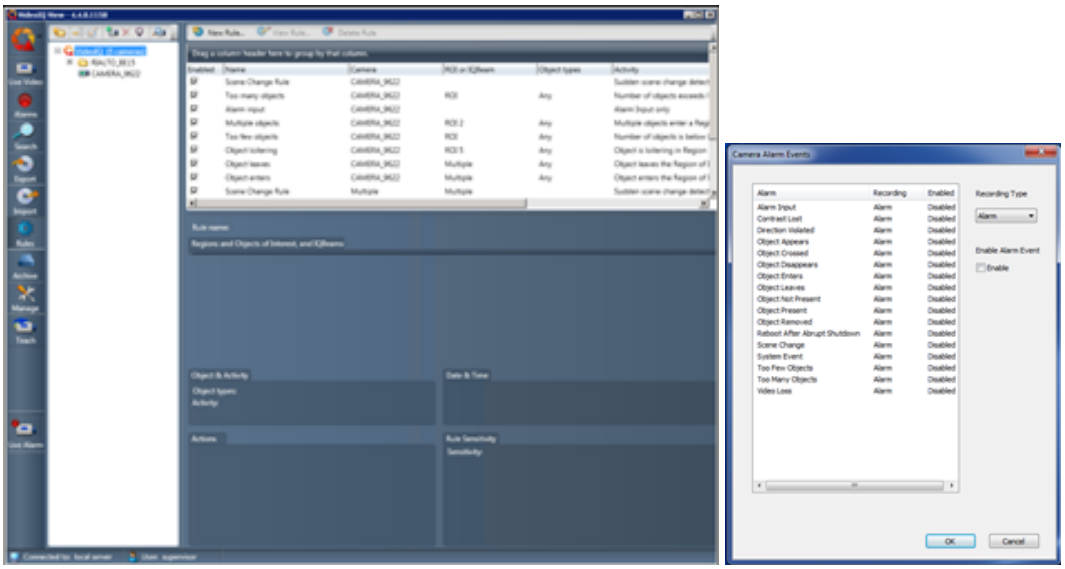
The VideoIQ camera can be configured to perform video analytics using the VideoIQ View software.

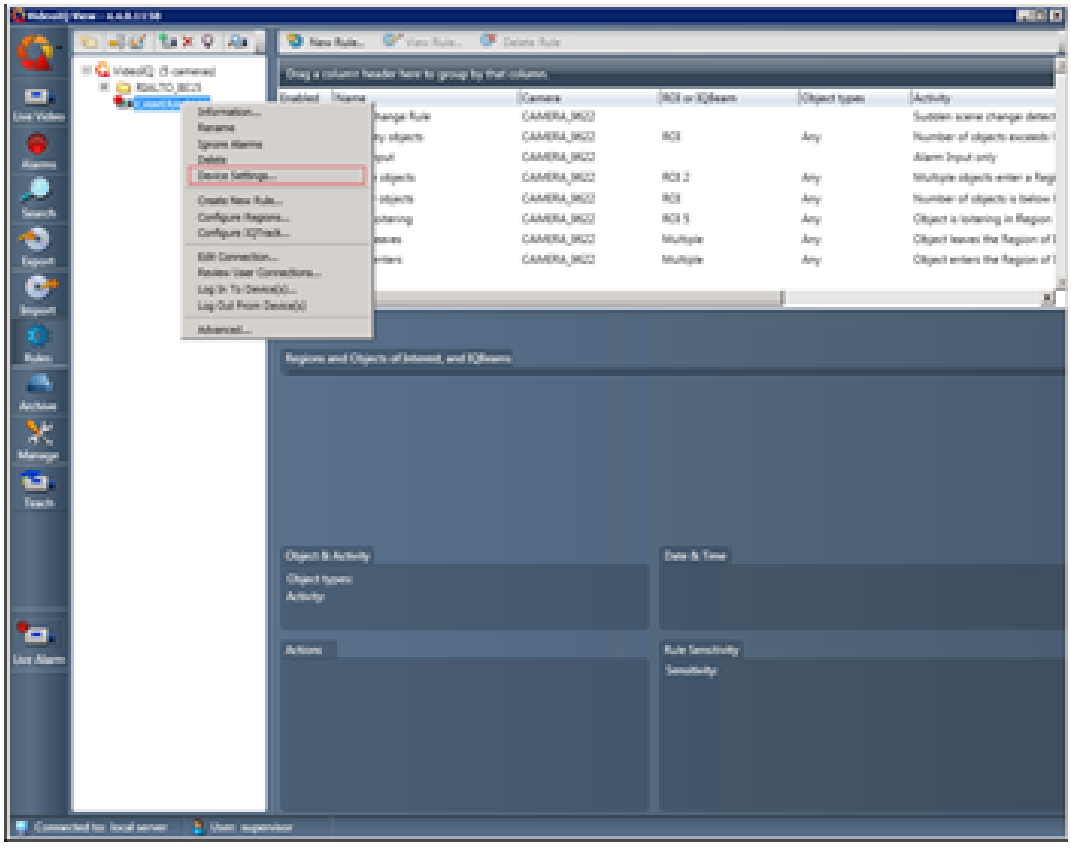
VideoIQ Analytics Configuration

1. Install the VideoIQ View software from the VideoIQ installation DVD as described in the VideoIQ user guide.
2. Add cameras as described in the VideoIQ user guide.
3. Configure rules to perform video analytics as described in the VideoIQ user guide.

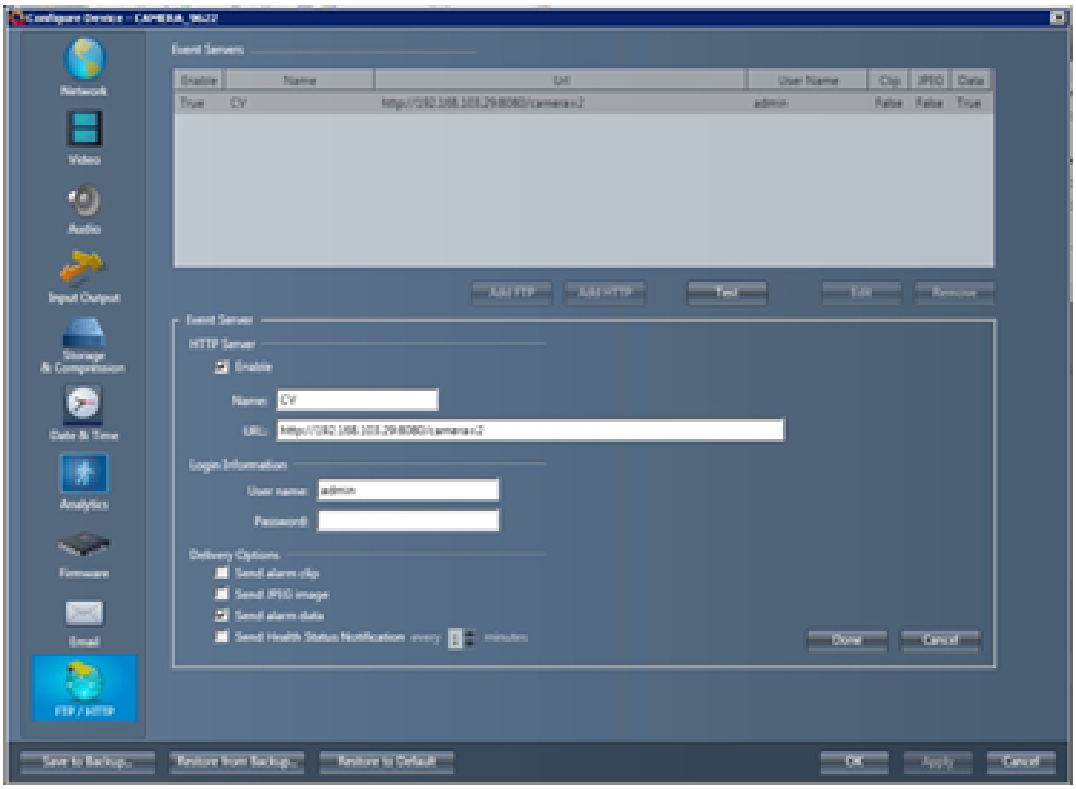
VideoIQ Integration With CompleteView

1. Enable the alarms in the CV Camera Alarm Events dialog that correspond to the configured VideoIQ analytics rules. Once the rules are configured, event notifications can be received for the same by configuring a HTTP server in the camera.





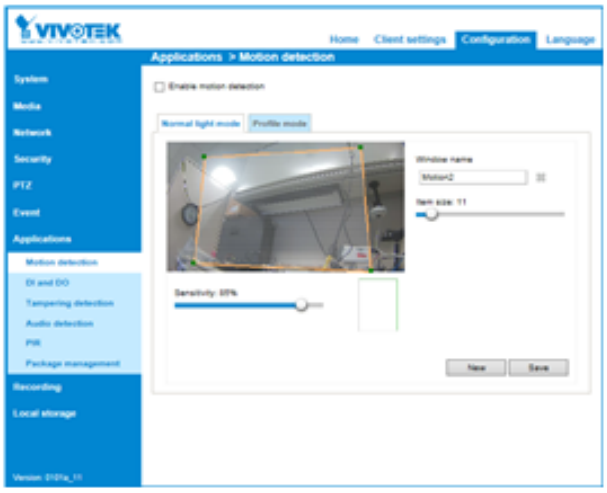
2. Go to the device settings of the camera as shown above
3. Configure HTTP server by selecting FTP/HTTP from the left menu

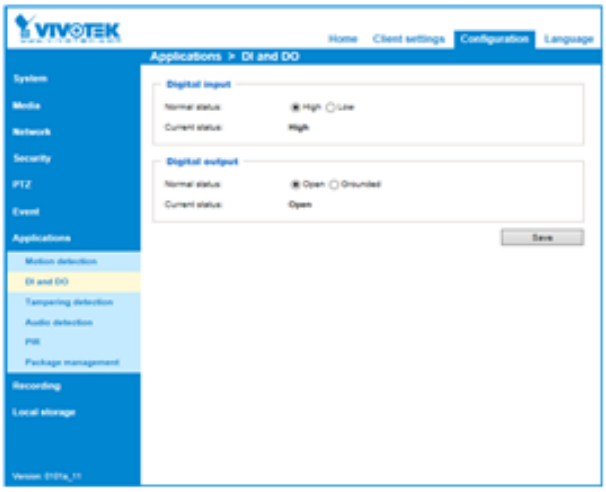


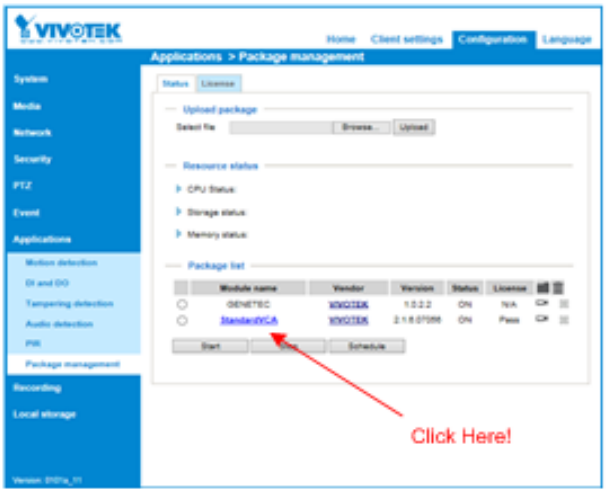
4. Click “Add HTTP”. Check the “Enable” check box
5. In the URL edit box, enter the URL to CompleteView’s HTTP web server as http://[CV server address]:[CV Web Server port number]/ camera=[CV camera number] as shown above
6. Ensure that web server is enabled in CompleteView Management Server
7. Provide CV server username and password for login information
8. Check the “send alarm data” check box and click “Done”
9. Once the above steps are completed, CV server will now start receiving alarm notifications every time an alarm/event is triggered. Ensure that alarm/motion recording is added to the schedule.

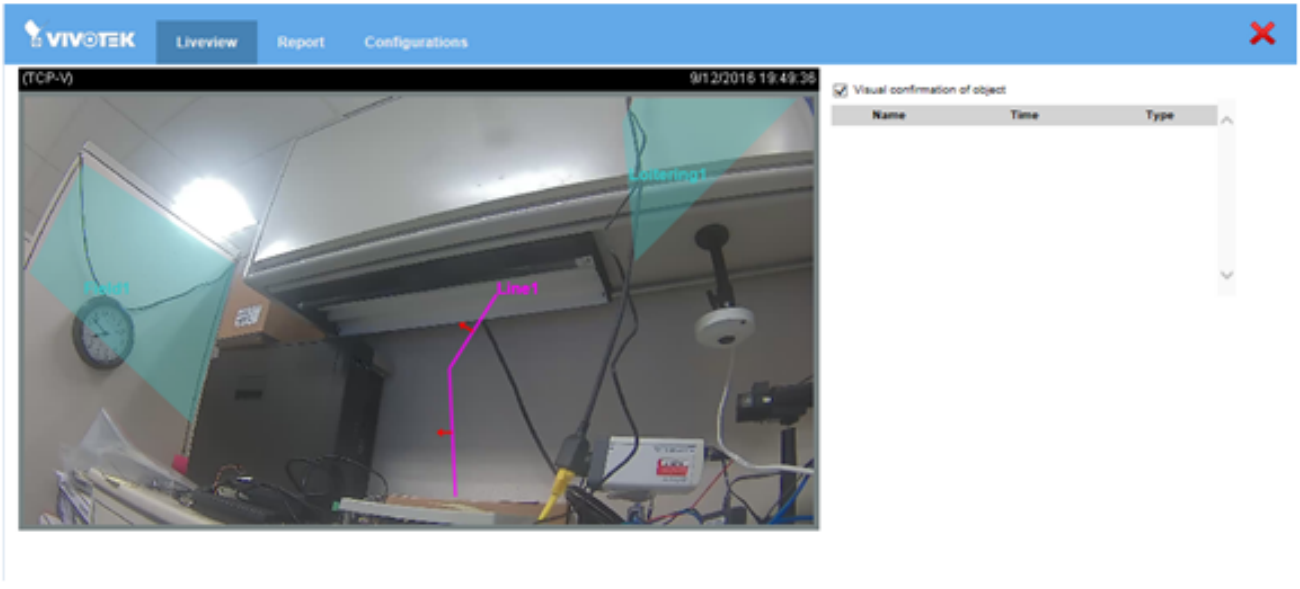
Vivotek Events Configuration

Use the VIVOTEK Web interface to configure the camera events1 (Audio detection & PIR not supported) under Configuration >> Applications.









The CompleteView VMS Camera Alarm Events dialog displays the supported VIVOTEK events as configured in the camera and allows the user to selectively enable and disable event reporting and the recording level at which the event is recorded.

NOTE: The Field Detect, Line Cross, and Loiter events are only supported as part of the VIVOTEK Standard VCA application, which must be obtained as a separate, loadable software component from VIVOTEK. See the VIVOTEK camera documentation for further details on obtaining and installing the VCA application package.

Digital Certificate Management and More

CompleteView contains facilities for secure web-based communications via HTTPS. To be used properly, these security facilities require local, per site management of digital certificates. This document presents a practical administrative guide for such. Note: More experienced administrators may find much (perhaps most) of this guide unnecessary.

Prerequisites

It is assumed that the reader is familiar with the basic concepts behind public key cryptography and digital certificates. For instance, this guide uses several important terms without explanation:

- Public and private keys
- Certificate authority (CA)
- Chain of trust

Here are some links that might serve for review and/or remedial learning:

https://developer.mozilla.org/en-US/docs/Glossary/Public-key_cryptography

This link provides an overview of public key cryptography.

http://www.fir3net.com/Concepts-and-Terminology/pki-chain-of-trust.html

This page is somewhat brief, but nicely describes the chain of trust concept.

General Troubleshooting Guidelines

If something does not work the way you expect, make sure that the corresponding functionality works with the non-secure (HTTP) web server, where applicable.

If you get stuck, always consider clearing the browser's cache, and/or restarting the browser. In particular, web browsers seem to have difficulty when the certificate used by a web server changes; in this case restarting the web browser is often necessary.

Additional Resources

Visit the Salient website, www.salientsys.com, for additional support and CompleteView training:

- Software downloads (https://www.salientsys.com/support/downloads/) – For current and legacy software.
- Manuals & Documentation (https://www.salientsys.com/support/salient-documentation/) – Includes all relevant manuals.
- Online Tech Support (https://www.salientsys.com/support/technical-support/) – Get quick access to online tech support modules that cover the most frequently asked product questions, such as "Adding IP Camera Licenses."
- Training (https://www.salientsys.com/support/training-overview/) – we offer both online and classroom training.
    - CompleteView™ Remote Certification – Instructor directed 2-day course, that the student accesses through their own computer, designed to provide you with certification on CompleteView video management software. Certification is valid for two years.
    - Please visit the Salient website to see the training calendar, agenda, and registration. Contact training@salientsys.com for questions.

Salient Systems
4616 W. Howard Ln.
Building 1, Suite 100
Austin, TX 78728
512.617.4800
512.617.4801 Fax
www.salientsys.com