Senstar Symphony User Guide

Version 8.12

Table of Contents

The Senstar Symphony Common Operating Platform is an intelligent moduler platform for video surveillance, security management, and access control.

Getting Started

The online help includes Getting Started pages for users based on their typical role.

My Role	Common Tasks
Operator	View live video, respond to alarms, search recorded footage, run reports
Administrator	Set up the Server, add cameras and devices, configure rules, manage users, plan backups

Contents

Section	Description
Getting Started	Product overview and how the pieces fit together.
Server	Configure a Senstar Symphony deployment: devices, security, rules, sites, and settings.
Windows Client	Use the Windows Client to monitor cameras, manage video, generate reports, and respond to alarms.
Web Client	Similar functionality to the Windows Client, in a browser.
Player	Offline application for viewing exported video files.
Appendix	Release notes, network port usage, glossary, and legal information.

Getting Started

Senstar Symphony provides a Common Operating Platform for intelligent video surveillance, video analytics, and security management.

Senstar Symphony installs on standard IT hardware, supports IP cameras from hundreds of manufacturers, provides a feature-rich, easy-to-use interface, and incorporates IT friendly features to make administration simple. Senstar Symphony can reside on a single computer or multiple computers in a server farm.

Senstar Symphony comprises the following components:

- **Server** — Configure Senstar Symphony through the Server configuration interface. The Server records video, runs the rule engine, and stores alarm and event history.
- **Windows Client** — A Windows desktop application that interacts with the cameras connected to the Server. Use it to view live video, play back recordings, respond to alarms, and run reports.
- **Web Client** — Provides functionality similar to the Windows Client, but in a web browser and without requiring installed software.
- **Player** — Plays video files that you export from the Windows Client.

Common Roles

My Role	Common Tasks
Operator	View live video, respond to alarms, search recorded footage, run reports
Administrator	Set up the Server, add cameras and devices, configure rules, manage users, plan backups

Operators

Operators use the Windows Client (and, optionally, the Web Client) to watch live and recorded video, respond to alarms, investigate incidents, and produce reports. Use this page to find the right procedure quickly; use User Interface if you want to learn about specific control or function.

Some procedures require permissions that your site administrator grants through security profiles. If a menu or button is not visible, your account may not have the relevant permission — ask your administrator.

The Basics

- Connect to a Server — Sign in to the Windows Client.
- User Interface — Learn what each part of the screen does.
- Load a camera view — Restore a saved layout of cameras.
- Alarm Console — Open the console for the current shift's alarm handling.
- Change your password — If site policy requires a periodic change.
- Disconnect from a server — Sign out of the application.

Monitoring Cameras and Sensors

- View a camera — Open a live video stream in a view panel.
- View a map — Watch a site map with device and alarm indicators.
- Carousels — Cycle through a set of cameras automatically.
- PTZ controls — Pan, tilt, and zoom PTZ cameras.
- Display a camera timeline — See when recorded activity and events occurred.

Responding to Alarms

See Managing Alarms for the end-to-end workflow.

- View alarms — View alarms waiting for response.
- Acknowledge an alarm — Take responsibility for an alarm and classify it (real, real actionable, false).
- Share an alarm — Escalate by forwarding an alarm to another operator.
- Retrieve alarms — Review older alarms from the for review.

Investigating an Incident

- View video by date — Jump to recorded video for a specific time.
- Search — Find clips by object class (person, vehicle) and behaviour (moving, loitering).
- Instant replay — Rewind recent live video without leaving the view panel.
- Bookmarks — Mark moments in recorded video so you or others can find them again.
- Protect footage — Prevent a section of recorded video from being deleted by retention settings.
- Visual tracking — Follow a subject across cameras using pre-configured links.
- Export video — Save a video to a file for sharing with others.

Generating Reports

See Reports and Logs for the full set of reports.

- Alarm report
- Alarm statistics report
- Face recognition report
- Heat map image report
- Object counts report
- View events (raw event log).

Customise the Windows Client

- Save a camera view — Preserve the current layout
- Customize settings — Adjust what appears in the toolbar and status areas.
- Display settings — Tune how video is rendered.
- Sound settings — Control alarm audio and notification tones.

- Regional settings — Set date, time, and language preferences.

Administrators

Administrators configure the Server: they add devices, define who can see and do what, build the rules that turn events into alarms and actions, and keep the system healthy over time. The pages below are grouped by the journey a new administrator actually takes — plan the deployment, set it up, then run it — rather than by the layout of the configuration interface. For a page-by-page view of the configuration interface, see Server.

Plan the deployment

Before adding anything to the system, decide:

- **Site layout** — how many cameras, where they sit, what they must see, and what events matter. This drives rule and analytic decisions later.
- **Storage** — video retention policy (days of footage to keep) drives disk sizing. See video storage for a server farm.
- **User roles** — which people will operate vs. administer the system, and whether you need view-only, full-operator, investigator, or site-administrator roles. See security profiles.
- **Network** — network ports that must be open between Server, clients, and cameras.
- **Backups** — where backups are stored and how they fit into your disaster recovery plan. See configure backups.

First-time setup

The first-time path for a fresh Server:

Step	Page
Sign in to the configuration interface	Login
Apply your licence	Licenses
Add the first camera and verify video	Add a camera
Define retention for the site	Video storage for a server farm
Add users and groups	Add a user · Add a group
Create security profiles for each role	Add a security profile
Build your first rule (event + action set + schedule)	Rules · Create a rule
Configure backups	Configure backups

Device management

- Devices overview — what the configuration interface calls "devices" and how the subtypes relate.
- Cameras — add, import, export, and edit cameras.
- Video analytics — turn on per-camera analytics such as motion detection, people tracking, and face recognition.

- Hardware · Integrations · Access devices — non-camera hardware.
- Templates — apply a saved configuration to many cameras at once.
- Device tree — organise how devices appear in the Windows Client.

Security and access control

- Users — add, copy, group, and disable users.
- Groups — container for users; permissions attach to groups, not individual users.
- Security profiles — reusable permission bundles (see role templates in user permissions).
- Active Directory — integrate with an existing directory rather than maintaining separate accounts.
- Security authentication — how credentials are stored and checked.
- Logins — inspect active and historical sessions.

Rules engine

Rules turn events into actions. A rule has three parts: an event (the trigger), an action set (what happens), and a schedule (when the rule is active). See Rules for the model and create a rule for the procedure.

Reports, monitoring, and maintenance

- Check CPU usage — spot overloaded servers.
- Manage services — control the background services.
- Cloud services — health monitoring, remote management, and cloud backup.
- Maintenance — automatic updates, server update checks, and client update policy.
- Protected footage — review the video that users have protected from deletion, and unprotect footage that is no longer needed.
- Backup and restore — scheduled backups and recovery paths.

Concepts

Foundation topics every administrator should read once:

- Rules, events, action sets, and schedules
- Permissions model: users → groups → profiles
- Video analytics pipeline
- Backup and restore

Server

The Server is the core of a Senstar Symphony deployment. It records video from connected cameras, runs the rules engine that turns events into alarms and actions, stores the alarm and event history, and enforces the permission model that controls who can see and do what.

Administrators configure the Server using the Server configuration interface and the Senstar Symphony setup wizard. You can open the configuration interface directly in a browser or from the Windows Client. The setup wizard runs from the start menu on the computer that hosts the Server.

For a task-oriented overview of Server administration, see Administrators.

Getting started

If you are setting up a new Server, work through these pages in order:

Step	Topic
Sign in to the configuration interface	Login
Apply your licence	Licenses
Add your first camera	Add a Camera
Set video storage and retention for the site	Video Storage for a Server Farm
Add users and groups	Add a User
Define security profiles for each role	Security Profiles
Build your first rule	Create a Rule
Configure backups	Configure Backups

Common tasks

Action	Topic
Add a camera	Add a Camera
Turn on a video analytic for a camera	Video Analytics
Add a perimeter intrusion detection sensor	Senstar Network Manager
Add an integration (access control, third-party sensors)	Add Integration Hardware
Create a rule (event + action set + schedule)	Create a Rule
Add a user and assign a security profile	Add a User
Schedule configuration backups	Configure Backups
Check server health	Check CPU Usage

Reference sections

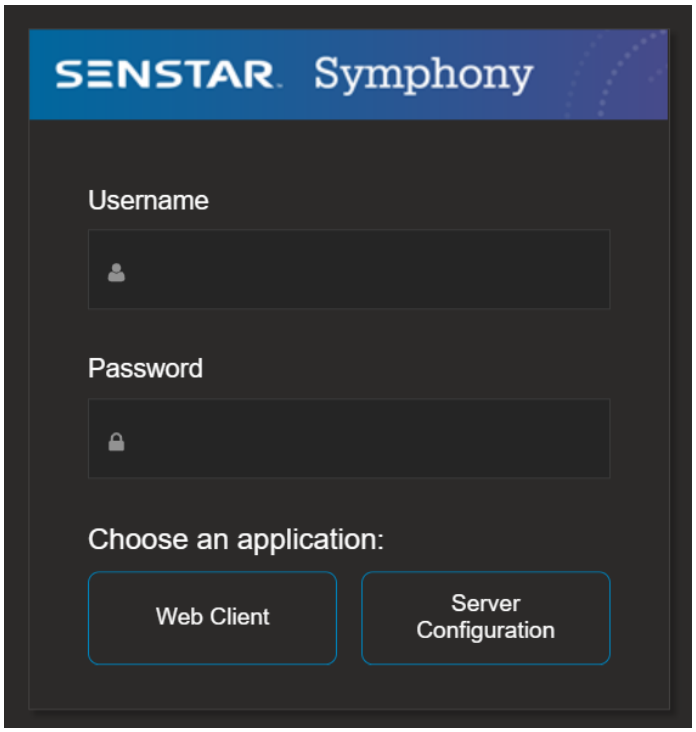
- Devices — cameras, hardware, integrations, access devices, templates.

- Security — users, groups, security profiles, logins, authentication.
- Rules — events, action sets, schedules.
- Licenses
- Settings — servers, general, cloud services, aggregates, maintenance, backup and restore, maps.
- Server management — CPU usage, services.

Login

You can open the Server configuration interface in several ways:

- Web browser: Use IP address of the server.
- Windows Client: Click the Server Configuration button in the toolbar and select Server Configuration.
- Web client: Click the Server Configuration button on its login screen or on the toolbar (after login).



Web Client Login

1. In a browser, navigate to the IP address of the Web Client.
2. Type your username and password.
3. Click Server Configuration.

Server Web Login

1. In a browser, navigate to the IP address of your Server.
2. Type your username and password.

3. Select the user interface language.
4. Click Login.

Devices

Senstar Symphony supports cameras, intrusion detection sensors, digital input/output devices, and access control devices. Configure each device type from the Server configuration interface; most admins start with cameras, then add the sensors, I/O, and access hardware that the site requires.

Section	Description
Cameras	Import cameras from major manufacturers.
Browsers	Configure web pages that appear in view panels alongside video streams and site maps.
Templates	Apply a saved collection of configuration settings to cameras.
Hardware	Configure sensors and I/O devices to trigger alarms and other events.
Integrations	Connect third-party security systems (access control, perimeter sensors, and similar) to the Server.
Access Devices	Manage door controllers and other access control devices.
Device Tree	Organize how cameras and devices appear in the Windows Client.
Carousels	Loop through multiple camera streams in a view panel and display video for a set time.

Cameras

The Server is compatible with analog and IP cameras from a wide variety of manufacturers.

The Server supports the following standards:

- ONVIF Profile S
- ONVIF Profile G
- ONVIF Profile T
- Real Time Streaming Protocol (RTSP)

The Server supports the most recent official firmware for cameras, as provided by camera manufacturers. For analog cameras, you connect the camera to the Server using a video encoder. For PTZ cameras, you need to configure the control port for the camera and select it in the Server configuration interface.

The Cameras page in the Server configuration interface lists the cameras that are connected to the Server. You can filter the list by typing or selecting values in the header and you can sort the list by clicking a column title.

Add a Camera

You can add a camera to the Server manually, automatically, or as a mobile camera.

Add a Camera Manually

You can manually add cameras to the Server in the Server configuration interface.

To add a camera using RTSP, add the RTSP URL in the Address field and select RTSP URL in the Driver list.

1. In the Server configuration interface, click Devices > Cameras.
2. Click Add Cameras.
3. Click Add Camera Manually.
4. In the Address field, type the IP address of the camera.
5. In the Driver list, select the manufacturer of the camera.
6. Type a the username and password for the camera.
7. Click Connect or Add without connecting.

Add a Camera Automatically

The Server can automatically detect cameras on the same network.

1. In the Server configuration interface, click Devices > Cameras.
2. Click Add Cameras.
3. Click Begin Automatic Discovery.
4. In the Credentials Required window, type the user name and password for the camera, and click Connect.
5. Select the camera and click Next.
6. Type a name for the camera in the Camera Name field or use the default name.
7. Select a camera template for the camera in the Template list.
8. In the Group list, select the device group to which the camera belongs.
9. In the Add-On list, select the video analytic to use on the camera.
10. Click Add 1 Selected Camera.

After the add the camera, the

Server configuration interface

opens the edit camera page. For more information, see the Edit a camera topic.

Add an Analog Camera

You can add a pure analog camera to the Server when the camera is connected to a video encoder or capture card. The Server treats the encoder as the network device and addresses each analog channel as a separate camera.

Before you begin:

- Connect the analog camera to a channel on a supported video encoder or capture card.
- Note the IP address of the encoder, the credentials for the encoder, and the channel number that the camera uses.
    1. In the Server configuration interface, click Devices > Cameras.
    2. Click Add Cameras.
    3. Click Add Camera Manually.

4. In the Address field, type the IP address of the video encoder.
5. In the Driver list, select the manufacturer of the video encoder.
6. Type the username and password for the encoder.
7. Click Connect.
8. Select the encoder channel that the analog camera uses.
9. In the Camera Name field, type a name for the analog camera.
10. In the Template list, select a camera template.
11. In the Group list, select the device group.
12. Click Add 1 Selected Camera.

After you add the camera, configure the PTZ protocol on the Edit Camera page if the analog camera is a PTZ camera. For more information, see the Edit a Camera topic.

Add a Mobile Camera

You can add the camera on a mobile device to the Server when you use the Senstar Symphony Mobile Bridge. The mobile camera must be on for the Server to receive video.

To use a mobile camera, you must open port 49900 on the firewall.

1. In the Server configuration interface, click Devices > Cameras.
2. Click Add Cameras.
3. Click Add Camera Manually.
4. In the Address field, type `0.0.0.0`.
5. In the Driver field, select Mobile.
6. In the User Name and Password fields, type the credentials for the Senstar Symphony Mobile Bridge.
7. Click Connect.
8. In the Camera Name field, type a name for the mobile camera.
9. In the Template field, select a template for the mobile camera.
10. In the Group field, select the group for the mobile camera.
11. In the Add-Ons field, select None.

Senstar Symphony video analytics do not support mobile cameras.

1. In the Server field, select the Server for the mobile camera.
2. Click Add 1 Selected Camera.
3. Configure the settings for the mobile camera.

The resolution on the mobile device must match the resolution set in the Server configuration interface to transmit video.

1. Click Save.

Edit a Camera

You can modify camera settings in the Server configuration interface.

After you add a camera to the Server (either manually or automatically), you edit the camera to configure the advanced options for the camera.

Some settings are unavailable if you apply a template to the camera. You must change the settings in the camera template.

1. In the Server configuration interface, click Devices > Cameras.
2. Select a camera and click Edit.
3. To change the name of the camera, type a new name in the Name field.
4. To change the template applied to the camera, select the template in the Template list.
5. Type a description for the camera in the Description field.
6. Type the text that appears as a decoration over the video in the Code field.
7. To change the RTSP port for an ONVIF camera, type the new port in the RTSP Port field.
8. To change the server that manages the camera, select the new server in the Managed By list.
9. To change how the camera responds in the case of a server failure, select or clear the Failover enabled box.
10. To configure the camera to support direct connections, select Support Direct Connect.
11. If the camera is connected using a video encoder, select whether the camera is a fixed camera or a PTZ camera.
12. If the camera is a PTZ camera connected using a video encoder, complete the following tasks:
    a. In the Max Locked Minutes field, set the maximum time that the camera can be locked.
    b. In the Auto-PTZ Priority field, set the priority that a user must exceed to control the PTZ when the Server attempts to move the PTZ camera for automatic tracking.
    c. In the Force-PTZ Priority field, set the priority that a user must exceed to control the PTZ when the Server attempts to force the PTZ camera to a location because of a rule.
    d. In the Type list, select the PTZ communication protocol for camera.
    e. In the Camera Address field, select the address of the camera. The default camera address is 1.
    f. In the Control Port list, select the communication port that the encoder uses for the camera. You configure the communication port on the video encoder when you connect the PTZ camera to the video encoder.
13. Click Save.

Add a Video Stream

You can add a video stream to a camera that the Server can use to display video at a reduced resource cost.

Some settings are unavailable if you apply a template to the camera. You must change the settings in the camera template.

1. In the Server configuration interface, click Devices > Cameras.
2. Select a camera and click Edit.
3. In the Video section, click Add Stream.
4. In the Resolution field, select the resolution for the stream.
5. In the FPS field, select the frames per second for the stream.
6. In the Video Codec field, select the video codec for the stream.
7. In the Transport field, select how the camera transmits video from the stream to the Server.
8. In the Bitrate field, select the bitrate for the stream.
9. In the Key Frame Interval list, select the frequency of frames in the video that the Server considers to be key frames.
10. In the Recording Mode list, select when the Server records video from the stream.
11. In the Schedule list, select when the recording mode is active for the stream.
12. Click Save.

Add a Video Analytic Stream

You can add a stream to a camera that the Server can use for video analytic processing.

To add a

video analytic

stream, you must first configure a

video analytic

for the camera.

The Server sets the resolution, frame rate, video codec, transport, bitrate, and key frame interval automatically.

Some settings are unavailable if you apply a template to the camera. You must change the settings in the camera template.

1. In the Server configuration interface, click Devices > Cameras.
2. Select a camera and click Edit.
3. In the Video section, click Add Analytics Stream.
4. In the Recording Mode list, select when the Server records video from the stream.
5. In the Schedule list, select when the recording mode is active for the stream.
6. Click Save.

Configure a Privacy Mask

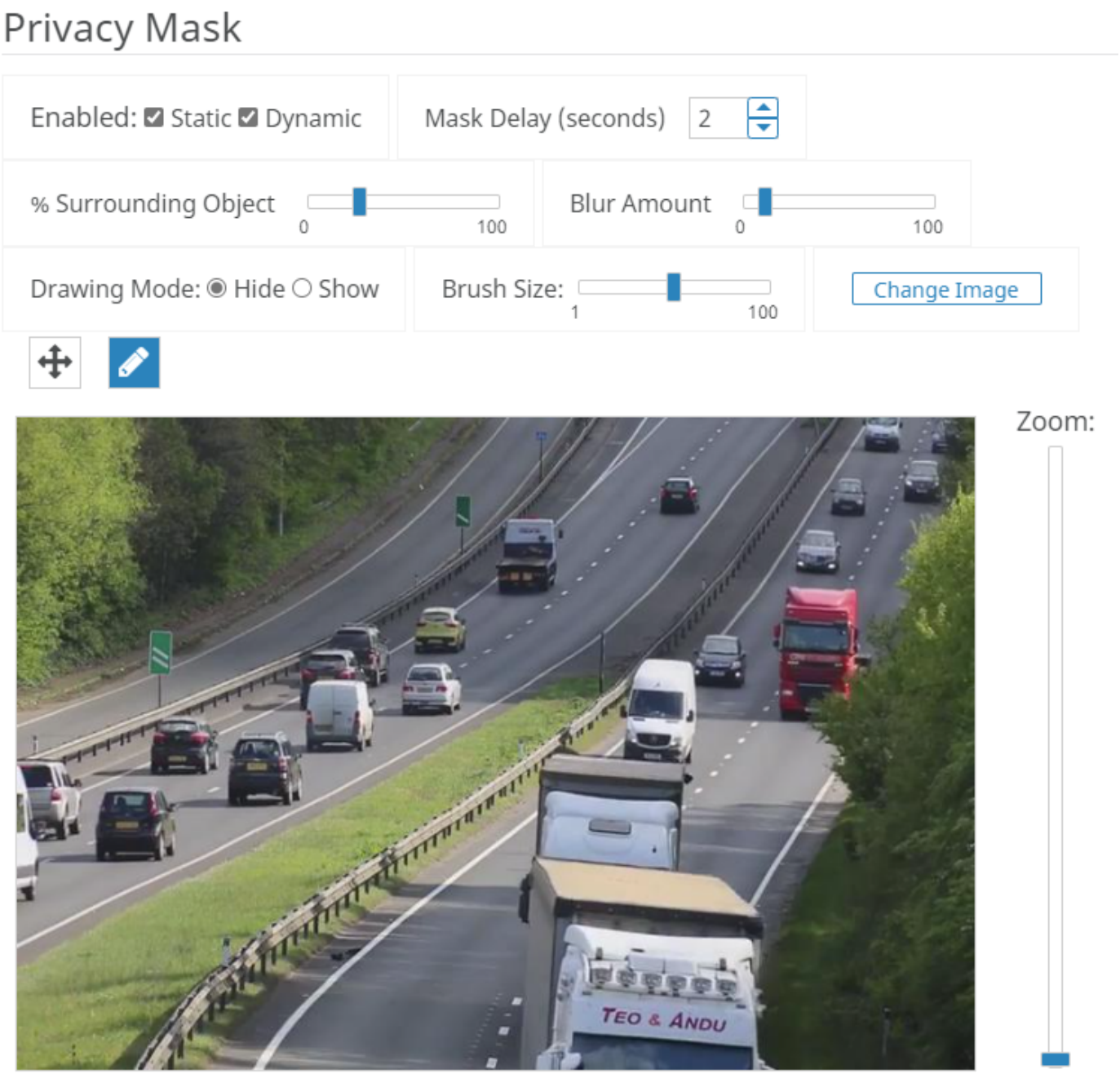
You can use a privacy mask to obscure areas in the camera view. A privacy mask obscures video (live and historical) so that a viewer cannot identify objects but allows the Server to analyze the video for alarms.

A static privacy mask obscures a defined area of the camera view. A dynamic privacy mask obscures

tracked objects.

Privacy masks for PTZ cameras also include a location list and a slider that allows you to zoom in on an image.

+



1. In the Server configuration interface, click Devices > Cameras.
2. Select a camera and click Edit.
3. In the Privacy Mask section, perform the following tasks:
    a. In the Enabled list, select whether the privacy is static, dynamic, or both.

b. In the Mask Delay field, set how long (in seconds) the Server remembers the position of tracked objects and continues to obscure the previous location of a tracked object. This setting only applies to dynamic privacy masks.

c. On the % Surrounding Object slider, select the area beyond a tracked object to which the Server applies the privacy mask. This setting only applies to dynamic privacy masks.

d. On the Blur Amount slider, select to what degree the Server obscures the camera view.

e. In the Drawing Mode list, select whether the paintbrush marks areas to hide or show. This setting only applies to static privacy masks.

f. On the Brush Size slider, select the size of the paintbrush. This setting only applies to static privacy masks.

g. To change the privacy mask image, click Change Image and select the image. This setting only applies to static privacy masks.

h. On the privacy mask image, use the paintbrush to define the areas to either hide or show. This setting only applies to static privacy masks.

4. Click Save.

Configure Digital Input and Output

You can configure how digital inputs and outputs appear in the Windows Client interface.

1. In the Server configuration interface, click Devices > Cameras.
2. Select a camera and click Edit.
3. In the Digital I/O section, perform the following tasks:
   a. To enable the input or output, select In Use.
   b. To set the name that appears in the Windows Client interface, type a name in the Output Name or Input Name field.
   c. In the Activate field, type the text that appears in the Windows Client interface when clicking on the input or output activates it.
   d. In the Deactivate field, type the text that appears in the Windows Client interface when clicking on the input or output deactivates it.
   e. In the Auto Deactivate field, set the time (in milliseconds) after which the input or output automatically deactivates.
   f. In the Camera Shortcut list, select the camera on which the input or output controls appear. Buttons that allow you to control the input or output appear in the camera view panel for the camera that you select.
4. Click Save.

Add a Camera to a Device Group

You can add a camera to a device group in the device tree.

Before you begin, make sure that you have created device groups for the device tree.

The camera appears as part of the group in the device tree in the Windows Client interface.

1. In the Server configuration interface, click Devices > Cameras.

2. Select a camera and click Edit.
3. In the Groups section, select a groups or groups to which you want to add the camera.
4. Click Save.

Configure Video Storage for a Camera

What it is

Every camera writes its recorded video to a storage path and keeps that video for a retention period. Senstar Symphony resolves these two values at three levels, with a clear precedence:

1. **Camera** (this page) — the per-camera override.
2. **Server** — the default for every camera on this Server.
3. **Server farm** — the default across all Server instances in the farm.

The **camera** setting takes precedence over the server setting, which takes precedence over the farm setting. Set values at the highest level that can be shared and override only where a camera needs something different.

When you'd use it

- A specific camera needs a longer retention window than the site default (for example, a sensitive entry point that must retain 90 days while most cameras retain 30).
- A camera must write to a different volume because the default is full, slow, or reserved for another tier of storage.
- A camera's recorded video must not be stored alongside other cameras for compliance reasons.

If every camera needs the same setting, change the server- or farm-level default instead of editing each camera.

Prerequisites

- Permission to edit camera settings.
- The camera is already added. See Add a Camera.
- If you are using a custom path: the path exists, is writable by the Server service account, and has enough free space for the retention window you plan to configure.

About storage paths

Storage paths can point to a local disk, an attached volume, or a mounted network share. A valid path:

- Exists before you save the setting — the Server does not create the directory.
- Is writable by the service account that runs the Server.
- Has enough free space for the retention window. A rough calculation: daily bitrate × hours recorded × retention days. When the Server runs out of space on a path, it begins deleting the oldest video from that path, regardless of the retention setting.

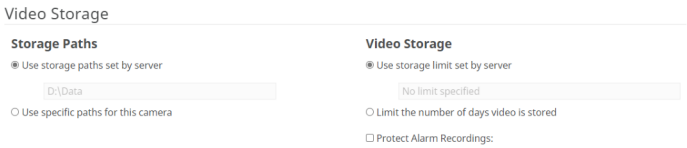
About retention

Retention sets the maximum age of recorded video. The Server deletes video older than the retention window as part of routine housekeeping. Two exceptions:

- **Disk pressure** — if a storage path is full, video is deleted from oldest to newest even before the retention window expires.

- **Alarm protection** — video associated with an alarm can be kept longer than the general retention (see **Protect Alarm Recordings** below).

Procedure



1. In the Server configuration interface, click **Devices** > **Cameras**.
2. Select a camera and click **Edit**.
3. In the **Storage Paths** section, choose one:
   - **Use storage paths set by server** — inherit from the server- or farm-level setting.
   - **Use specific paths for this camera** — type the override path.
4. In the **Video Storage** section, choose one:
   - **Use storage limit set by server** — inherit the retention policy.
   - **Limit the number of days video is stored** — set a per-camera retention window in days.
5. (Optional) To retain alarm-associated video longer than the general retention, do the following in **Protect Alarm Recordings**:
   a. Select **Protect Alarm Recordings**.
   b. In **Days**, set how long (in days) the Server keeps alarm-associated video.
   c. In **Pre Alarm**, set how many seconds of video **before** the alarm trigger to include.
   d. In **Post Alarm**, set how many seconds of video **after** the alarm trigger to include.
6. Click **Save**.

Related tasks

- Configure Video Storage for a Server
- Configure Video Storage for a Server Farm
- Edit a Camera

Add an Auxiliary Command

You can add auxiliary commands to PTZ cameras or video encoders that you add to the Server.

Auxiliary commands are custom commands the you can add to PTZ cameras and encoders to use additional functionality in the Windows Client interface.

1. In the Server configuration interface, click Devices > Cameras.
2. Select a camera and click Edit.
3. In the Auxiliary section, perform the following tasks:
   a. Select Enable auxiliary commands.
   b. Click Add.

c. In the Label field, type a name for the command.

d. In the Command field, type the custom command.

e. In the Method field, select whether the command is a GET or PUT command.

4. Click Save.

To remove an auxiliary command, click the X beside the command.

Add an Overlay Command

You can add the output of an I/O device to a camera as a overlay command. When you view the camera in the Windows Client interface, the command appears as a button in the camera view that, when clicked, activates the output of the I/O device.

After you add an overlay command to a camera. the command appears in the Windows Client interface as it appears in the Server configuration interface (including aliases). You can add multiple overlay commands to a camera.

1. In the Server configuration interface, click Devices > Cameras.
2. Select a camera and click Edit.
3. In the Overlay Commands section, select the hardware device that you want to command.
4. In the Choose a command list, select what the command does (e.g., Activate, Deactivate, Toggle State, etc.).
5. Click Save.

Configure Camera Failover

You can choose, on a per-camera basis, whether the Server moves the camera to a redundant Server during a failover event.

Server-level redundancy determines which Server takes over when a primary Server stops responding. Camera-level failover determines whether an individual camera participates in that move. By default, every camera fails over with its server. You might clear the failover setting for cameras that are not critical, that have limited bandwidth, or whose video is not licensed on the redundant Server.

Before you begin, configure server redundancy. For more information, see the Server Redundancy topic.

1. In the Server configuration interface, click Devices > Cameras.
2. Select the camera and click Edit.
3. To include the camera in failover, select the Failover enabled box.
4. To exclude the camera from failover, clear the Failover enabled box.
5. Click Save.

A camera that is excluded from failover is unavailable while its primary Server is offline. The Server resumes processing the camera when the primary Server returns to service.

Import Cameras

You can import cameras from a CSV file.

You can create a CSV file of cameras by either exporting a list or cameras or by creating a blank import file to use as a template.

1. In the Server configuration interface, click Devices > Cameras.
2. Click Add Cameras.
3. Click Import Cameras From File.
4. Navigate to the camera list file and click Open.

Find a Camera

To quickly find a specific camera, use filters and sorting.

Filter

You can filter the camera list using the following filters:

- camera ID (ID)
- camera name (Name)
- Server to which the camera connects (Server)
- camera type (Type)
- IP address of the camera (IP Address)
- camera brand (Brand)
- camera model (Model)
- template applied to the camera (Template)
- camera resolution (Resolution)
- camera frame rate (FPS)
- groups to which the camera belongs (Groups)
- video analytic active on the camera (Add-on)
    1. In the Server configuration interface, click Devices > Cameras.
    2. Click the magnifying glass to make the filter text fields visible.
    3. Define the filter criteria.
    4. Click Apply filter.

Sort

You can sort the list of cameras by clicking the column name. Clicking the column name toggles between ascending and descending order.

Clear

To reset the filter and restore the list of cameras, click Clear Filter.

Export Cameras

You can export the camera list from the Server to a CSV file.

1. In the Server configuration interface, click Devices > Cameras.

2. Click Export.

You can use the CSV file to import the cameras to another Server.

Create a Blank Import File

You can create a blank CSV file to use for importing cameras to the Server.

The blank import file includes instructions for adding and importing cameras.

1. In the Server configuration interface, click Devices > Cameras.
2. Click Add Cameras.
3. Click Create Blank Import File.

The Server saves a file named import.csv to your download location.

Set a Camera Password

You can set a new password that the Server pushes to the camera.

If you set a new password for a camera, you must use that password when you log in to the camera Web interface.

1. In the Server configuration interface, click Devices > Cameras.
2. Select a camera.
3. Click the Set Password button.
4. Type and confirm the new password.
5. Click the Set Password button.

Move a Camera

You can move a camera to a different Server in your server farm.

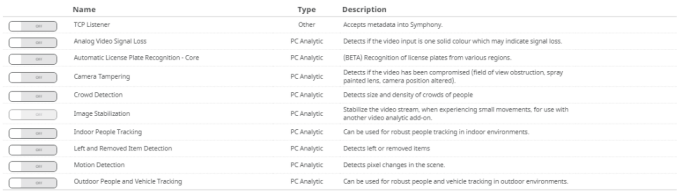
1. In the Server configuration interface, click Devices > Cameras.
2. Select a camera.
3. Click Move to Server.
4. In the server list, select the server.
5. Click OK.

Video Analytics

Senstar Symphony video analytics provide real-time alerts, smart video search, and reporting.

To use a video analytic, you purchase the appropriate license and install the video analytic on the computer that hosts the Server. Once installed, you can enable and configure the video analytic on a camera in the Server configuration interface.

+



	Name	Type	Description
	TCP Listener	Other	Accepts metadata into Symphony.
	Analog Video Signal Loss	PC Analytic	Detects if the video input is one solid colour which may indicate signal loss.
	Automatic License Plate Recognition - Core	PC Analytic	(BETA) Recognition of license plates from various regions.
	Camera Tampering	PC Analytic	Detects if the video has been compromised (field of view obstruction, spray painted lens, camera position altered).
	Crowd Detection	PC Analytic	Detects size and density of crowds of people
	Image Stabilization	PC Analytic	Stabilize the video stream, when experiencing small movements, for use with another video analytic add-on.
	Indoor People Tracking	PC Analytic	Can be used for robust people tracking in indoor environments.
	Left and Removed Item Detection	PC Analytic	Detects left or removed items
	Motion Detection	PC Analytic	Detects pixel changes in the scene.
	Outdoor People and Vehicle Tracking	PC Analytic	Can be used for robust people and vehicle tracking in outdoor environments.

+

Add a Video Analytic License to a Camera

To use a video analytic on a camera, you must add a license that includes the video analytic to the camera.

Before you begin:

- Purchase a license for the video analytic.
- Download and install the video analytic.

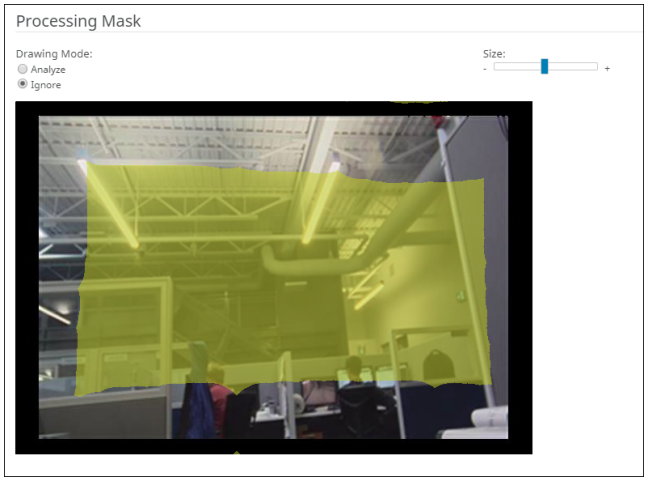
1. In the Server configuration interface, click Devices > Cameras.
2. Select a camera.
3. Click Edit.
4. In the Add-Ons section, select an appropriate license in the Analytic License Requested list.
5. Click Update License.
6. Click Save.

Draw a Processing Mask

You can draw a processing mask for a video analytic in the Server configuration interface to define the area in the camera view that the video analytic analyzes.

Drawing a processing mask is part of configuring a video analytic.

1. In the Server configuration interface, click Devices > Cameras.
2. Select the camera and click Edit.
3. In the Add-Ons list click Configure for the video analytic.
4. In the Processing section, perform the following tasks:
   a. In the Drawing Mode list, select whether the paintbrush marks areas in the processing mask image to include (Analyze) or exclude (Ignore).
   b. Using the Size slider, select the size of the paintbrush that you use in the processing mask image.
   c. Use the mouse to draw the processing mask. If you make an error, you can reverse the drawing mode and modify the processing mask.



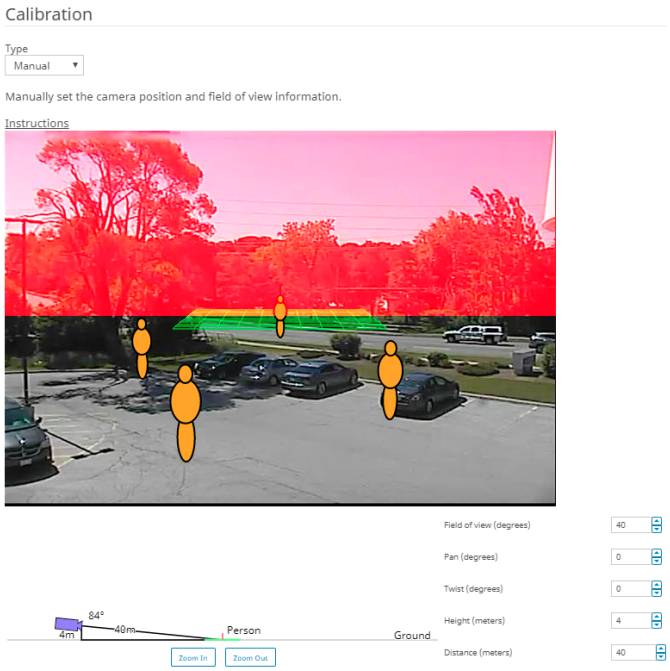
5. Click OK.

Calibrate a Camera

For some video analytics, you must calibrate the camera to achieve optimum performance and accuracy.

Calibrating a camera is part of configuring a video analytic.

1. In the Server configuration interface, click Devices > Cameras.
2. Select the camera and click Edit.
3. In the Add-Ons list click Configure for the video analytic.
4. In the Calibration section, perform the following tasks:
   a. Click on the calibration image to place avatars on the image. The avatars help you visualize people in the sample image.
   b. In the Field of view field, type the camera's field of view in degrees.
   c. In the Pan field, type the angle (degrees) of horizontal rotation around the vertical access of the camera.
   d. In the Twist field, type the angle (degrees) of rotation around the long axis of the camera.
   e. In the Twist field, type the angle (degrees) of rotation around the long axis of the camera.
   f. In the Height field, type the height of the camera.
   g. In the Distance field, type the distance between the camera and the center of the calibration grid.
5. Click Save.



Additionally, you can drag the camera in the calibration diagram to place it in relation to the scene. The Zoom In and Zoom Out buttons adjust the scale of the calibration diagram.

TCP Listener

The TCP Listener is a video analytic that listens for incoming metadata over a TCP socket and associates the metadata with an image or video.

The Server can use the metadata to search for images and video.

Enable the TCP Listener

1. In the Server configuration interface, click Devices > Cameras.
2. Select the camera and click Edit.
3. In the Add-Ons list, turn TCP Listener on.
4. Click Save.

Analog Video Signal Loss

The Analog Video Signal Loss video analytic is a video analytic that can detect when video from a camera is unavailable.

This video analytic does not require configuration and uses minimal CPU resources. It is recommended for all cameras.

Enable Analog Video Signal Loss

1. In the Server configuration interface, click Devices > Cameras.
2. Select the camera and click Edit.
3. In the Add-Ons list, turn Analog Video Signal Loss on.
4. Click Save.

Automatic License Plate Recognition

The Automatic License Plate Recognition video analytic is a video analytic for the Server that can detect and index license plates.

The Automatic License Plate Recognition video analytic can recognize and log license plates from different countries and regions on vehicles traveling up to 30 kph (19 mph). It can analyze video in real time without requiring an external trigger.

With the Automatic License Plate Recognition video analytic, a 720p network camera can analyze up to two lanes of traffic if the license plate images are at least 32 pixels in height for Latin characters or 40 pixels in height for non-Latin characters.

Typical uses for the The Automatic License Plate Recognition video analytic include:

- Toll collection in parking garages
- Traffic control
- Border crossings
- Pattern of use analysis

Configure Automatic License Plate Recognition

Configure the Automatic License Plate Recognition video analytic for each camera that runs the video analytic.

1. In the Server configuration interface, click Devices > Cameras.
2. Select the camera on which you want to run the Automatic License Plate Recognition video analytic and click Edit.
3. In the Add-Ons section, click the button beside Automatic License Plate Recognition to turn it on.
4. Click the Configure button beside Automatic License Plate Recognition.
5. In the Overview section, configure analysis options and select whether the advanced options are hidden (simple mode on) or visible (simple mode off).
6. If the image in the Processing Mask and Plate Detection sections do not include an image that is suitable for license plate detection, update the image.
    a. Click Change Image.
    b. Use the timeline and video controls to navigate to an image that is suitable for license plate detection.
    c. Click OK.
7. In the Processing Mask image, define the areas that the video analytic analyzes and ignores.
    a. In the Drawing Mode list, select whether to draw an area to analyze or ignore.
    b. Using the Size slider, select the size of drawing circle.
    c. On the image, click and drag the drawing circle to define the areas to analyze or ignore.
8. In the Plate Detection image, draw a frame around the license plate so that the edges of the text on the license plate fall within the green frame.
    a. Click and drag the frame on the image.
    b. To move the frame, click in the middle of the green frame and drag the frame.

c. To change the size of the frame, click an edge of the frame and drag the line to change the size.

d. To adjust the slant and slope of the frame, click a corner of the frame and drag the corner to change the slant or slope.

9. Using the Reporting Confidence slider, select how sensitive the video analytic is to potential license plates.
10. Click OK.

Automatic License Plate Recognition Settings

Overview

Setting	Description
Analysis Resolution	Select the resolution that the Automatic License Plate Recognition video analytic uses to analyze video frames.
Analysis FPS	Select the number of frames per second that the Automatic License Plate Recognition video analytic uses to analyze video.
Simple Mode	Turn off to make the advanced settings visible.
Region For Plate Analysis	Select the regional engine that the Automatic License Plate Recognition video analytic uses to analyze the license plates that this camera detects. The list includes the regions that you select during installation.
V9 Dongle	Select this option if you are using a new license with the Default or China engine.
Enable with Motion Detection	Select this option to only perform analysis when the camera detects motion.
Enable with Relay	Select this option to only perform analysis when a relay device records an input event. When you select this option, additional fields appear that allow you to select the relay and configure how theAutomatic License Plate Recognition video analytic responds to the input event.

Processing Mask

Setting	Description
Drawing Mode	Select whether to draw areas to analyze or ignore on the processing mask.
Size	Define the size of the circle to draw on the processing mask.

Plate Detection

Use the plate detection image to draw a frame around the license plate in an image that represents a typical license detection situation. The frame can only surround one line of characters and outside boundaries of the characters should fall within the green frame.

This is an example of a good plate detection frame:

+

This is an example of a poor plate detection frame:

+

Setting	Description
Reporting Confidence	Use the slider bar to define the sensitivity of the Automatic License Plate Recognition video analytic. The reporting confidence is 50% by default. A lower reporting confidence results in more detection and might affect performance.
Minimum height	This field displays the height of the inner rectangle.
Maximum height	This field displays the height of the outer rectangle.
Minimum width	This field displays the width of the inner rectangle. This setting is only available for the Automatic License Plate Recognition Core video analytic.
Maximum width	This field displays the width of the outer rectangle. This setting is only available for the Automatic License Plate Recognition Core video analytic.

Setting	Description
Minimum slant	This field displays the minimum slant of the vertical lines. This setting is only available for the Automatic License Plate Recognition Peripheral video analytic.
Maximum slant	This field displays the maximum slant of the vertical lines. This setting is only available for Automatic License Plate Recognition Peripheral video analytic.
Minimum slope	This field displays the minimum slope of the horizontal lines. This setting is only available for Automatic License Plate Recognition Peripheral video analytic.
Maximum slope	This field displays the maximum slope of the horizontal lines. This setting is only available for Automatic License Plate Recognition Peripheral video analytic.

Advanced

The advanced settings are visible when the simple mode is off.

Changing the advanced settings can adversely affect the performance of the video analytic.

Setting	Description
Minimum Plate Length	Define the minimum number of characters that the Automatic License Plate Recognition video analytic must detect before it recognizes the text as a potential license plate.
Plate Dwell Time	Define the time (in seconds) that a potential license plate must be visible before the Automatic License Plate Recognition video analytic begins analyzing the potential license plate.
Queue Time	Define how much video the Automatic License Plate Recognition video analytic retains for analysis. Frames that fall outside of the queue time are ignored by the video analytic.
Analysis Timeout	Define how much time can elapse before the Automatic License Plate Recognition video analytic stops processing a license plate.
Plate Display Time	Define how long the Automatic License Plate Recognition video analytic displays the license plate decoration in the Windows Client interface.
Plate Look Time	Define the time (in seconds) that the Automatic License Plate Recognition video analytic spends analyzing the license plate. During this time, the video analytic records all the characters that it recognizes (for example, the video analytic might detect a character as multiple similar characters as the license plate moves through the scene). After the time elapses, the video analytic selects and reports the best result. However, all results that the video analytic detects are saved to the database. If you set this value to 0 (zero), the video analytic reports the first result that it detects.
Import XML	Click this button to import a configuration XML file.
Export XML	Click this button to export the configuration XML file.

Setting	Description
Show XML	Click this button to display the configuration XML.

Camera Tampering

The Camera Tampering video analytic is a video analytic that can detect when a camera's field of view is obstructed.

The Camera Tampering video analytic can be enabled on a camera that is running another video analytic to ensure continuous operation of the camera. It can detect when the direction of the camera changes, when the camera is blocked, or when the lighting in the scene changes.

When the Camera Tampering video analytic detects a significant change to the scene (approximately 25% of the scene changes), it uses a previous frame as a reference and compares the subsequent frames to that reference frame. If the change persists for the minimum tampering time threshold, the Camera Tampering video analytic concludes that the camera is obstructed. For example, the Camera Tampering video analytic can detect when the lens of a camera is covered in spray paint, when a camera is moved, when a large object is place in front of a camera, or when the lights in the scene are turned off.

Configure Camera Tampering

Configure the Camera Tampering video analytic in the Server configuration interface.

1. In the Server configuration interface, click Devices > Cameras.
2. Select the camera and click Edit.
3. In the Add-Ons list, turn Camera Tampering on and click Configure.
4. Adjust the settings for the Camera Tampering video analytic.
5. Click OK.

Camera Tampering Settings

Setting	Description
Analysis Resolution	Set the resolution for the camera on which the Camera Tampering video analytic is active.
Simple Mode	Select whether to hide or display the advanced settings. Simple mode is the default mode. Advanced mode is intended for system integrators and technical support staff.
Minimum tampering time threshold	Set how long a camera must be blocked before it triggers an alarm. This setting is useful for scenes that experience temporary obstructions such as people passing by the camera. You can set the threshold so that the video analytic ignores temporary obstructions.
Scene consistency threshold	Set the size of the scene change that indicates a camera obstruction. This setting is useful for scenes that experience lighting changes. You can set the threshold so that the video analytic ignores the lights in the scene turning on and off, but registers other camera obstructions.

Crowd Detection

The Crowd Detection video analytic is a video analytic that offers crowd detection, event triggering,

and alarms.

You can define the area that the Crowd Detection video analytic monitors for the number of people in the monitored area (capacity) and the percentage of the monitored area with people (occupancy). The Crowd Detection video analytic can trigger alarms when it detects a specific capacity or occupancy.

The Crowd Detection video analytic can display informational decorations in the camera view panel. In addition to displaying tracking boxes around areas where it detects people, Crowd Detection video analytic can display the following decorations:

- The Occupancy decoration displays the percentage of the scene that contains people.
- The Capacity decoration displays the estimated number of people in the scene as a percentage of the maximum capacity.
- The Crowd Est. decoration displays the estimated number of people in the scene.

The Crowd Detection video analytic can detect people that are 8 pixels or larger in the scene. When placing a camera for use with the Crowd Detection video analytic, consider the following guidelines.

- Mount the camera so that it has an overview of the area. Do not place the camera directly overhead (90°) because the Crowd Detection video analytic cannot detect people from directly overhead and do not place the camera close to horizontal (0°) because people in the front obscure the crowd behind.
- Mount the camera or use the processing mask so that the scene does not includes crowds larger than 50 people. The Crowd Detection video analytic does not work reliably on scenes with more than 50 people.
- Mount the camera or use the processing mask so that the scene does not include other moving objects (e.g., vehicles) or moving shadows.

When the Crowd Detection video analytic starts, it takes approximately 2 minutes to learn the scene. During this time, the results are inaccurate.

Configure Crowd Detection

Configure the Crowd Detection video analytic in the Server configuration interface.

To configure the Crowd Detection video analytic, you should use an image that includes at least one person from the camera that you are configuring. Adjust the settings so that the reference people and the grid lines in the calibration image match the scene. You can move and add reference people in the

calibration image.

1. In the Server configuration interface, click Devices > Cameras.
2. Select the camera and click Edit.
3. In the Add-Ons list, turn the Crowd Detection video analytic on and click Configure.
4. On the Crowd Detection page, define the Overview, Processing Mask, Capacity, Calibration, and Sensitivity settings.
5. Click OK.

Crowd Detection Settings

Overview

Setting	Description
Analysis Resolution	Set the resolution for the camera on which the Crowd Detection video analytic is active.
Automatically Select Resolution Based on Calibration	Select to automatically set the analysis resolution based on the settings in the Calibration section.
Analysis FPS	Set the frames per second for the camera on which the Crowd Detection video analytic is active.
Simple Mode	Select whether to hide or display the advanced settings.

Processing Mask

Setting	Description
Drawing Mode	Select whether the paintbrush marks areas in the processing mask image to include (Analyze) or exclude (Ignore).
Size	Select the size of the paintbrush that you use in the processing mask image.

Capacity

Setting	Description
Maximum Capacity	Use the slider to define the maximum capacity for the scene.

Calibration

Setting	Description
Type	Select the type of calibration. Manual allows you to set the camera position. Automatic allows the Crowd Detection video analytic to set the camera position and field of view. Uncalibrated runs the video analytic without camera position and field of view information.
Zoom In	Click to make the calibration diagram larger.
Zoom Out	Click to make the calibration smaller.
Field of view (degrees)	Define the horizontal field of view (in degrees) for the camera.
Pan (degrees)	Define the rotation around the vertical axis of the camera in relation to the scene.
Twist (degrees)	Define the rotation around the horizontal axis of the camera in relation to the scene.

Setting	Description
Height (meters)	Define the vertical distance from the camera to the ground.
Distance (meters)	Define the horizontal distance from the camera to the center of the scene.

Sensitivity

Setting	Description
Occupancy	Use the slider to set how sensitive the Crowd Detection video analytic is to the area occupied by people.
Capacity	Use the slider to set how sensitive the Crowd Detection video analytic is to the number of people in the scene.

Image Stabilization

The Image Stabilization video analytic can stabilize video when a camera experiences vibrations or other small movements.

This video analytic is beneficial when you use it to supplement another video analytic. This video analytic does not require configuration.

Enable Image Stabilization

1. In the Server configuration interface, click Devices > Cameras.
2. Select the camera and click Edit.
3. In the Add-Ons list, turn Image Stabilization on.
4. Click Save.

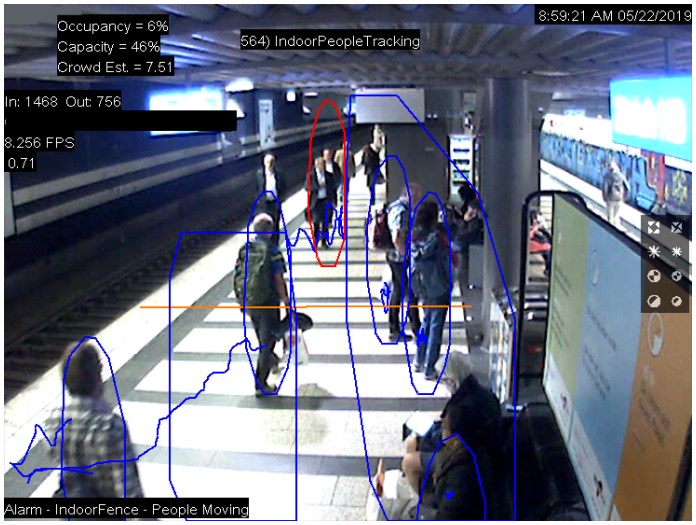
Indoor People Tracking

The Indoor People Tracking video analytic offers people counting, dwell-time detection, event triggering, and alarms.

For people counting, the Indoor People Tracking video analytic uses counting lines that you draw on the scene to count how many people pass through the scene.

The Indoor People Tracking video analytic can detect people that are 16 pixels or larger in the scene.

+



+

Configure Indoor People Tracking

1. In the Server configuration interface, click Devices > Cameras.
2. Select the camera and click Edit.
3. In the Add-Ons list, turn Indoor People Tracking on and click Configure.
4. Adjust the settings for the Indoor People Tracking video analytic. The simple mode configuration uses the default detection settings for the Indoor People Tracking. To view the default settings, you can turn off the simple mode to make the default settings visible in the Advanced section.

   Changing the advanced settings can adversely affect the performance of the video analytic.

1. Click OK.

Indoor People Tracking Settings

Overview

Setting	Description
Analysis Resolution	Set the resolution for the camera on which the Indoor People Tracking video analytic is active.
Automatically Select Resolution Based on Calibration	Select to automatically set the analysis resolution based on the settings in the Calibration section.
Analysis FPS	Set the frames per second for the camera on which the Indoor People Tracking video analytic is active.
Simple Mode	Select whether to hide or display the advanced settings. Simple mode is the default mode. Advanced mode is intended for system integrators and technical support staff.

Processing Mask

Setting	Description
Drawing Mode	Select whether the paintbrush marks areas in the processing mask image to include (Analyze) or exclude (Ignore).

Setting	Description
Size	Select the size of the paintbrush that you use in the processing mask image.

Counting Line

Setting	Description
Create	On the image, click and hold the left mouse button, move the mouse to draw the new counting line, and release the left mouse button.
Delete	Click a counting line to select it and press Delete.
Move	Hold the CTRL key, click and hold the left mouse button on the counting line endpoint, and drag the endpoint to the
Add a connected counting line	Click and hold the left mouse button on the endpoint of an existing counting line, move the mouse to draw the new counting line, and release the left mouse button.
Change the counting direction	Click an arrow on the counting line to toggle counting for that direction on and off.

Calibration

Setting	Description
Type	Select the type of calibration. Manual allows you to set the camera position. Automatic allows the Indoor People Tracking video analytic to set the camera position and field of view. Uncalibrated runs the Indoor People Tracking video analytic without camera position and field of view information.
Zoom In	Click to make the calibration diagram larger.
Zoom Out	Click to make the calibration smaller.
Field of view (degrees)	Define the horizontal field of view (in degrees) for the camera.
Pan (degrees)	Define the rotation around the vertical axis of the camera in relation to the scene.
Twist (degrees)	Define the rotation around the horizontal axis of the camera in relation to the scene.
Height (meters)	Define the vertical distance from the camera to the ground.
Distance (meters)	Define the horizontal distance from the camera to the center of the scene.

Sensitivity

This section is only visible in simple mode.

Setting	Description
Object Contrast	Use the slider to set how sensitive the Indoor People Tracking video analytic is to the contrast between objects and the background.
Object Motion	Use the slider to set how sensitive the Indoor People Tracking video analytic is to the movement of objects.
Background Motion	Use the slider to set how sensitive the Indoor People Tracking video analytic is to movement in the background.

Setting	Description
Shadow Suppression	Select this option to have the Indoor People Tracking video analytic ignore the presence and movement of shadows.

Left and Removed Item Detection

The Left and Removed Item Detection video analytic can detect when an object is added to or removed from the scene.

The Left and Removed Item Detection video analytic does not differentiate between left items and removed items. The video analytic compares the pixels in the scene with the pixels in previous scenes and uses tracking boxes to identify the areas with change.

Configure Left and Removed Item Detection

1. In the Server configuration interface, click Devices > Cameras.
2. Select the camera and click Edit.
3. In the Add-Ons list, turn Left and Removed Item Detection on and click Configure.
4. Adjust the settings for the Left and Removed Item Detection video analytic. The simple mode configuration uses the default detection settings for the Left and Removed Item Detection video analytic. To view the default settings, you can turn off the simple mode to make the default settings visible in the Advanced section.

Changing the advanced settings can adversely affect the performance of the video analytic.

1. Click OK.

Left and Removed Item Detection Settings

Overview

Setting	Description
Analysis Resolution	Set the resolution for the camera on which the Left and Removed Item Detection video analytic is active.
Automatically Select Resolution Based on Calibration	Select to automatically set the analysis resolution based on the settings in the Calibration section.
Analysis FPS	Set the frames per second for the camera on which the Left and Removed Item Detection video analytic is active.
Simple Mode	Select whether to hide or display the advanced settings. Simple mode is the default mode. Advanced mode is intended for system integrators and technical support staff.

Processing Mask

Setting	Description
Drawing Mode	Select whether the paintbrush marks areas in the processing mask image to include (Analyze) or exclude (Ignore).
Size	Select the size of the paintbrush that you use in the processing mask image.

Calibration

Setting	Description
Zoom In	Click to make the calibration diagram larger.
Zoom Out	Click to make the calibration smaller.
Field of view (degrees)	Define the horizontal field of view (in degrees) for the camera.
Pan (degrees)	Define the rotation around the vertical axis of the camera in relation to the scene.
Twist (degrees)	Define the rotation around the horizontal axis of the camera in relation to the scene.
Height (meters)	Define the vertical distance from the camera to the ground.
Distance (meters)	Define the horizontal distance from the camera to the center of the scene.

Advanced

The advanced settings are visible when the simple mode is off.

Changing the advanced settings can adversely affect the performance of the video analytic.

Setting	Description
Left item duration	Set the time (seconds) that an object must be present or missing before the Left and Removed Item Detection video analytic considers it left or removed. The default setting is 15 seconds.
Check for object drop-off	Select whether the Left and Removed Item Detection video analytic ignores items that a person picks up or drops off. The default setting is selected.
Initial background model learn time	Set the time (seconds) that the Left and Removed Item Detection video analytic takes to learn the background of the scene. During this time, the Left and Removed Item Detection video analytic does not attempt to detect any objects. The default setting is 1 second.
Reach width	Set the distance (pixels) for a person in a retail store to reach the item. The default setting is 9 pixels.
Object merge distance	Set the distance (pixels) at which the Left and Removed Item Detection video analytic merges two object into one object. The default setting is 20 pixels.
Reduce false alarms from still people	Select whether the Left and Removed Item Detection video analytic waits to detect people in the scene as a left or removed item. This setting uses the Time to wait for still people setting. The default setting is false.

Setting	Description
Time to wait for still people	Set how long (seconds) the Left and Removed Item Detection video analytic waits to detect people in the scene. This setting is activated by selecting the Reduce false alarms from still people setting. The default setting is 60 seconds.
Appearance	
Lower bound	
Upper bound	
Reduce reflection	Select whether the Left and Removed Item Detection video analytic tries to ignore reflections.
Reflection reduction threshold	Set the how sensitive to reflections the Left and Removed Item Detection video analytic is to reflections. A lower value causes the video analytic to ignore more reflections. A higher value causes the video analytic to process more reflections.
Camera looking at shelf	Select if the camera is facing a shelf. This setting is active only if you select Check for object drop-off.
Time to clear long-term representation	Set how long (seconds) before the Left and Removed Item Detection video analytic clears the background.
Time to clear short-term representation	Set how long (seconds) before the Left and Removed Item Detection video analytic clears the cache.
Minimum fill rate	Set the percent of the item's smallest bounding box the item must fill for the Left and Removed Item Detection video analytic considers it an item. The default value is 10.
Time to remove or drop an item	Set how long (seconds) a item must be present before the Left and Removed Item Detection video analytic starts processing the item. Setting a longer time reduces the processing load of the video analytic.
Background reset time after an object is deleted	Set how long (seconds) the Left and Removed Item Detection video analytic waits before it deletes an object.
Minimum valid object dimension	Set how large (pixels) an item must be, in both height and width, and how far from the edge of the scene an item must be for the Left and Removed Item Detection video analytic to consider the item to be left or removed.
Reset camera if this percentage of image becomes foreground in 1 frame	Set the percentage of the image that must change in a single frame before the camera resets the background. This prevents the Left and Removed Item Detection video analytic from considering sudden large changes as items.
Reset camera if this percentage of image becomes foreground in 5 frames	Set the percentage of the image that must change in five frames before the camera resets the background. This prevents the Left and Removed Item Detection video analytic from considering gradual large changes as items.
Merge small objects closer than	Set the distance (pixels) between two items at which the Left and Removed Item Detection video analytic merges the two items into a single item. The default value is 8.

Setting	Description
Grayscale background update rate	Set the rate at which the Left and Removed Item Detection video analytic updates the background image. Setting a lower value catches more left and removed items but increases the processing load. The default value is 5.

Motion Detection

The Motion Detection video analytic offers motion detection, event triggering, and alarms.

The Motion Detection video analytic detects pixel changes in the scene.

+

+

Configure Motion Detection

What it is

The Motion Detection video analytic flags pixel changes in a camera's video stream as motion events. These events feed the rules engine, so you can use motion as a trigger for recording, alarms, or actions.

Motion Detection is lightweight compared to the classification-based analytics (outdoor people and vehicle tracking, Senstar Symphony AI Object Detection and Tracking). It detects **that** something moved, not **what** moved. If you need to distinguish people from vehicles or filter out wildlife, use a classification analytic instead.

When you'd use it

- A camera needs to record only when something in the scene moves (motion-triggered recording to reduce storage).
- You want a simple "something moved after hours" alarm on a low-traffic camera.
- A scene is too simple or too resource-constrained to justify a classification analytic.

Do not use it alone for high-false-positive scenes (foliage in wind, snow, rain, passing traffic beyond the area of interest) — tune the processing mask to exclude those areas, or switch to a classification analytic.

Prerequisites

- Permission to edit camera settings.

- A camera that is already added to the Server. See Add a Camera.
- For guidance on what the individual fields do, see Motion Detection Settings.

Procedure

1. In the Server configuration interface, click **Devices** > **Cameras**.
2. Select the camera and click **Edit**.
3. In the **Add-Ons** list, turn **Motion Detection** on and click **Configure**.
4. Tune the following:
   - **Sensitivity** — how much pixel change counts as motion. Start at the default, then raise it if real motion is being missed, or lower it if the analytic triggers on noise (lighting changes, compression artefacts).
   - **Processing mask** — mark the areas of the frame the analytic should ignore. Mask out moving foliage, flags, water, roads you don't care about, and time/date overlays that change every second.
   - **Minimum object size** — filter out small pixel changes that are too small to be the objects you care about.

     See Motion Detection Settings for the full field reference.
5. Click **OK**.
6. Click **Save** on the camera to apply the change.

Tuning tips

- Tune during the scene's worst conditions — night, bad weather, peak activity — not during a calm afternoon.
- After tuning, watch the event log for a shift or two (View Events) to confirm the false-positive rate is acceptable.
- If you cannot achieve both good detection and a low false-positive rate with Motion Detection alone, switch to a classification analytic.

Related tasks

- Motion Detection — overview of the analytic.
- Motion Detection Settings — full field reference.
- Motion Detection Event Settings — use motion events in rules.
- Draw a Processing Mask

Motion Detection Settings

Overview

Setting	Description
Analysis Resolution	Set the resolution for the camera on which the Motion Detection video analytic is active.
Analysis FPS	Set the frames per second for the camera on which the Motion Detection video analytic is active.
Simple Mode	Select whether to hide or display the advanced settings.

Processing Mask

Setting	Description
Drawing Mode	Select whether the paintbrush marks areas in the processing mask image to include (Analyze) or exclude (Ignore).
Size	Select the size of the paintbrush that you use in the processing mask image.

Grid View

Setting	Description
Minimum Foreground Fill (percent)	Use the slider to define what percentage of a grid square must change for the Motion Detection video analytic to detection in that grid square.
Grid Spacing	Use the slider to define the size of the grid squares.
Foreground Sensitivity	Use the slider to define how sensitive the Motion Detection video analytic is to motion when determining the foreground fill.
Adjust sensitivity based on camera noise	Select to automatically change the foreground sensitivity to accommodate random variations or brightness or color from the camera.

Outdoor People and Vehicle Tracking

The Outdoor People and Vehicle Tracking video analytic offers people and vehicle detection in outdoor environments with weather and lighting changes.

The Outdoor People and Vehicle Tracking video analytic can detect objects that are 8 pixels or larger in the scene.

+

+

Configure Outdoor People and Vehicle Tracking

1. In the Server configuration interface, click Devices > Cameras.
2. Select the camera and click Edit.

3. In the Add-Ons list, turn Outdoor People and Vehicle Tracking on and click Configure.
4. Adjust the settings for the Outdoor People and Vehicle Tracking video analytic. The simple mode configuration uses the default detection settings for the Outdoor People and Vehicle Tracking video analytic. To view the default settings, you can turn off the simple mode to make the default settings visible in the Advanced section.

Changing the advanced settings can adversely affect the performance of the video analytic.

1. Click Save.

Outdoor People and Vehicle Tracking Settings

Overview

Setting	Description
Analysis Resolution	Set the resolution for the camera on which the Outdoor People and Vehicle Tracking video analytic is active.
Automatically Select Resolution Based on Calibration	Select to automatically set the analysis resolution based on the settings in the Calibration section.
Analysis FPS	Set the frames per second for the camera on which the Outdoor People and Vehicle Tracking video analytic is active.
Simple Mode	Select whether to hide or display the advanced settings.

Processing Mask

Setting	Description
Drawing Mode	Select whether the paintbrush marks areas in the processing mask image to include (Analyze) or exclude (Ignore).
Size	Select the size of the paintbrush that you use to draw on the processing mask image.

Calibration

Setting	Description
Type	Select the type of calibration. Manual allows you to set the camera position. Automatic allows the Outdoor People and Vehicle Tracking video analytic to set the camera position and field of view. Uncalibrated runs the Outdoor People and Vehicle Tracking video analytic without camera position and field of view information.
Zoom In	Click to make the calibration diagram larger.
Zoom Out	Click to make the calibration smaller.
Field of view (degrees)	Define the horizontal field of view (in degrees) for the camera.
Pan (degrees)	Define the rotation around the vertical axis of the camera in relation to the scene.
Twist (degrees)	Define the rotation around the horizontal axis of the camera in relation to the scene.
Height (meters)	Define the vertical distance from the camera to the ground.
Distance (meters)	Define the horizontal distance from the camera to the center of the scene.

Sensitivity

The sensitivity settings are visible when the simple mode is on.

Setting	Description
Object Contrast	Use the slider to set how sensitive the Outdoor People and Vehicle Tracking video analytic is to differences between objects and the background.
Object Motion	Use the slider to set how sensitive the Outdoor People and Vehicle Tracking video analytic is to foreground motion when detecting objects.
Background Motion	Use the slider to set how sensitive the Outdoor People and Vehicle Tracking video analytic is to background motion when detecting objects.
Shadow Suppression (Simple)	Select to use simple shadow suppression. Simple shadow suppression is effective where there are light shadows in the scene.  Do not use shadow suppression with thermal cameras.
Shadow Suppression (Complex)	Select to use complex shadow suppression. Complex shadow suppression in effective when there are dark shadows in the scene.  Do not use shadow suppression with thermal cameras.
Snow Suppression	Select to have the Outdoor People and Vehicle Tracking video analytic ignore the motion of snow in the scene.
Dynamic Background	Select to have the Outdoor People and Vehicle Tracking video analytic ignore periodic movement in the scene. This setting is effective for outdoor scenes where weather can cause motion in the background.
Detect Distant Objects	Select to have the Outdoor People and Vehicle Tracking video analytic attempt to detect objects in the distance.

PTZ Auto-Tracking

The PTZ Auto-Tracking video analytic can automatically control PTZ cameras when activity is detected.

The PTZ Auto-Tracking video analytic requires that the Indoor People Tracking video analytic or Outdoor People and Vehicle Tracking video analytic is active on the camera. You can add the PTZ Auto-Tracking video analytic as an action for a rule.

Configure PTZ Auto-Tracking

1. In the Server configuration interface, click Devices > Cameras.
2. Select the camera and click Edit.
3. Turn on and configure either the Indoor People Tracking video analytic or Outdoor People and Vehicle Tracking video analyticfor the camera.
4. In the Add-Ons list, turn PTZ Auto-Tracking on and click Configure.
5. Configure the video analytic.
6. Click Save.

PTZ Auto-Tracking Settings

Overview

Setting	Description
Analysis Resolution	Set the resolution for the camera on which the PTZ Auto-Tracking is active.
Analysis FPS	Set the frames per second for the camera on which the PTZ Auto-Tracking video analytic is active.
Simple Mode	Select whether to hide or display the advanced settings. Simple mode is the default mode. Advanced mode is intended for system integrators and technical support staff.

Face Recognition

The Face Recognition video analytic offers facial recognition, event triggering, and alarms.

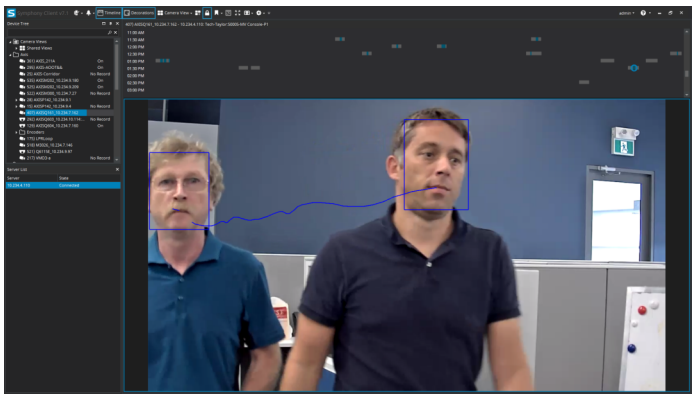
The Face Recognition video analytic uses profiles to represent individuals. Each profile can include multiple images of an individual's face. Use the Windows Client interface to create profiles, add images of faces, and set whether the profile is blocked or allowed. When the Face Recognition video analytic identifies a face in video, it can trigger events on the Server.

The Face Recognition video analytic can detect faces when there is greater than 29 pixels between the eyes and it works best when the resolution of the camera is greater than or equal to 640 x 480.

The Face Recognition video analytic includes spoof attack detection. The video analytic can detect the difference between pictures of faces and real faces. You can use spoof attack detection to generate alarms when the video analytic detects spoofed faces.

The Face Recognition video analytic cannot generate alarms on real faces and spoofed faces at the same time. You must create two rules to generate alarms on both.

In the Windows Client interface, a blue square surrounds a tracked face and a red square surrounds a tracked face that triggers an alarm.



Configure Face Recognition

What it is

The Face Recognition video analytic detects faces in a camera's video stream and matches them against an enrolled-face database. Matches drive rules and appear in the Face Recognition report.

Face Recognition is resource-intensive. It is appropriate for a small number of cameras placed where

people pass through a known field of view (entrances, turnstiles, choke points) rather than for general-purpose coverage.

When you'd use it

- Watch for known persons of interest at building entrances.
- Generate alerts when a VIP or a banned individual is seen on camera.
- Produce a report of who was seen where and when.

Do not enable Face Recognition on cameras where the face size is too small, the angle is steep, or the field of view is too wide — detection and match quality collapse under those conditions.

About spoof-attack detection

A spoof attack is an attempt to fool Face Recognition by presenting a photograph, a printed mask, or video playback of someone else's face to the camera. Spoof-attack detection analyses the presented face for liveness cues so a photograph or screen is less likely to produce a match.

- **Enable** spoof-attack detection when the camera guards a high-value asset and the extra processing cost is acceptable.
- **Disable** when processing headroom is tight and the spoofing risk is low (for example, an overhead or long-range camera where presenting a photograph is implausible).

About the processing mask

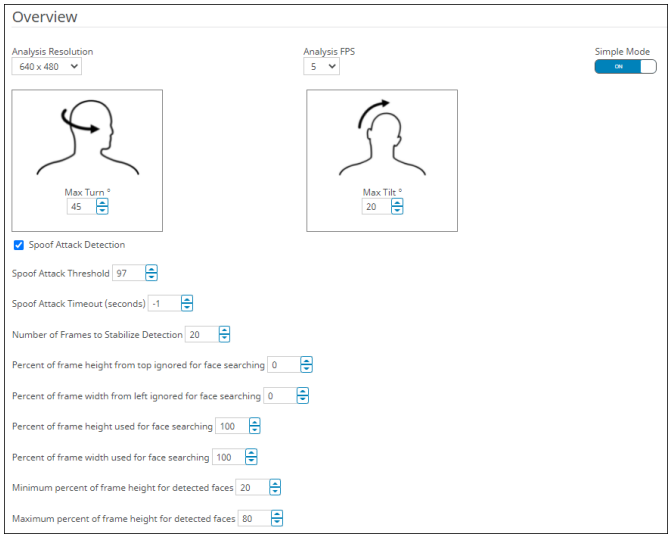
The processing mask tells the analytic which parts of the frame to analyse. Mask out areas where faces cannot plausibly appear (sky, ground, walls, printed signs that contain face-like patterns). Anything inside the mask is ignored — the analytic will not search for or recognise faces there.

Prerequisites

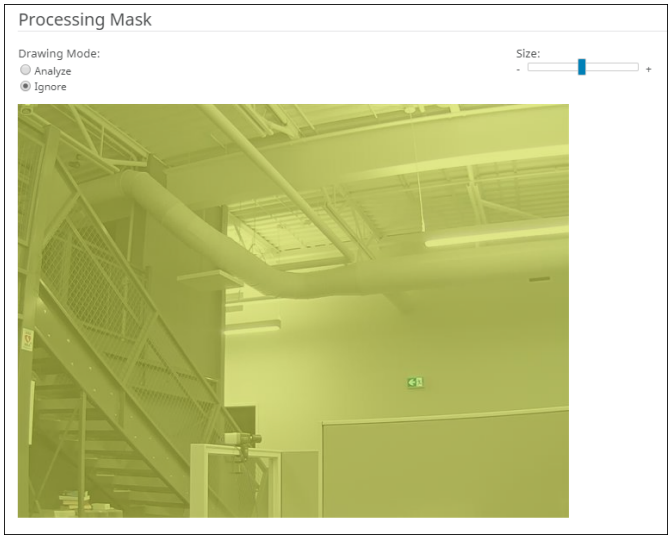
- Permission to edit camera settings.
- A camera that is already added. See Add a Camera.
- Enough GPU/CPU headroom on the Server for Face Recognition at the planned number of cameras.
- An enrolled-face database (see the Face Recognition feature pages).

Procedure

1. In the Server configuration interface, click **Devices** > **Cameras**.
2. Select the camera and click **Edit**.
3. In the **Add-Ons** list, turn **Face Recognition** on and click **Configure**.
4. In the **Overview** section, set the detection parameters: the face search frame (the area of the image where Face Recognition looks for faces) and the spoof-attack detection settings.



5. In the **Processing Mask** section, mark the areas the analytic should ignore.



Any area covered by the processing mask is ignored. If a face appears in a masked region, it will not be detected or recognised.

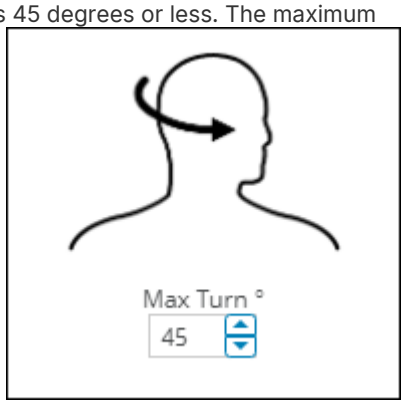
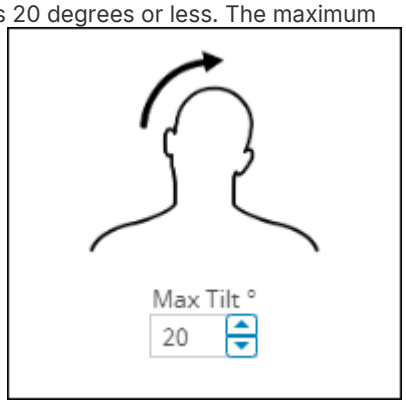
6. Click **OK**.
7. Click **Save**.

Related tasks

- Face Recognition — overview of the analytic.
- Face Recognition Settings — full field reference.
- Face Recognition Event Settings — use face recognition events in rules.
- Face Recognition Report

Face Recognition Settings

Overview

Setting	Description
Analysis Resolution	Set the resolution for the camera on which the Face Recognition video analytic is active.
Analysis FPS	Set the frames per second for the camera on which the Face Recognition video analytic is active.
Face Confidence Threshold	Set how confident the Face Recognition video analytic must be that objects are faces before it tracks objects.
Max Turn	Set the horizontal angle (in degrees) from center where the Face Recognition video analytic does not track objects. The recommended value is 45 degrees or less. The maximum value is 70 degrees. + 
Max Tilt	Set the vertical angle (in degrees) from center where the Face Recognition video analytic does not track objects. The recommended value is 20 degrees or less. The maximum value is 45 degrees. + 
Spoof Attack Detection	Select to enable spoofing attack detection. This setting is disabled by default.
Spoof Attack Threshold	Set how confident the video analytic must be that a face is spoofed to trigger a rule. This setting becomes visible when you select Spoof Attack Detection. The value range is 0 to 100. The default value is 99.

Setting	Description
Spoof Attack Timeout (seconds)	Set how long the video analytic waits before resetting the spoof attack status. This setting becomes visible when you select Spoof Attack Detection. The range for this setting is -1 (no timeout) to 100. The default value is -1 (no timeout).
Number of Frames to Stabilize Detection	Set the number of frames for which the video analytic must be confident of a spoofed face to trigger a rule. This setting becomes visible when you select Spoof Attack Detection. The range for this setting is 1 to 100. The default value is 10.
Percent of frame height from top ignored for face searching	Define the area at the top of the image that the video analytic ignores as a percentage of the height of the sample image.
Percent of frame width from left ignored for face searching	Define the area at the left side of the image that the video analytic ignores as a percentage of the width of the sample image.
Percent of frame height used for face searching	Define the height of the area in which the video analytic attempts to detect faces as a percentage of the height of the sample image. This percentage is applied after the ignored percentage.
Percent of frame width used for face searching	Define the width of the area in which the video analytic attempts to detect faces as a percentage of the width of the sample image. This percentage is applied after the ignored percentage.
Minimum percentage of frame height for detected faces	Define the minimum size of a face that the video analytic should detect as a percentage of the sample image.
Maximum percent of frame height for detected faces	Define the maximum size of a face that the video analytic should detect as a percentage of the sample image.

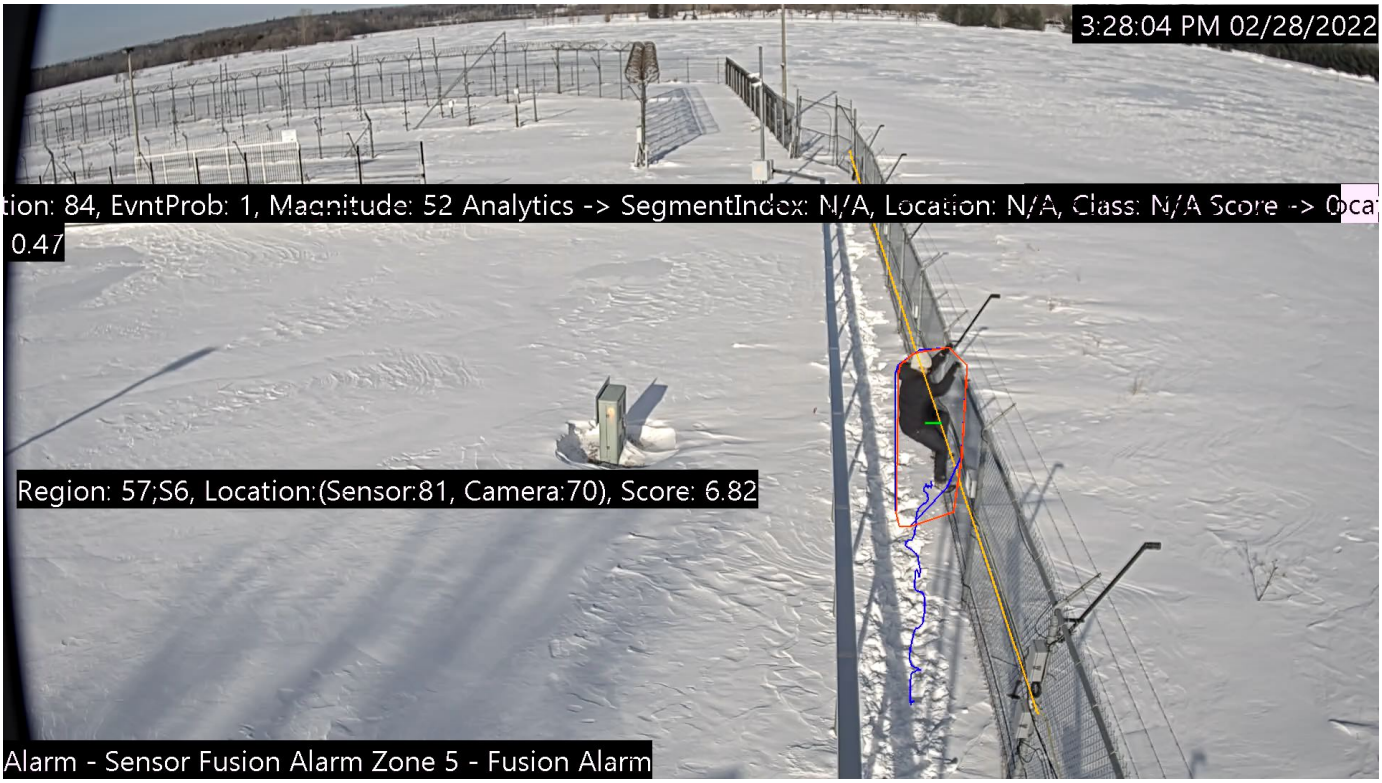
Processing Mask

Setting	Description
Drawing Mode	Select whether the paintbrush marks areas in the processing mask image to include (Analyze) or exclude (Ignore).
Size	Select the size of the paintbrush that you use in the processing mask image.

Senstar Sensor Fusion

The Senstar Sensor Fusion combines a perimeter intrusion detection system data with a dedicated video analytic to significantly improve perimeter intrusion detection while reducing false alarms from each individual sensor.

The Senstar Sensor Fusion uses a video analytic to analyze objects close to the fence and correlates the results with data from the perimeter intrusion detection system. The Senstar Sensor Fusion calculates a probability from the video analytic (data including time, object classification, history, and location) and the perimeter intrusion detection system (data containing time, location, magnitude, and frequency), and uses that probability to trigger an alarm with a higher accuracy than alarms triggered by each system individually.



In addition, the Senstar Sensor Fusion provides redundancy if one of the components experiences a failure. When one component experiences a failure, the Senstar Sensor Fusion shifts the weight of the probability to the functional component and triggers alarms based on that probability.

The Senstar Sensor Fusion currently supports the following Senstar perimeter intrusion detection system technology:

- Senstar FlexZone

Configure the Senstar Sensor Fusion

Configure the Senstar Sensor Fusion in the Server configuration interface.

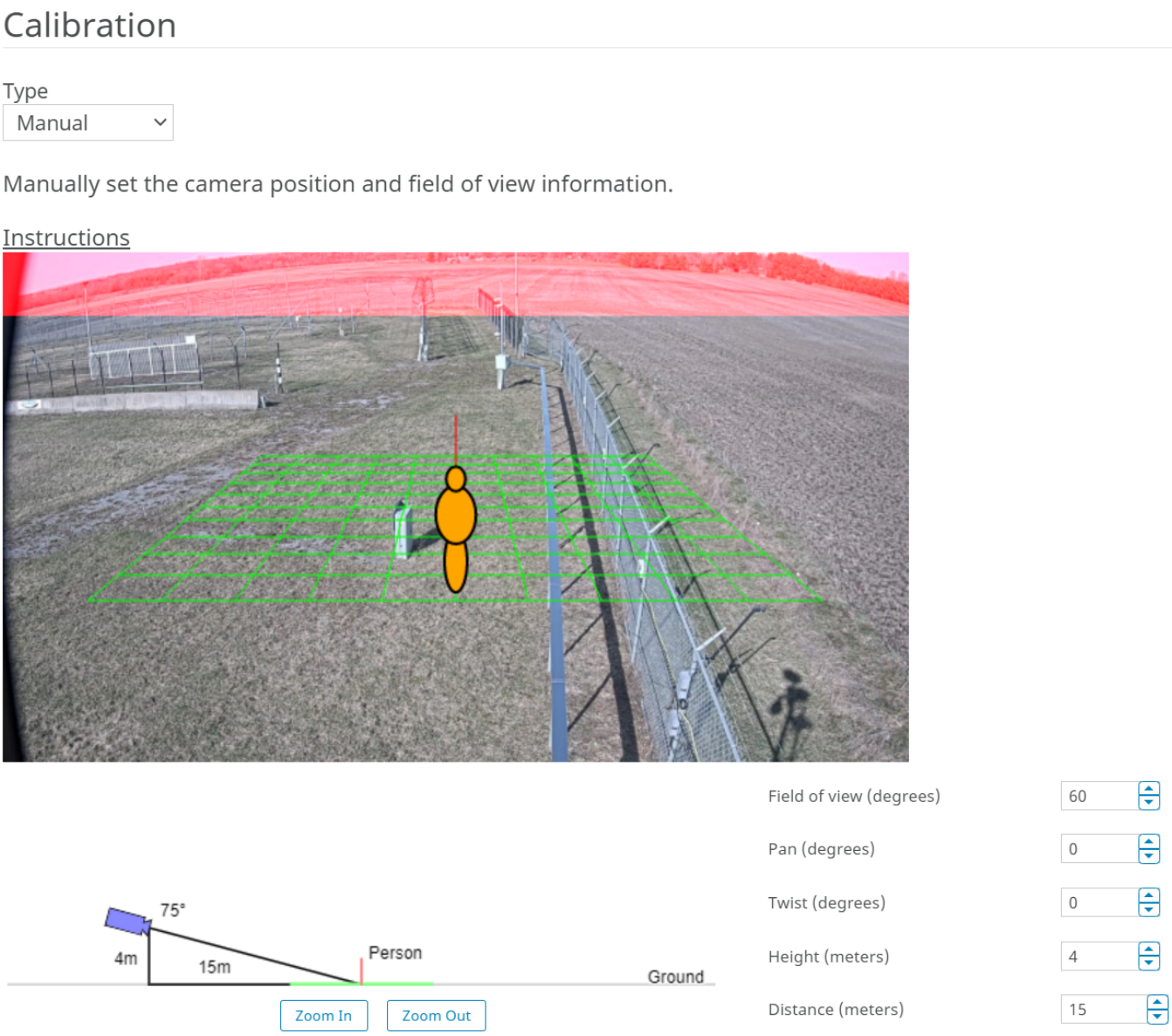
For information about specific Senstar Sensor Fusion settings, see the Senstar Sensor Fusion settings topic.

1. In the Server configuration interface, click Devices > Cameras.
2. Select the camera and click Edit.
3. In the Add-Ons list, turn Senstar Sensor Fusion on and click Configure.
   image::vis_fusion_configure_01.png[]
4. In the Overview section, configure the resolution and FPS for the camera.
5. In the Processing Mask section, set the areas in the image that the camera ignores or analyzes.
   image::vis_fusion_configure_processing_mask.png[]
6. In the Calibration section, calibrate the camera to the scene. Select Automatic to have the video analytic automatically determine the camera position and view information.

Select Uncalibrated to run the video analytic without camera position and view information.

Selecting this option greatly reduces the accuracy of the video analytic.

Select Manual to manually set the camera position and view information. You can drag the camera to the correct position or adjust the parameters in the applicable fields. The reference person in the image should match, as closely as possible, the size and position of a real person in the view. +



1. In the Sensitivity section, set how sensitive the Senstar Sensor Fusion is to contrast and motion, and select which options to enable to optimize the camera for the environment. image::vis_fusion_configure_sensitivity.png[]
2. In the Sensor Segments section, draw the segments of the of the perimeter intrusion detection system. image::vis_fusion_configure_sensor_segments.png[]

The sensor segments do not have to cover the entire perimeter intrusion detection system. The coverage of the Senstar Sensor Fusion does not depend on the perimeter intrusion detection system zone configuration; the sensor segments can be part of a single zone, part or multiple zones, or match a zone exactly.

a. In the image, click and drag to draw a sensor segment that matches both the position and location

of the applicable perimeter intrusion detection system zone.

b. Select Show Measures. Displaying measurements is optional, but the measurements make it easier to add sensor segments.

c. In the Name field, type a name for the sensor segment.

d. In the Select a Device list, select the perimeter intrusion detection system that provides information to the Senstar Sensor Fusion.

e. In the Zone list, select the perimeter intrusion detection system zone that the sensor segment matches.

f. Set the length of the sensor segment in the Range and To fields. The Range value should match the starting point of the perimeter intrusion detection system zone.

PIDS zone	PIDS length	Range value	To value
1	10	0	10
2	20	10	30
3	10	30	40

a. In the Reference Points field, select how many reference points you want on the sensor segment. You should add as many reference points as there are fence posts in the perimeter intrusion detection system zone.

When you add additional reference points to the sensor segment, the yellow lines that mark the buffer zone will converge on the end of the sensor segment. The buffer zones lines will return to normal once you set the Scale value in the next step.

a. In the Scale field, adjust the scale of the sensor segment so that the reference points match the fence posts included in the length of the sensor segment.

To set the scale correctly, focus on two reference points and adjust the scale so that the reference points in the image match the fence posts.

a. In the Confidence field, set how confident the Senstar Sensor Fusion must be to raise an alarm.

b. In the Buffer Zone Distance field, set how far from the sensor segment (and the perimeter intrusion detection system zone) the video analytic looks for objects.

1. Click OK.
2. Click Save.

Senstar Sensor Fusion Settings

Overview

Setting	Description
Analysis Resolution	Select the resolution that the Senstar Sensor Fusion uses to analyze video frames.
Analysis FPS	Select the number of frames per second that Senstar Sensor Fusion uses to analyze video.
Automatically Select Resolution Based on Calibration	Select to automatically set the analysis resolution based on the settings in the Calibration section.

Setting	Description
Simple Mode	Select whether to hide or display the advanced settings. Warning: Changing the advanced settings can adversely affect the performance of the video analytic.

Processing Mask

Setting	Description
Drawing Mode	Select whether the paintbrush marks areas in the processing mask image to include (Analyze) or exclude (Ignore).
Size	Select the size of the paintbrush that you use to draw on the processing mask image.

Calibration

Setting	Description
Type	Select the type of calibration. Manual allows you to set the camera position. Automatic allows the video analytic to set the camera position and field of view. Uncalibrated runs the video analytic without camera position and field of view information.
Zoom In	Click to make the calibration diagram larger.
Zoom Out	Click to make the calibration diagram smaller.
Field of view (degrees)	Define the horizontal field of view (in degrees) for the camera.
Pan (degrees)	Define the rotation around the vertical axis of the camera in relation to the scene.
Twist (degrees)	Define the rotation around the horizontal axis of the camera in relation to the scene.
Height (meters)	Define the vertical distance from the camera to the ground.
Distance (meters)	Define the horizontal distance from the camera to the center of the scene.

Sensitivity

Setting	Description
Object Contrast	Use the slider to set how sensitive the Senstar Sensor Fusion is to differences between objects and the background.
Object Motion	Use the slider to set how sensitive the Senstar Sensor Fusion is to foreground motion when detecting objects.
Background Motion	Use the slider to set how sensitive the Senstar Sensor Fusion is to background motion when detecting objects.
Shadow Suppression (Simple)	Select to use simple shadow suppression. Simple shadow suppression is effective where there are light shadows in the scene.  Do not use shadow suppression with thermal cameras.

Setting	Description
Shadow Suppression (Complex)	Select to use complex shadow suppression. Complex shadow suppression is effective where there are dark shadows in the scene.  Do not use shadow suppression with thermal cameras.
Snow Suppression	Select to have the video analytic ignore the motion of snow in the scene.
Dynamic Background	Select to have the video analytic ignore periodic movement in the background of the scene. This setting is effective for outdoor scenes where weather can cause motion in the background.
Thermal Camera	Select if the camera is a thermal camera.
Detect Distant Objects	Select to have the video analytic attempt to detect objects in the distance.

Sensor Segments

Setting	Description
Show measures	Select to show the distance (meters) between reference points on the image.
Segment name	Type a name for the sensor segment.
Select a Device	Select the perimeter intrusion detection system that provides the data to the Senstar Sensor Fusion.
Select a Zone	Select the zone from the perimeter intrusion detection system that you want to configure the .
Range Start	Set the distance where the camera starts monitoring the fence. This value corresponds to the distance from the perimeter intrusion detection system.
Range End	Set the distance where the camera stops monitoring the fence. This value corresponds to the distance from the perimeter intrusion detection system.
Reference Points	Set how many reference points are on the sensor segment. The reference points need to map to equidistant fence posts or markers placed manually near the fence. The Senstar Sensor Fusion video analytic uses the reference points to generate accurate alarms.
Scale	Set the scale to adjust the distance between the reference points.
Confidence Level	Set how confident the video analytic must be to raise an alarm. The range for this setting is 1 to 10, where 1 is the lowest level of confidence and 10 is the highest level of confidence. A setting of 1 will generate more alarms and a setting of 10 will generate fewer alarms.
Buffer Zone Distance (m)	Set the distance (meters) from the sensor segment where the video analytic starts analyzing the scene. For example, if you set the buffer zone to 5 meters, the video analytic analyses any object that comes within 5 meters of the sensor segment.

Import / Export

Setting	Description
Import XML	Click this button to import a configuration XML file.
Export XML	Click this button to export the configuration XML file.

Senstar Symphony AI Object Detection and Tracking

The Senstar Symphony AI Object Detection and Tracking uses deep neural network machine learning to detect and track objects.

This video analytic intelligently classifies people and vehicles while effectively ignoring background movement. In addition this video analytic maintains detection in poor conditions.

The Senstar Symphony AI Overhead People Tracking and Counting uses a DNN model that is optimized for generic object detection and tracking.

Senstar Symphony AI Object Detection and Tracking Settings

Overview

Setting	Description
Analysis Resolution	Select the resolution that the video analytic uses. Note: This setting is only available if you do not select Automatically Select Resolution Based on Calibration.
Automatically Select Resolution Based on Calibration	Select to let the Server select the analysis resolution.
Use GPU instead of CPU	Select to use a supported GPU for analysis. This setting requires an NVIDIA GPU that supports CUDA 11.0 or later.
Analysis FPS	Select the frame rate that the video analytic uses.
Simple Mode	Select whether to hide or display the advanced settings. Warning: Changing the advanced settings can adversely affect the performance of the video analytic.

Processing Mask

Setting	Description
Drawing Mode	Select whether the paintbrush marks areas in the processing mask image to include (Analyze) or exclude (Ignore).
Size	Select the size of the paintbrush that you use to draw on the processing mask image.

Counting Line

Setting	Description
Create	On the image, click and hold the left mouse button, move the mouse to draw the new counting line, and release the left mouse button.
Delete	Click a counting line to select it and press Delete.
Move	Hold the CTRL key, click and hold the left mouse button on the counting line endpoint, and drag the endpoint to the

Setting	Description
Add a connected counting line	Click and hold the left mouse button on the endpoint of an existing counting line, move the mouse to draw the new counting line, and release the left mouse button.
Change the counting direction	Click an arrow on the counting line to toggle counting for that direction on and off.

Calibration

Setting	Description
Type	Select the type of calibration. Manual allows you to set the camera position. Automatic allows the video analytic to set the camera position and field of view. Uncalibrated runs the video analytic without camera position and field of view information.
Zoom In	Click to make the calibration diagram larger.
Zoom Out	Click to make the calibration smaller.
Field of view (degrees)	Define the horizontal field of view (in degrees) for the camera.
Pan (degrees)	Define the rotation around the vertical axis of the camera in relation to the scene.
Twist (degrees)	Define the rotation around the horizontal axis of the camera in relation to the scene.
Height (meters)	Define the vertical distance from the camera to the ground.
Distance (meters)	Define the horizontal distance from the camera to the center of the scene.

Sensitivity

Setting	Description
Maximum Hidden Seconds	Set how many seconds an object can remain hidden before the video analytic stops tracking the object. If, after this time elapses, the video analytic detects the object again, the video analytic treats the object as a new object (i.e., the video analytic gives the object a new ID).
Minimum Confidence	Set how confident the video analytic must be in object detection to classify the object.
Minimum Tracking Threshold	Set how confident the video analytic must be in object detection to track the object.

Senstar Symphony AI Overhead People Tracking and Counting

The Senstar Symphony AI Overhead People Tracking and Counting uses deep neural network machine learning to track and count people.

This video analytic intelligently detects and counts people using an overhead camera.

The Senstar Symphony AI Overhead People Tracking and Counting uses a DNN model that is optimized for overhead cameras.

Senstar Symphony AI Thermal Object Detection and Tracking Settings

Overview

Setting	Description
Analysis Resolution	Select the resolution that the video analytic uses. Note: This setting is only available if you do not select Automatically Select Resolution Based on Calibration.
Automatically Select Resolution Based on Calibration	Select to let the Server select the analysis resolution.
Use GPU instead of CPU	Select to use a supported GPU for analysis. This setting requires an NVIDIA GPU that supports CUDA 11.0 or later.
Analysis FPS	Select the frame rate that the video analytic uses.
Simple Mode	Select whether to hide or display the advanced settings. Warning: Changing the advanced settings can adversely affect the performance of the video analytic.

Processing Mask

Setting	Description
Drawing Mode	Select whether the paintbrush marks areas in the processing mask image to include (Analyze) or exclude (Ignore).
Size	Select the size of the paintbrush that you use to draw on the processing mask image.

Counting Line

Setting	Description
Create	On the image, click and hold the left mouse button, move the mouse to draw the new counting line, and release the left mouse button.
Delete	Click a counting line to select it and press Delete.
Move	Hold the CTRL key, click and hold the left mouse button on the counting line endpoint, and drag the endpoint to the
Add a connected counting line	Click and hold the left mouse button on the endpoint of an existing counting line, move the mouse to draw the new counting line, and release the left mouse button.
Change the counting direction	Click an arrow on the counting line to toggle counting for that direction on and off.

Calibration

Setting	Description
Type	Select the type of calibration. Manual allows you to set the camera position. Automatic allows the video analytic to set the camera position and field of view. Uncalibrated runs the video analytic without camera position and field of view information.
Zoom In	Click to make the calibration diagram larger.
Zoom Out	Click to make the calibration smaller.
Field of view (degrees)	Define the horizontal field of view (in degrees) for the camera.
Pan (degrees)	Define the rotation around the vertical axis of the camera in relation to the scene.

Setting	Description
Twist (degrees)	Define the rotation around the horizontal axis of the camera in relation to the scene.
Height (meters)	Define the vertical distance from the camera to the ground.
Distance (meters)	Define the horizontal distance from the camera to the center of the scene.

Sensitivity

Setting	Description
Maximum Hidden Seconds	Set how many seconds an object can remain hidden before the video analytic stops tracking the object. If, after this time elapses, the video analytic detects the object again, the video analytic treats the object as a new object (i.e., the video analytic gives the object a new ID).
Minimum Confidence	Set how confident the video analytic must be in object detection to classify the object.
Minimum Tracking Threshold	Set how confident the video analytic must be in object detection to track the object.

Senstar Symphony AI Thermal Object Detection and Tracking

The Senstar Symphony AI Thermal Object Detection and Tracking video analytic uses deep neural network machine learning to detect and track objects.

This video analytic intelligently classifies people and vehicles while effectively ignoring background movement when you are using thermal cameras.

The Senstar Symphony AI Thermal Object Detection and Tracking uses a DNN model that is optimized for thermal cameras.

Senstar Symphony AI Thermal Object Detection and Tracking Settings

Overview

Setting	Description
Analysis Resolution	Select the resolution that the video analytic uses. Note: This setting is only available if you do not select Automatically Select Resolution Based on Calibration.
Automatically Select Resolution Based on Calibration	Select to let the Server select the analysis resolution.
Use GPU instead of CPU	Select to use a supported GPU for analysis. This setting requires an NVIDIA GPU that supports CUDA 11.0 or later.
Analysis FPS	Select the frame rate that the video analytic uses.
Simple Mode	Select whether to hide or display the advanced settings. Warning: Changing the advanced settings can adversely affect the performance of the video analytic.

Processing Mask

Setting	Description
Drawing Mode	Select whether the paintbrush marks areas in the processing mask image to include (Analyze) or exclude (Ignore).
Size	Select the size of the paintbrush that you use to draw on the processing mask image.

Counting Line

Setting	Description
Create	On the image, click and hold the left mouse button, move the mouse to draw the new counting line, and release the left mouse button.
Delete	Click a counting line to select it and press Delete.
Move	Hold the CTRL key, click and hold the left mouse button on the counting line endpoint, and drag the endpoint to the
Add a connected counting line	Click and hold the left mouse button on the endpoint of an existing counting line, move the mouse to draw the new counting line, and release the left mouse button.
Change the counting direction	Click an arrow on the counting line to toggle counting for that direction on and off.

Calibration

Setting	Description
Type	Select the type of calibration. Manual allows you to set the camera position. Automatic allows the video analytic to set the camera position and field of view. Uncalibrated runs the video analytic without camera position and field of view information.
Zoom In	Click to make the calibration diagram larger.
Zoom Out	Click to make the calibration smaller.
Field of view (degrees)	Define the horizontal field of view (in degrees) for the camera.
Pan (degrees)	Define the rotation around the vertical axis of the camera in relation to the scene.
Twist (degrees)	Define the rotation around the horizontal axis of the camera in relation to the scene.
Height (meters)	Define the vertical distance from the camera to the ground.
Distance (meters)	Define the horizontal distance from the camera to the center of the scene.

Sensitivity

Setting	Description
Maximum Hidden Seconds	Set how many seconds an object can remain hidden before the video analytic stops tracking the object. If, after this time elapses, the video analytic detects the object again, the video analytic treats the object as a new object (i.e., the video analytic gives the object a new ID).
Minimum Confidence	Set how confident the video analytic must be in object detection to classify the object.

Setting	Description
Minimum Tracking Threshold	Set how confident the video analytic must be in object detection to track the object.

Multicasting

Multicasting allows numerous Windows Client instances to connect directly to cameras without requiring dedicated video streams for each Windows Client.

Multicasting can reduce the load on both the Server and camera when a large number of Windows Client instances need to display video from a camera. To use multicasting, both the cameras and the network switches must support multicasting. To check if a camera supports multicasting, check the Supported Video Devices list.

To configure multicasting, complete the following workflow:

1. Configure multicasting on the network switch.
2. Configure multicasting on the camera.
3. In the Server configuration interface, add the camera and select Multicast as the transport for the camera.
4. In the Windows Client interface, set the camera connection mode to Connect directly, if the camera supports it.

Edge Storage

Edge storage uses an SD card or other on-camera storage so that the camera continues recording when it cannot reach the Server, and so that the Windows Client can play back that video directly from the camera.

Edge storage covers gaps caused by network outages, Server downtime, and maintenance windows. The camera writes video to its local storage on its own schedule, independent of the Server. When the Server is reachable again, it can synchronize the recordings from the camera into the regular video archive. When the Server is not reachable, an authorized Windows Client can pull the video directly from the camera over an ONVIF connection.

Before you begin:

- Install supported storage media (typically an SD card) in the camera.
- Format the storage media using the camera's web interface.
- Verify that the camera supports ONVIF Profile G (edge recording and retrieval).

Enable Edge Storage on a Camera

1. In the Server configuration interface, click Devices > Cameras.
2. Select the camera and click Edit.
3. In the Edge Storage section, select Enable Edge Storage.
4. Select the recording mode:
   a. Continuous records video to the camera's storage at all times.
   b. On Connection Loss records video only when the camera cannot reach the Server.
5. Set the recording schedule and retention.

6. Click Save.

Synchronize Edge Recordings with the Server

When the Server can reach the camera again, it copies the recordings that were made on the camera into the regular video archive. The synchronized video appears on the timeline alongside server-recorded video.

1. In the Server configuration interface, click Devices > Cameras.
2. Select the camera and click Edit.
3. In the Edge Storage section, select Synchronize on Reconnect.
4. Click Save.

Pull Edge Recordings to the Windows Client

When the Server is unavailable, the Windows Client can connect directly to the camera and play video from edge storage.

1. In the Windows Client, open the camera in a view panel.
2. On the timeline, select Edge as the playback source.
3. Drag the timeline indicator to the time that you want to view.

The Windows Client streams the requested time range from the camera over ONVIF. Playback uses the recordings on the camera and is independent of the Server.

Browsers

The Windows Client can display a Web page in a camera view panel.

When you add a browser in the Server configuration interface, it appears in the Windows Client interface on the device tree under the Browser heading. You can display the webpage in a camer view panel.

The Windows Client uses the Microsoft Edge browser to render the Web pages in the camera view panels, but the panel does not include any browser controls (navigation, address field, settings, etc.).

Add a Browser

1. In the Server configuration interface, click Devices > Browsers.
2. Click Add Browser.
3. In the Name field, type a name for the browser to appear in the Windows Client interface.
4. In the Url field, type the address of the page.
5. Click Save.

Find a Browser

To quickly find a specific browser, use filters and sorting.

Filter

You can filter the browser list using the following filters:

- browser name (Name)

- browser address (Url)
    1. In the Server configuration interface, click Devices > Browsers.
    2. Click the magnifying glass to make the filter text fields visible.
    3. Define the filter criteria.
    4. Click Apply filter.

Sort

You can sort the list of browsers by clicking the column name. Clicking the column name toggles between ascending and descending order.

Clear

To reset the filter and restore the list of browsers, click Clear Filter.

Templates

A template is a collection of configuration settings that you can apply to cameras.

If you apply a template to a camera, some of the configuration settings for the camera are restricted. For example, you cannot add an additional stream to a camera if you apply a template to a camera.

Find a Template

To quickly find a specific template, use filters and sorting.

Filter

You can filter the template list using the following filter:

- template name (Name)
    1. In the Server configuration interface, click Devices > Templates.
    2. Click the magnifying glass to make the filter text fields visible.
    3. Define the filter criteria.
    4. Click Apply filter.

Sort

You can sort the list of templates by clicking the column name. Clicking the column name toggles between ascending and descending order.

Clear

To reset the filter and restore the list of templates, click Clear Filter.

Template Settings

General

Setting	Description
Failover enabled	Select and specify whether failover is enabled or disabled.
Support Direct Connect	Select whether the camera allows direct connections through a browser.
Enable Audio Input	Select whether the camera can record audio.

Setting	Description
Enable Audio Output	Select whether the camera can play audio.
Rotate Degrees	Select whether to rotate the footage from the camera.
Change frame rate on alarm to	Select to change the frame rate of the video from the camera.
Limit the number of days video is stored	Specify the maximum time (days) for which the Server keeps the video.
PTZ Maximum Locked Time	Specify the maximum time (minutes) that PTZ cameras can remain in a locked state.
Enable panoramic technology	Select to enable panoramic technology for the camera and specify the panoramic type and camera position.

Stream

Setting	Description
Resolution	Specify the resolution for the camera.
Frame Rate	Specify the frame rate for the camera.
Video Codec	Select the video codec that the camera uses.
Bitrate	Specify the bitrate (in kilobits per second) for the camera.
Key frame interval	Specify the key frame interval.
Video Recording	Select when the camera records video.
Pre Event	Specify how much video (in seconds) the camera records before an event.
Post Event	Specify how much video (in seconds) the camera records after an event.
Schedule	Select to set the schedule.
Audio recording	Select when the camera records audio.

Create a Template

Create a template in the Server configuration interface.

1. Click Devices > Templates.
2. Click Add Template.
3. In the Name field, type a name for the template.
4. Configure the settings for the template.
5. Click Save.

Copy a Template

You can copy a template to use it as the starting point for a new template.

1. In the Server configuration interface, click Devices > Templates.
2. Select the template and click Clone.
3. In the Name field, type a name for the template. By default, the name of the new template include Clone of

before the original template name.

1. Configure the settings for the template.
2. Click Save.

Hardware

The Hardware tab enables Sympony to connect and control specific devices such as intrusion panels. For managing device networks, such as access control readers or perimeter sensors, see Integrations.

The Server supports the following manufacturers:

- Bosch
- CommBox
- Senstar (legacy only, see Integrations)

Add a Hardware Device

You can add DIO, access control, and Senstar Thin Client devices to the Server from the Hardware tab in the Server configuration interface.

1. In the Server configuration interface, click Devices > Hardware.
2. Click Add Hardware.
3. In the Manufacturer list, select the manufacturer of the hardware device. If the manufacturer is not in the list, try adding the hardware device as an integration (Add an integration) or as an access control device (Add an access control device).
4. In the General section, specify the settings for the hardware device. The settings are specific to both the manufacturer and the type of device.
5. Click Connect to Device to test the connection.
6. Click Save.

Find a Hardware Device

To quickly find a specific hardware device, use filters and sorting.

Filter

You can filter the hardware list using the following filter:

- hardware ID (ID)
- hardware brand (Brand)
- hardware name (Name)
- IP address of the hardware device (IP Address)
- groups to which the hardware device belongs (Groups)
    1. In the Server configuration interface, click Devices > Hardware.
    2. Click the magnifying glass to make the filter text fields visible.
    3. Define the filter criteria.
    4. Click Apply filter.

Sort

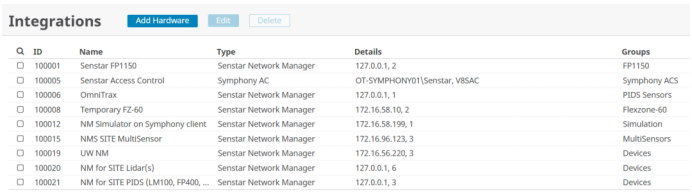
You can sort the list of hardware devices by clicking the column name. Clicking the column name toggles between ascending and descending order.

Clear

To reset the filter and restore the list of hardware devices, click Clear Filter.

Integrations

The Integrations tab in the Server configuration interface is where you add security solutions to the Server.



The Integrations tab allow you to add multiple security solutions to the Server. For example, you can add multiple Senstar Symphony Access Control and Senstar Network Manager instances to the Server concurrently.

Add Integration Hardware

What it is

An integration connects a third-party system to the Server. Once integrated, the system's devices and events become first-class citizens in Senstar Symphony: they appear in the device tree, their events can trigger rules, and operators can see them in the Windows Client.

Integrations differ from raw hardware in that the Server speaks the third party's protocol natively and understands its event model. Use an integration when one exists for your device; fall back to the generic Add a Hardware Device path only when it does not.

When you'd use it

- You are deploying an access control system and want door events to trigger rules.
- You are deploying a perimeter intrusion sensor (fence sensor, radar) and want its detections to generate alarms.
- You have DIO hardware whose inputs should trigger rules and whose outputs should be driven by action sets.

Prerequisites

- Permission to edit device configuration.
- Network reachability from the Server to the third-party device or its controller (IP address and port).
- The device's credentials (username, password, API key, or certificate as required by the manufacturer).
- The manufacturer's documentation for protocol-specific fields, event mappings, and firmware requirements.

Procedure

1. In the Server configuration interface, click **Devices** > **Integrations**.
2. Click **Add Hardware**.
3. In the **Manufacturer** list, select the manufacturer. If the manufacturer is not listed, try Add a Hardware Device (generic) or Add an Access Control Device instead.
4. In the **General** section, complete the connection fields. Most manufacturers require some combination of:
   - **Address or hostname** — how the Server reaches the device.
   - **Port** — the manufacturer's protocol port (check manufacturer documentation).
   - **Credentials** — username and password, or API key / token.
   - **Polling or heartbeat interval** — how often the Server contacts the device.
   - **Event mapping or channel selection** — which of the device's events or channels the Server should surface.

     Required fields and valid values are manufacturer-specific. Refer to the manufacturer's documentation for what is required for your hardware model and firmware version.
5. Click **Connect to Device** to verify the settings. A successful test confirms the address, credentials, and protocol are correct. Fix any errors before continuing — an integration that cannot connect will not surface events to rules.
6. In the **Groups** list, select the Windows Client device groups to which this integration belongs. Group membership controls where the device appears in the device tree and which security profiles can see it.
7. Click **Save**.

After adding

The integration's events are now available in the events catalogue. To turn an event into an alarm or action, create a rule that uses the event.

Related tasks

- Associate a Camera with a Source — link integration events to a camera so operators see video alongside the event.
- Add an Access Control Device
- Senstar Network Manager — dedicated integration for Senstar perimeter sensors.
- Senstar Symphony Access Control

Find Integration Hardware

To quickly find a specific integration, use filters and sorting.

Filter

You can filter the integration list using the following filter:

- integration ID (ID)
- integration name (Name)
- integration type (Type)

- information about the integration (Details)
- groups to which the integration belongs (Groups)

1. In the Server configuration interface, click Devices > Integrations.
2. Click the magnifying glass to make the filter text fields visible.
3. Define the filter criteria.
4. Click Apply filter.

Sort

You can sort the list of integrations by clicking the column name. Clicking the column name toggles between ascending and descending order.

Clear

To reset the filter and restore the list of integrations, click Clear Filter.

Device Aliases

You can rename the sensors, commands, events, and states on a hardware or integration device so that they appear with meaningful, descriptive names in the device tree, device tree, rules, and alarms.

By default, devices expose their sensors, commands, events, and states using the labels reported by the device, which are often generic (for example, `Input 1`, `Relay 2`). You can replace these labels with aliases that describe the role of the item at your site (for example, `Front Door Contact` or `Lobby Strobe`).

To use a device alias:

1. In the Server configuration interface, click Devices > Device Tree.
2. Expand the device.
3. Right-click the sensor, command, event, or state that you want to rename.
4. Click Rename.
5. Type the alias and press Enter.

To restore the original label, right-click the item, click Rename, clear the alias, and press Enter.

Symphony AC

Senstar Symphony Access Control is a standalone application that integrates with the Server to manage hardware controllers used for access control, intrusion, and HVAC systems.

You can integrate the Senstar Symphony Access Control with the Server to use events from Senstar Symphony Access Control nodes for alarming and monitoring.

For the Server to receive alarms from the Senstar Symphony Access Control, the regional and time settings on the computer that hosts the Senstar Symphony Access Control must match the regional and time settings on the computer that hosts the Server.

Connect to Senstar Symphony Access Control

Connect the Server to the Senstar Symphony Access Control to use events from the Senstar Symphony Access Control to trigger actions.

1. In the Server configuration interface, click Devices > Integrations.

2. Click Add Hardware.
3. In the Device Type list, select Symphony AC.
4. In the Name field, type a meaningful name for the Senstar Symphony Access Control. This name will appear in the device list in the

Server configuration interface

and the device tree in the

Windows Client interface

.

1. In the Database Server field, type the full address of the Microsoft SQL Server instance for the Senstar Symphony Access Control. For example,

COMPUTER1\SQLEXPRESS2012

.

1. In the Database Name field, type the name of the Senstar Symphony Access Control database.
2. In the Username field, type the username that the Server uses to access the Senstar Symphony Access Control database.
3. In the Password field, type the password that the Server uses to access the Senstar Symphony Access Control database.
4. Click Connect to Device.
5. In the Sources list, select the nodes that you want to add to the Server. If you want your selection to apply to all child nodes, click the

Cascade Selection

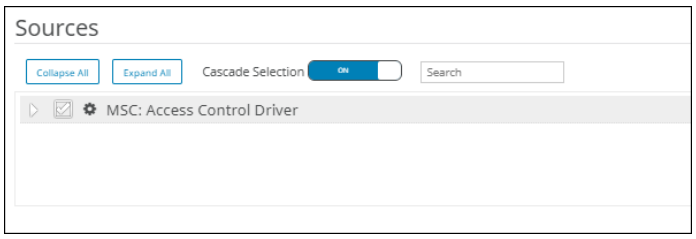
toggle switch to turn it on. To prevent your selection from affecting other nodes, click the

Cascade Selection

toggle switch to turn it off. To search for a node, type the terms in the

Search

field—the source list is filtered by the search terms.



1. In the Groups list, select the device tree folder in which the Senstar Symphony Access Control appears.
2. Click Save.

Senstar Symphony Access Control Settings

General

Setting	Description
Name	Type a meaningful name for the Senstar Symphony Access Control instance. This name appears in the device tree.
Type	This field displays the type of integration. You select the type when you add hardware.
Database Server	Type the full address of the Microsoft SQL Server instance for the Senstar Symphony Access Control.
Database Name	Type the name of the Senstar Symphony Access Control database.
Username	Type the username that the Server uses to access the Senstar Symphony Access Control database.
Password	Type the password that the Server uses to access the Senstar Symphony Access Control database.
Import XML	Click to import an XML file that contains configuration information.
Export XML	Click to export an XML file that contains configuration information.
Show XML	Click to view the configuration information.

Connect

Setting	Description
Save and Reconnect	Click to save the changes to the general settings and try to connect to the Senstar Symphony Access Control.

Sources

Setting	Description
Collapse All	Click to collapse the source tree to display only the top levels.
Expand All	Click to expand the source tree to display all levels.
Cascade Selection	Toggle on to automatically select all of the lower levels when you select a device. Toggle off to only select the device that you select.
Search	Type search terms to filter the source list.

Senstar Network Manager

The Senstar Network Manager connects Senstar security networks to the Server. The Server supports the Senstar Network Manager 2.32 and later.

You can integrate the Senstar Network Manager with the Server to use events from Senstar Network Manager nodes for alarming and monitoring. You use the Integration tab in the Server configuration interface to connect to and configure the Senstar Network Manager.

Devices connected to the Senstar Network Manager appear in the device tree in the Windows Client interface. In addition, the device tree displays the state of devices attached to the Senstar Network Manager.

You can connect multiple instances of the Senstar Network Manager to the Server.

Automatically Generated Rules

When you add a Senstar Network Manager integration, the Server can automatically generate rules for the sensors and devices connected to the Senstar Network Manager. Generating rules automatically can save time when adding Senstar Network Manager with numerous devices or sensors. By default, the Server generates sensor alarms for Trouble, Alarm, and Tamper incidents; and Communication Fail, Communication Fault, Diagnostic Warnings, Diagnostic Fatal, and Enclosure Tamper incidents.

When you automatically generate rules, the Server selects to raise alarms on the first camera by camera ID. If you do not have any cameras connected to the Server, the Server selects to raise alarms on the first map alphabetically. If you do not have cameras and maps connected to the Server, the Serverselects to raise alarms on all devices.

You can configure automatic rule generation when you add the Senstar Network Manager as an integration to the Server or you can edit the integration afterwards.

If you edit the Senstar Network Manager integration generation settings and the Automatically generate rules checkbox is selected, the Server will delete the existing automatically generated rules and generate new rules. To retain your original automatically generated rules, clear the Automatically generate rules checkbox before saving your changes.

Connect to Senstar Network Manager

Connect the Server to the Senstar Network Manager to use events from the Senstar Network Manager to trigger actions.

1. In the Server configuration interface, click Devices > Integrations.
2. Click Add Hardware.
3. In the Device Type list, select Senstar Network Manager.
4. In the Name field, type a meaningful name for the Senstar Network Manager. This name will appear in the device list in the

Server configuration interface

and the device tree in the

Windows Client interface

.

1. In the IP Address field, type the IP address of the Senstar Network Manager.
2. In the Secondary IP Address field, type the IP address of a secondary (redundant) Senstar Network Manager.
3. In the Unit ID field, type the ID of the Senstar Network Manager.
4. Click Connect to Device.
5. In the Sources list, select the nodes that you want to add to the Server. If you want your selection to apply to all child nodes, click the

Cascade Selection

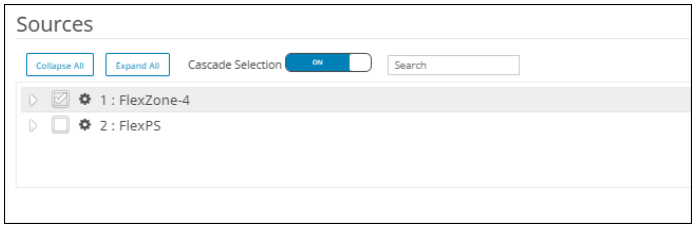
toggle switch to turn it on. To prevent your selection from affecting other nodes, click the

Cascade Selection

toggle switch to turn it off. To search for a node, type the terms in the

Search

field—the source list is filtered by the search terms.



1. In the Rules section, configure if and how the Server automatically generates rules for the Senstar Network Manager integration. image::air_network_manager_connect_rules.png[]

You can automatically create both sensor rules and device rules.

For sensor rules, you can select your level of granularity: global, device, or sensor. If you select Global rule, the Server creates a single rule for all of the sensors that you select. If you select Device alarm rules, the Server creates a rule for each of the devices that you select. If you select Sensor alarm rules, the Server creates a rule for each of the sensors that you select. Additionally, you can select to combines all incident types into a single rule or you can create separate sensor rules for each incident type.

For device rules, you can choose to create a global diagnostic rule for all of the devices that you select or you can choose to create a device diagnostic rule for each device that you select.

1. In the Groups list, select the device tree folder in which the Senstar Network Manager appears.
2. Click Save.

Senstar Network Manager Settings

General

+

+

Setting	Description
Name	Type a meaningful name for the Senstar Network Manager instance. This name appears in the device tree.
Type	This field displays the type of integration. You select the type when you add hardware.
IP Address	Type the IP address of the Senstar Network Manager.
Secondary IP Address	Type the secondary IP address of the Senstar Network Manager. The secondary IP address is the IP address of the secondary Senstar Network Manager when redundancy is configured.

Setting	Description
Unit ID	Type the unit ID of the Senstar Network Manager. The unit ID is set when the Senstar Network Manager is installed. Contact the Senstar Network Manager administrator for more information.
Import XML	Click to import an XML file that contains configuration information.
Export XML	Click to export an XML file that contains configuration information.
Show XML	Click to view the configuration information.

Connect

Setting	Description
Save and Reconnect	Click to save the changes to the general settings and try to connect to the Senstar Network Manager.

Sources

Setting	Description
Collapse All	Click to collapse the source tree to display only the top levels.
Expand All	Click to expand the source tree to display all levels.
Cascade Selection	Toggle on to automatically select all of the lower levels when you select a device. Toggle off to only select the device that you select.
Search	Type search terms to filter the source list.

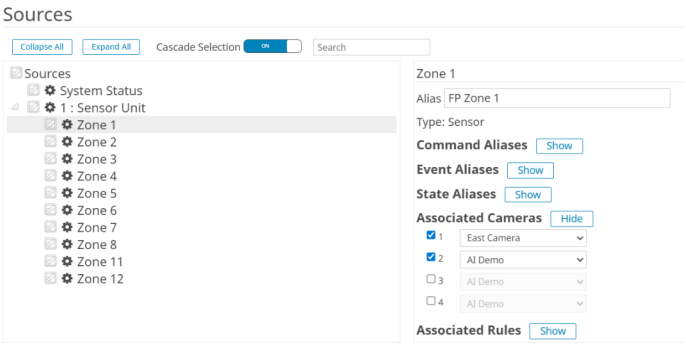
Rules

Setting	Description
Automatically generate rules	Select to make the Server automatically generate rules for the Senstar Network Manager integration.
No sensor rules	Select to prevent the Server from automatically generating rules for sensors attached to the Senstar Network Manager or to make the Server delete any existing automatically generated sensor rules.
Global rule	Select to make the Server automatically generate a single rule that applies to all of the sensors attached to the Senstar Network Manager. You can create a single rule for all incident types (grouped) or create rules to each incident type (separate).
Device alarm rules	Select to make the Server automatically generate a separate rule for each device that you select in the Sources list. You can create a single rule for all incident types (grouped) or create rules to each incident type (separate).
Sensor alarm rules	Select to make the Server automatically generate a separate rule for each sensor that you select in the Sources list. You can create a single rule for all incident types (grouped) or create rules to each incident type (separate).

Setting	Description
No diagnostic rules	Select to prevent the Server from automatically generating diagnostic rules for devices attached to the Senstar Network Manager or to make the Server delete any existing automatically generated device rules.
Global diagnostic rule	Select to make the Server automatically generate a single diagnostic rule that applies to all of the devices attached to the Senstar Network Manager.
Device diagnostic rules	Select to make the Server automatically generate a separate diagnostic rule for each device that you select in the Sources list.

Associate a Camera with a Source

You can associate up to four cameras with a hardware source so that you can monitor the area in which the hardware source is located.



1. In the Server configuration interface, click Devices > Integrations.
2. Select the hardware.
3. Click Edit.
4. In the Sources section, select the hardware source to which you want to associate cameras. If you select multiple hardware sources and you want to associate the cameras with all of the selected sources, click the

Selected

box.

1. Beside Associated Cameras, click Show.
2. For each camera that you want to associate, select the camera spot and pick the camera from the list. image::air_server_integrations_sources_camera_associate_01.png[]
3. Click Save.

Access Devices

The Server can use data from access control devices to trigger events.

You can use the Server configuration interface to integrate an access control device with the Server. Once you have added the access control device, you can select the access control devices in the solution to use as sources for events.

The Server supports the following manufacturers:

- Axiom
- Axis PACS
- Gallagher
- JCI P2000
- Siemens SPC
- Software House

Add an Access Control Device

You can add access control devices to the Server from the Access Devices tab in the Server configuration interface.

In some cases, you might need to perform additional tasks on the access control device. For information on a specific access control device, search the Senstar Xnet for the manufacturer of the access control device.

1. In the Server configuration interface, click Devices > Access Devices.
2. In the Manufacturer list, select the manufacturer of the access control system. The fields that appear depend on the manufacturer that you select. If the manufacturer is not in the list, try adding the access control device as hardware (Add hardware) or as an integration (Add an integration).
3. In the Server list, select the Server to which you want to add the access control device.
4. In the IP Address field, type the IP address of the access control system.
5. In the Username and Password fields, type the credentials for the access control system.
6. Click Connect.
7. In the Sources list, select the devices in the access control system that can trigger events on the Server.
8. Click Save.

Device Tree

The device tree organizes and displays devices in the Windows Client interface.

Find a Device

To quickly find a specific device, use a filter.

Filter

Use the filter field at the top of the device tree to narrow the list to devices whose name matches the entered text.

Clear

To reset the filter and restore the list of devices, click Clear Filter.

Manage Device Groups

You can organize the devices in groups. Changes that you make appear immediately in the Windows

Client interface.

Create a Device Group

You can use device groups to organize your devices.

1. In the Server configuration interface, click Devices > Device Tree.
2. Click Create Group. A new folder named

New Group

appears in the device tree.

1. Type a name for the group and press Enter.
2. Drag devices into the group.
3. Click Save.

Modify a Device Group

You can change the name of the device group or add and remove devices from the device group.

1. In the Server configuration interface, click Devices > Device Tree.
2. To modify the name of the device group, perform the following tasks:
   a. Select the device group.
   b. Click Edit.
   c. Type a name for the device group.
   d. Click Save.
3. To move a device to the device group, perform the following tasks:
   a. Click and drag a device to the device group.
   b. Click Save.

Copy a Device Group

You can copy a device group to act as a template for a new device group.

1. In the Server configuration interface, click Devices > Device Tree.
2. Select a device group.
3. Click Clone.
4. Type a name for the new device group.
5. Click Save.

Delete a Device Group

You can delete a device group from the device tree. When you delete a device group, the devices in the group move to the root folder of the device tree.

1. In the Server configuration interface, click Devices > Device Tree.
2. Select a device group.
3. Click Delete.

Associate Cameras with Sensors and Zones

You can associate one or more cameras and rules with a sensor or zone so that the Windows Client displays the related video and rules whenever the sensor or zone is selected.

When a sensor or zone activates, an operator can quickly bring up the video that covers the area without first having to find the right camera in the device tree. The association is stored on the Server and applies to every Windows Client that connects to the server.

Associate Cameras with a Sensor or Zone in the Device Tree

1. In the Server configuration interface or the Windows Client, open the device tree.
2. Right-click the sensor or zone.
3. Click Associate Cameras.
4. Select one or more cameras from the list.
5. Click Save.

Associate Rules with a Sensor or Zone

1. In the device tree, right-click the sensor or zone.
2. Click Associate Rules.
3. Select one or more rules from the list.
4. Click Save.

Associate Cameras with a Sensor or Zone on a Map

1. In the Windows Client, open the map that contains the sensor or zone.
2. Right-click the sensor or zone icon.
3. Click Associate Cameras.
4. Select one or more cameras from the list.
5. Click Save.

After you associate cameras with a sensor or zone, the associated cameras appear in the right-click menu for that sensor or zone. Selecting an associated camera opens the camera in the active view panel.

Carousels

Carousels are configurations for video panels in the Windows Client interface that can loop through multiple cameras and display video for a set time.

In the Server configuration interface, you add cameras to the carousel and then set how long the video panel in the Windows Client interface displays video before moving to the next camera. The device tree in the Windows Client interface lists all available carousels. You can open a carousel in any video panel.

Find a Carousel

To quickly find a specific carousel, use filters and sorting.

Filter

You can filter the carousel list using the following filter:

- carousel name (Name)
    1. In the Server configuration interface, click Devices > Carousels.
    2. Click the magnifying glass to make the filter text fields visible.
    3. Define the filter criteria.
    4. Click Apply filter.

Sort

You can sort the list of carousels by clicking the column name. Clicking the column name toggles between ascending and descending order.

Clear

To reset the filter and restore the list of carousels, click Clear Filter.

Manage Carousels

You can create, modify, copy, and delete carousels.

Create a Carousel

1. In the Server configuration interface, click Devices > Carousels.
2. Click Add Carousel.
3. Type a name for the carousel.
4. In the Available Cameras on Servers list, select the cameras to add to the carousel and click Add Selected.
5. In the Camera list, drag and drop the cameras to define the carousel order and define the number of seconds for which the camera view panel displays the camera.
6. Click Save.

Modify a Carousel

1. In the Server configuration interface, click Devices > Carousels.
2. Select the carousel and click Edit.
3. Perform any of the following tasks:
    a. To modify the name of the carousel, type a new name in the Name field.
    b. To add a camera to the carousel, select the camera in the Available Cameras on Servers list and click Add Selected.
    c. To remove a camera from the carousel, highlight the camera in the Camera list and click the X button.
    d. To modify the amount of time for each camera, type new values in the Seconds fields.
4. Click Save.

Copy a Carousel

1. In the Server configuration interface, click Devices > Carousels.
2. Select the carousel and click Clone.
3. Modify the carousel.

4. Click Save.

Delete a Carousel

1. In the Server configuration interface, click Devices > Carousels.
2. Select the carousel and click Delete.

Security

Security settings on the Server allow you to configure authentication for users, set and change permissions for users and groups quickly, and add watermarks to video.

You access the security settings on the Security tab in the Server configuration interface. The Security tab includes the Users, Groups, Security Profiles, and Logins tabs.

Users

Users are individuals with permission to access and use the Server, Windows Client, and the Web Client.

Add a User

What it is

A user in Senstar Symphony is an identity that can sign in to the Server or a client application. Users inherit permissions from the groups they belong to, not from themselves directly — adding a user is a matter of creating the identity and placing it in the right groups.

If your site uses Active Directory, prefer associating an Active Directory group over managing users one by one in the Server.

When you'd use it

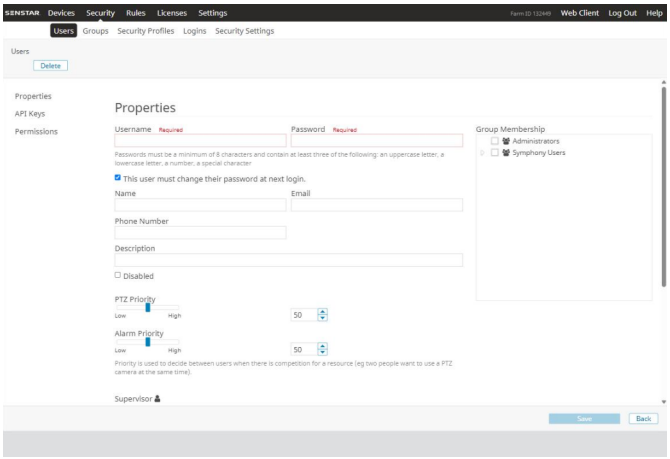
- A new person joins the team and needs to sign in.
- You are seeding a fresh deployment with service accounts, shift operators, and administrators.
- You need a throwaway account for a short-term contractor — set **Disabled** with a reason when the engagement ends rather than deleting the record, so reports remain coherent.

Prerequisites

- Permission to add users (see User Permissions).
- The groups that will hold the new user already exist.
- If the user will supervise others, the supervisor group exists.

Procedure

1. In the Server configuration interface, click **Security** > **Users**.
2. Click **Add**.
3. Enter the user's identity fields (name, sign-in name, password, email, phone, description).



4. (Optional) To disable the user without deleting the record, select **Disabled** and type a reason. Disabled users cannot sign in but remain in reports and audit logs.
5. Set **PTZ Priority**. When two users try to control the same PTZ camera simultaneously, the user with the higher priority wins; a user with equal or lower priority is blocked until the higher-priority user releases control. The slider ranges from 1 (lowest) to 10 (highest). Use 10 only for supervisors or dispatchers who must always be able to take control.
6. Set **Alarm Priority**. When two-stage enhanced alarms are in use, the user with the higher priority sees the alarm first. Use the same 1–10 scale; most operators sit at the default.
7. In **Group Membership**, select the groups the user belongs to. Permissions come from these groups — a user with no group memberships can sign in but can do almost nothing.
8. In **Supervisor**, select the group whose members are allowed to impersonate this user. Leave blank if the site does not use supervisor impersonation.
9. Click **Save**.

After adding

Share the sign-in details with the user through your organisation's secure channel (not email in the clear). If site policy requires a change on first login, use Force a Password Change.

Related tasks

- Copy a User — faster than re-entering fields for a similar user.
- Add a User to a Group
- Force a Password Change
- User Permissions

Copy a User

You can copy a user to use it as a template for a new user.

1. In the Server configuration interface, click Security > Users.
2. Select a user and click Clone.
3. Enter information for the user.
4. To disable the user, select the Disabled box and type a reason.

5. Using the Priority slider or text box, define a priority for the user to help resolve resource conflicts.
6. In the Group Membership pane, select the groups to which the user belongs.
7. In the Supervisor list, select the group that contains users who can impersonate this user.
8. Click Save.

Add a User to a Group

You can add a user to a group at any time to grant the permissions for that group to a user.

1. In the Server configuration interface, click Security > Users.
2. Select a user and click Edit.
3. In the Group Membership pane, select the group to which you want to add the user.
   image::air_server_user_group_add_8_group_membership.png[]
4. Click Save.

Force a Password Change

You can force a user to change a password when the user next logs in to the Server, the Windows Client, or the Web Client.

1. In the Server configuration interface, click Security > Users.
2. Select the user and click Edit.
3. Select This user must change their password at next login.
4. Click Save.

When the user next logs in, the user is prompted to change the password.

Supervisor Impersonation

Supervisor impersonation allows two users with lesser permissions to log in simultaneously to impersonate a single user with greater permissions.

Supervisor impersonation is the application of the two-person rule to add additional security to the Windows Client. You can use this feature to ensure that two people are present when a user performs an operation in the Windows Client interface.

Configure a User for Supervisor Impersonation

To use supervisor impersonation, you must configure a user the two other users can impersonate.

1. In the Server configuration interface, click Security > Users.
2. Perform one of the following tasks:
   - To create a new user for supervisor impersonation, click Add.
   - To use an existing user for supervisor impersonation, select the user and click Edit.
3. In the Properties section, select Enable Two Person Rule.
4. In each of the group lists, select the groups from which the users can impersonate the user.
5. Click Save.

Enable Supervisor Impersonation

To make the supervisor impersonation option available in the Windows Client, you must add the feature to the configuration file.

1. Open the acc.ini file at %appdata%\Senstar8.
2. In the `[Main]` section, add the following text:

```
ShowTwoManRule=True
```

1. Save and close the acc.ini file.

The

Supervisor Logon

option is visible on the login page for the

Windows Client

.

Impersonate a Supervisor

Two users can log in to the Windows Client to impersonate a user and gain access to additional functionality.

1. In the Windows Client interface, click the user name and then click Log On/Switch User to open the Logon window.
2. In the Server list, select the Server for which you have configured supervisor impersonation.
3. Type the credentials for the first user.
4. Select the Supervisor Logon box.
5. Type the credentials for the second user.
6. Type the name of the supervisor-impersonation user.
7. In the Reason field, type the reason for impersonating a supervisor.
8. Click OK.

Groups

Groups are collections of users with similar permissions for the Server and Windows Client.

Groups can contain users that you create and maintain on the Server or, if you use Active Directory authentication, groups can synchronize membership with an associated Active Directory group.

Add a Group

You can add a group to create a collection of customized permissions for users.

1. In the Server configuration interface, click Security > Groups.
2. Click Add.
3. Type a name for the group.
4. Select the parent group.

5. Type a description for the group.
6. To associate the group with an Active Directory group, perform the following steps:
   a. Click Associate.
   b. Search for and select the Active Directory group.
   c. Click OK.
7. Click Save.

After you create a group, you need to set the permissions for each security profile that you use.

Copy a Group

You can copy a group to use it as a template for a new group.

When you copy a group, the permissions for all of the security profiles are cloned to the new group.

1. In the Server configuration interface, click Security > Groups.
2. Select a group and click Clone.
3. In the Name field, type a name for the group.
4. In the Group Parents field, select the groups that act as parent groups.
5. In the Description field, type a description for the group.
6. To associate the group with an Active Directory group, perform the following steps:
   a. Click Associate.
   b. Search for and select the Active Directory group.
   c. Click OK.
7. Click Save.
8. In the Group Membership pane, select the groups to which the user belongs.
9. In the Supervisor list, select the group that contains users who can impersonate this user.
10. Click Save.

Security Profiles

A security profile is a collection of permissions that you can apply across all users and groups. Security profiles make it easy to switch the permissions for users and groups in the Server.

Typically, you add security profiles to the Server to be more responsive to external changes. Each user and user group can have a specific set of permissions within each security profile. When you activate a security profile, all users and user groups switch to the permissions in that security profile.

Security Profiles Workflow

1. Add a security profile to create a new container for user and group permissions.
2. Set the security profile permissions to define the permissions that users and groups have when the security profile is active.
3. Activate the security profile to apply the permissions to users and groups.

Use-case Example

For example, you can create a default security profile and a fire response security profile. For normal operation, the default security profile is active and the permissions assigned to the users and user groups are also active. In the case of a fire incident, you activate the fire response security profile that grants a fire response group permission to view all cameras in the facility, broadcast audio from cameras, and search footage to help facilitate the emergency response. When the fire response team resolves the incident, you reactivate the default security profile and return to normal operation.

Add a Security Profile

You can copy an existing security profile to add another security profile to the Server.

The Server includes the Default security profile. You can use this security profile as a template for other security profiles.

1. In the Server configuration interface, click Security > Security Profiles.
2. Select a security profile and click Copy.
3. In the Name field, type a name for the security profile.
4. (Optional) In the Description field, type a description for the security profile.
5. Click Save.

Set the Security Profile Permissions

You can set the security profile permissions for a user or group. When you activate the security profile, the Server applies the permissions associated with the security profile to the users and groups.

In most cases, you will set the permissions for the default security profile. However, if you use multiple security profiles, you might need to set custom permissions for each security profile.

If you want to make extensive changes to the default security profile, consider creating a new security profile for regular use and keep the default security profile as a template for addition security profiles.

1. In the Server configuration interface, perform one of the following tasks:
   - To set the security profile permissions for a user, click Security > Users.
   - To set the security profile permissions for a group, click Security > Groups.
2. Select a user or group and click Edit.
3. In the Security Profile list, select the security profile for which you want to set permissions.
4. In the permissions tree, click the permission category that you want to set.
   image::air_server_security_profile_permissions_set_8_permissions.png[]
5. In the permission list, set the permissions.
   image::air_server_security_profile_permissions_set_8_permission_list.png[]
6. Click Save.

Site Permissions

General

Permission	Description
Change IO State	This permissions allows a user to change the IO state of devices in the Windows Client interface.
Configure Maps	This permission allows a user to configure maps in the Windows Client interface.
Connect	This permission allows a user to connect to servers.
Delete Footage	This permission allows a user to delete video footage in the Windows Client interface.
Export Video	This permission allows a user to export video from the Windows Client interface.
Get Logs	This permission allows a user to view and download logs in the Windows Client interface.
Manage Bookmarks	This permission allows a user to create and edit bookmarks in the Windows Client interface.
Manage Services	This permission allows a user to start, stop, and restart Senstar Symphony services in the Windows Client interface.
Play Sounds	This permission allows a user to play audio in the Windows Client interface.

Configuration

Permission	Description
Add Devices	This permission allows a user to add devices in the Server configuration interface.
Change Access Control	This permission allows a user to configure access control devices in the Server configuration interface.
Change Settings	This permission allows a user to change the general settings in the Server configuration interface.

Alarm

Permission	Description
Add Alarm	This permission allows a user to create alarms in the Windows Client interface.
Manage Alarms	This permission allows a user edit and delete alarms in the Windows Client interface.
Mark Alarms	This permission allows a user to mark alarms as an alarm, false alarm, or real actionable in the Windows Client interface.
View Alarms	This permission allows a user to view alarms in the Windows Client interface.

Backup

Permission	Description
Backup	This permission allows a user to configure backup options in the Server configuration interface.
Restore	This permission allows a user to restore a configuration in the Server configuration interface.

Face Recognition

Permission	Description
Change faces/people	This permission allows a user to edit faces and associated information for the Face Recognition video analytic in the Windows Client interface.
Manage Face Lists	This permission allows a user to add faces to or remove faces from a list.
View faces/people	This permission allows a user to view faces and associated information for the Face Recognition video analytic in the Windows Client interface.

LPR

Permission	Description
Add or Edit License Plate Metadata	This permission allows a user to add or edit license plate information for the Automatic License Plate Recognition video analytic in the Windows Client interface.
Delete License Plate	This permission allows a user to delete license plate information from the Automatic License Plate Recognition video analytic in the Windows Client interface.
Export License Plates	This permission allows a user to export license plate information from the Automatic License Plate Recognition video analytic in the Windows Client interface.
Manage License Plate Lists	This permission allows a user to create and edit license plate lists for the Automatic License Plate Recognition video analytic in the Windows Client interface.
Manage Special Characters	This permission allows a user to add special character mappings for the Automatic License Plate Recognition video analytic in the Windows Client interface.
Perform License Plate Search	This permission allows a user to search for license plate information from the Automatic License Plate Recognition video analytic in the Windows Client interface.
View License Plate Log	This permission allows a user to view the license plate log from the Automatic License Plate Recognition video analytic in the Windows Client interface.
View License Plate Metadata Configuration	This permission allows a user to view the license plate metadata configuration for the Automatic License Plate Recognition video analytic in the Windows Client interface.

Messenger

Permission	Description
Modify Pre-written Messages	This permission allows a user to edit the canned messages in the messenger in the Windows Client interface.
Send Messages	This permission allows a user to send messages using the messenger in the Windows Client interface.

Point of Sale

Permission	Description
Change POS data	This permission allows a user to modify the point-of-sale data in the Windows Client interface.

Permission	Description
View POS data	This permission allows a user to view point-of-sale data in the Windows Client interface.

Report

Permission	Description
Execute Report	This permission allows a user to run reports in the Windows Client interface.

Rule

Permission	Description
Add Rules	This permission allows a user to create rules in the Server configuration interface.

Search

Permission	Description
Convert Searches	This permission allows a user to convert search results to AVI or MPEG files in the Windows Client interface.
Delete Searches	This permission allows a user to delete searches in the Windows Client interface.
Search	This permission allows a user to perform searches in the Windows Client interface.

Security

Permission	Description
Activate Security Profile	This permission allows a user to activate security profiles in the Server configuration interface.
Change Authentication Mode	This permission is not used.
Edit Security	This permission allows a user to edit security settings in the Server configuration interface.
Manage Security Profiles	This permission allows a user to add, edit, and delete security profiles in the Server configuration interface.

Subscription

Permission	Description
Change Subscriptions	This permission allows a user to change the notification settings in the Server configuration interface.
View Subscriptions	This permission allows a user to view the notification settings in the Server configuration interface.

UI

Permission	Description
Change Carousels	This permission allows a user to edit camera carousels in the Server configuration interface.

Permission	Description
Configure Visual Tracking	This permission allows a user to add, edit, and delete visual tracking links in the Windows Client interface.
Lock UI	This permission allows a user to lock the Windows Client interface.
Manage Shared Views	This permission allows a user to edit and save shared views in the Windows Client interface.
View Carousels	This permission allows a user to view camera carousels in the Windows Client interface.

User

Permission	Description
Add Users	This permission allows a user to create users in the Server configuration interface.
Multiple Logins	This permission allows a user to log in to multiple Windows Client interface and Server configuration interface instances concurrently.

Video Wall

Permission	Description
Change Video Wall Client	This permission allows a user to configure video wall clients in the Windows Client interface.
Control Video Walls	This permission allows a user to remotely control video wall clients in the Windows Client interface.
Create Video Walls	This permission allows a user to create video walls in the Windows Client interface.

Device Permissions

General

Permission	Description
Basic Access	This permissions allows a user to access cameras or other devices.
View Group	This permissions allows a user to view the devices in device groups.
View IO State	This permissions allows a user to view the input/output state of devices.

Configuration

Permission	Description
Add Members	This permission allows a user to add devices to a device group.
Change IO State	This permission allows a user to change the input and output state of a device.
Change Settings	This permission allows a user to change the settings for a device.

Permission	Description
Configure Analytics	This permission allows a user to configure analytics for a device.
Delete	This permission allows a user to remove a device from the Server.
Delete Group	This permission allows a user to delete a device group.
Edit Device Security	This permission allows a user to modify the authentication settings for devices.
Edit Group Membership	This permission allows a user to modify to which groups a device group belongs.
Edit Group Properties	This permission allows a user to modify the properties for device groups.
Edit Group Security	This permission allows a user to modify the security profiles for device groups.
Edit Membership	This permission allows a user to modify devices are in a device group.
Remove Members	This permission allows a user to remove a device from a device group.

Alarm

Permission	Description
Manage Alarms	This permission allows a user to mark an alarm as an alarm, false alarm, or as real and actionable, and to view and edit alarm details in the Windows Client interface.
Trigger Manual Alarm	This permission allows a user to add an alarm to a camera timeline in the Windows Client interface.

Audio

Permission	Description
Listen to camera	This permission allows a user to listen to the audio that a camera records using the Windows Client interface.
Talk through camera	This permission allows a user to broadcast audio from a camera using the Windows Client interface.

LPR

Permission	Description
Edit License Plate	This permission allows a user to edit license plates that cameras detect using the Windows Client interface.

PTZ

Permission	Description
Calibrate PTZ Camera	This permission allows a user to calibrate a PTZ camera in the Windows Client interface.
Control PTZ	This permission allows a user to pan and tilt a PTZ camera using the Windows Client interface.

Permission	Description
Control zoom via clients	This permission allows a user to zoom a PTZ camera using the Windows Client interface.
PTZ Presets	This permission allows a user to move a PTZ camera to a preset position using the Windows Client interface.

Search

Permission	Description
Search Footage	This permission allows a user to search video footage using the Windows Client interface.

Video

Permission	Description
Manage Recording	This permission allows a user to manage recordings.
Protect Footage	This permission allows a user to protect footage from deletion using the Windows Client interface.
Unprotect Footage	This permission allows a user to remove protection from footage on the Settings > Protected Footage page in the Server configuration interface.
View Historical Video	This permission allows a user to view historical video.
View Live Video	This permission allows a user to view live video.
View Private Video	This permission allows a user to view video that is hidden by a privacy mask.
View Restricted Historical Video	This permission allows a user to view video that has been marked as restricted. The Server can mark historical video as restricted based on the Time based video playback restriction applied at setting on the Settings > General Settings page in the Server configuration interface.

User Permissions

This page lists the permissions in the **User** category. These permissions attach to security profiles; security profiles attach to groups; users get their permissions by belonging to groups. Other permission categories (site, device, rule, video wall, shared view) follow the same model.

Role templates

Most deployments don't need to hand-pick individual permissions. Start from one of the role templates below and adjust.

Role	Recommended User-category permissions
View-only operator — watches video, does not respond to alarms	None from this category.
Full operator — responds to alarms, generates reports, works a monitoring shift	**View User**, **View Group**.
Supervisor — manages operators during a shift, can end a stuck session	**View User**, **View Group**, **Terminate user session**.

Role	Recommended User-category permissions
User administrator — owns the day-to-day user list for the site	All **View** and **Configuration** permissions below except **Edit Group Security** and **Edit Security**.
Site administrator — owns users, security profiles, and the full permission model	All permissions in this category.

Grant site-level and device-level permissions separately; see the related pages linked above.

General

Permission	Description
View User	See users in the user list. Required for anyone who needs to know who has an account — including most operators so they can see who is on shift.
View Group	See groups in the group list.
Terminate user session	End another user's active session. Typical use: a shift supervisor ending a stuck session so another operator can sign in.

Configuration

Permission	Description
Add Members	Add existing users to a group.
Remove Members	Remove users from a group.
Edit Membership	Add or remove **users** in groups. A superset of Add Members + Remove Members for user membership.
Edit Group Membership	Add or remove **groups inside other groups** (group nesting). Distinct from Edit Membership: this governs the group-of-groups relationship, not user-to-group.
Edit Group Properties	Change a group's name, description, and Active Directory association.
Edit User Properties	Change a user's phone number, email, description, and similar non-security properties.
Edit Group Security	Change the security profile attached to a group. High-impact — granting this is equivalent to granting every permission any security profile confers.
Edit Security	Change the security profile attached to an individual user. Same caveat as Edit Group Security.
Delete Group	Remove a group from the Server. Users in the group lose the permissions that the group granted.
Delete User	Remove a user from the Server.

Notes

- **Edit Group Security** and **Edit Security** are privilege-escalation permissions. Only grant them to administrators you trust with the full permission model.
- **Edit Group Membership** is often confused with **Edit Membership**. Use the former when you build hierarchical group structures; use the latter for the more common case of adding and removing users from a flat set of groups.
- Permissions are additive across a user's group memberships. If a user belongs to two groups, the effective permission set is the union of both.

Related tasks

- Add a User

- Add a Group
- Add a Security Profile
- Set the Security Profile Permissions

Video Wall Permissions

General

Permission	Description
Change Panel	This permission allows a user to modify the camera views in a video wall panel.
Change Window	This permission allows a user to modify the panels in a video wall window.
Move Window	This permission allows a user to move video wall panels in the video wall.
Use Panel Context Menu	This permission allows a user to view and use the contextual menu for video wall panels.
Use Window Context Menu	This permission allows a user to view and use the contextual menu for video wall windows.
View	This permission allows a user to view video walls.
View Group	This permission allows a user to view video wall groups.

Configuration

Permission	Description
Add Members	This permission allows a user to add users to a video wall group.
Delete	This permission allows a user to remove a video wall from the Server.
Delete Group	This permission allows a user to delete a video wall group.
Edit Group Membership	This permission allows a user to modify to which groups a video wall group belongs.
Edit Group Properties	This permission allows a user to modify the properties for video wall groups.
Edit Group Security	This permission allows a user to modify the security profiles for video wall groups.
Edit Security	This permission allows a user to modify the security profiles of users.
Modify	This permission allows a user to modify the configuration of video walls.
Remove Members	This permission allows a user to remove a user from a video wall group.

Rule Permissions

General

Permission	Description
View Rule	This permission allows a user to view rules in the Server configuration interface.

Configuration

Permission	Description
Change Rule	This permission allows a user to change rules in the Server configuration interface.

Shared View Permissions

General

Permission	Description
View Shared View	This permission allows a user to view shared views in the Windows Client interface.

Activate a Security Profile

You can activate a security profile to apply all of the permissions that you configure for users and groups under that security profile.

When you activate a security profile, the permissions for the security profile replace the permissions of the previous security profile. The functionality in the Server configuration interface and Windows Client interface that is available to users can change significantly when you activate a security profile.

1. In the Server configuration interface, click Security > Security Profiles.
2. Select a security profile and click Activate Security Profile.

Remove a Security Profile

You can remove a security profile from the Server as long as the security profile is not active. You cannot remove the default security profile.

Removing a security profile from the Server does not change the active permissions for users or groups.

1. In the Server configuration interface, click Security > Security Profiles.
2. Select a security profile and click Delete.

Logins

The Logins page displays sessions for both the Server and the Windows Client.

The Active Sessions section displays information about users who are currently logged in to the Server configuration interface and the Windows Client interface.

The Historical Sessions section displays information about users who previously logged in to the Server configuration interface and the Windows Client interface.

The Banned Devices and Groups section displays the devices and device groups for which you have suspended video. If you do not suspend access to video in the Windows Client interface, this section will be empty.

Stop an Active Session

You can stop the active sessions for users that are logged into the Windows Client.

Administrator users can stop the active sessions for all other users. Users that are not administrator users can only end their own sessions.

1. In the Server configuration interface, click Security > Logins.
2. Beside the active session that you want to stop, click Terminate.

View Historical Sessions

1. In the Server configuration interface, click Security > Logins.
2. Click Load Historical Sessions.
3. To export the historical sessions to a CSV file, click Export CSV file and open or save the file.

Security Settings

You can configure the password policy for the Server in Security Settings.

For information about managing accounts with Active Directory, see Active Directory Integration.

Passwords

Use the Passwords page to define the password policy that applies to Server user accounts.

Password expiry (days)

When selected, passwords expire after the specified number of days. The default value is 90.

Require complex passwords

When selected, passwords must meet complexity requirements.

Minimum password length

When Require complex passwords is selected, specifies the minimum number of characters in a password. The default value is 8.

Password history length

Specifies the maximum number of previous passwords that the Server stores and checks when a user changes their password. Users cannot change their password to one of their recent passwords. The minimum value is 1, which checks only the current password.

Password attempts before lockout

Specifies the number of failed login attempts before the Server locks the user account. The default value is 3.

Password lockout (minutes)

Specifies the number of minutes that a locked user account remains locked. The default value is 15.

Active Directory Integration

The Active Directory authentication security mode uses Active Directory to authenticate users.

For this authentication method, the Senstar Symphony Database stores user names and security identifiers for user accounts, but not the passwords. When a user attempts to log in, the Server checks the credentials against Active Directory. When you add a user account to the Server, you must associate the user account with a user account in Active Directory.

If you subsequently remove the user from Active Directory, the Server deletes the user.

The Server automatically synchronizes with Active Directory once a day at 12:00 AM server time.

Additionally, you can synchronize the Server manually.

Integrate with Active Directory

You can configure the Server to integrate with the Active Directory domain.

You can integrate the Server with Active Directory during installation of the the Server or after installation by using the Senstar Symphony setup wizard.

The Server connects to the Active Directory Global Catalog for user and group synchronization. In the Server configuration interface, you create groups and associate those groups with groups in Active Directory.

In addition, the Server connects to an Active Directory user as the default administrative user.

1. In the Symphony Security Security section on the Farm Configuration tab, click Edit. image::air_server_activedirectory_configure_8_edit.png[]
2. Select Active Directory Integration. image::air_server_activedirectory_configure_8_adintegration.png[]
3. In the LDAP URL field, perform one of the following tasks:
   - Type the URL for the LDAP global catalog.
   - Click Auto Discover to automatically detect the LDAP global catalog.
4. Type a username and password of the Active Directory user who acts as the default administrative user for the Server.
5. Click Verify.

Associate a Group

If you use Active Directory authentication, you must associate groups that you create in Senstar Symphony with groups in Active Directory.

1. In the Server configuration interface, click Security > Groups.
2. Select a group and click Edit.
3. Click Associate. image::air_server_group_associate_8_associate.png[]
4. In the Search For box, type a group name and click Search. image::air_server_group_associate_8_search.png[]
5. Click the group and click OK. image::air_server_group_associate_8_select.png[]

Synchronize Groups with Active Directory

You can manually synchronize groups that are associated with Active Directory groups to implement changes in Active Directory.

1. In the Server configuration interface, click Security > Groups.
2. Click Synchronize.

Security Authentication

The Senstar Symphony security authentication mode authenticates usernames and passwords that you create for users in the Server configuration interface.

For this authentication method, the Senstar Symphony Database stores user names and passwords for user accounts. When a user attempts to log in, the Senstar Symphony checks the credentials against the Senstar Symphony Database.

Watermarking

The Senstar Symphony uses watermarking to detect tampered video and audio. Watermarking works in the Windows Client, Player, and Web Client.

If the Senstar Symphony successfully verifies the watermark, the video plays normally. If the watermark verification fails, the video displays an error message when you try to view video in the Web Client or the Player.

Enable Watermarking

When you enable watermarking, the Server adds watermarks to recorded video and the Windows Client verifies watermarks when playing video.

1. In the Windows Client interface, click Server Configuration > Manual Configuration Editor.
2. Click Add a new setting.
3. Add the following values:

```
Type: Global
Section: Main
Key: EnableWatermark
Value: True
```

1. Click OK.
2. Restart the Senstar Symphony services.

Rules

The Server can generate alarms from rules. Rules include events, action sets, and schedules.

Alarm Generation

Alarms do not happen in isolation; they are the output of a logical chain within the Symphony Server:

- Event: A raw trigger (e.g., a "Line Crossing" analytic detection, a door forced open, or a fence sensor detecting a cut).
- Action Set: The specific consequences of the event, which include creating the Alarm, sending emails, or moving a PTZ camera to a preset
- Schedule: A timeframe during which the rule is active (e.g., "After Hours").
- Severity: The alarm's significance on a scale from 1 (hightest) to 5 (lowest).

You create rules in the Server configuration interface. When you create a rule, you either associate existing events, action sets, and a schedule with the rule, or you create new events, action sets, and a schedule for the rule.

An action set defines the actions that the Server takes when an event triggers a rule. Examples include displaying or recording footage from a camera, sending an email, and switching a relay. You can select

how the Server performs all of the actions for multiple alarms of the same type by using the multiple invocation behavior settings: append actions sets performs all of the actions for each alarm and replace queued actions performs all the actions for only the latest alarm.

A schedule defines when a rule is active. An event must occur during an active time in the schedule to trigger a rule.

When a rule is enabled, the occurrence of an event associated with the rule during an active period in the rule's schedule causes the Server to perform the actions defined in the rule's action set.

Metadata

Metadata is the structured data that video analytics and integrations produce alongside video. The rule engine on the Server evaluates metadata to decide whether to trigger an event.

What Metadata Is

A camera produces video frames. A video analytic, an access control device, or another integration produces metadata that describes what those frames or events mean. Metadata is structured (XML-style) data that travels with the video and is stored on the Server. Examples of metadata include the following:

- The bounding box, classification (person, vehicle, animal), and trajectory of an object that an analytic detects.
- The license plate text, confidence value, and region that the Automatic License Plate Recognition analytic reports.
- The matched identity and confidence value that the Face Recognition analytic reports.
- The cardholder, door, and result (granted or denied) that an access control event reports.
- The sensor name, zone, and state change that a perimeter integration reports.

Metadata is generated continuously while the source is active. The Server stores metadata next to the video that it describes so that you can search, filter, and replay both at the same time.

How the Rule Engine Uses Metadata

When you create an event on the Server, you choose a metadata source (for example, a video analytic or an integration) and you specify the conditions under which the event triggers. The rule engine evaluates incoming metadata against those conditions in real time. When the conditions match, the rule engine triggers the event, and the rule that uses that event runs its action set.

For example, an Outdoor People and Vehicle Tracking analytic produces metadata for every tracked object. A rule that uses a Line Crossing event examines the trajectory metadata for each object and triggers when an object crosses the configured line during an active schedule.

Metadata is also what makes search work in the Windows Client. When you search for a person, vehicle, or license plate, the Windows Client queries the metadata that the Server has stored, not the video pixels.

Where Metadata Comes From

The following sources produce metadata:

- Video analytics running on a camera or on the Server.
- Integrations with access control, perimeter detection, and other external systems.

- The TCP Listener, which accepts metadata from third-party sources over the network.

Create a Rule

You can create a rule to trigger the Server to perform actions.

1. In the Server configuration interface, click Rules > Rules.
2. Click Add.
3. Type a name for the rule.
4. Enable or disable the rule.
5. Add an existing event to the rule or create a new event to add to the rule.
6. If you add multiple events to the rule, select how the events must occur to trigger the rule.
    - Select in sequence to trigger a rule when the events occur in the order in which the Server configuration interface lists the events.
    - Select within a time period of and specify the number of seconds to trigger an rule when all of the events occur in the specified time period.
7. To add action sets to the rule, perform the following tasks:
    a. In the list, select the action set and click Add.
    b. In the Delay field, set how much time must elapse after the rule occurs before the action triggers.
    c. In the Multiple Invocation behavior list select Append action sets to trigger that actions for each occurrence of the rule or Replace queued actions to trigger the actions for only the most recent occurrence of the rule.

You can add multiple actions to each rule.

1. Add an existing schedule to the rule or create a new schedule to add to the rule.
2. In the Severity field, select the severity for the alarm.
    - 1 is considered high severity in the Windows Client
    - 2 and 3 are considered medium severity in the Windows Client
    - 4 and 5 are considered low severity in the Windows Client

You can use alarm severity to sort alarms in the

Windows Client

.

1. Click Save.

Edit a Rule

You can edit a rule to change the events, action set, and schedule associated with the rule.

1. In the Server configuration interface, click Rules > Rules.
2. Select a rule.
3. Click Edit.

4. Modify the rule.
5. Click Save.

Delete a Rule

You can remove a rule to prevent events from triggering on the Server.

When you delete a rule, the events, action set, and schedule associated with the rule are not deleted.

1. In the Server configuration interface, click Rules > Rules.
2. Select a rule.
3. Click Delete.
4. Click Yes.

Events

Events define the condition that must exists for a rule to trigger an alarm on the Server.

Create an Event

You can create an event that triggers a rule on the Server.

When the Server receives input from a source, it can trigger a rule. Different sources can trigger rules in different ways. For additional information on devices, see the manufacturer's documentation.

1. In the Server configuration interface, click Rules > Events.
2. Click New Event.
3. Type a name for the event.
4. To add a source, perform the following tasks:
   a. Click Add Sources.
   b. Select the device, rule or schedule to trigger the rule.
   c. Click OK.
5. Perform one of the follow tasks:
   - If you add a camera, select the video engine and configure how it triggers a rule.
   - If you add a metadata device, select the input and configure how it triggers a rule.
   - If you add an access control device, select the readers and inputs, and configure how they trigger a rule.
   - If you add a rule, select the action that triggers a rule.
   - If you add a schedule, select when to trigger a rule.
6. Click Save.

Edit an Event

You can edit an event to change what triggers a rule.

1. In the Server configuration interface, click Rules > Events.

2. Select an event.
3. Click Edit.
4. Modify the event.
5. Click Save.

Delete an Event

You can delete an event to remove it from the Server.

1. In the Server configuration interface, click Rules > Events.
2. Select an event.
3. Click Delete.
4. Click Yes.

Automatic License Plate Recognition Event Settings

The event settings for the Automatic License Plate Recognition video analytic are visible when you select it as the video engine for an event.

Setting	Description
Alarm type	Select whether the event triggers the rule when Automatic License Plate Recognition video analytic detects a license plate, detects a license plate not on the list (white list), or detects a license plate on the list (black list).

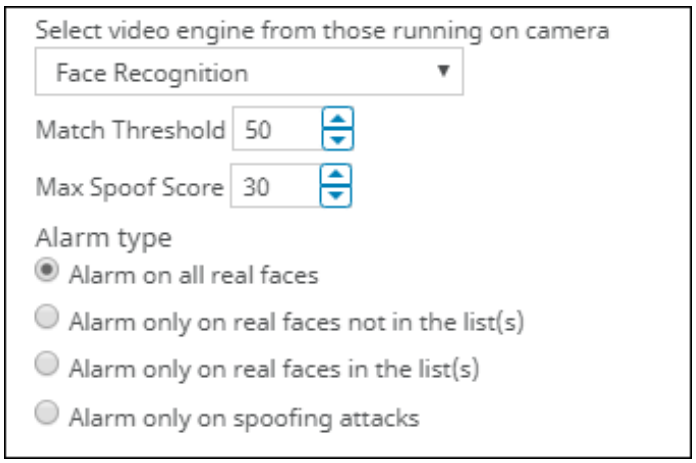
Crowd Detection Event Settings

The event settings for Crowd Detection video analytic are visible when you select it as the video engine for an event.

Setting	Description
Alarm type	Select whether the event responds to capacity (number of people) or occupancy (area occupied by people).
Duration	Set the amount of time over which the Crowd Detection video analytic averages values. A higher duration reduces the number of alarms but increases the possibility of missed alarms. A lower duration increases the number of alarms but increases the possibility of false alarms.
Threshold	Use the slider bar to define the values that trigger the event. Values that fall outside of the threshold trigger the event. For the capacity alarm type, the slider represents the percentage of the maximum capacity that you configure for the Crowd Detection video analytic. For the occupancy alarm type, the slider represents the percentage of the scene (defined by the processing mask) occupied by people.

Face Recognition Event Settings

+



+

Setting	Description
Match Threshold	Set how closely the detected face must match a face on the blocked list to trigger an alarm or a face on the allowed list to not trigger an alarm. This setting does not apply if you select Alarm on all faces.
Max Spoof Score	Set the score that a face must exceed for the Face Recognition video analytic to consider the face a spoof. The default value is 30.
Alarm on all real faces	Select to trigger an alarm when the Face Recognition video analytic detects a face.
Alarm only on real faces not in the list(s)	Select to trigger an alarm when the Face Recognition video analytic detects a face that is not on the lists that you select. The list options include the default lists (Allowed and Blocked) and any custom lists that you create.
Alarm only on real faces in the list(s)	Select to trigger an alarm when the Face Recognition video analytic detects a face that on the lists that you select. The list options include the default lists (Allowed and Blocked) and any custom lists that you create.
Alarm only on spoofing attacks	Select to trigger an alarm only when the Face Recognition video analytic detects a face with a spoof score greater than the max spoof score.

Left and Removed Item Detection Event Settings

The event settings for the Left and Removed Item Detection video analyticare visible when you select it as the video engine for an event.

Setting	Description
Processing mask	Draw a processing mask to determine what areas can trigger an event.
Alarm based on percentage of object inside alarm mask	Select if the event triggers rules based on the percentage of the object inside of the processing mask.
Alarm size	Define the maximum and minimum size of objects that can trigger the rule.

Setting	Description
Alarm only if	Select to alarm only if there are multiple alarms in a specific time. You can define both the number of alarms and the time.
Or at least	Select to alarm if a number of pixels change in a specific time. You can define both the number of pixels and the time.

Motion Detection Event Settings

The event settings for Motion Detection are visible when you select it as the video engine for an event.

Setting	Description
Processing mask	Draw a processing mask to determine what areas can trigger an event.

Outdoor People and Vehicle Tracking Event Settings

The event settings for the Outdoor People and Vehicle Tracking video analytic are visible when you select it as the video engine for an event.

Setting	Description
Class	Select the class of object that triggers the rule.
Behavior	Select whether an object moving for a time or loitering for a time triggers the rule, and set the time.
Use Mask	Select what movement to use when triggering the rule. Select whether the beginning, end, or any part of the movement track triggers the alarm, and select whether any part of the object can trigger the rule.
Use Fences	Select whether to trigger rules when an object crosses any of the fences or when an object crosses all of the fences.

TCP Listener Event Settings

The event settings for the TCP Listener video analytic are visible when you select it as the video engine for an event.

Setting	Description
Alarm type	Select whether the events responds to any metadata or metadata that contains specific text.
Alarm on metadata that contains	Specify the text that triggers the event when you select to alarm on metadata that contains specific text.

Senstar Network Manager Event Settings

Events from Senstar Network Manager can trigger rules on the Server.

Setting	Description
Activated	Select to trigger a rule on the Server when an output connected to the Senstar Network Manager is activated.
Deactivated	Select to trigger a rule on the Server when an output connected to the Senstar Network Manager is deactivated.
Alarm	Select to trigger a rule on the Server when an input connected to the Senstar Network Manager enters an alarm state.

Setting	Description
Alarm Secure	Select to trigger a rule on the Server when an input connected to the Senstar Network Manager exits an alarm state.
Communication Fail	Select to trigger a rule on the Server when device connected to the Senstar Network Manager enters a communication failure state.
Communication Fail Secure	Select to trigger a rule on the Server when a device connected to the Senstar Network Manager exits a communication failure state.
Communication Fault	Select to trigger a rule on the Server when a device connected to the Senstar Network Manager enters a communication fault state.
Communication Fault Secure	Select to trigger a rule on the Server when a device connected to the Senstar Network Manager exits a communication fault state.
Diagnostic Warning	Select to trigger a rule on the Server when a device connected to the Senstar Network Manager enters a diagnostic warning state.
Diagnostic Warning Secure	Select to trigger a rule on the Server when a device connected to the Senstar Network Manager exits a diagnostic warning secure state.
Diagnostic Fatal	Select to trigger a rule on the Server when a device connected to the Senstar Network Manager enters a fatal diagnostic state.
Diagnostic Fatal Secure	Select to trigger a rule on the Server when a device connected to the Senstar Network Manager exits a fatal diagnostic state.
Enclosure Tamper	Select to trigger a rule on the Server when a device connected to the Senstar Network Manager enters an enclosure-tampered state.
Enclosure Tamper Secure	Select to trigger a rule on the Server when a device connected to the Senstar Network Manager exits an enclosure-tampered state.
Tamper	Select to trigger a rule on the Server when an input connected to the Senstar Network Manager enters a tampered state.
Tamper Secure	Select to trigger a rule on the Server when an input connected to the Senstar Network Manager exits a tampered state.
Trouble	Select to trigger a rule on the Server when an input connected to the Senstar Network Manager enters a trouble state.
Trouble Secure	Select to trigger a rule on the Server when an input connected to the Senstar Network Manager exits a trouble state.

Senstar Symphony Access Control Event Settings

Events from Senstar Symphony Access Control can trigger rules on the Server.

Some events are listed twice in the Server configuration interface to accommodate both proximity card readers and magnetic-strip card readers. Events with the >> label are the default for proximity card readers and down swipes for magnetic-strip card readers. Events with the << label apply to up swipes for magnetic-strip card readers.

Setting	Description
Door Forced Open	Select to trigger a rule on the Server when a door contact connected to the Senstar Symphony Access Control detects a door forced open.
Door Held Open	Select to trigger a rule on the Server when a door contact connected to the Senstar Symphony Access Control detects a door held open.
Door is Closed	Select to trigger a rule on the Server when a door contact connected to the Senstar Symphony Access Control detects that the door is closed.
Door is Opened	Select to trigger a rule on the Server when a door contact connected to the Senstar Symphony Access Control detects that the door is open.
Request To Exit	Select to trigger a rule on the Server when a door contact or request to exit device connected to the Senstar Symphony Access Control detects a request to exit.
Request To Exit (Door Used)	Select to trigger a rule on the Server when a request to exit device connected to the Senstar Symphony Access Control detects a request to exit with the door used.
Request to Exit (Door Not Used)	Select to trigger a rule on the Server when a request to exit device connected to the Senstar Symphony Access Control detects a request to exit with the door not used.
Door is Locked	Select to trigger a rule on the Server when a door strike device connected to the Senstar Symphony Access Control detects that the door is locked.
Door is Unlocked	Select to trigger a rule on the Server when a door strike device connected to the Senstar Symphony Access Control detects that the door is unlocked.
Deadbolt Disengaged	Select to trigger a rule on the Server when a door strike device connected to the Senstar Symphony Access Control detects that the deadbolt lock is disengaged.
Deadbolt Engaged	Select to trigger a rule on the Server when a door strike device connected to the Senstar Symphony Access Control detects that the deadbolt lock is engaged.
Door Schedule is Disabled	Select to trigger a rule on the Server when a door strike device connected to the Senstar Symphony Access Control detects that the door schedule is disabled.
Door Schedule is Enabled	Select to trigger a rule on the Server when a door strike device connected to the Senstar Symphony Access Control detects that the door schedule is enabled.
Door is Momentarily Unlocked	Select to trigger a rule on the Server when a door strike device connected to the Senstar Symphony Access Control detects that the door is momentarily unlocked.
Double Locked	Select to trigger a rule on the Server when a door strike device connected to the Senstar Symphony Access Control detects that both the deadbolt and handle lock are engaged. This event applies to Assa Abloy wireless locks only.

Setting	Description
Locked Down	Select to trigger a rule on the Server when a door strike device connected to the Senstar Symphony Access Control detects that a command to lock the door and set the reader mode to disabled is issued. This event applies to Assa Abloy wireless locks only.
Locked Open	Select to trigger a rule on the Server when a door strike device connected to the Senstar Symphony Access Control detects that a command to restore the door and reader to normal operation after a Locked Down event. This event applies to Assa Abloy wireless locks only.
Control Point Deactivated	Select to trigger a rule on the Server when a door sounder device connected to the Senstar Symphony Access Control detects that a control point is deactivated.
Control Point Activated	Select to trigger a rule on the Server when a door sounder device connected to the Senstar Symphony Access Control detects that a control point is activated.
Control Point Pulse	Select to trigger a rule on the Server when a control point device connected to the Senstar Symphony Access Control detects that the control point receives a command to momentarily activate a relay or output.
Reader Mode: Disabled	Select to trigger a rule on the Server when a reader device connected to the Senstar Symphony Access Control is disabled.
Reader Mode: Unlocked	Select to trigger a rule on the Server when a reader device connected to the Senstar Symphony Access Control is unlocked.
Reader Mode: Locked (REX Only)	Select to trigger a rule on the Server when a reader device connected to the Senstar Symphony Access Control is locked and can only be unlocked with a request to exit (REX).
Reader Mode: Facility Code Only	Select to trigger a rule on the Server when a reader device connected to the Senstar Symphony Access Control can only be unlocked when the facility code on a card matches the facility code in the system configuration.
Reader Mode: Card Only	Select to trigger a rule on the Server when a reader device connected to the Senstar Symphony Access Control is set to accept cards only.
Reader Mode: PIN Only	Select to trigger a rule on the Server when a reader device connected to the Senstar Symphony Access Control is set to accept PINs only.
Reader Mode: Card and PIN	Select to trigger a rule on the Server when a reader device connected to the Senstar Symphony Access Control is set to accept cards with PINs only.
Reader Mode: Card or PIN	Select to trigger a rule on the Server when a reader device connected to the Senstar Symphony Access Control is set to accept cards or PINs.
User Command Requested	Select to trigger a rule on the Server when a reader device connected to the Senstar Symphony Access Control detects that the terminal keypad requests a user code.
Reader Mode: Fingerprint Only	Select to trigger a rule on the Server when a reader device connected to the Senstar Symphony Access Control is set to accept fingerprints only.

Setting	Description
Reader Mode: Card and Fingerprint	Select to trigger a rule on the Server when a reader device connected to the Senstar Symphony Access Control is set to accept cards with fingerprints only.
Reader Mode: Card or Fingerprint	Select to trigger a rule on the Server when a reader device connected to the Senstar Symphony Access Control is set to accept cards or fingerprints.
Reader Mode: Office First	Select to trigger a rule on the Server when a reader device connected to the Senstar Symphony Access Control is set to respond to the first person in situation.
Reader Mode: Blocked	Select to trigger a rule on the Server when a reader device connected to the Senstar Symphony Access Control is disabled. This event applies to Assa Abloy wireless locks only.
Reader Mode: Emergency Lock	Select to trigger a rule on the Server when a reader device connected to the Senstar Symphony Access Control enters the emergency locked state.
Reader Mode: Emergency Unlock	Select to trigger a rule on the Server when a reader device connected to the Senstar Symphony Access Control exits the emergency locked state.
Access Granted	Select to trigger a rule on the Server when a reader device connected to the Senstar Symphony Access Control grants access.
Access Denied: Level	Select to trigger a rule on the Server when a reader device connected to the Senstar Symphony Access Control denies access to a card because of an insufficient access level.
Access Denied: Time	Select to trigger a rule on the Server when a reader device connected to the Senstar Symphony Access Control denies access to a card because of an insufficient access level during a specific time.
Access Denied: Locked	Select to trigger a rule on the Server when a reader device connected to the Senstar Symphony Access Control denies access and locks the door.
Access Denied: Card	Select to trigger a rule on the Server when a reader device connected to the Senstar Symphony Access Control denies access to a card.
Access Denied: Facility	Select to trigger a rule on the Server when a reader device connected to the Senstar Symphony Access Control denies access to a card because of an incorrect facility code.
Access Denied: Passback	Select to trigger a rule on the Server when a reader device connected to the Senstar Symphony Access Control denies access because of a card passback.
Access Denied: Issue Code	Select to trigger a rule on the Server when a reader device connected to the Senstar Symphony Access Control denies access because of an incorrect issue code. An issue code comprises a facility code, re-issue code, and card number. Issue codes are used with Mercury controllers to track the number of times a card is re-issued.
Access Denied: Invalid	Select to trigger a rule on the Server when a reader device connected to the Senstar Symphony Access Control denies access because of a invalid card format.

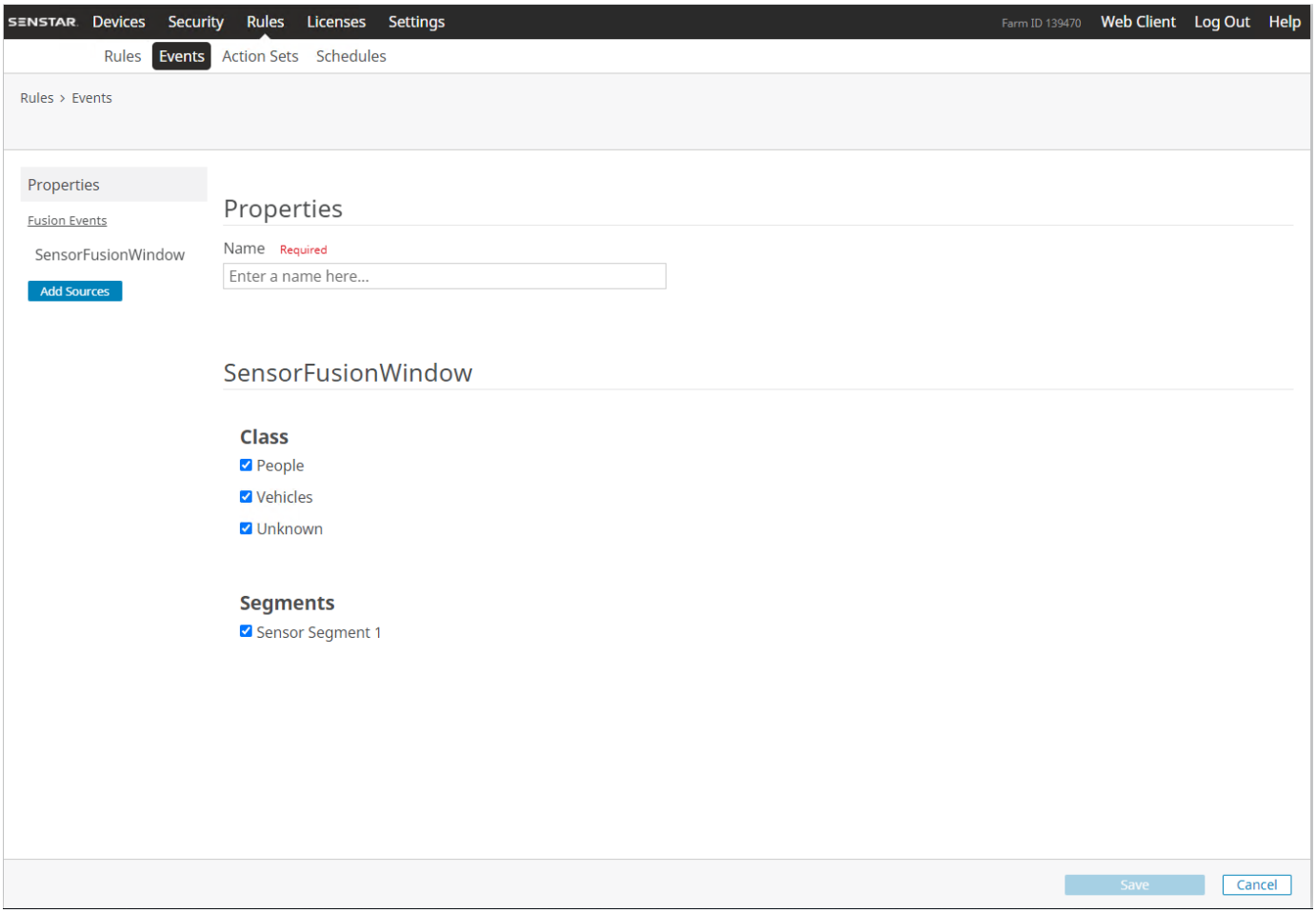
Setting	Description
Card Information Event	Select to trigger a rule on the Server when a reader device connected to the Senstar Symphony Access Control detects a card information event. Card information events are special events that display information about a previous event. For example, if a card is denied for an incorrect facility code, the card information event displays the incorrect facility code.
Access Granted: Unlocked	Select to trigger a rule on the Server when a reader device connected to the Senstar Symphony Access Control grants access and unlocks the door.
Access Granted: Door Not Used	Select to trigger a rule on the Server when a reader device connected to the Senstar Symphony Access Control grants access but the door was not used.
Access Granted: Door Used	Select to trigger a rule on the Server when a reader device connected to the Senstar Symphony Access Control grants access and the door was used.
Access Denied: Deactivated Card	Select to trigger a rule on the Server when a reader device connected to the Senstar Symphony Access Control denies access because of a deactivated card.
Access Denied: Before Activation Date	Select to trigger a rule on the Server when a reader device connected to the Senstar Symphony Access Control denies access because the card is not yet active.
Access Denied: After Expiration Date	Select to trigger a rule on the Server when a reader device connected to the Senstar Symphony Access Control denies access because the card is expired.
Access Denied: Invalid PIN	Select to trigger a rule on the Server when a reader device connected to the Senstar Symphony Access Control denies access because the PIN is invalid.
Access Denied: 2nd Card not Presented	Select to trigger a rule on the Server when a reader device connected to the Senstar Symphony Access Control denies access because the second card (required for two-person authentication) was not presented.
Access Denied: Occupancy Limit Reached	Select to trigger a rule on the Server when a reader device connected to the Senstar Symphony Access Control detects that the reader denied access because the occupancy limit has been reached.
Access Denied: Area not Enabled	Select to trigger a rule on the Server when a reader device connected to the Senstar Symphony Access Control denies access because the area is not enabled.
Access Denied: Use Limit	Select to trigger a rule on the Server when a reader device connected to the Senstar Symphony Access Control denies access because the card has exceeded the number of times that the card can be used.
Access Denied: Duress Code Detected	Select to trigger a rule on the Server when a reader device connected to the Senstar Symphony Access Control denies access because duress code was used.
Access Denied: Duress (Door Used)	Select to trigger a rule on the Server when a reader device connected to the Senstar Symphony Access Control denies access because a duress code was used and the door was used.

Setting	Description
Access Denied: Duress (Door Not Used)	Select to trigger a rule on the Server when a reader device connected to the Senstar Symphony Access Control detects that the reader denied access because a duress code was used and the door was not used.
Access Denied: Unauthorized Assets	Select to trigger a rule on the Server when a reader device connected to the Senstar Symphony Access Control denies access because the assets are not authorized for the card.
Access Denied: Biometric Verification Error	Select to trigger a rule on the Server when a reader device connected to the Senstar Symphony Access Control denies access because duress code was used and the door was not used.
Access Granted: Verification Confirmed	Select to trigger a rule on the Server when a reader device connected to the Senstar Symphony Access Control grants access because the verification was confirmed.
Access Denied: No Biometric Record	Select to trigger a rule on the Server when a reader device connected to the Senstar Symphony Access Control denies access because the user does not have a biometric record.
Access Denied: No Biometric Device	Select to trigger a rule on the Server when a reader device connected to the Senstar Symphony Access Control that does not have biometric functionality is put in biometric mode and a card is presented. This event applies to ZK devices only.
Intrusion Area: Armed	Select to trigger a rule on the Server when a reader device connected to the Senstar Symphony Access Control detects that the area is armed and is ready to alarm.
Intrusion Area: Disarmed	Select to trigger a rule on the Server when a reader device connected to the Senstar Symphony Access Control detects that the area is disarmed and is not ready to alarm.
Intrusion Request Attempt: Denied	This event is not applicable.
Intrusion Disarm Attempt: Denied	Select to trigger a rule on the Server when a reader device connected to the Senstar Symphony Access Control denies a disarm attempt because of insufficient permission.
Access Granted: Office First Door Unlocked	Select to trigger a rule on the Server when a reader device connected to the Senstar Symphony Access Control grants access and is unlocked because the first person in situation occurs.
Access Granted: Office First Door Locked	Select to trigger a rule on the Server when a reader device connected to the Senstar Symphony Access Control grants access and is locked because the first person in situation occurs.
Access Denied: Punch Interval	Select to trigger a rule on the Server when a reader device connected to the Senstar Symphony Access Control denies access because the interval between two cards is too short. This event applies to ZK devices only.
Access Granted: Passback (Door Not Used)	Select to trigger a rule on the Server when a reader device connected to the Senstar Symphony Access Control grants access on a card passback and the door was not used.
Access Granted: Passback (Door Used)	Select to trigger a rule on the Server when a reader device connected to the Senstar Symphony Access Control grants access on a card passback and the door was used.

Senstar Sensor Fusion Event Settings

The following settings determine when the Senstar Sensor Fusion triggers events on the Server.

You can configure the Senstar Sensor Fusion to trigger events from the video analytic, the perimeter intrusion detection system, or both.



Setting	Description
People	Select if the Senstar Sensor Fusion should trigger events when it detects a person.
Vehicles	Select if the Senstar Sensor Fusion should trigger events when it detects a vehicle.
Unknown	Select if the Senstar Sensor Fusion should trigger events when it detects an unknown object.
Segments	Select the sensor segments for which the Senstar Sensor Fusion should trigger events.

Action Sets

Action sets are combinations of actions that the Server takes when a rule generates an alarm.

Create an Action Set

You can create an action set to determine what actions the Server takes when rule is triggered.

1. In the Server configuration interface, click Rules > Action Sets.
2. Click New Action Set.
3. Type a name for the action set.
4. In the Alarm section, perform the following tasks:
   a. In the device list, select the devices that you want to display in view panels in the Windows Client interface. The device list is grouped into device groups by default. If you want to view the devices in an alphabetic list, select

Hide Device Groups

.

   a. In the field beside the selected device, type a name for the panel in which you want to display the device. If you do not type an panel name, the

Windows Client

displays the device in the default view panel.

1. To select where the alarm appears, perform one of the following tasks:
   - To associate the alarm with a camera and display the alarm in a camera timeline, select the camera in the Choose a Camera list.
   - To associate the alarm with a map and display the alarm on the map, select the map in the Choose a Map list.
2. In the Record list, select the cameras that record footage when an alarm occurs.
3. To add other actions, perform the following tasks:
   a. In the Pick an item list, select an action. image::air_server_rules_action_set_create.png[]
   b. Click Add.
   c. Configure the settings for the action.
4. Click Save.

Edit an Action Set

You can edit an action set to change what actions the Server takes when a rule is triggered.

1. In the Server configuration interface, click Rules > Action Sets.
2. Select an action set.
3. Click Edit.
4. Modify the action set.
5. Click Save.

Delete an Action Set

You can delete an action set to remove it from the Server.

If the action set is associated with a rule, you will see an additional warning message and a request for confirmation when deleting an action set. If you choose to remove the action set in this case, the rule will not function as expected.

1. In the Server configuration interface, click Rules > Action Sets.
2. Select an action set.
3. Click Delete.
4. Click Yes.

Schedules

Schedules determine when rules are active in the Server.

You can create a schedule as part of the rule creation process or independently in the Server configuration interface. Schedules use half hour blocks and support daily exceptions that can recur every year.

Create a Schedule

You can create a schedule to determine when a rule is active.

1. In the Server configuration interface, click Rules > Schedules.
2. Click Add Schedule.
3. Type a name for the schedule.
4. Define the active and inactive times for the schedule.
5. If required, add exceptions to the schedule.
    a. Select a date.
    b. Select whether to repeat the exception every year on that date.
    c. Click Add Exception.
    d. Define the active and inactive times for the exception.
6. Click Save.

Edit a Schedule

You can edit a schedule to change when a rule is active.

1. In the Server configuration interface, click Rules > Schedules.
2. Select a schedule.
3. Click Edit.
4. Modify the schedule.
5. Click Save.

Clone a Schedule

You can clone a schedule to use it as a template for a new schedule.

1. In the Server configuration interface, click Rules > Schedules.

2. Select a schedule.
3. Click Clone.
4. Modify the schedule.
5. Click Save.

Delete a Schedule

You can delete a schedule to remove it from the Server.

You cannot delete a schedule if it is associated with a rule.

1. In the Server configuration interface, click Rules > Schedules.
2. Select a schedule.
3. Click Delete.
4. Click Yes.

Licenses

License settings for the Server allow you to view and refresh licenses.

You access the license settings on the Licenses tab in the Server configuration interface.

The Properties section displays the characteristics of your Server license. The section displays the date at which the license expires and the software version to which the license applies.

The Licenses in Farm section displays the video analytic licenses, the camera licenses, and the MAC addresses of servers that are permitted in the server farm.

The Unlicensed Devices section displays the cameras on the network that do not have an associated license.

Refresh Licenses

You can refresh your licenses to check for newer versions from the Senstar Xnet or to manually apply updates.

1. In the Server configuration interface, click Licenses.
2. Click Refresh Licenses.
3. Perform one of the following tasks:
   a. To refresh the license from senstar.com, select Refresh license from senstar.com.
   b. To refresh the license from a file, select Refresh license from file, browse to the license file or drag the license file into the window.
4. Click OK.

Show License XML

You can view the XML for your license.

1. In the Server configuration interface, click Licenses.
2. Click Show Raw License.

Settings

The settings for the Server allow you to configure servers, general settings, cloud services, alarm aggregates, updates, backup and restore, maps, and protected footage.

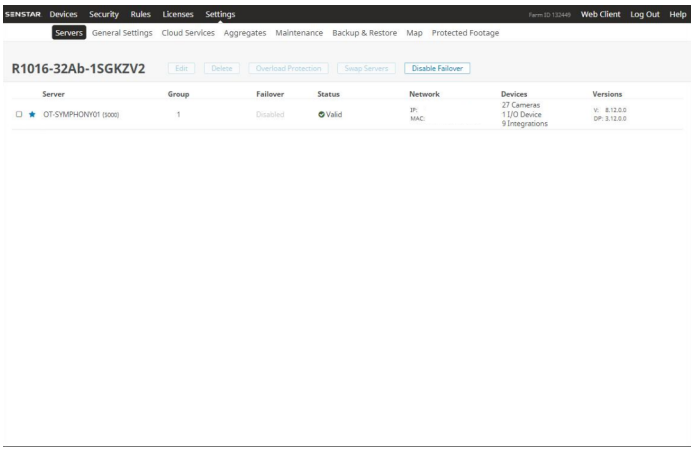
You access the settings on the Settings tab in the Server configuration interface. The Settings tab includes the Servers, General Settings, Cloud Services, Aggregates, Maintenance, Backup & Restore, Maps, and Protected Footage tabs.

Servers

The Servers tab in the Server configuration interface is the interface for configuring settings specific to individual Server instances in the server farm.

The Servers tab allows you to edit server settings, configure video storage, and set up server redundancy.

+



+

Configure Video Storage for a Server

You can configure how the Server stores and maintains video footage. These settings apply to the Server that you select.

You can configure where the Server stores video footage, how much video footage the Server stores, and under which conditions the Server erases video footage. In addition, you can specify backup locations for video footage.

1. In the Server configuration interface, click Settings > Servers.
2. Select a server and click Edit.
3. To specify a storage path, complete the following tasks in the Video Storage section:
    a. Specify the path to which the Server should save footage files.
    b. To add another storage path, click Add Another Path and specify the path.
    c. To save footage files to only one storage path, select Failover. The

Server

attempts to save footage files to the first path in the list. If that path is not available, the

Server

attempts to save footage files to the next path in the list.

a. To save footage files to all storage paths, select Redundant.
b. Select the path from which the Server should read footage files in the Force disk reads from.
    1. To specify a secondary (archive) storage path, complete the following tasks:
c. Select Archive video to secondary storage path.
d. Type the path to which the Server should save footage files. You must type a secondary (archive) storage path for each of the primary storage paths.
e. In the Days to store before archiving field, set how many days must occur before the Server saves the footage files to the secondary (archive) storage path. This value must be less than the

Limit the number of days video is stored

value.

1. To set a limit based on the amount of disk space left, set the disk space in the MB field or the percentage of disk space in the % field.
2. To set the maximum number of days for which the Server can retain footage files, select Limit the number of days video is stored and set the number of days.
3. To retain metadata after the Server deletes footage files, select Keep metadata longer and set the number of days.
4. To copy footage files generated during a failover back to the restored primary server from the redundant server, select SAN Failover mode: Copy files to owner server. Both the primary

Server

and redundant

Server

must have read and write permission for the storage paths on each

Server

.

1. In the Cameras list, define any storage paths specific to cameras. By default, the

Server

saves footage files from all cameras to the storage paths.

1. Click Save.

SAN Failover Mode

SAN failover mode works in conjunction with server redundancy to move local footage files from the redundant Server back to the primary Server when the primary Server recovers from the outage.

When the primary Server recovers from the outage, it attempts to copy footage files from the redundant Server and collate those footage files with the existing footage files in local storage.

To use SAN failover mode, complete the following workflow:

1. In the Server configuration interface, create a redundancy group and add each Server to the redundancy group.
2. On every computer that hosts a Server in the redundancy group, make sure that the data folder has the same drive letter assignment as all of the other computers.
3. On every computer that hosts a Server in the redundancy group, create a share for the data folder and name the share DATAX, where X is the drive letter assignment. For example, name the share DATAG if the share is on the G drive.
4. Grant the user accounts that run the Senstar Symphony services on every other Server in the redundancy group read and write permission for the data folder share.
5. In the Server configuration interface, select the SAN failover mode box for every Server in the redundancy group. +
image::air_server_san_failover_01.png[]

You do not typically need to use SAN failover if you use a common network location for storage of the data folders of every Server in the redundancy group.

Configure Overload Protection

You can configure a Server to automatically move cameras to anotherServer when the CPU load grows too great.

1. In the Server configuration interface, click Settings > Servers.
2. Select a server and click Overload Protection.
3. Select whether to move cameras to a different server when the CPU load is too high.
4. Select whether to use redundant servers. If you use redundant servers to accept cameras in the case of overload, you cannot use the server redundancy feature.
5. Set the CPU threshold (in percent) above which the Server considers itself to be overloaded.
6. Set the polling frequency (in seconds) to determine how often the Server monitors the CPU load.
7. Set the maximum number of cameras to move to the new server.
8. Click Save.

Manage Services

You can configure how the Server manages the Senstar Symphony services.

Managing services allows you to make bulk changes to Senstar Symphony services. You can start and stop multiple Senstar Symphony services at one time, set the Senstar Symphony services to start automatically, and change the user account that the Server uses to run the Server.

1. In the Server configuration interface, click Settings > Servers.
2. Select a server and click Edit.
3. In the Services section, perform the following tasks:
    a. To change the state of a Senstar Symphony service, select the service and click Toggle Selected. Performing this task stops a running service or starts a stopped service.
    b. To refresh the service list, click the Refresh button.
    c. To automatically start the Senstar Symphony services when the computer that hosts the Server

starts, select Automatically start Symphony services on system startup.

d. To set the user account that runs the Senstar Symphony services, either select Log on as Local System account to use the local system account or select This account and type the account credentials to use another account. The local system account is the default account that the

Server

uses to run

Senstar Symphony

services, but you change the account to access data in a shared network location.

1. Click Save.

Server Redundancy

The Server supports server redundancy in server farms. If the primary Server stops responding, the camera and device processing moves to a redundant Server.

To use server redundancy you must have at least one primary Server and one redundant Server in a redundancy group. The primary Server actively performs camera and device processing. The redundant Server is active, but it does not have any cameras or devices associated with it. There must be at least one redundant server available in the server farm at all times.

When failover occurs, the redundant Server takes over the camera and device processing from the primary Server while it is unavailable. When the primary Server recovers from the outage, one of the following things happens:

- You can move the camera and device processing back to the primary Server automatically by enabling failback in the Server configuration interface.
- You can move the camera and device processing back to the primary Server manually by swapping servers in the Server configuration interface.
- You can use the primary Server as a redundant Server.

Master Server

In a server farm, one Server is the master server. The master server is the Server that coordinates the farm and decides when failover and failback occur.

The master server is responsible for the following tasks:

- Detecting when a primary Server has stopped responding and declaring a failover event.
- Selecting the redundant Server that takes over the camera and device processing.
- Coordinating failback when the primary Server returns to service.
- Holding the authoritative copy of the configuration so that every Server in the farm sees the same settings.

The master server continues to perform its own camera and device processing while it carries out these tasks.

If the master server becomes unavailable, the remaining servers in the farm automatically elect a new master server so that failover decisions can continue without administrator intervention. When the original master server returns to service, it does not automatically reclaim the role.

You can manually select which Server is the master server by clicking the star icon beside the Server

on the Servers page in the Server configuration interface.

Add a Server to a Redundancy Group

You can add a server to a redundancy group or create a new redundancy group.

1. In the Server configuration interface, click Settings > Servers.
2. Select a server and click Edit.
3. In the Server Group list, perform one of the following tasks:
   - To add the server to an existing redundancy group, select the group.
   - To add the server to a new redundancy group, select <New>.
4. Click Save.

Configure Failover

You can configure the Server to move cameras to a secondary Server if the primary Server goes offline.

Before you begin, you must configure video storage for the Server.

1. In the Server configuration interface, click Settings > Servers.
2. Select a server and click Edit.
3. In the Server Group list, select a server group that includes a server that does not have any cameras.
4. Click Enable Failover.

Configure Failback

You can configure the Server to move cameras back to the primary Server after a failover when the primary Server comes back online.

Before you begin, you must configure failover for the Server.

If you do not configure failback, you must manually move the cameras back to the primary Server.

1. In the Server configuration interface, click Settings > Servers.
2. Select a server and click Edit.
3. Click Enable Failback.

Move Cameras

You can move all of the cameras from one Server to a different Server in your server farm.

You can only move all of the cameras from one Server to another Server if the destination server does not have any cameras associated with it.

1. In the Server configuration interface, click Settings > Servers.
2. In the server list, select the server from which to move cameras.
3. In the server list, select the server to which to move the cameras.
4. Click Swap Servers.

Add an Alternate Server Address

You can add multiple IP addresses for the Server to facilitate communication with the Server when it is part of a multi-server farm.

1. In the Server configuration interface, click Settings > Servers.
2. Select a server and click Edit.
3. Click the plus beside Alternate Server Addresses.
4. In the Alternate Server Addresses field, type the alternate address for the Server.
5. Select the port.
6. Click Save.

Add an SSL Certificate

You can add an SSL certificate to the Server in the Server configuration interface. This topic only applies to Server 8.6.0. In the Server 8.6.1, the SSL certificate settings moved to the setup wizard. See the Senstar Symphony Installation Guide for more information.

The Server uses the SSL certificate to secure connections from browsers and the Senstar Symphony Mobile Application. The Server supports PFX certificate files.

1. In the Server configuration interface, click Settings > Servers.
2. Select the Server and click Edit.
3. Navigate to the SSL Certificate section.
4. In the Password field, type the password for the certificate.
5. Drag the certificate file into the field or browse for the certificate file.
6. Click Save.

Configure Mobile Connections

You can configure the Server to support connections with the Senstar Symphony Mobile Application on mobile devices.

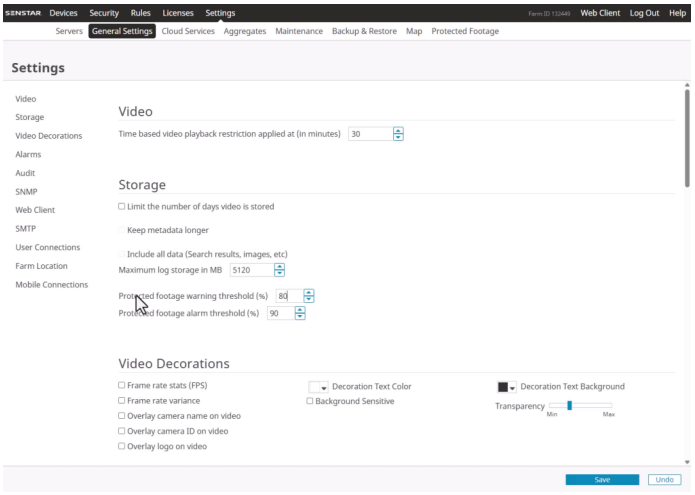
You configure the SSL certificate that the Server uses for mobile connections in the Senstar Symphony setup wizard.

1. In the Server configuration interface, click Settings > Servers.
2. Select the Server and click Edit.
3. Navigate to the Mobile Connections section.
4. To select the SSL certificate, click Change, select the certificate, and click OK.
5. To select the network adapter for mobile connections, click Change, select the network adapter, and click OK.
6. In the Mobile Port field, set the port that the Server uses to listen for requests from mobile devices.
7. In the Video Proxy Port field, set the port that the Server uses to stream video to and receive video from mobile devices.
8. Click Save.

General Settings

The General Settings tab is used to configure settings that apply to all of the server instances in the server farm.

To view the General Settings tab, click Settings > General Settings in the Server configuration interface. The General Settings tab includes the Video, Storage, Video Decorations, Alarms, Audit, SNMP, Web Client, SMTP, User Connections, Farm Location, and Mobile Connections sections.



The Storage section includes the settings for video retention and the warning and alarm thresholds for protected footage. For more information, see Storage and Protected Footage.

Video

The Video section in General Settings determines how long after a video is recorded that a user can view it before it is marked as restricted.

Setting	Description
Time based video playback restriction applied at	How long (in minutes) after video is recorded that a user can view the video in the Windows Client. After the time elapses, the Server marks the video as restricted and a user requires the View Restricted Historical Video permission to view the restricted historical video.

Storage

The Storage section in General Settings determines how long the server farm retains video, video metadata, and log files. This global setting takes effect if you do not configure video storage settings for individual server instances.

The Server does not automatically delete protected footage. The protected footage thresholds determine when the Server warns you that protected footage is filling video storage. For more information, see Protected Footage.

Setting	Description
Limit the number of days video is stored	Deletes video older than the configured number of days.
Keep metadata longer	Retains metadata from video for the configured number of days after its associated video is deleted.

Setting	Description
Include all data	Retains all data (e.g. search results, images, etc.) for the configured number of days.
Maximum log storage in MB	The maximum size of log files, in Megabytes
Protected footage warning threshold (%)	The percentage of video storage that protected footage can use before the Server raises a warning. The default value is 80.
Protected footage alarm threshold (%)	The percentage of video storage that protected footage can use before the Server raises an alarm. The default value is 90.

Video Decorations

The Video Decorations section in General Settings determines what overlay information appears in video and how it is styled. You can set color, background color, and background transparency of the decorations.

Setting	Description
Frame rate stats	Frame rate (in frames per second)
Frame rate variance	Show how much the frame rate changes over the last 50 frames
Overlay camera name on video	Camera name
Overlay camera ID on video	Camera ID
Overlay logo on video	Use a supplied image as a logo. The image is uploaded from the TBD page.
Decoration Text Color	Color of the text
Background Sensitive	Automatically adjust text color based on the colors in the video in order to provide more contrast
Decoration Text Background	Background color for text
Transparency	Transparency of text background (Min is solid, Max is tranparent)

Alarms

The Alarms section in General Settings configures alarm aggregation and advanced alarm processing for the server farm. Alarm aggregation combines multiple alarms from the same source (e.g. zone) together in order to reduce operator overload. Advanced alarm processing configures the conditions in which an alarm can be processed by an operator.

Alarm Aggregation

Setting	Description
No Aggregation	Disables alarm aggregation.
Aggregate	Enables alarm aggregation. Once acknowledged, subsequent alarms will not trigger a new alarm state.
Aggregate and Re-Alarm	Enables alarm aggregation but enables subsequent alarms to trigger a new alarm state.
Aggregation Maximum Alarms	Configures the maximum number of alarms that can be included in an alarm aggregate.
Aggregation Timeout	Select to set how much time can elapse between alarms before new alarms are added to a new alarm aggregate.

Advanced Alarm Processing

Setting	Description
Enable advanced alarm processing	Select this option to enable advanced alarm processing in the Windows Client. Advanced alarm processing allows a user to acknowledge an alarm to claim the alarm before processing the alarm.
Reason text field is optional for masking hardware nodes	Whether a reason is required when masking hardware nodes. This option is available when you enable advanced alarm processing.
Require Integration State Change	Select this option to require that the hardware node state changes before you can reset the alarm. This option requires that you resolve the issue with the hardware node before you are able to reset the alarm. This option is available when you enable advanced alarm processing.
Acknowledgement Timeout	Select to set how much time can elapse without marking an acknowledged alarm before it returns to an unacknowledged state.

Audit

The Audit section in General Settings determines whether the Server logs events and how it archives audit logs.

Setting	Description
Enable Audit	Enable/disable the logging of events.
Never archive audit	Prevent the Server from archiving audits.
Archive audit weekly	Archive audits every week.
Audit archive retention	How long (in days) the Server retains archived audits.

SNMP

The SNMP section in General Settings configures the Server to expose telemetry to a Simple Network Management Protocol (SNMP) client.

Setting	Description
Enable SNMP	Enable/disable SNMP support.
Data polling rate	How often (in seconds) the SNMP agent polls the Server for data.
Footage size polling rate	How often (in seconds) the SNMP agent polls the Server for the size of video footage.

Configure SNMP

You can configure the Server to send SNMP data to a SNMP client.

1. In the Server configuration interface, click Settings > General Settings.
2. Select Enable SNMP.
3. In the Data polling rate, set how often (in seconds) SNMP sub-agents poll for data.
4. In the Footage size polling set how often (in seconds) the Server updates the size of the footage.

5. Click Save.
6. Restart the Senstar Symphony services.
7. Configure the Windows SNMP Agent Service on the computer that hosts the Server.

SNMP Object Identifiers

Server Information

Object	Description	Trap
serverId	Unique identifier of the Server.	No
serverName	Name of the Server.	No

Version Information

Object	Description	Trap
serverVersion	Assembly version of the Server software.	No
webserviceVersion	Version of the Server Web service protocol.	No
cameraMessageVersion	Version of the Server camera message protocol.	No
streamingVersion	Version of the Server streaming protocol.	No

Client Bandwidth

Object	Description	Trap
connectedClientNumber	Number of Windows Client instances that are connected to the Server.	No
connectedClientIndex	Unique identifier of the Windows Client.	No
connectedClientIpAddress	IP address of the Windows Client.	No
connectedClientUsername	Username that the Windows Client uses to connect to the Server.	No
connectedClientDuration	How long the Windows Client has been connected to the Server.	No
connectedClientDataReceived	How much data (in kilobytes) the Windows Client has received from the Server.	No
connectedClientCurrentBandwidth	Amount of data (in kilobytes per second) transmitted between the Windows Client and the Server.	No

Camera Information

Object	Description	Trap
cameraNumber	Number of cameras that are connected to the Server.	No
cameraId	Unique identifier for the camera.	No
cameraName	Name of the camera.	No
footagePath	Storage path for footage from the camera.	No

Object	Description	Trap
footageSize	Size (in bytes) of the footage at the storage path.	No

Storage Information

Object	Description	Trap
storagePoolNumber	Number of storage pools that are connected to the Server.	No
storagePath	The path of the storage pool.	No
storageCapacity	Total capacity (in megabytes) of the storage pool.	No
storagePercentAvailable	Available capacity (in megabytes) of the storage pool.	No
storageFootageSize	Size (in megabytes) of the footage in the storage pool.	No
storageFootageFiles	Number of footage files in the storage pool.	No

Service Information

Object	Description	Trap
infoServiceStatus	Status of the AI InfoService service.	No
netSendHistStatus	Status of the AI NetSendHist service.	No
schedulerStatus	Status of the AI Scheduler service.	No
trackNumber	Number of active AI Tracker services.	No
trackerId	Unique identifier for the AI Tracker service.	No
trackerStatus	Status of the AI Tracker service.	No

Login Monitor Information

Object	Description	Trap
authorizedLoginNotif	Notification sent when a login is successful.	Yes
unauthorizedLoginNotif	Notification sent when a login is unsuccessful.	Yes
loginNotifyIpAddress	IP address of the Windows Client.	No
loginNotifyUsername	Username that the Windows Client used to connect to the Server.	No
loginNotificationMessage	Additional details about the login.	No

Alarm Monitor Information

Object	Description	Trap
alarmNotif	Notification sent when an alarm occurs.	Yes
alarmNotifyCameraId	Identifier of the camera that recorded the alarm.	No

Object	Description	Trap
alarmNotifyCameraName	Name of the camera that recorded the alarm.	No
alarmNotifyUserId	Identifier of the user who marked the alarm.	No
alarmNotifyUserName	Name of the user who marked the alarm.	No
alarmNotifyMarkedDelay	Time at which the alarm was marked.	No
alarmNotifyFalseAlarm	Is the alarm a false alarm.	No
alarmNotifyRuleId	Identifier of the rule causing the alarm.	No
alarmNotifyRuleName	Name of the rule causing the alarm.	No
alarmNotifyDBId	Identifier of the alarm.	No
alarmNotifyComment	Comment associated with that alarm.	No
alarmNotifyMSSinceChange	Number of milliseconds between when the alarm occurred and when it was detected.	No

Device Movement Monitor Information

Object	Description	Trap
devicesMovedNotif	Notification sent when a device moves from one server to another server.	Yes
sourceServerId	Identifier of the server from which the device moved.	No
destinationServerId	Identifier of the server to which the device moved.	No
numberDevicesMoved	Number of devices that moved from the source server to the destination server.	No

Health Monitor Information

Object	Description	Trap
healthMonitorFaultNotification	Notification sent when the health monitor detects a fault.	Yes
healthMonitorActionNotification	Notification sent when the health monitor takes an action in response to a fault.	Yes
healthMonitorName	Name of the associated health monitor.	No
healthMonitorAction	The action that the health monitor took in response to a fault.	No

Web Client

The Web Client section in General Settings configures load-balancing, refresh rate (how often the client receives updates from server), and ICE server settings for the Web Client.

Setting	Description
Randomly redirect master server logins to other available servers in the farm	Configures if the master Server redirects users to other servers in the server farm. This provides load balancing for the Web Client.

Setting	Description
Refresh rate	How often the Web Client updates information from the Server.
Use an ICE Server	Select if you are using an Interactive Connectivity Establishment (ICE) server with the Web Client.
Type	The type of an ICE Server you are using, STUN or TURN. This setting is available when you select Use an ICE Server.
URL	URL of the ICE Server. This setting is only available when you select Use an ICE Server.
Username	User name for the ICE Server. This setting is only available when you select Use an ICE Server.
Password	Password for the ICE Server. This setting is available when you select Use an ICE Server.

SMTP

The SMTP section in General Settings configures the email server that the Server uses to send email notifications.

Setting	Description
SMTP server	URL of the SMTP server.
Use Secure Sockets Layer	Use SSL for communication with the SMTP server.
Sender email account	Defines the email account that the Server uses to send email.
SMTP server requires authentication	Configures if the SMTP requires authentication.
Username	User name that the Server uses to authenticate with the SMTP server. This setting is only available when you select SMTP server requires authentication.
Password	Password that the Server uses to authenticate with the SMTP server. This setting is only available when you select SMTP server requires authentication.
Send a test email to address	Use this field to test the SMTP settings. Type an email address and click Send Test to send a test email.

User Connections

The User Connections section in General Settings restricts concurrent logins and idle sessions to the Server configuration interface.

Setting	Description
Do not allow more than one concurrent connection per user	Configures if users can log in to more than one Server configuration interface concurrently per server farm.
Automatically log out inactive Server Configuration users	Configures if the Server automatically logs users out of the Server configuration interface after a period of inactivity.
Minutes of Inactivity	The timeout period for the Server configuration interface.

Farm Location

The Farm Location section in General Settings sets the GPS coordinates of the Server farm.

Setting	Description
GPS Latitude	Latitudinal coordinate of the Server farm.
GPS Longitude	Longitudinal coordinate of the Server farm.

Mobile Connections

The Mobile Connections section in General Settings enables push notifications for iOS (e.g. iPhone) devices.

Setting	Description
Enable iOS Notifications	Enable/disable push notifications for iOS devices.

Per-server mobile connection settings (mobile port, video proxy port, and SSL certificate) are configured under Settings > Servers. See Configure Mobile Connections and Add an SSL Certificate.

Cloud Services

The Cloud Services tab in the Server configuration interface is the interface for configuring cloud services that provide additional functionality for the server farm.

Health Monitoring

If you purchased the Maintenance and Support option, you can turn on health monitoring. Health monitoring sends telemetry data from the server to the Senstar Xnet. You can log in to the Senstar Xnet and view the status of all servers.

1. In the Server configuration interface, click Settings > Cloud Services.
2. In the Health Monitoring section, move the Send Packets to Senstar XNet toggle switch to On.

To turn off health monitoring, move the Send Packets to Senstar XNet toggle switch to Off.

Senstar Enterprise Manager

You can manage the server or farm using the Senstar Enterprise Manager.

If you have created users or groups, those users and groups are replaced with the users from the Senstar Enterprise Manager when you add the server to the Senstar Enterprise Manager. This includes administrator users. Senstar recommends that you back up your configuration settings or database before you manage your server or server farm with the Senstar Enterprise Manager.

1. Click Settings > Cloud Services.
2. In the Enterprise Manager section, move the Current State toggle switch to On.
3. In the Address field, type the IP address of the Senstar Enterprise Manager.
4. In the Site Name field, type a name for the site. The Senstar Enterprise Manager uses this site name to identify the server or server farm.
5. In the Organization Name field, type the Senstar Enterprise Manager organization name.
6. In the Passphrase field, type the Senstar Enterprise Manager password.

7. Click Save.

Cloud Proxy

You can connect the server to the Senstar Cloud to facilitate authentication and communication between the Server and mobile devices. Before you begin, configure the Senstar Cloud and obtain the API key.

1. Click Settings > Cloud Services.
2. Click the Enable Cloud Proxy heartbeat switch to turn the heartbeat on.
3. In the Cloud Proxy API key field, type the API key from the Senstar Cloud.
4. Click Save.

After you connect the server to the Senstar Cloud, you can log in to the Senstar Cloud to confirm that the connection is active.

Aggregates

An aggregate is a collection of cameras that can combine the people count from all of the cameras and present that information on an HTML page. You can use aggregates to provide comprehensive occupancy counts and instructions to customers.

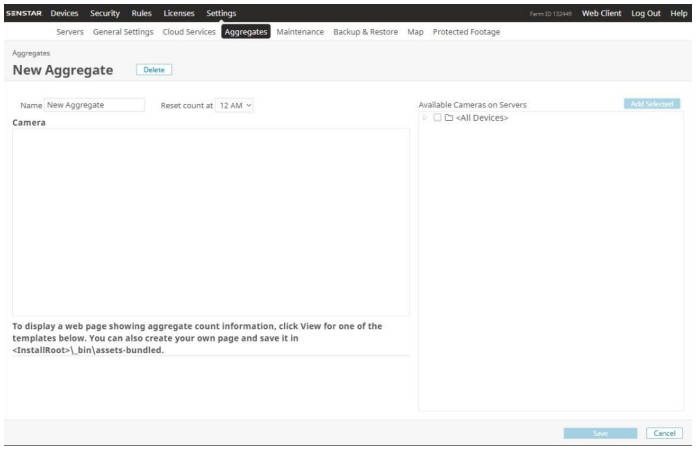
Manage Aggregates

You can create, modify, copy, and delete aggregates, and customize the aggregated people counter HTML page.

Create an Aggregate

Configure the aggregated people counter video analytic in the Server configuration interface.

A camera must be running the Indoor People Tracking video analytic to be visible in the Available Cameras on Servers list.



1. In the Server configuration interface, click Settings > Aggregates.

2. Click Add Aggregate.
3. In the Name field, type a meaningful name for the aggregate count.
4. In the Reset count at list, select the hour at which the aggregate count resets to zero. The list contains the 24 hours of the day (12 AM through 11 PM). Resetting the count daily helps maintain accuracy.
5. In the Available Cameras on Servers tree, expand the device tree, select the cameras that you want to include in the aggregate count, and click Add Selected. The selected cameras appear in the Camera list. Only cameras that are running the Indoor People Tracking video analytic are eligible.
6. (Optional) To remove a camera from the aggregate, select it in the Camera list and click the X button beside it.
7. (Optional) In the templates list below the Camera list, click View beside a template (for example, Aggregate-en) to preview the HTML page that the Server uses to display the aggregate count. You can create your own page and save it in `<InstallRoot>\_bin\assets-bundled` to make it available as a template.
8. Click Save.

After you add an aggregate, the Server creates an HTML page that you can use to display occupancy information and instructions. To open the HTML page, click the link at the bottom of the Aggregates page.

Modify an Aggregate

1. In the Server configuration interface, click Settings > Aggregates.
2. Select the aggregate and click Edit.
3. Perform any of the following tasks:
   a. To modify the name of the aggregate, type a new name in the Name field.
   b. To change the reset time, select a new value in the Reset count at list.
   c. To add a camera to the aggregate, select the camera in the Available Cameras on Servers list and click Add Selected.
   d. To remove a camera from the aggregate, highlight the camera in the Camera list and click the X button.
4. Click Save.

Copy an Aggregate

1. In the Server configuration interface, click Settings > Aggregates.
2. Select the aggregate and click Clone.
3. Modify the aggregate.
4. Click Save.

Delete an Aggregate

1. In the Server configuration interface, click Settings > Aggregates.
2. Select the aggregate and click Delete.

Modify the Aggregated People Counter HTML

You can modify the HTML page that the aggregated people counter video analytic uses to display occupancy counts and instructions to customers.

You can also copy an existing HTML file to create multiple HTML files to display different occupancy counts and instructions for other aggregates or situations.

1. On the computer that hosts the Server, navigate to _bin\assets-bundled.
2. Open the HTML file (for example, Aggregate-en.html) with a text editor.
3. To change the occupancy thresholds, modify the following code:

```
var thresholdYellow = 50;
var thresholdRed = 75;
```

1. To change the messages, modify the following code:

```
 function showGreen(difference) {
            document.getElementById("message").innerHTML = "LIMITED STORE<br />CAPACITY";
            document.getElementById("instructions").innerHTML = "PLEASE PROCEED WITH
CAUTION";
```

```
function showYellow(difference) {
            document.getElementById("message").innerHTML = "LIMITED STORE<br />CAPACITY";
            document.getElementById("instructions").innerHTML = "PLEASE MAINTAIN SOCIAL
DISTANCING";
```

```
function showRed(difference) {
            document.getElementById("message").innerHTML = "MAXIMUM<br />CAPACITY";
            document.getElementById("instructions").innerHTML = "PLEASE WAIT FOR
ASSISTANCE";
```

```
<div style="padding-top: 2vw; font-size: 1.5vw; ">CURRENT NUMBER<br />OF PEOPLE</div>
```

```
<div style="padding-top: 2vw; font-size: 1.5vw; ">MAXIMUM NUMBER<br />OF PEOPLE
ALLOWED</div>
```

1. Save and close the HTML file.

Find an Aggregate

To quickly find a specific aggregate, use filters and sorting.

Filter

You can filter the aggregate list using the following filter:

- aggregate name (Name)
  1. In the Server configuration interface, click Settings > Aggregates.
  2. Click the magnifying glass to make the filter text fields visible.
  3. Define the filter criteria.
  4. Click Apply filter.

Sort

You can sort the list of aggregates by clicking the column name. Clicking the column name toggles between ascending and descending order.

Clear

To reset the filter and restore the list of aggregates, click Clear Filter.

Maintenance

The Maintenance tab in the Server configuration interface configures when the Windows Client applies software updates and when the Server downloads and installs updates.

Client Updates

The Client Updates section determines when Windows Client instances connected to this server farm apply software updates.

Setting	Description
Immediately	Update the Windows Client as soon as an update is available.
During time frame	Update the Windows Client only between the Begin and End times.
Never	Prevent automatic updates to the Windows Client.

Server Updates

The Server Updates section shows the last time the Server checked for updates, lets you check manually, and configures automatic updates.

Setting	Description
Last check for updates	The date and time of the most recent update check, or Never if no check has been performed.
Check for Updates	Manually check for available updates. This option is available for standalone (single-server) farms only.
Enable automatic updates	Whether the Server automatically downloads and installs updates.
Automatically download and install at	The time of day at which to download and install updates.
Update from the following location	Use a local file path as the update source.
Update from product web site	Use the Senstar product web site as the update source. This setting is available when you select Enable automatic updates.

If automatic updates are incompatible with installed components (for example, Face Recognition), the page lists those components and you must update them manually

before automatic updates can run.

Backup & Restore

The Backup & Restore tab in the Server configuration interface is the interface for backing up and restoring Server configurations.

You can use configurations to move settings between different Server instances or to restore an existing Server.

If you have a Server farm, it is strongly recommended that you save the backups to a location that is not on one of the servers in the farm, but is available to all of the servers in the farm (e.g., a NAS). This helps to recover servers in disaster recovery situations. Additionally, if you have a Maintenance and Support license, you can save backups online to the Senstar Xnet.

The Server does not support restoring a configuration from an earlier version of the Server.

Configure Backups

What it is

A Server backup is a snapshot of the server's configuration — site layout, devices, rules, events, action sets, schedules, users, groups, security profiles, licences, and general settings. It does **not** contain recorded video. Recorded video lives under the video storage paths and is retained according to each camera's retention policy; see video storage for a camera.

You can store backups locally (a path on the server or a mounted share) and, with a Maintenance & Support licence, also to the Senstar Xnet for off-site recovery.

When you'd use it

- **Recover from hardware failure** — restore the configuration onto replacement hardware rather than rebuilding by hand.
- **Roll back a change** — revert a bad rule, security profile, or integration change.
- **Migrate** — move a configuration to a new server.
- **Comply with your organisation's backup policy** — include the Server in nightly or weekly backups.

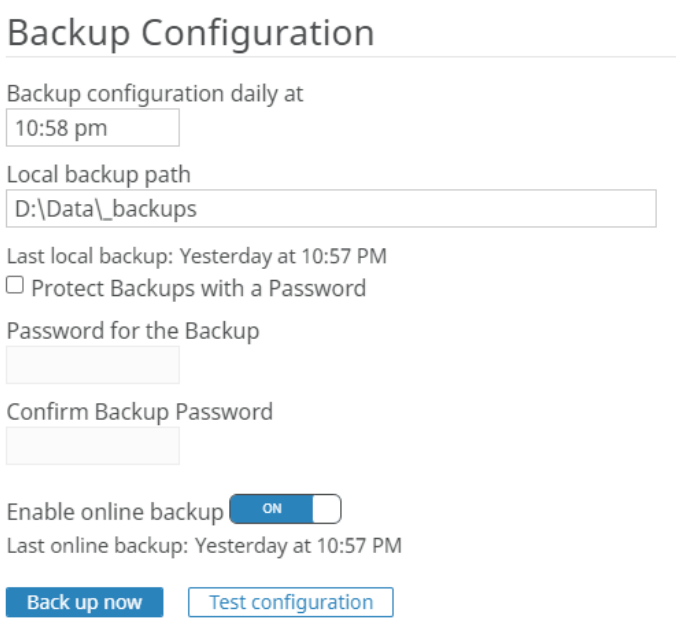
Prerequisites

- Permission to edit Server settings.
- A writable path for local backups (a local drive, an attached volume, or a mounted network share with credentials the Server service account can use).
- For online backup, a Maintenance & Support licence and internet access from the Server to the Senstar Xnet.

How often to run

The default schedule is a single daily backup at 23:00 server time. Most sites keep the daily cadence and change only the time so the backup runs outside heavy recording windows. For sites that change configuration frequently (new cameras, frequent rule tuning), consider combining the nightly backup with a manual **Back up now** before and after significant changes.

Procedure



1. In the Server configuration interface, click **Settings** > **Backup & Restore**.
2. In the **Backup configuration daily at** field, set the time at which the Server creates the backup. Choose a time when the server is not under heavy load.
3. In the **Local backup path** field, set the path where the Server writes the backup. Use a volume or share that is backed up as part of your broader IT backup policy — a backup that lives only on the Server will not survive a disk failure.
4. To encrypt the backup file with a password, do the following:
   a. Select **Protect Backups with a Password**.
   b. Type the password in **Password for the Backup**. The password must meet the complexity requirements configured for the Server.
   c. Re-enter the password in **Confirm Backup Password**.

      Record the password in your organisation's password manager. Without it, the backup cannot be restored.
5. To also upload backups to the Senstar Xnet, turn **Enable online backup** on.

   Online backup requires a Maintenance & Support licence.
6. Click **Test configuration** to confirm the path is writable and, if online backup is enabled, that the Server can reach the Senstar Xnet.
7. Click **Back up now** to create an immediate backup.

Related tasks

- Restore from a Local Backup
- Restore from Online Backup
- Restore from File

Restore from a Local Backup

You can restore configuration settings for the Server from the local backup path.

1. In the Server configuration interface, click Settings > Backup & Restore.
2. To restore the configuration settings from a Server that is not part of the server farm, select Restore backup from different hardware, excluding license.
3. Click the Restore local backup tab.
4. To show compatible backup files in the local path, select Show only compatible versions.
5. Select the backup file.
6. Click Restore.

Restore from Online Backup

You can restore configuration settings for a Server from the Senstar Xnet.

This feature requires a Maintenance & Support license.

1. In the Server configuration interface, click Settings > Backup & Restore.
2. Click the Restore online backup.
3. To show compatible backup files in the local path, select Show only compatible versions.
4. Select the backup file.
5. Click Restore.

Restore from File

You can restore configuration settings for a Server from a file.

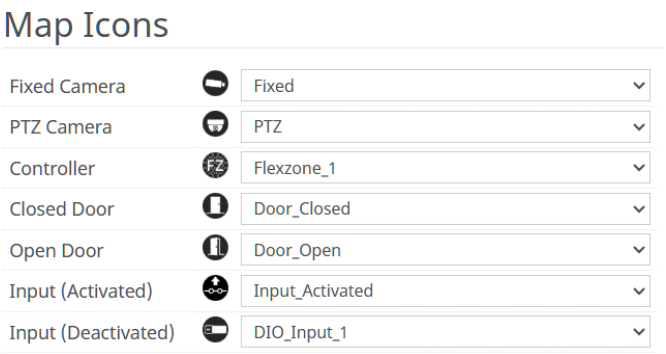
1. In the Server configuration interface, click Settings > Backup & Restore.
2. To restore the configuration settings from a Server that is not part of the server farm, select Restore backup from different hardware, excluding license.
3. Click the Restore from file.
4. Drag the file into the interface or browse to the backup file.
5. Click Restore.

Map

Map settings let you change the icons placed on a map to match specific deployed equipment and customize the colors used to represent device states, such as Alarm, Supervision, Mask, Fault, Warning, and Normal.

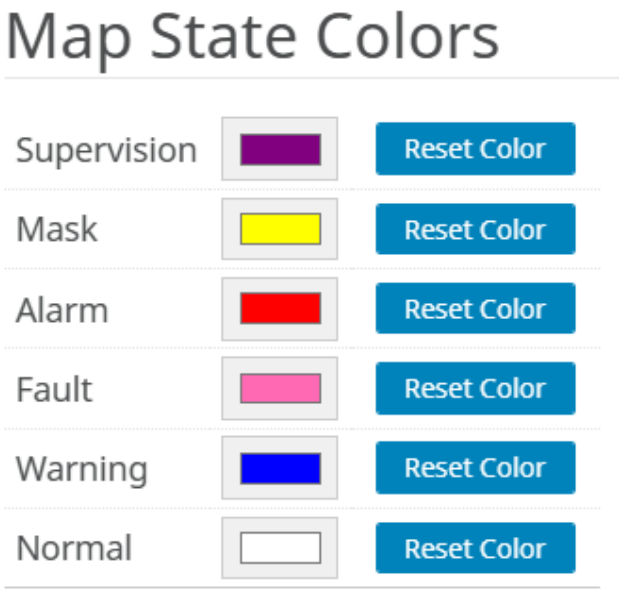
Map Icons

Use the Map Icons settings to choose the icon that represents each device type on a map. For each device type, select an icon from the list to match the deployed equipment.



Map State Colors

Use the Map State Colors settings to change the color that represents each device state on a map. Click the color swatch beside a state to pick a new color, or click Reset Color to restore the default.

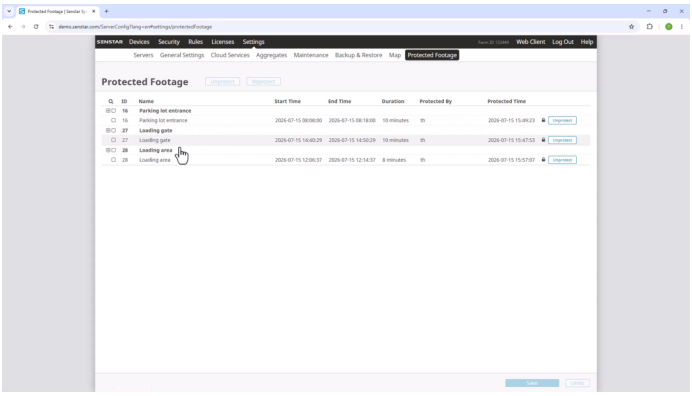


Protected Footage

Protected footage is recorded video that a user has protected so that the Server does not delete it. The Server excludes protected footage from automatic storage cleanup and retention settings. Protected footage remains on the Server until a user removes the protection.

Users protect footage from the camera timeline in the Windows Client interface. For more information, see Protect Footage. To remove or restore protection, see Unprotect Footage.

The Protected Footage page lists every protected section of footage on the Server, grouped by camera. To view the Protected Footage page, click Settings > Protected Footage in the Server configuration interface.



Column	Description
ID	The identifier of the camera.
Name	The name of the camera.
Start Time	The start of the protected time range.
End Time	The end of the protected time range.
Duration	The length of the protected time range.
Protected By	The user that protected the footage.
Protected Time	The time at which the user protected the footage.

The Protected By and Protected Time columns provide an audit trail for protected footage. To support the audit trail, use individual user accounts rather than shared logins.

Because the Server excludes protected footage from automatic storage cleanup, protected footage can accumulate and fill video storage. The Server can raise a warning and an alarm when protected footage reaches a configured percentage of video storage. For more information, see Storage.

Protecting footage and unprotecting footage are separate permissions. You can allow operators to protect footage and reserve unprotecting footage for administrators. For more information, see Device Permissions.

Unprotect Footage

You can unprotect footage so that the Server applies its normal retention settings to the footage. Once you unprotect footage, automatic storage cleanup can delete the footage. For more information about retention settings, see Storage.

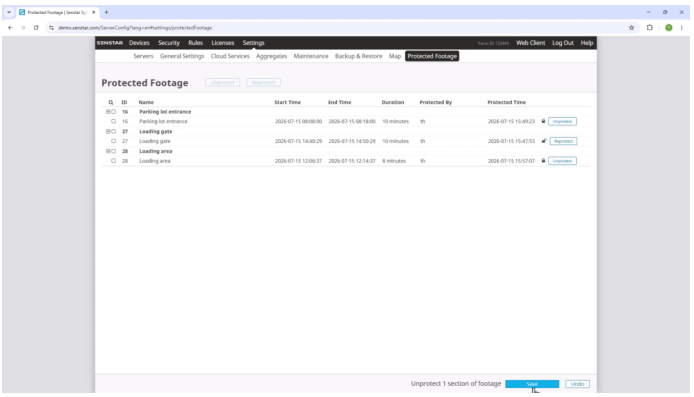
Users protect footage from the camera timeline in the Windows Client interface. For more information, see Protect Footage.

Review the Protected Footage page periodically and unprotect footage that you no longer need so that the Server can release the storage. The Unprotect and Reprotect buttons are available only if your group has the Unprotect Footage permission. For more information, see Device Permissions.

1. In the Server configuration interface, click Settings > Protected Footage.
2. Perform one of the following tasks:
   - To unprotect one section of footage, click Unprotect in the row for that section.
   - To unprotect multiple sections of footage, select the checkbox for each section and click Unprotect at the top of the list.

3. Click Save.

The Server displays the pending change at the bottom of the page (for example, Unprotect 1 section of footage). Before you click Save, you can click Reprotect in a row to cancel the change for that section, or click Undo to discard all pending changes.



Server Management

The Server runs the following services.

Service	Function
AI Authentication Service	• Performs single sign-on authentication • Log file prefix: ◦ sso
AI AxisPACSListenerService	• Communicates with Axis access control devices • Optional service/Manual installation • Log file prefix: ◦ aacl
AI DataAccessService	• Communicates with the Senstar Symphony Database • Log file prefix: ◦ da
AI Enterprise Management Service	• Communicates with the Senstar Enterprise Manager • Updates the Server software automatically when using the Senstar Enterprise Manager to make configuration changes • Log file prefix: ◦ fs

Service	Function

`AI InfoService`	• Hosts the Senstar Symphony Web service that receives all requests from the Windows Client
	• Hosts the Web server for the Server configuration interface
	• Retrieves timeline data from footage storage
	• Log file prefixes:
	  ◦ `is` (information service)
	  ◦ `isac` (access control)
	  ◦ `isbk` (automatic backup)

`AI Mobile Bridge`	• Facilitates communication between mobile devices and the Server • Facilitates communication between the Senstar Thin Client and the Server • Log file prefix: ◦ `mo`
`AI NetSendHist`	• Retrieves historical video from the footage storage • Streams video • Creates historical images • Log file prefix: ◦ `hs`
`AI OPCServer`	• Communicates with the OPC Server • Optional service/Manual installation • Log file prefix: ◦ `op`

`AI Scheduler`	• Polls hardware alarm inputs
	• Generates alarms
	• Generates reports
	• Removes expired video files
	• Retrieves search results (video and XML) from the NAS
	• Log file prefixes:
	  ◦ `sc` (scheduler)
	  ◦ `scac` (actions)
	  ◦ `scax` (access)
	  ◦ `sccl` (cleaner)
	  ◦ `sccp` (CPU/memory)
	  ◦ `scis` (multicaster)
	  ◦ `scpm` (PTZ)
	  ◦ `scse` (searches)

`AI SNMP Registry`	• Registers sub-agents

Service	Function
AI Tracker	• Analyzes video • Saves video to storage • Log file prefix: ◦ cs The Server creates an instance of the AI Tracker service for each camera. The names of the AI Tracker service instances include the ID of the camera.

AI Watchdog	• Monitors and starts Senstar Symphony services
	• Log file prefixes:
	  ◦ hm (health monitoring)
	  ◦ nu (health monitor)

Check CPU Usage

You can use the ShowCPUUsage command to check the CPU usage on the computer that hosts the Server.

The ShowCPUUsage command displays the CPU usage as a percentage of the capacity of a single core. For example, if the computer has four cores and the Server is using 30% of each core, the result is 120.

Prior to Senstar Symphony 8.5, you could check the CPU usage by using the KillAll 8 command.

1. On the computer that hosts the Server, run a command prompt as administrator.
2. In the command prompt, type `ShowCPUUsage` and press Enter.

Manage Services

You can use the KillAll command to stop, start, and restart Senstar Symphony services.

The following parameters are used with the KillAll command to manage the Senstar Symphony services.

Parameter	Description
1	Stop the Senstar Symphony services gracefully.
2	Terminate the Senstar Symphony services.
4	Terminate the Senstar Symphony services only if necessary (excluding the AI InfoService service).
5	Start the Senstar Symphony services gracefully (excluding the AI InfoService service).
6 pid	Terminate the Senstar Symphony service with process ID equal to pid.
7	Restart the AI InfoService service.
9	Terminate the Senstar Symphony services only if necessary (including the AI InfoService service).
a	Start the Senstar Symphony services.
d	Disable all of the Senstar Symphony services.

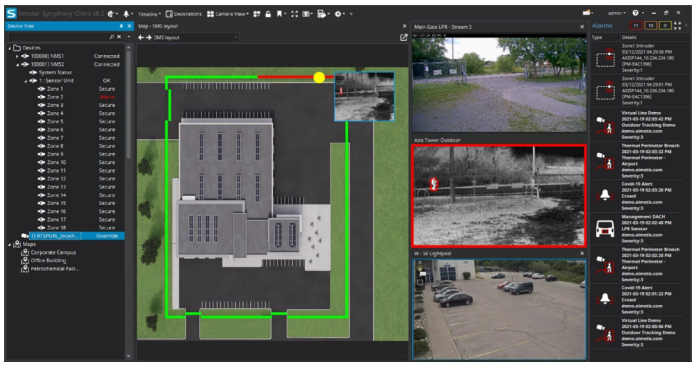
Parameter	Description
e	Enable all of the Senstar Symphony services. The AI Tracker service is set to manual and all other Senstar Symphony services are set to automatic.
r	Terminate the Senstar Symphony services only if necessary (including the AI InfoService service) and start the Senstar Symphony services gracefully (excluding the AI InfoService service).
s	Restart the Senstar Symphony services in sequence.
t tracker_id	Restart the AI Tracker service with the ID equal to tracker_id.
x	Terminate the Senstar Symphony services only if necessary (including the AI InfoService service) and stop any instances of the Windows Client running on the computer.

1. On the computer that hosts the Server, run a command prompt as administrator.
2. In the command prompt, type `KillAll` `parameter` and press Enter.

   Where *parameter* is the number or letter that defines the specific function of the `KillAll` command.

Windows Client

The Windows Client is an application that enables operators to monitor cameras and alarms, while administrators can use the client to manage video, generate reports, configure the display of alarms. It's automatically installed with the server but can also be installed on workstations. As, Senstar Symphony is licensed per camera or device, you can install the Windows Client on as many machines as you would like.



Getting Started

Action	Topic
Learn the basics	User Interface
Connect to a Symphony server	Connect to a Server
View the video stream from a camera	Viewing a Camera's Video Stream
Monitor and respond to alarms	Managing Alarms
Save recorded video to a file	Exporting Video
Customize the client layout and appearance	Interface Customizations

Change Your Password

You can change the password for your user account in the Windows Client interface.

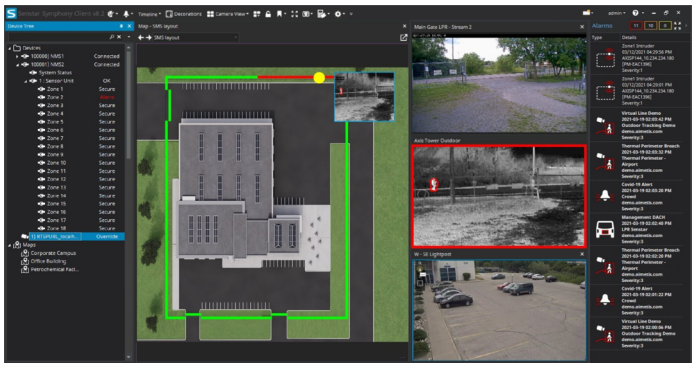
This process changes your password for the Server farm that the Windows Client is connected to.

This feature is not available if you use Active Directory authentication for your Server.

1. In the Windows Client interface, click your user name in the toolbar and then click Change Password.
2. In the Old Password field, type your password.
3. In the New Password field, type the password that you want to change to.
4. In the Confirm Password field, type the password that you want to change to again.
5. Click Change Password.

User Interface

The Windows Client interface is organized into several panes and panels that you use to monitor cameras, respond to alarms, navigate maps, and configure the system.



Device Tree

The device tree lists the servers, cameras, camera views, carousels, maps, and other devices that are available on the connected servers. Use the device tree to select a device to view, search for a device, or change the state of a device.

View Panels

View panels display video from cameras, maps, web browsers, and other content. You can arrange view panels in the workspace, save layouts as camera views, and open additional panels in floating or docked windows.

Toolbar

The toolbar provides quick access to common commands such as opening views, switching layouts, and managing alarms. You can customize the toolbar to show the commands that you use most often.

Alarm Console

The Alarm Console lists active and historical alarms from the connected servers. Use the Alarm Console to view, acknowledge, and share alarms.

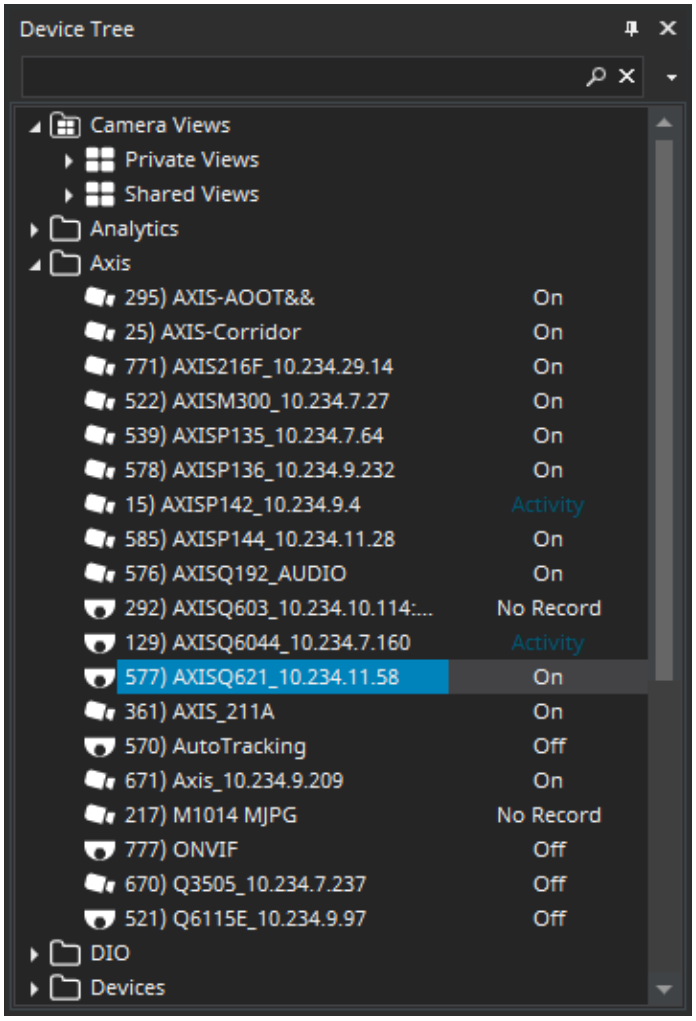
Timeline

The timeline shows recorded video, alarms, and events for the cameras that you are viewing. Use the timeline to navigate recorded video and to review activity over a period of time.

Device Tree

The device tree in the Windows Client interface lists the cameras, devices, and carousels available on the Server.

+



+

You can search for cameras, devices, and carousels in the device tree. To search, type your search criteria in the search field and click Search. The Windows Client filters the device tree to show only those results that match your search criteria. To restore the device tree, press the X in the search field.

The device tree also displays the states of cameras and devices connected to the Server.

The device tree includes a context menu that lets you send commands to devices. If you right-click a device in the device tree, the Windows Client displays applicable commands.

Search the Device Tree

You can search the device tree for cameras, devices, inputs and outputs, and carousels.

When you search the device tree, the Windows Client filters the device tree to only includes devices that match your search criteria.

1. In the Windows Client interface, type the search term in the search field of the device tree.
2. In the list, select the properties that you want to search. You can search the camera ID, camera name, camera code, and description.
3. To limit the results to items that exactly match you search terms, select Exact Matches Only.

4. To exclude items that match you search terms from the search results, select Exclude Matches. For example, you can use

On

as a search term and select

Exclude Matches

to display all items that do not have the status of On.

1. Click the search icon.

To restore the device tree list, click the X icon.

Display a List of Users Viewing a Camera

You can view a list of users who are logged in to a Windows Client that has a camera active in a camera view panel.

To display a list of users viewing a camera, you must be an administrator user.

1. In the Windows Client interface, right-click a camera.
2. Click Users Viewing Camera.
3. To refresh the list of users viewing the camera, click Refresh.

Suspending Access to Video

The Server includes functionality to suspend access to video (ban video) from a camera or camera group for a specific user group.

To use this feature, you must create a user group called UserBanGroup. When you suspend access to video, the users in the UserBanGroup group cannot view video from the camera, while other users can view video from the camera. The users in the UserBanGroup group cannot view video again until you resume access to video (unban video).

When you suspend access to video from a camera or camera group, the camera or camera group appears in the Server configuration interface.

Create a User Group for Suspending Access to Video

To suspend access to video, you must create a user group and add the group to the Server.

1. In the Windows Client interface, perform the following tasks:
   a. Create a group called UserBanGroup.
   b. Add any users that you want to prevent from viewing video to the UserBanGroup.
   c. If you want to suspend access to video on video walls, add users who can log in to video wall clients to the UserBanGroup.
2. In the Windows Client interface, perform the following tasks:
   a. Click Server Configuration > Manual Configuration Editor.
   b. Click Add a new setting.
   c. Enter the following values:

```
Type = Global
```

```
Section = Main
ID = <empty>
Key = LiveBanGroup
Value = UserBanGroup
```

a. Press Enter.
b. Click OK.

Create a Camera Tour

You can create a tour of preset locations for a PTZ camera to visit in the Windows Client interface.

1. In the Windows Client interface, right-click a camera in the Device Tree.
2. Click Camera Tour.
3. For each location in the camera tour, perform the following tasks:
   a. Use the PTZ controls to move the camera to the desired location and zoom.
   b. Click Add Live View PTZ Location To The List.
   c. Click the tour location and edit its details.
4. To set the schedule for the camera tour, perform the following tasks:
   a. Click Set Schedule For This Tour.
   b. In the schedule list, select an existing schedule or Create new schedule.
   c. If you create a new schedule, type a name for the schedule.
   d. Mark the cells as either active or inactive.
   e. Click OK.
5. Click OK.

Change IO State

You can change the state of the outputs on devices in the Windows Client interface.

1. In the Windows Client interface, right-click a camera in the Device Tree.
2. Click Change IO state.
3. In the Device list, select the device on which to change the output state.
4. In the Relay # field, specify the module and port for the output.
5. Click Activate or Deactivate.

Link a Camera View

You can link camera views so that multiple camera views open when you open a camera view. When you open the primary camera view, the Windows Client opens the linked camera views in new floating views.

Before you begin, save at least two camera views (one primary and one secondary).

Linking camera views is an easy way to open numerous camera view panels.

1. In the Windows Client interface, right-click a camera view in the Device Tree.
2. Click Configure Camera View.
3. In the Select linked view list, select the secondary camera views that open when you open the primary camera view.
4. To close any unused camera view panels when you open a new camera view, select Close overlapping views.
5. Click OK.

Disconnect Audio

You can disconnect the audio from a camera so that the Windows Client does not receive any audio from the camera.

When you disconnect audio, the Enable Audio Input setting for the camera in the Server configuration interface is cleared.

Connecting and disconnecting audio causes the Windows Client to restart the connection to the camera.

1. In the Windows Client interface, right-click a camera in the Device Tree.
2. Click Disconnect audio. Any video that the

Windows Client

displays or records from the camera when the audio is disconnected does not include audio.

To connect the audio again, click

Connect audio

.

Two-Way Audio

You can use two-way audio in the Windows Client to speak through a camera that has a connected speaker while you continue to listen to the camera's microphone.

Before you begin:

- The camera must support two-way audio and have a microphone and speaker connected.
- The camera must have audio input and audio output enabled in the Server configuration interface.
- Your Windows Client workstation must have a microphone connected.
- Your security profile must allow audio output.

Start a Two-Way Audio Session

1. In the Windows Client interface, open the camera in a view panel.
2. Right-click the camera in the view panel or in the device tree.
3. Click Talk to Camera.
4. Hold the Push to Talk button or press the configured keyboard shortcut while you speak.

The Windows Client sends audio from your microphone to the camera's speaker for as long as you hold

the button. The camera's microphone audio continues to play in the Windows Client the entire time.

End a Two-Way Audio Session

1. Right-click the camera in the view panel or in the device tree.
2. Click Stop Talking.

Only one Windows Client can talk to a camera at a time. If another operator is already using two-way audio with the camera, the Talk to Camera option is unavailable until the other operator stops.

Hide Device Status

You can hide the status of devices in the device tree.

1. In the Windows Client interface, click View > Settings.
2. Click the Customize tab.
3. In the Device Tree pane, clear the Show Device Status box.
4. Click OK. /

Server List

The Windows Client interface lists the Server instances to which the Windows Client is connected and the state of those instances. You can select a Server to access the cameras and devices that are connected to that instance.

By default, the Windows Client interface displays the Server instances to which the Windows Client can access in the Farm list on the toolbar.

Optionally, you can configure the Windows Client interface to display the Server instances to which the Windows Client can connect in a server list panel. Enabling the server list panel hides the server list in the toolbar.

The farm list and the server list panel include all of the Server instances to which you have configured a connection.

Select the Active Server Using the Farm List

You can select the active Server in the farm list on the toolbar.

The farm list is visible in the Windows Client interface by default.

1. In the Windows Client interface, click the down arrow in the farm list.
2. In the server list, click the Server that you want to be active in the Windows Client.

Enable the Server List Pane

You can display the service list as a panel in the Windows Client interface.

1. Open the acc.ini file at %appdata%\Senstar8.
2. Set the `ShowFarmDropDown` value in the `Main` to `False`.
3. Save and close the acc.ini file.
4. Start the Windows Client.

5. In the Windows Client interface, click View > Server List.

Select the Active Server Using the Server List

Before you begin, you must enable the server list pane.

In the Server List pane of the Windows Client interface, click the Server that you want to be active in the Windows Client.

View Panels

View panels can display live video, recorded video, decorations from cameras, browser pages, and maps in the Windows Client interface.

View panels can display overlays with controls for the camera. To hide the overlays, you can press and hold the Shift key while you perform actions (for example, box zoom) in the camera view panel.

+

+

View a Camera

You can view a camera in each camera view panel in the Windows Client interface.

Before you begin:

- Add a camera to the Server
- Open a floating or docked camera view
    1. In the Windows Client interface, click a camera view.
    2. In the device tree, click the camera that you want to view.

View a Browser

You can view a browser in each camera view panel in the Windows Client interface.

Before you begin:

- Add a browser to the Server
- Open a floating or docked camera view
    1. In the Windows Client interface, click a camera view panel.
    2. In the device tree, click the browser that you want to view.

View a Map

You can view a map in each camera view panel in the Windows Client interface.

Before you begin:

- Add a map to the Windows Client
- Open a floating or docked camera view

1. In the Windows Client interface, click a camera view panel.
2. In the device tree, click the browser that you want to view.

View a Senstar Thin Client

You can view a Windows Client interface device in the Windows Client interface.

Before you begin:

- Add a Senstar Thin Client to the Server

When you view a Senstar Thin Client in the Windows Client interface, the Senstar Thin Client opens in a new floating view.

In the device tree, click the Senstar Thin Client that you want to view.

View Picture in Picture

You can view live video in a nested window when viewing recorded video.

The picture-in-picture window displays live video while the main camera view panel displays historical video.

1. In a camera view panel in the Windows Client interface, perform one of the following tasks:
   a. Right-click in the camera view panel and click Show Picture in Picture.
   b. Hover in the camera view panel and click the Picture in Picture icon.
2. View recorded video in the main camera view panel to display live video in the picture-in-picture window.
3. To move the picture-in-picture window, click one of the icons in the corner of the picture-in-picture window to move the window to that corner of the camera view panel.

View Instant Replay

You can play historical video either 5 or 10 seconds behind live video in the in the Windows Client.

You can select the instant replay duration on the Video Settings page in the Windows Client settings.

1. In the Windows Client interface, set the instant replay duration.
2. In a video pane in the Windows Client interface, click the Instant Replay icon.
3. View recorded video.

To end the instant replay, click the

Go to live view

icon.

Save a Camera View

You can save the layout of a docked or floating view to provide easy access to the view configuration.

1. In the Windows Client interface, click Camera View > Save Current View.
2. In the Save As window, perform one of the following tasks:
   - To overwrite an existing camera view, select Existing Camera View and select the existing camera view to overwrite.
   - To save as a new camera view, select New Camera View and type a name for the camera view.
3. To make the saved camera view public, select Shared with other users.
4. Click OK.

Load a Camera View

1. In the Windows Client interface, click Camera View > Load Camera View.
2. Select the camera view to load.

Open a Docked Camera View

You can open a camera view in the Windows Client interface.

The Windows Client includes camera views with 1, 4, 6, 9, 16, and 25 camera view panels.

1. In the Windows Client interface, click Camera View > New Docked View.
2. Click the camera view that you want to open.

Open a Floating Camera View

You can open a camera view in an new window.

The Windows Client includes camera views with 1, 4, 6, 9, 16, and 25 camera view panels.

To prevent the view panels in the floating from changing, click the Prevent panel selection icon (lock) in the floating view. Although you cannot select the panel, you can still place the focus on the panelby clicking in the panel.

1. In the Windows Client interface, click Camera View > New Floating View.
2. Click the camera view that you want to open.

Add a Camera View Panel

You can add a camera view panel to the Windows Client interface. A new camera view panel appears as a floating camera view panel, but you can dock it in the Windows Client interface.

1. In the Windows Client interface, click Add Camera View Panel.
2. Drag the camera view panel to the desired location.

Add an Alarm

You can add a manual alarm to a camera in the Windows Client.

You can use manual alarms to activate the action set associated with the manual rule.

1. In the Windows Client interface, open the camera to which you want to add an alarm in a camera

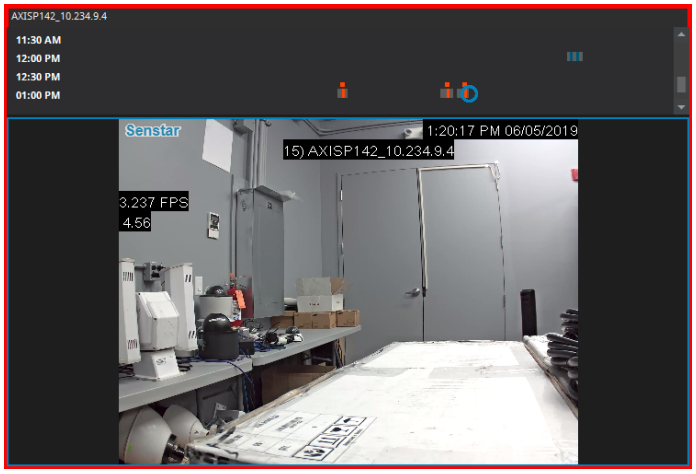
view panel.

2. Hover over the camera view panel containing the camera to which you want to add an alarm and click the Alarm icon.

Add an Alarm Indicator

You can display an alarm indicator around a camera view panel. The alarm indicator flashes for a specific time or until you acknowledge the alarm.

+



+

1. In the Windows Client interface, click View > Settings.
2. Click the Alarms tab.
3. Select Flash panel on alarm.
4. In the Number of seconds to flash alarm field, type how long the camera view panel flashes when the camera records an alarm.
5. Click OK.

Configure a Camera View Panel

1. In the Windows Client interface, right-click a camera view panel.
2. Click Settings.
3. Configure the settings for the camera view panel.
4. To apply the settings to all of the camera view panels, click Other > Apply To All.
5. Click Apply.
6. Click OK.

Change the View Panel Name

You can change the name of the panels in the Windows Client.

By default, panel names include the name of the computer, the port, a label for either a docked view or a floating view, and an identifier for the panel.

1. In the Windows Client interface, right-click in the panel.
2. Click Settings.
3. On the Child tab, type the new name in the Panel Name field.
4. Click OK.

View Alarm Cameras in the Panel

You can select the view panel that displays the camera that you want to view on alarm by default.

If you select more than one camera to view on alarm, the panel that you chose to view alarm cameras becomes the starting panel with other panels from left to right and from top to bottom rows in the Windows Client interface displaying any additional cameras that you select to view on alarm.

1. In the Windows Client interface, right-click the view panel that you want to display cameras from the alarm.
2. Click Settings.
3. On the Activity tab, select Switch view when an alarm occurs.
4. To display other cameras listed in the view on alarm list in different view panels, select Show alarm cameras in other panels.
5. To limit changes to specific cameras and alarms, select Limit action to specific cameras or alarms and select the cameras and alarms in the list.
6. Click Apply.
7. Click OK.

Prevent View Panel Content from Changing

In the Windows Client, you can prevent a view panel from changing the content (e.g., camera, map, or browser) it displays.

You can prevent content changes in view panels by using the context menu for each view panel. To prevent view panel content from changing in a docked view, you can click the Prevent panel content changes (lock) icon in the toolbar of the docked view window.

1. In the Windows Client interface, right-click the view panel.
2. Click Prevent panel content changes.

To toggle this setting, click

Allow panel content changes

.

Camera View Settings

Appearance

Setting	Description
Lock Timeline Height When Resize Occurs	Select to prevent the timeline from resizing when you change the size of the camera view panel.
Overlay Camera Messages	Select to display messages from the camera in the camera view panel.

Setting	Description
Overlay Time	Select to display the time in the camera view panel.
Overlay Tracking Boxes	Select to display boxes for video analytics in the camera view panel.
Overlay video retention on video	Select to display how many days of video for the camera.
Overlay Messenger Messages	Select to display messages in the camera view panel and set how many seconds the messages remain visible.
Overlay Tracking Paths	Select to display paths for video analytics in the camera view panel.
Overlay Date	Select to display the date in the camera view panel.
Overlay Thick Decoration	Select to display tracking boxes and paths as larger lines.
Overlay Recording Indicator	Select to display the recording indicator in the camera view panel.
Video Quality	Select the resolution for the camera view panel. The default resolution is the resolution set for the camera.
Display Mode	Select the size and aspect ratio of the video to display in the camera view panel.

Activity

Setting	Description
Switch view when an alarm occurs	Select to switch the camera view panel when an alarm occurs.
Switch view when motion occurs	Select to switch the camera view panel when motion occurs.
Show alarm cameras in other panels	If the rule for the alarm includes the View other cameras on alarm option, select this option to switch the other camera view panels to those cameras. This setting becomes visible when you select Switch view when an alarm occurs.
Limit action to specific cameras or alarms	Select this option and specify the cameras to limit the activity of the camera view panel to specific cameras or alarms. This setting becomes visible when you select Switch view when an alarm occurs or Switch view when motion occurs.
Ensure Visible	Select to bring the camera view panel into focus whenever an alarm or motion occurs.
Display	Select the whether the camera view panel changes to video or a still image.
Perform action after switch	Select to perform an action when an alarm or motion occurs.
Disable switching after switch occurs	Select to prevent the camera view panel from switching to another camera after a subsequent alarm or motion occurs.
Hide switched view after seconds	Set how many seconds the camera view panel displays the switched camera view.
Go back to previous state after seconds	Select this option and specify the number of seconds to return the camera view panel to the state prior to the alarm switch.

Child

Setting	Description
Show latest alarm when the camera displayed in another panel changes	Select to display the latest alarm from the primary camera view panel.
Panel Name	You can use the panel name with the video wall feature and the Senstar Symphony SDK. You can use the default name or change it to something more meaningful.

Tracking

Setting	Description
Digitally zoom in on hot spots	Select to automatically zoom in on objects that video analytics detect. This setting works for both live and recorded video.

Other

Setting	Description
Apply To All	Click to apply your changes to all of the active camera view panels.

Search

You can search video from a camera for objects and events.

1. In the Windows Client interface, perform one of the following tasks:
   - Right-click the camera view panel and click Search.
   - Hover over the camera view panel and click the Search icon.
2. In the Class pane, select the type of object for which to search.
3. In the Behaviorpane, select whether the object should be moving or loitering and for how long it should demonstrate the behavior.
4. Select whether to define the search area by a mask or fences.
5. In the Include pane, select the parts of the object or object movement the must pass through the search area for the object to be included in the search results.
6. In the Draw pane, select whether to add or remove mask area or fences.
7. Define the search period in the From and To fields.
8. In the Search For pane select whether to search for any events or only events that trigger alarms. Changing this selection changes the settings that are available in the

Search

window.

1. In the Add-Ons pane (available if you search for any events), select the video analytic events to search.
2. In the Rules pane, select the rule events to search.
3. In the Stream list, select the stream to search.
4. Click Search.

View Video by Date

You can view video from a specific date and time in a camera view panel.

Dates for which the camera has video appear as bold in the calendar.

1. In a camera view panel in the Windows Client interface, perform one of the following tasks:
   a. Right-click in the camera view panel and click Date.
   b. Hover in the camera view panel and click the Date icon.
2. Specify a date and time.
3. Click Select.

Record Video Manually

You can manually start recording video from a camera that is not set to always record.

You can start recording from the view panel that is displaying video from the camera in the Windows Client interface. When you start recording from the view panel, video is recorded for increments of 10 minutes.

Additionally, you can start and stop recording for a camera from the context (right-click) menu in the device tree in the Windows Client interface. If you start recording from the context menu, there is no time limit and the camera will continue to record until you manually stop recording from the context menu.

1. In the Windows Client interface, click the Start Recording button to record 10 minutes of video from the camera.
2. To add 10 more minutes, click the Start Recording button again. You can click the button multiple times to add multiple 10-minute increments.

The camera view panel displays an icon to show that the

Server

is recording video.

Open by Address

You can open an alarm, camera, or video from a specific time in the active camera view panel.

After you enter a valid address, the active camera view panel will display the video that you specify.

1. In the Windows Client interface, press the F5 key.
2. In the Enter address window, perform one of the following tasks:
   - Type an alarm ID.
   - Type a camera ID.
   - Type the server name and camera ID. Use the format `http://computer_name/camera_id/date_time`.
3. Click OK.

View Summary Video

You can view summary video from a camera that is running a video analytic.

Summary video skips footage in which the video analytic does not detect any events and shows

footage in which the video analytic detects events at a speed of 16 X.

1. In the Windows Client interface, view video from a camera that is running a video analytic.
2. In the timeline, navigate to historical video.
3. Click the Summarize Video icon to play summary video.

Video Controls

Control	Description
	Reduce the speed of playback.
	Slide to adjust the speed of playback.
	Increase the speed of playback.
	Navigate to the previous bookmark.
	Navigate to the previous alarm.
	Navigate to the previous activity.
	Go back ten seconds.
	Go back one second.
	Go back one frame.
	Play video.
	Pause video.
	Go forward one frame.
	Go forward one second.
	Go forward ten seconds.
	Navigate to the next activity.
	Navigate to the next alarm.
	Navigate to the next bookmark.
	Show live video

PTZ Controls

Control	Description
	Move the PTZ camera to a preset location.
	Increase the zoom on the PTZ camera.

Control	Description
	Decrease the zoom on the PTZ camera.
	Move the PTZ camera to the home position.
	Move the PTZ camera.
	Lock or unlock PTZ camera movement.
	Open the Camera Tour configuration page.
	Expand or collapse the camera controls.

Camera Controls

Control	Description
	Open or close the iris of the camera to adjust how much light enters the lens of the camera.
	Increase or decrease the brightness of the camera.
	Adjust the focus of the camera.
	Adjust the contrast of the camera.

Maps

Maps can display the location of cameras, camera views, digital inputs and output devices, links, and labels in the Windows Client interface.

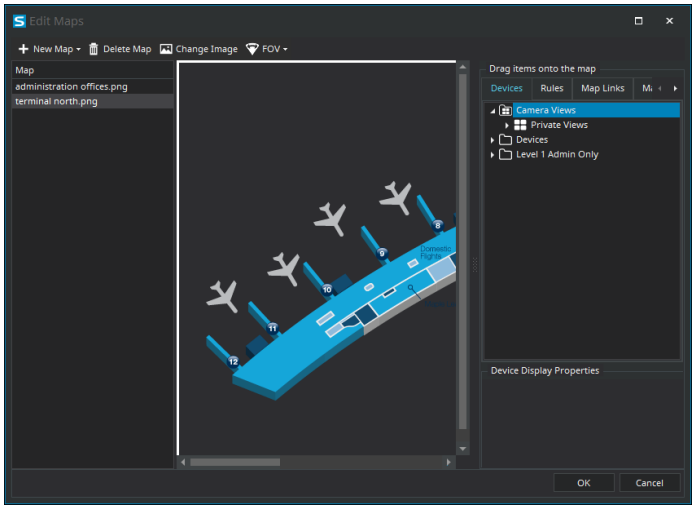
Map Editor

The Map Editor is a component in the Windows Client that you use to manage maps.

You can use the Map Editor to add maps to the Windows Client. A map can be an image file (jpg, gif, or bmp file), a CAD file (DWG 2013 format or earlier), or a map provided by a GIS service.

You can use the Map Editor to add cameras, camera views, digital inputs and output devices, links, and labels to a map. Items that you add to a map appear in and can add functionality to the map pane in the Windows Client interface.

+



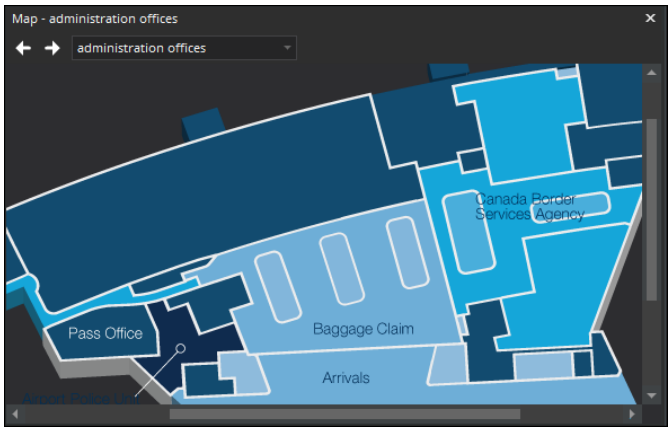
+

Map Navigation

When you turn on map navigation, the Windows Client interface displays the map pane.

Clicking an icon in the map pane performs the following actions:

- Clicking a camera icon displays the camera view in the active video panel.
- Clicking a camera view icon loads the camera view in the Windows Client interface.
- Right-clicking an output device opens a context menu with commands that you can send to the device.



===== Add a Map

You can add a map to the Windows Client.

1. In the Windows Client interface, click View > Map Editor.
2. Click New Map > Upload File.
3. Browse to the map file and click Open.
4. To change the name of the map, click the name of the map in the list and type the new name.
5. Click OK.

Add a GIS Map

You can add a map from the ArcGIS service to the Windows Client.

1. In the Windows Client interface, click View > Map Editor.
2. Click New Map > GIS Map.
3. In the Map Name field, type a name for the map that will appear in the map list.
4. In the Server Address field, type the URL of the map service.
5. Click Add Map.
6. Click OK.

View a Map

You can open the map panel and view a map in the Windows Client interface.

You can navigate on the map by using the scroll bars or clicking and dragging the map.

1. In the Windows Client interface, click View > Map Navigation.
2. In the map panel, use the arrows to navigate through maps or select the map in the list.

Add a Device to a Map

You can add cameras, camera views, access control devices, Senstar Symphony Access Control, and Senstar Network Manager to a map.

When you add a device to a map, the map displays a link that either opens the camera or camera view, or displays the status of the access control device.

1. In the Windows Client interface, click View > Map Editor.
2. Select a map.
3. Click the Devices tab.
4. Drag a device on to the map.
5. To rotate the camera icon, perform the following steps:
   a. Right-click the camera icon.
   b. Click Rotate.
   c. Move the mouse until the camera is facing the correct direction and click the mouse button.
6. Click OK.

Add a Label to a Map

You can add a label to a map.

In addition to defining the text and formatting of the label, you can also add a hyperlink to the label.

1. In the Windows Client interface, click View > Map Editor.
2. Select a map.
3. Click the Map Labels tab.
4. To create a new label, perform the following tasks in the Map Label pane:

a. In the Name field, type the name that the Map Editor displays in the list of labels.
b. In the Text field, type the text that you want to appear on the map.
c. In the Font Name field, select the typeface to use for the label.
d. In the Font Size field, select the size of the text on the map.
e. In the Foreground field, select the color of the text on the map.
f. In the Background field, select the color and opacity of the banner behind the text.
g. In the Width field, set the width of the banner behind the text.
h. In the Height field, set the height of the banner behind the text.
i. In the URL field, type the hyperlink.
j. Click Save.

After you save a new label, the label appears in the label list.

1. Click and drag a label from the label list to the location on the map.
2. Click OK.

To remove a label from a map, right-click the label, click
Remove from Map
, and click
OK
.

Add a Rule to a Map

You can add a label to a map.

In addition to defining the text and formatting of the label, you can also add a hyperlink to the label.

1. In the Windows Client interface, click View > Map Editor.
2. Select a map.
3. Click the Map Labels tab.
4. To create a new label, perform the following tasks in the Map Label pane:
   a. In the Name field, type the name that the Map Editor displays in the list of labels.
   b. In the Text field, type the text that you want to appear on the map.
   c. In the Font Name field, select the typeface to use for the label.
   d. In the Font Size field, select the size of the text on the map.
   e. In the Foreground field, select the color of the text on the map.
   f. In the Background field, select the color and opacity of the banner behind the text.
   g. In the Width field, set the width of the banner behind the text.
   h. In the Height field, set the height of the banner behind the text.
   i. In the URL field, type the hyperlink.

j. Click Save.

After you save a new label, the label appears in the label list.

1. Click and drag a label from the label list to the location on the map.
2. Click OK.

To remove a label from a map, right-click the label, click

Remove from Map

, and click

OK

.

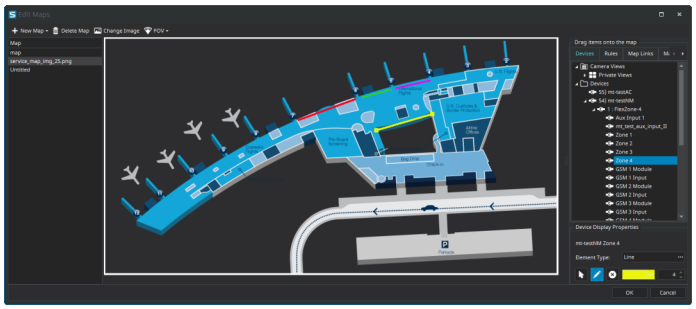
Add a Zone to a Map

You can add an alarm zone for hardware nodes to a map.

A zone appears as a line on the map. You can set the position, color, and thickness of the line. In addition, you can add multiple segments to the line to accurately represent the location of the hardware node on the map.

When the hardware node experiences an event, the zone on the map displays an alarm icon.

+



+

1. In the Windows Client interface, click View > Map Editor.
2. Select a map.
3. Click the Devices tab.
4. Drag an alarm zone onto the map.
5. Click the icon for the alarm zone.
6. In the Element Type field, click the ellipsis and click Line. The icon changes to a line.
7. To change the line, perform any of the following tasks:
   - To change the color of the line, select the line, click the ellipsis in the color field, select a new color, and click OK.
   - To change the thickness of the line, select the line, click the up or down arrows in the thickness field.
   - To change the position or size of the line, click and hold the endpoint of the line and move it to

the new location.

8. To add a segment to the zone, perform the following tasks:
   a. Click the pencil icon to activate Draw Tool.
   b. Move the pencil icon to an endpoint of an existing line.
   c. Click the endpoint.
   d. Move the mouse to draw the new segment and click to end the segment. An endpoint appears and a new segment starts.
   e. Repeat step d to draw additional segments.
   f. Press the ESC key or click the arrow icon to deactivate the Draw Tool.
9. To remove a segment from the zone, perform the following tasks:
   a. Click the X icon to activate the Delete Tool.
   b. Move the X icon to an endpoint of an existing line.
   c. Click the endpoint. The segments attached to the endpoint are removed from the zone. If the endpoint is the end of the zone, the segment is removed. If the endpoint is a junction between two segments, both segments are removed and a new segment appears between the remaining endpoints.
   d. Repeat step c to remove additional segments.
   e. Press the ESC key or click the arrow icon to deactivate the Delete Tool.
10. Click OK.

Add Site Information to a Map

You can add site information that appears on a map in the map navigation panel in the Windows Client interface.

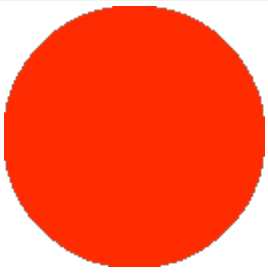
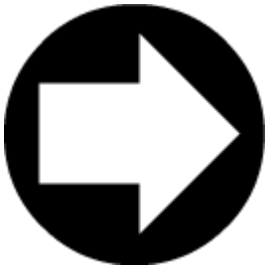
To add site information to a map, you add a label and then use a content editor to add the information. The map editor in the Windows Client interface includes four fields for site information, three sizes for the text, and two locations for the content.

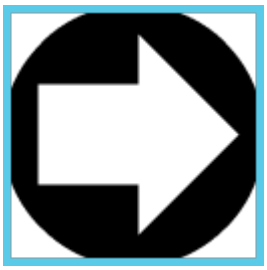
1. In the Windows Client interface, click View > Map Editor.
2. Select a map.
3. Click the Map Properties tab.
4. In the Site Information pane, complete the following tasks:
   a. Select Display Site Information.
   b. In the label field, type a label for the information.
   c. To open the content editor, click the ellipsis button.
   d. Type the information that you want to add to the map and click save.
   e. In the Format Size list, select the font size.
   f. In the Position list, select where on the map you want the information to appear.
5. Click OK.

After you add site information to a map, it appears in the map navigation panel in the
Windows Client interface
as the
Site Information

1. Clicking the button, reveals (and hides) the site information.

Map Icons

Icon	Description
	Rule
	Digital input • Activated: yellow background • Not activated: white background
	Digital output • Activated: yellow background • Not activated: white background
	Camera • Online camera: gray arrow • Offline camera: white arrow • Motion detected: blue arrow • Alarm: orange arrow • Selected camera: orange circle

Icon	Description
	PTZ camera • Online camera: gray arrow • Offline camera: white arrow • Motion detected: blue arrow • Alarm: Orange arrow
	Access control device • Access granted: green • Access denied: red
	Senstar Symphony Access Control and Senstar Network Manager devices

Display Field of View

You can display the field of view for cameras on maps in the Windows Client interface.

If you display the field of view for a PTZ camera, the graphic on the map changes when you move the camera.

1. In the Windows Client interface, click View > Map Editor.
2. Select a map.
3. Click FOV > Show FOV.
4. To change the color of the field-of-view graphic, perform the following tasks:
   a. Click FOV > Change Color.
   b. Select the color using the color picker or define the color using the RGB values or hex color codes.
   c. Click OK.
5. Click OK.

Senstar Symphony Messenger

The Senstar Symphony Messenger allows you to send messages to any user who is logged in to the Windows Client or Web Client.

Send a Message

You can send messages to users or groups.

1. In the Windows Client interface, click Setting > Messenger to open the Senstar Symphony Messenger window.
2. In the user and group list, select the recipients for the message.
3. In the text field, type your message.
4. Click Send.

Carousels

Carousels can loop through multiple cameras across multiple servers in the same server farm, pausing on each camera for a defined time.

You can assign a carousel to a video panel in the Windows Client interface. The video panel will automatically loop through the cameras and will include controls to pause and move forward and backward through cameras in the carousel.

You can create a carousel in the Server configuration interface. Once created, carousels appear in the device tree in the Windows Client interface.

Add a Carousel

Add a carousel in the Server configuration interface.

1. In the Server configuration interface, click Devices > Carousels.
2. Click Add Carousel.
3. In the Name field, type a name for the carousel. The name of the carousel appears in the device tree in the

Windows Client interface

.

1. Perform one of the following tasks:
   - Select Add to bottom of list to add cameras to the bottom of the carousel camera list.
   - Select Insert below currently selected camera in list to add cameras below the selected camera in the carousel camera list.
2. In the Available Cameras on Servers list, select the cameras to include in the carousel and click Add Selected.
3. In carousel camera list, perform the following the tasks:
   a. Set the order of cameras by moving camera by clicking and holding the arrow button beside a camera, dragging the camera to the desired location, and releasing the mouse button.
   b. Set the time that the carousel pauses on the camera before moving to the next camera in the carousel.
4. Click Save.

Edit a Carousel

Edit a carousel in the Server configuration interface.

1. In the Server configuration interface, click Devices > Carousels.
2. Select the carousel and click Edit.
3. Perform any of the following tasks:
   - To remove a camera from the carousel, hover over the camera, and click the X button.
   - To add a camera, select the camera in the Available Cameras on Servers list, and click Add Selected.
   - To change the time that the carousel pauses on the camera, edit the number in the Seconds

field.

4. Click Save.

Delete a Carousel

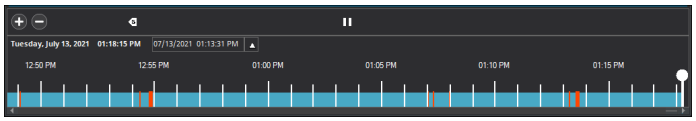
Remove a carousel in the Server configuration interface.

1. In the Server configuration interface, click Devices > Carousels.
2. Select the carousel.
3. Click Delete.
4. To confirm the deletion, click Yes.

Timeline

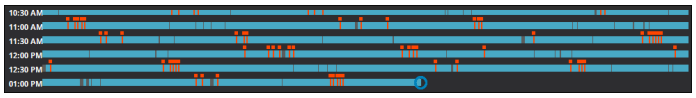
A timeline displays activities and alarms for cameras in the Windows Client interface. The Windows Client includes a consolidated timeline that displays information from numerous cameras a camera timeline that displays information from an individual camera.

The consolidated timeline displays information from numerous cameras and is available when Locked Times on Navigation is turned on.



+

The camera timeline displays information from a specific camera.



+

You can click on a timeline to navigate to a specific time or event in the footage.

Timeline Colors

The Windows Client interface uses the following colors to mark events on the timeline.

Color	Event
Dark blue (#005670)	Activity
Dark green (#008080)	Video downloaded from the camera
Light yellow (#FFFF00)	Access denied
White (#FFFFFF)	Access granted
Red (#FF0000)	Access other Alarms
Gray (#5C5C5C)	No activity
Dark gray (#231F20)	No signal
Light gray (#808080)	Not used

Color	Event
Transparent (#00FFFFFF)	No record
Light blue (#59CBE8)	Zoom

Display a Camera Timeline

You can display a camera timeline to display the information for an individual camera in a camera view panel.

1. To turn on a camera timeline for a single camera, complete the following steps:
   a. In the Windows Client interface, right-click a video panel.
   b. Click Show Timeline.
2. To turn on the camera timelines for all of the cameras in a view, complete the following steps:
   a. In the Windows Client interface, click Timeline.
   b. Click Show panels.

The camera timeline appears for the cameras that you selected.

To hide a timeline, right-click the video panel and click Show Timeline again.

Display the Consolidated Timeline

You can display the consolidated timeline to display information from all of the cameras in a view.

To display the consolidated timeline, you must turn on

Lock Times On Navigation

.

1. In the Windows Client interface, click Timeline.
2. Click Show consolidated.

The consolidated timeline appears at the bottom of the camera view.

Interface Customizations

You can customize the Windows Client interface in several ways, including changing the toolbar, adjusting display and regional settings, locking the layout, and configuring how alarms, video, and sound are presented.

Toolbar

Customize the toolbar to show the commands that you use most often. For more information, see Customize the Toolbar.

Settings

The Windows Client provides settings that control the appearance and behavior of the interface, including:

- Display Settings
- Customize Settings
- Regional Settings

- Startup Settings
- Alarms Settings
- Video Settings
- Sound Settings

Layout

You can lock the layout of the Windows Client to prevent changes to the arrangement of view panels. For more information, see Lock Settings and Lock Times.

Customize the Toolbar

You can change the icons that appear on the toolbar in the Windows Client interface.

1. In the Windows Client interface, click the down arrow.
2. Click Add or Remove Buttons > Main Menu
3. Select the icons to add to or remove from the toolbar.
4. To restore the toolbar to the default, click Reset Toolbar and click OK.

Multiple Monitors

You can use the Windows Client across multiple monitors on a single workstation so that an operator can see more video and tools at the same time.

Multiple monitors are different from a Video Wall. A Video Wall is a managed display surface that operators can push views to from any registered Windows Client. Multiple monitors are simply additional screens connected to the operator's own workstation.

Stretch the Main Window Across Monitors

1. Drag the main Windows Client window so that it spans the monitors.
2. Click the maximize button.

The view panel grid expands to fill the new window size.

Open Floating Camera Views on Other Monitors

You can open floating camera views and move them to any monitor. Each floating view is independent of the main window.

1. In the Windows Client interface, click View > New Floating Camera View.
2. Drag the floating view to the monitor that you want.
3. Add cameras, maps, alarms, or other content to the floating view.

For more information, see the Open a Floating Camera View topic.

Run Multiple Instances of the Windows Client

You can run more than one instance of the Windows Client on the same workstation, each on its own monitor and each connected to the same or different servers.

1. Start the Windows Client.
2. Drag the window to the first monitor.

3. Start the Windows Client again from the Start menu.
4. Drag the second window to a different monitor.
5. Sign in on each instance.

Each instance uses its own resources. The number of instances you can run is limited by the CPU, GPU, and bandwidth available on the workstation.

Managing Video

The Windows Client provides tools for viewing live and recorded video, manually recording video, searching for events, exporting video for use outside the Windows Client, and protecting video from deletion.

Video Export

The Windows Client includes functionality to export video. The Player can play the exported video.

By default, the vide export includes the two minutes of video prior to when you click Export (for the active camera) or Export All (for all cameras in view panels). To export video with a greater duration, you can mark the start and end of the video on the panel timeline.

The longer the video that you want to export, the longer it will take the Windows Client to complete the export process.

The Windows Client can export video to a file or to the Senstar Xnet, from which users can download the video. The export can include video from one or multiple cameras and the Windows Client can generate a summary video that plays video at a faster speed to highlight events.

The Windows Client also includes functionality to view the status of video exports.

Export Video to the Cloud

You can export video from the Windows Client to the cloud and with a link to download the video.

To export video to the cloud, you must associate an email address with your

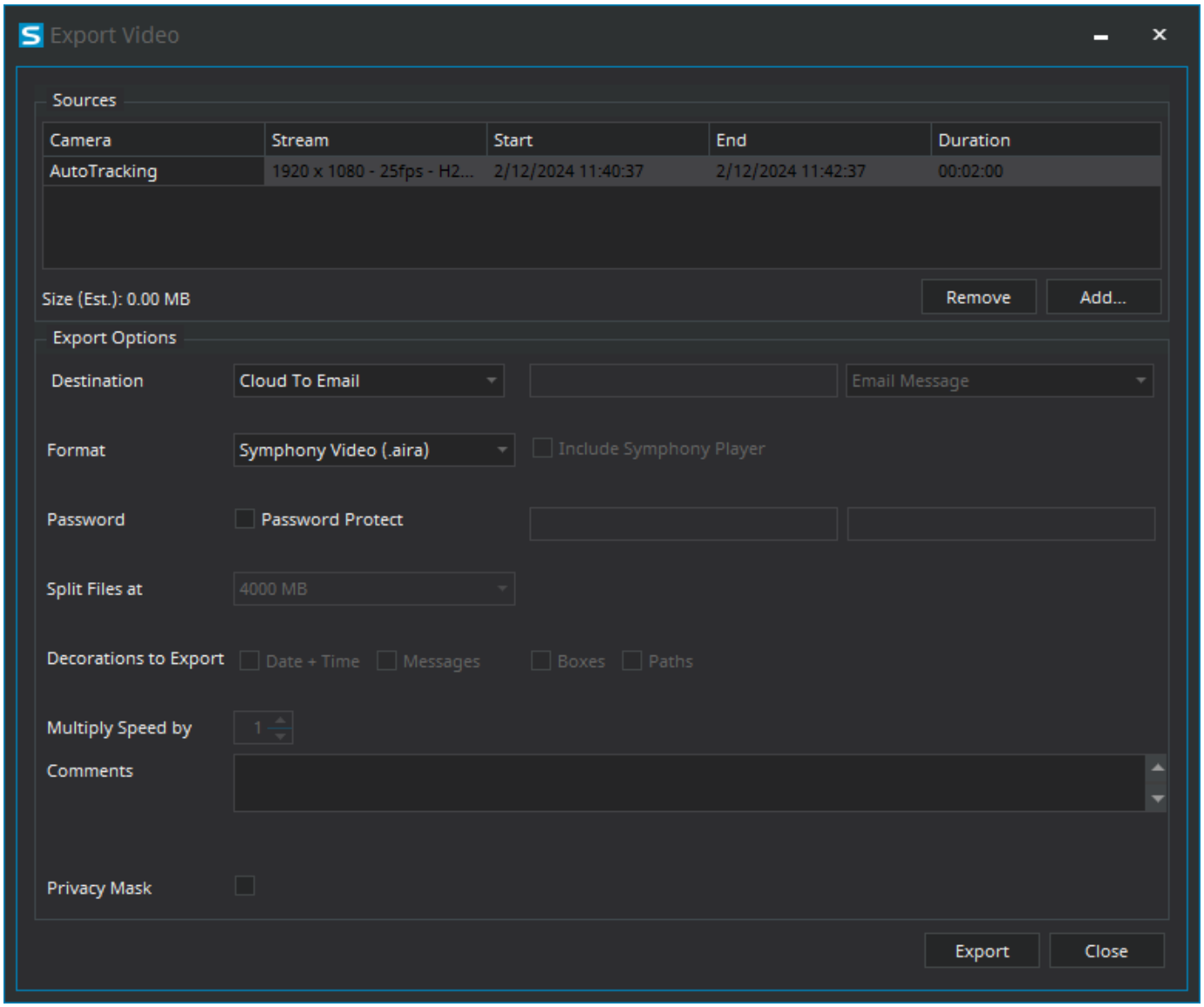
Senstar Symphony

user account.

The Windows Client uploads the video files to the Senstar Xnet and sends an email with a link to download the video files to the email address associated with your Senstar Symphony user account. You can then forward the link to other recipients.

When exporting video to the cloud, the Windows Client splits the video into files with a maximum size of 4000 MBs, does not include decorations, and does not support increasing the speed of the video.

+



1. In the Windows Client interface, perform one of the following tasks:
   - Right-click the view panel and click Export to export video from the camera that is active in the view panel or Export All to export video from all of the cameras that are active in view panels.
   - Hover over the view panel and click the Export icon.
   - Right-click the timeline to mark the export start and export end, and click Export to export video from the camera that is active in the view panel or Export All to export video from all of the cameras that are active in view panels.
2. To add a camera stream to the export, perform the following tasks:
   a. Click Add.
   b. Select the camera and click Add.
   c. In the sources list, select the stream in the Stream column.
   d. If required, modify the start and end time for the export.

3. In the Destination list, select Cloud To Email.
4. To add a custom email message to the email message, perform the following tasks:
   a. Click the Email Message field.
   b. In the text window, type the email message.
   c. Click OK.
5. To protect the video export files with a password, perform the following tasks:
   a. Select Password Protect.
   b. Type and confirm the password.
6. In the Comments field, type any text that you want to include in the text file that is associated with the video export.
7. To add a privacy mask to video export, perform the following tasks:
   a. Select Privacy Mask.
   b. In the Privacy Mask pane, draw the privacy mask on the sample image.
8. Click Export.

The

Server

sends you an email that includes a link to manage your exported video. You can use the link to delete exported videos.

Lock Times

You can lock times on navigation in the Windows Client interface to make all camera view panels display video from the same time.

For example, if you have four camera view panels open in the Windows Client interface, and you click a bookmark for video from the previous day, all of cameras in the camera view panels will attempt to show video from the time of the bookmark.

Locking times on navigation supports a maximum of four camera view panels.

In the Windows Client interface, click the Lock Times On Navigation icon (clock).

Adjust the Number of Locked Camera View Panels

You can set the maximum number of camera panels to which you can apply the Lock Times On Navigation feature.

By default, the limit is four camera view panels. Increasing the limit and applying the Lock Times On Navigation feature to more camera view panels increases the system resources that the Windows Client uses.

1. Open the acc.ini file at %appdata%\Senstar7.
2. Add the following values:

```
[VideoRecvCTRL]
LockTimesPanelLimit=number_of_panels
```

Where number_of_panels is the maximum number of camera view panels on which you can use the Lock Times On Navigation feature.

1. Save and close the acc.ini file.

Bookmarks

A bookmark identifies specific footage that you can return to later. Bookmarks can refer to live videos, recorded videos, or still images.

When you add a bookmark, it refers to the video on a specific camera at a specific time. Bookmarks appear in the bookmarks list in the Windows Client interface.

Create a Bookmark

You can create a bookmark to reference video from a specific time and camera.

When you create a bookmark, it creates a connection to the camera that is active in the Windows Client interface at the time that is showing in the display panel when you create the bookmark.

If you create a bookmark for a camera that is not recording, you will not be able to access the video later.

You can share a bookmark so that other users can open the video that you mark.

1. In the Windows Client interface, click Bookmarks > Add Bookmark.
2. Type a name for the bookmark.
3. Select whether you want to share the bookmark with other users.
4. Click OK.

Delete a Bookmark

You can remove bookmarks that you create.

1. In the Windows Client interface, click Bookmarks > Manage Bookmarks.
2. Select Delete for the bookmark.
3. Click OK.

Visual Tracking

The visual tracking feature allows you to add links to cameras that will automatically switch the camera view panel to an adjacent camera. You can use this feature to track a moving subject across multiple cameras.

Visual tracking links appear as transparent overlays in the camera view panel. The link includes the camera identification number for the camera to which the link goes. You can customize both the location and shape of the links to adjacent cameras to make the links more meaningful in the scene. For example, you can customize the location and shape of a link to cover a door that leads to an area in the scene the adjacent camera.

When you click a visual tracking link, the camera view panel switches to the camera that the link references.

Add a Visual Tracking Link

You can add to visual tracking link to a camera view panel in the Windows Client interface.

1. In the Windows Client interface, open the camera to which you want to add the visual tracking link in a camera view panel.
2. Press and hold the Alt key.
3. In the device tree, left-click and hold the camera to which you want to link.
4. Drag the target camera to the desired location.
5. Release the Alt key and mouse button.
6. To move the link, perform the following steps:
    a. Press and hold the Alt key.
    b. Click the link.
    c. Left-click and hold the hand icon.
    d. Drag the link to the desired location.
    e. Release the Alt key and mouse button.
7. To change the shape of the link, perform the following steps:
    a. Press and hold the Alt key.
    b. Click the link.
    c. Left-click and hold an anchor point.
    d. Drag the anchor point to the desired location.
    e. Release the Alt key and mouse button.

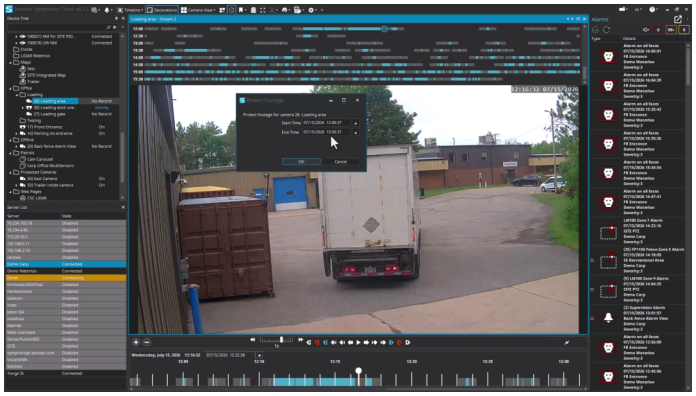
Protect Footage

You can protect a section of recorded video so that the Server does not delete it. The Server excludes protected footage from automatic storage cleanup and retention settings, and the footage remains on the Server until a user removes the protection.

Protect footage to preserve video of incidents and investigations without exporting the video or changing the retention settings. Protection applies to a specific camera and time range. The Server records the user that protects each section of footage and the time of the protection.

The Protect Footage option is available only if your group has the Protect Footage permission. For more information, see Device Permissions.

1. In the Windows Client interface, select a camera in the device tree.
2. Use the timeline to navigate to the footage that you want to protect.
3. Right-click the timeline and select Protect Footage.
4. In the Protect Footage window, set the start time and end time for the section of footage that you want to protect.
5. Click OK.



Select the shortest time range that covers the event. The Server does not automatically delete protected footage, so large protected sections consume storage until a user removes the protection.

Administrators can view protected footage on the Protected Footage page in the Server configuration interface, and can remove the protection when the footage is no longer needed. For more information, see Protected Footage and Unprotect Footage.

Delete Recorded Video

You can delete recorded video for a specific time or delete all recorded video.

1. In the Windows Client interface, click Server Configuration > Delete Recorded Video.
2. Perform one of the following tasks:
   - Specify a date range and click Delete Footage in Above Date Range On All Cameras.
   - Click Delete everything.
3. Click Yes.

Managing Alarms

An alarm is a high-priority event triggered when a video analytic or an integrated security device (such as a fence sensor or access control reader) detects conditions that match a predefined rule. Alarms are the mechanism that transitions the system from passive monitoring to active response: once a rule raises an alarm, the system records it, displays it, and expects an operator to classify it.

Alarm lifecycle

Every alarm moves through the same stages. An operator's job is to move it through them promptly.

1. **Triggered** — a rule fires. The Server records the alarm, captures the surrounding video (pre- and post-alarm duration set in the rule), and sends it to the Windows Client.
2. **Displayed** — the alarm surfaces in the Alarm Console, Alarms panel, and on maps and timelines as configured.
3. **Acknowledged** — an operator takes responsibility and classifies the alarm. Until acknowledged, the alarm continues to demand attention (audio, flashing indicators, pop-ups).
4. **Resolved** — any follow-up action (dispatch, report, escalation) completes.

5. **Archived** — the alarm is written to the alarm database for later retrieval and reporting.

If no operator acknowledges within the configured timeout (see alarms settings and the rule's two-stage settings), the alarm escalates. Administrators define what escalation means for each rule.

Viewing Alarms

Depending on how the site is configured, the Windows Client presents alarms in several places at once. An operator usually watches the Alarm Console during active monitoring and relies on the other indicators as ambient signals.

Location	What it shows
Alarms panel	Live list of unacknowledged alarms in the current view. Click an alarm to jump to the associated camera.
Alarm Console	The primary workspace for responding to alarms. Includes the alarm list, video of the incident, any instructions that administrators attached to the rule, and the acknowledgment controls.
Timeline indicator	Coloured marks on the timeline show when alarms occurred for the selected camera. Useful during investigation.
Video panel flash	A view panel can flash its border when the associated camera raises an alarm. Configure in view panels.
Map icon/line flash	Icons and zones on a map flash when the corresponding device raises an alarm.
Popup window	Optional pop-up that surfaces an incoming alarm regardless of the current workspace. Configure in alarms settings.
Device Tree status	The device tree shows the alarm state of each device as an icon overlay.

Responding to Alarms

An operator's job on an alarm is to acknowledge it and classify it correctly. The classification drives reporting accuracy and, for rules that use it, downstream automation.

Acknowledge

See Acknowledge an alarm for the step-by-step procedure. At a high level:

1. Open the alarm in the Alarm Console.
2. Review the video clip (pre-alarm footage shows what led up to the trigger).
3. Read any instruction text attached to the rule.
4. Classify the alarm (see below).
5. Add a comment describing what you saw and what you did.

Classify

Classification is a judgement call. The typical options and when to use them:

Classification	Use when
Real alarm	The event occurred as the rule intended, and someone (security, police, site staff) acted on it.
Real actionable	The event occurred as intended and you took the required action yourself (dispatched a guard, locked a door, contacted a driver).
False alarm	The event did not actually match the rule's intent — weather, lighting, an animal, a known vehicle, or a tuning issue caused the trigger.

If you see repeated false alarms from the same rule or camera, flag it to an administrator. Persistent false alarms usually point to motion detection tuning or a video analytic threshold that needs adjustment.

Share or escalate

If the alarm needs a colleague's attention — another operator, a supervisor, or a specialist — use share an alarm to forward it. Sharing preserves the acknowledgment state and the attached comments.

Configuring Alarms

Administrators configure alarms on the Server. An alarm is simply a rule whose action set includes the "create an alarm" action.

- Rules — the model: event + action set + schedule + severity.
- Create a rule — build a rule that raises an alarm.
- Events — the triggers available (motion, analytic detection, integration event, digital input, etc.).
- Action sets — what happens when the rule fires (record, alarm, email, output, etc.).
- Schedules — when the rule is active (always, business hours, after-hours, custom).

On the Windows Client side, operators tune how alarms appear using alarms settings and sound settings.

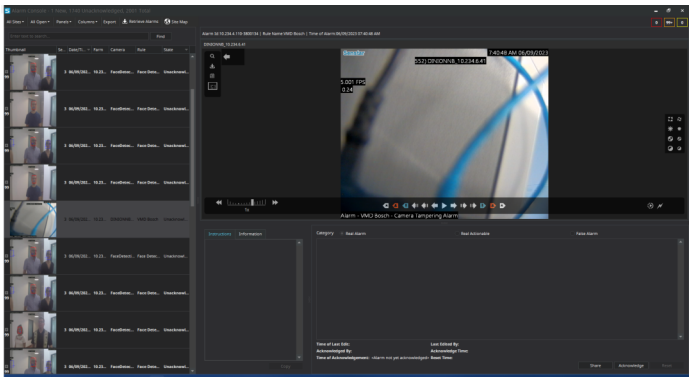
Alarm Console

The Alarm Console in the Windows Client includes functionality to view and manage alarms.

The Alarm Console appears in the Windows Client interface as a collapsible sidebar by default. When in the sidebar, the Alarm Console displays a list of alarms that includes an icon to illustrate the alarm type and alarm details. Clicking an alarm in the list will display the alarm video in the active camera view panel. The Alarm Console includes buttons to acknowledge and reset alarms (for two-stage alarms), and counters to indicate the number and type of alarms.

The Alarm Console also includes an advanced mode that opens the Alarm Console in its own window. In advanced mode, the Alarm Console includes additional functionality to filter, export, and manage alarms. When the Alarm Console is in the advanced mode, it does not appear as a sidebar in the Windows Client interface.

+



+

The advanced Alarm Console includes the following components:

- Alarm list
  - Displays the alarms that match your selection criteria
- View panels
  - Displays one to four view panels in the advanced Alarm Console (configure on the Action Sets page in the Server configuration interface)
- Instruction pane
  - Displays instructions (as text or an attached file) for the alarm (define instructions on the Action Sets page in the Server configuration interface)
  - If you add a file, you can zoom on the file by hold the CTRL button and using the mouse scroll wheel
- Information pane
  - Displays additional information about the alarm from access control systems or the Senstar Network Manager
- Acknowledgment pane
  - Share, acknowledge, or reset and alarm
  - Mark an alarm as real, real actionable, or false
  - Add or view comments associated with the alarm
  - Displays information and alarm processing

View Alarms

You can refine the list of alarms that appear in the advanced Alarm Console.

1. In the Windows Client interface, click Advanced Mode to open the advanced Alarm Console.
2. In the sites list, select the sites from which you want to view alarms.
3. In the type list, select which type of alarms you want to view.
4. In the panels list, select whether you want to view one view panel or four view panels.
5. In the columns list, select which columns you want to see in the alarm list.

As you make changes, the alarm list updates to include alarms that match the parameters that you select.

Retrieve Alarms

You can retrieve alarms for dates that are not included in the alarm list.

Depending on how you sort the alarm list, the alarms that you retrieve might not appear at the top of the list.

1. In the Windows Client interface, click Advanced Mode to open the advanced Alarm Console.
2. Click Retrieve Alarms.
3. Select a date.

The alarm list in the advanced

Alarm Console

displays alarms for the date you selected.

Export an Alarm List

You can export alarms from the Windows Client interface.

When exporting alarms, the Server supports the following formats:

- PDF
- HTML
- MHT
- RTF
- DOCX
- XLS
- XLSX
- CSV
- Text
- Image

1. In the Windows Client interface, click Advanced Mode to open the advanced Alarm Console.
2. Filter and sort the alarms until you get the list that you want to export.
3. Click Export. The amount of time it takes the

Server

to process the export file increases with the number of alarms you want to export.

1. In the Preview window, click File > Export Document.
2. Click the file format.
3. Specify the options for the output and click OK.
4. In the Save As window, select the location to save the file and click Save.

Share an Alarm

You can share an alarm with any user who is logged in to the Windows Client.

When you share an alarm with a user, the Windows Client displays a message for the user in the Windows Client interface.

1. In the alarm console sidebar, click Advanced Mode.
2. Select the alarm.
3. Click Share.
4. In the Share Event window, select a user.
5. Click Share.

Acknowledge an Alarm

You can acknowledge an alarm to claim the alarm while you process it.

When two-stage alarm processing is turned on, you claim the alarm when you acknowledge it so that you can process the alarm. When two-stage enhanced alarm processing is turned on, a user with a higher priority (configured in the Server configuration interface) can claim the alarm from a user with a lower priority.

You have until the acknowledgement timeout (configured in the Server configuration interface) elapses to process it. Once the acknowledgement timeout elapses, the alarm returns to an unacknowledged state.

1. In the alarm console sidebar, click Advanced Mode.
2. Select the alarm.
3. Click Acknowledge.
4. To view instructions that are associated with the alarm, click the Instructions tab.
5. To view location information, click the Information tab.
6. Select the type of the alarm.
    - Real Alarm
    - Real Actionable
    - False Alarm
7. Type any comments that you want to add to the alarm.
8. Click Reset to close and archive the alarm.

Client Options

Disabling Alarms

You can disable alarms at the camera/device or serveer level if your account as the necessary permissions.

Disabling alarms hides alarms generated by a camera. To hide alarms generated by a device, see the Mask section.

Disable Alarms for a Camera

You can disable the alarms for a camera in the Windows Client.

1. In the Windows Client interface, right-click a camera in the device tree.
2. Click Disable Alarms for Camera.
3. Specify the time (minutes) for which the alarms are disabled.
4. Click OK.

To enable the alarm again, right-click the camera and click Enable Alarms for Camera.

Disable Alarms for a Server

You can disable the alarms for cameras on the Server to which the Windows Client is connected.

1. In the Windows Client interface, click Alarms > Disable Alarms for Server.
2. Specify the number of minutes for which to disable the alarms.
3. Click OK.

To manually enable alarms without waiting for the time to elapse, click Alarms > Enable Alarms for Server.

Settings

You can use the settings in the Windows Client to customize the Windows Client interface.

View Camera Activity

You can view the activity for multiple cameras and open camera view panels for specific times from each camera's timeline.

Viewing camera activity allows you to compare the timelines and track activity across multiple cameras. You can open video from different times and cameras to view the complete video for an activity or an alarm.

1. In the Windows Client interface, click View > Activity For Cameras.
2. Specify the start and end dates for the activity you want to view and click Reload.
3. In the Pick Cameras list, select the cameras for which you want to view the activity.
4. Use the Zoom In and Zoom Out to set the correct resolution.
5. Perform one of the following tasks:
   - To open video in a single docked camera view panel each time you click on a camera timeline, toggle the One Camera View button on.
   - To open video in a new floating camera view panel each time you click a camera timeline, toggle the One Camera View button off.
6. Click a camera timeline to view video.

Customize the Toolbar

You can add or remove icons from the toolbar in the Windows Client interface.

1. Click the down arrow in the toolbar.
2. Click Add or Remove Buttons > Main Menu.
3. Click to show or hide the buttons, or click Reset Toolbar.

Change Timeline Colors

You can change the colors that the Windows Client uses in the timeline.

When you change the timeline colors, you also change the colors that the Windows Client uses for map icons.

1. In the Windows Client interface, click View > Settings.
2. Click the Timeline Colors tab.

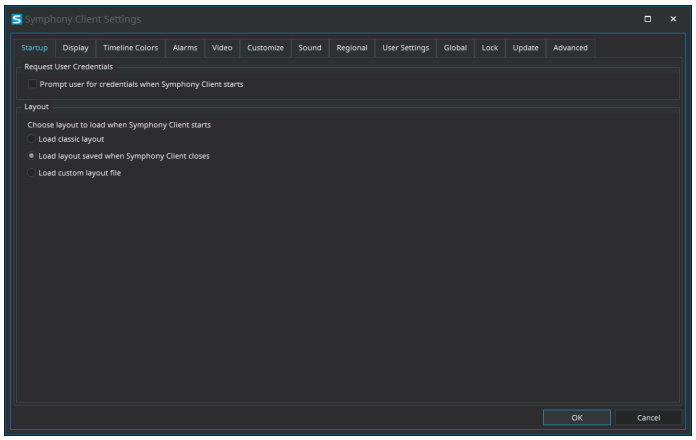
3. Select the colors for each timeline event.
4. Click OK.

You can also reset the colors to the default colors at any time or use the classic colors from Senstar Symphony 6.14.

Startup Settings

The startup settings determine how the Windows Client behaves when it starts.

+



+

Request User Credentials

Setting	Description
Prompt user for credentials when Windows Client starts	Select to make users provide a valid username and password before using the Windows Client.

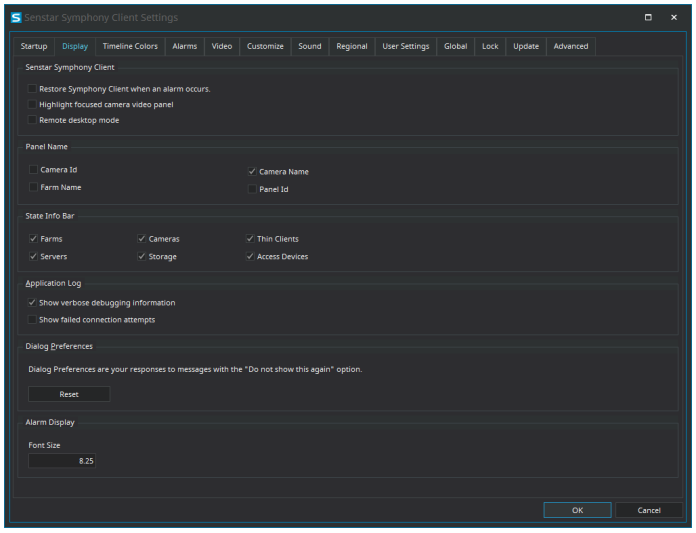
Layout

Setting	Description
Load classic layout	Select to load the default layout when the Windows Client starts.
Load layout saved when Windows Client closes	Select to load the layout from the last session when the Windows Client starts.
Load custom layout file	Select to load the layout from a saved layout file when the Windows Client starts.

Display Settings

The display settings determine what information the Windows Client displays and what is included in log files.

+



+

Windows Client

Setting	Description
Restore Windows Client when an alarm occurs	Select to restore the Windows Client interface to full size when an alarm occurs.
Highlight focused camera video panel	Select to highlight the camera view panel that is in focus.
Remote desktop mode	Select if you are using a remote desktop or virtual machine to access the Windows Client. This setting removes the dependency of overlays and navigation controls in the Windows Client interface on DirectX.

Panel Name

Setting	Description
Camera Id	Select to display the camera ID in the name of the camera view panel.
Farm Name	Select to display the farm name in the name of the camera view panel.
Camera Name	Select to display the camera name in the name of the camera view panel.
Panel Id	Select to display the panel ID in the name of the camera view panel.

State Info Bar

Setting	Description
Farms	Select to display warning messages for farms in the notification bar.
Servers	Select to display warning messages for servers in the notification bar.
Cameras	Select to display warning messages for cameras in the notification bar.

Setting	Description
Storage	Select to display warning messages for video storage in the notification bar.
Senstar Thin Clients	Select to display warning messages for Senstar Thin Client devices in the notification bar.
Access Devices	Select to display warning messages for access control devices in the notification bar.

Application Log

Setting	Description
Show verbose debugging information	Select to display verbose debugging information in the application log.
Show failed connection attempts	Select to show failed connection attempts in the application log.

Dialog Preferences

Setting	Description
Reset	Click to reset all dismissed dialog boxes in the Windows Client interface.

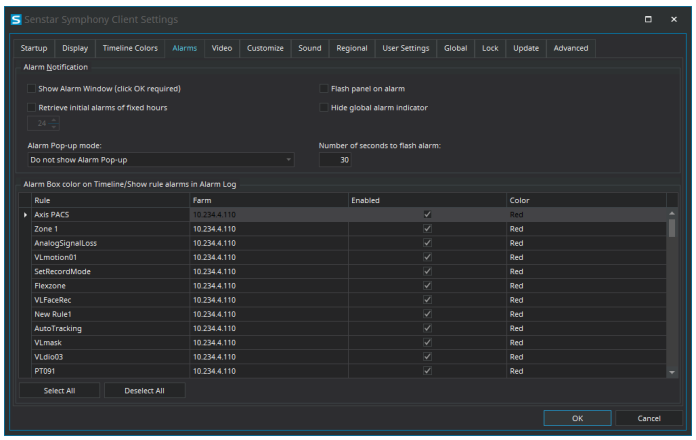
Alarm Display

Setting	Description
Font Size	Select the size (in pixels) of the font in the alarm console.

Alarms Settings

The alarm settings determine how alarms appear in the Windows Client.

+



+

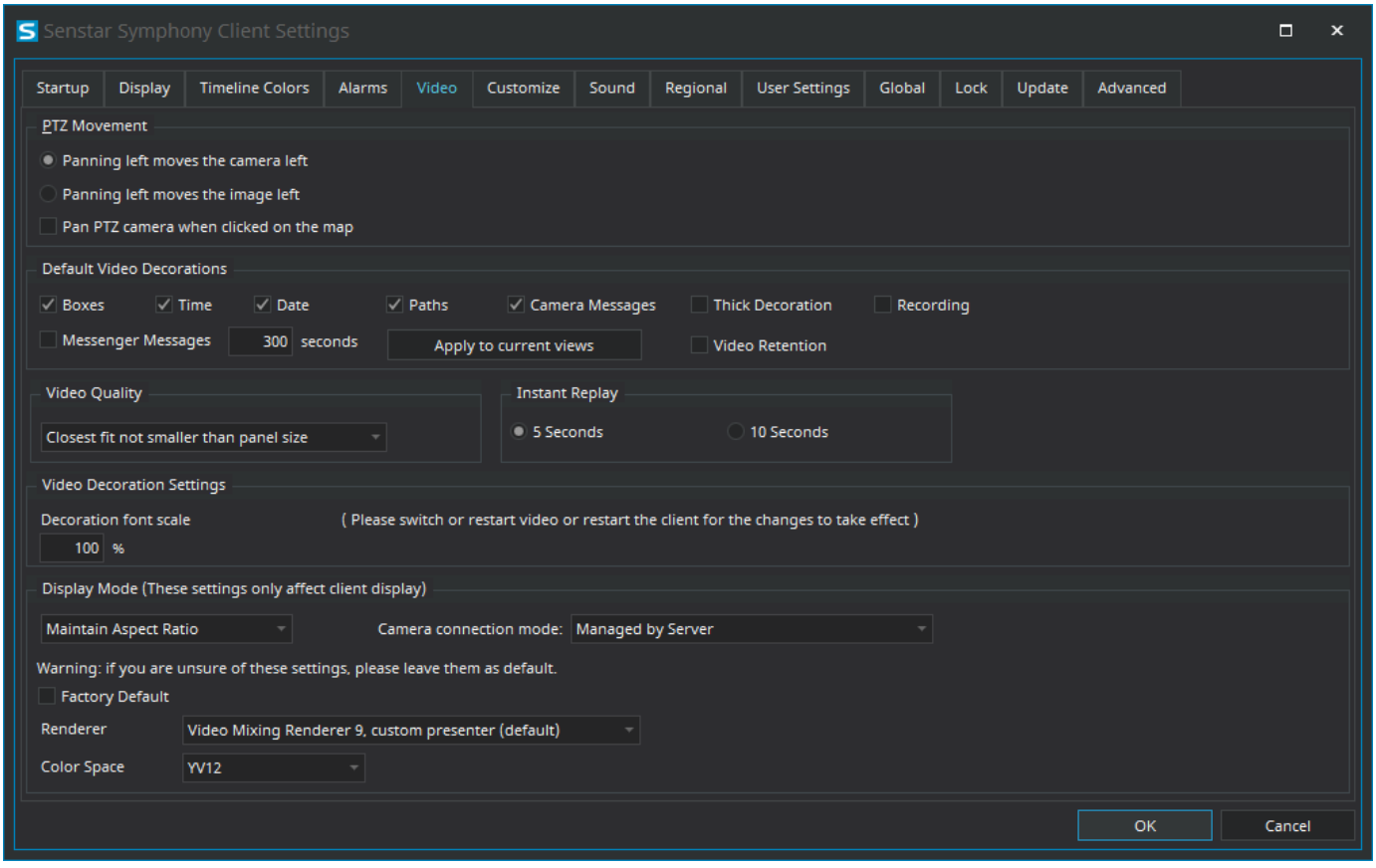
Setting	Description
Show Alarm Window (click OK required)	Select to make the Windows Client display a dialog box when an alarm occurs.

Setting	Description
Retrieve initial alarms of fixed hours	Select to retrieve alarms from the amount of time that you specify in the hour field below (1 to 24 hours).
Alarm Pop-up mode	Select how the Windows Client displays alarm dialog boxes.
Flash panel on alarm	Select to display an alarm indicator around camera view panels when cameras record alarms.
Hide global alarm indicator	Select to hide the colored alarm indicators in the Windows Client interface.
Number of seconds to flash alarm	Specify how long the alarm indicator flashes when cameras record alarms. The alarm indicator will flash until the time elapses or you acknowledge the alarm.
Alarm Box color on Timeline/Show rule alarms in Alarm Log	Select whether the alarm appears in the alarm log and set the color for the alarm in the timeline.

Video Settings

The video settings determine the behavior of PTZ cameras, the appearance of video decorations, instant replay, and the characteristics of video in the Windows Client.

+



PTZ Movement

Setting	Description
Panning left moves the camera left	Select to use the default directions for the pan buttons (i.e., the left pan button pans the camera to the left and/or digitally pans the image to the right).
Panning left moves the image left	Select to use the inverted directions for the pan buttons (i.e., the left pan button pans the camera to the right and/or digitally pans the image to the left).
Pan PTZ camera when clicked on the map	Select to pan PTZ cameras to the location that you click on a map.

Default Video Decorations

Setting	Description
Boxes	Select to display video analytic boxes over the video in the camera view panel.
Time	Select to display the time over the video in the camera view panel.
Date	Select to display the date over the video in the camera view panel.
Paths	Select to display video analytic paths over the video in the camera view panel.
Camera messages	Select to display information from cameras over the video in the camera view panel.
Thick decoration	Select to make the video analytic decoration (boxes and paths) thicker.
Recording	Select to display when the Windows Client is recording.
Video Retention	Select to display video retention capacity over the video in the camera view panel.
Messenger messages	Select to display messages from the Senstar Symphony Messenger over the video in the camera view panel.
Seconds	Select how long the messages remain visible.
Apply to current views	Click to apply the decoration settings to the current views.

Video Quality

Setting	Description
Lowest resolution	Select to display video at the lowest possible resolution.
Closest fit to panel size	Select to display video at the resolution that most closely matches the size of the video panel, including resolutions that are smaller than the video panel.
Closest fit not smaller than panel size	Select to display video at the resolution that most closely matches the size of the video panel, excluding resolutions that are smaller than the video panel.
Highest resolution	Select to display video at the highest possible resolution.

Instant Replay

Setting	Description
5 seconds	Select to set the instant replay function to 5 seconds.

Setting	Description
10 seconds	Select to set the instant replay function to 10 seconds.

Video Decoration Settings

Setting	Description
Decoration font scale	Define the size of the text in video panels.

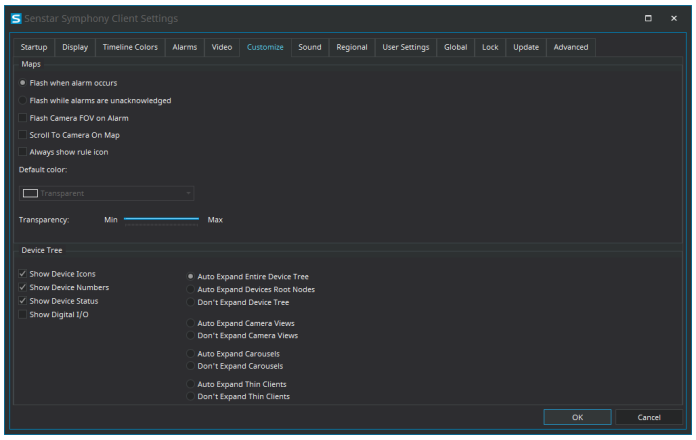
Display Mode

Setting	Description
Actual Size	Select to set the video panel to display the video at the size from the camera.
Maintain Aspect Ratio	Select to set the video panel to display the video at the aspect ratio.
Fit to Window	Select to fit the video to the video panel.
Camera connection mode	Select how the Windows Client connects to cameras.
Factory Default	Select to use the default video renderer.
Renderer	Select a video renderer.
Color Space	Select the color space for the Windows Client.

Customize Settings

The customize settings determines the appearance and behavior of maps and the device tree in the Windows Client.

+



+

Maps

Setting	Description
Flash when alarm occurs	Select to flash the alarm icon on a map when the alarm occurs.
Flash while alarms are unacknowledged	Select to flash the alarm icon while the alarm is unacknowledged.

Setting	Description
Flash Camera FOV on Alarm	Select to flash the camera field of view on a map for 10 seconds when an alarm occurs. The camera field of view will continue to flash if you select the Flash while alarms are unacknowledged option.
Scroll To Camera On Map	Select to center the map on a camera when you click the camera in the Map Navigation pane of the Windows Client interface.
Always show rule icon	Select to always show the rule icon on the map.
Default color	Select the color for the rule icon.
Transparency	Set the transparency for the rule icon on the map.

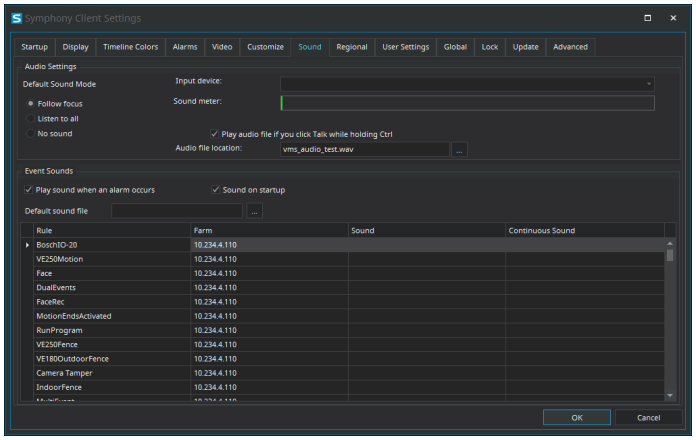
Device Tree

Setting	Description
Show Device Icons	Select to show device icons in the device tree.
Show Device Numbers	Select to show device numbers in the device tree.
Show Device Status	Select to show the statuses of devices in the device tree (e.g., On. Off, Activity, etc.).
Show Digital I/O	Select to show digital I/O devices in the device tree.
Auto Expand Entire Device Tree	Select to expand all levels of the device tree when the Windows Client interface starts.
Auto Expand Devices Root Nodes	Select to expand the top level of the device tree when the Windows Client interface starts.
Don’t Expand Device Tree	Select keep the device tree collapsed when the Windows Client interface starts.
Auto Expand Camera Views	Select to expand the camera views in the device tree when the Windows Client interface starts.
Don’t Expand Camera Views	Select to keep the camera views collapsed in the device tree when the Windows Client interface starts.
Auto Expand Carousels	Select to expand the carousels in the device tree when the Windows Client interface starts.
Don’t Expand Carousels	Select to keep the carousels collapsed in the device tree when the Windows Client interface starts.
Auto Expand Thin Clients	Select to expand the Senstar Thin Client group in the device tree when the Windows Client interface starts.
Don’t Expand Thin Clients	Select to keep the Senstar Thin Client group collapsed in the device tree when the Windows Client interface starts.

Sound Settings

The sound settings determine the noises that the Windows Client generates from cameras and events.

+



+

Audio Settings

Setting	Description
Default Sound Mode	Set how the Windows Client plays or mutes audio for video. Select Follow focus to play audio from the active video panel. Select Listen to all to play audio from all video panels. Select No sound to mute all audio.
Input device	Select the audio input device.
Play audio file if you click Talk while holding Ctrl	Select to play an audio file when you click the Talk button while pressing the Ctrl key.
Audio file location	Select the audio file to play when you click the Talk button while pressing the Ctrl key.

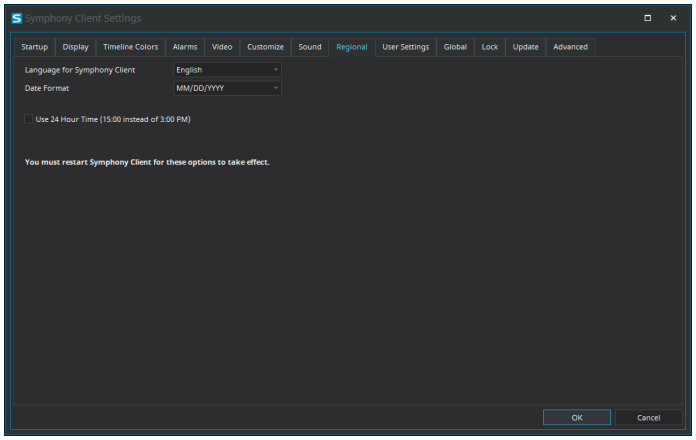
Event Sounds

Setting	Description
Play sound when an alarm occurs	Select to play a sound when an alarms occurs. You can set both the alarm sound and the continuous sound for each rule.
Sound on startup	Select to play the default sound file when the Windows Client interface starts.
Default sound file	Select the default audio file.

Regional Settings

The regional settings determine the language and the date/time format for the Windows Client.

+



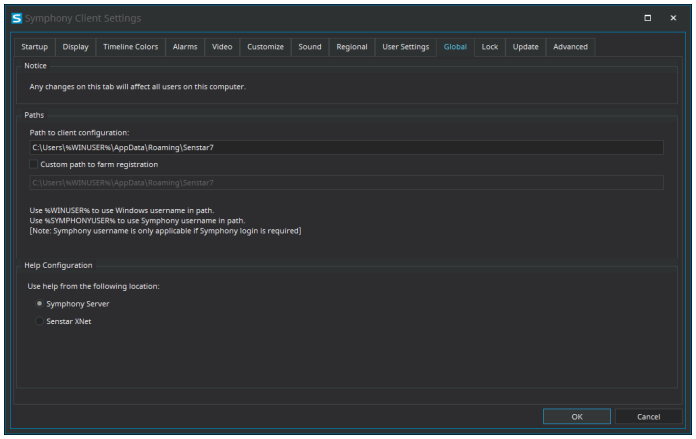
+

Setting	Description
Language for Windows Client	Select the language for the Windows Client interface.
Date Format	Select the format for dates in the Windows Client interface.
Use 24 Hour Time	Select to display time in the 24-hour format in the Windows Client interface.

Global Settings

The global settings determine the location of configuration files and which version of the Senstar Symphony help the Windows Client uses (either the help included with the installation of the Server or the online help).

+



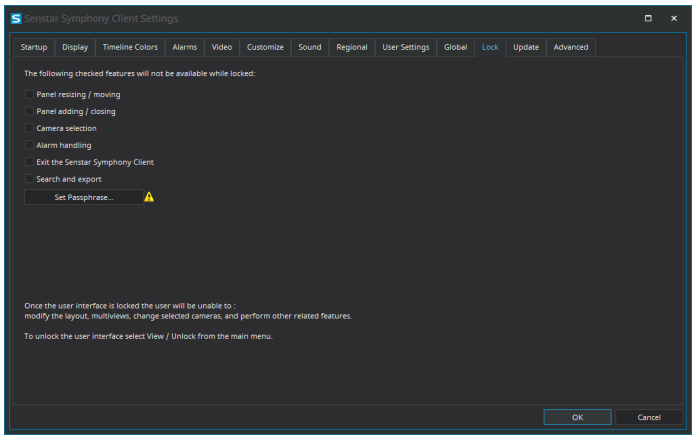
+

Setting	Description
Path to client configuration	Define the path to configuration data for the Windows Client.
Custom path to farm registration	Select to define a custom path for farm registration information.
Use help from the following location	Select whether the Windows Client opens help that is included with the Server or help from the Internet.

Lock Settings

The lock settings determine the functionality that is available to users when you lock the Windows Client and allows you to set the pass phrase for unlocking the Windows Client.

+



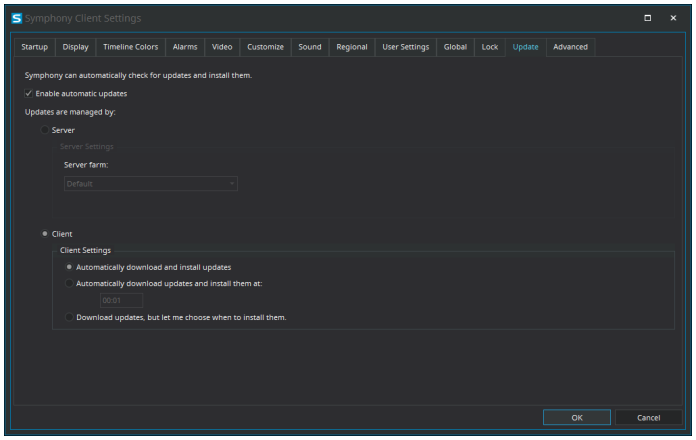
+

Setting	Description
Panel resizing/moving	Select to prevent users from resizing or moving panels (e.g., camera view, map editor, device tree, etc.) in the Windows Client interface.
Panel adding/closing	Select to prevent users from adding or closing panels (e.g., camera view, map editor, device tree, etc.) in the Windows Client interface.
Camera selection	Select to prevent users from selecting different cameras.
Alarm Handling	Select to prevent users from processing alarms.
Exit the Windows Client	Select to prevent users from closing the Windows Client.
Search and export	Select to prevent users from searching for and exporting video.
Set Passphrase	Click to set the pass phrase that unlocks the Windows Client.

Update Settings

The update settings determine how the Windows Client checks for and applies updates.

+



+

Setting	Description
Enable automatic updates	Select to turn on automatic updates for the Windows Client.
Updates are managed by	Select whether the Server or the Windows Client manages the updates.

Server Settings

Setting	Description
Server farm	If you manage updates with the Server, select the Server farm that manages the updates.

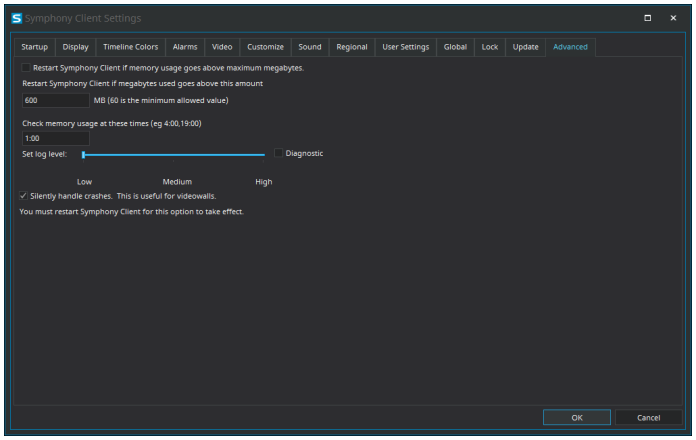
Client Settings

Setting	Description
Automatically download and install updates	If you manage updates with the Windows Client, select this to download and install updates as soon as they become available.
Automatically download updates and install them at	If you manage updates with the Windows Client, select this to download and install updates at a specific time.
Download updates but let me choose when to install them	If you manage updates with the Windows Client, select this to download updates only. If you select this option, you must install the updates manually.

Advanced Settings

The advanced settings determines how and when the Windows Client restarts and how much information it includes in log files.

+



+

Setting	Description
Restart Windows Client if memory usage goes above maximum megabytes	Select to automatically restart the Windows Client when memory usage reaches a specific level.
Restart Windows Client if megabytes goes above this amount	Type the limit of memory usage (in MBs) above which the Windows Client restarts. This setting becomes active when you select the Restart Windows Client if memory usage goes above maximum megabytes setting.
Check memory usage at these times	Set when the Windows Client checks memory usage. This field accepts comma separated values in the 24-hour format (hh:mm).
Set log level	Using the slider, set the log level for the Windows Client.
Diagnostic	Select to set the log level to diagnostic. This setting generates the most comprehensive logging information. If you select this option, it overrides the log level that you set using the Set log level slider.
Silently handle crashes	Select to hide the CMD window when the Windows Client creates a dump file.

Video Wall

The video wall feature in Senstar Symphony can display footage from multiple cameras in the server farm on multiple monitors.

Any Windows Client can act as a video wall client, and you can include any monitors connected to the computers that host the Windows Client in the video wall.

Register a Client

Register each computer that hosts the Windows Client that you want to include in the video wall.

1. In the Windows Client interface, click View > Video Wall.
2. Click the Video Wall Client Configuration tab.
3. Click Register current Client.

4. Click Save.

Create a Video Wall

1. In the Windows Client interface, click View > Video Wall.
2. On the Video Wall Client Configuration tab, click Design Video Wall.
3. Click New.
4. To define a name for the video wall, perform the following steps:
   a. Double-click the default name for the video wall.
   b. Type a new name.
   c. Press Enter.
5. Select the name of the video wall and click Open.
6. Drag a video wall monitor from the Tool Box pane to the video wall grid.
7. Click the monitor box in the video wall grid.
8. In the Label field, type a name for the monitor and click Apply.
9. Move and size the video wall monitor.
10. Click Save.

Server Configuration

Although you perform most configuration for the Server in the Server configuration interface, the Windows Client interface includes functionality to configure some settings on the Server.

Connect to a Server

You can connect a Windows Client to multiple Server instances.

1. In the Windows Client interface, click Server Configuration > New Symphony Server Registration.
2. In the Address field, perform one of the following tasks:
   - Select the Server from the list of discovered servers.
   - Type the IP address of the Server.
   - Type the DNS name of the Server.
3. In the Name field, type a meaningful name for the Server. This name will appear in the Server List in the

Windows Client interface

.

1. To log in to the Server, perform one of the following tasks:
   - To use your Windows account to authenticate with the Server, select the Windows Authentication check box.
   - Type your username and password.

2. Click OK.

Disconnect from a Server

You can disconnect from a Server to remove the cameras associated with that server from the Windows Client.

1. In the Windows Client interface, click Server Configuration > Delete Symphony Server Registration.
2. Select the server from which to disconnect.
3. Click Remove.

Get Information About the Server

You can gather information about the Server to which the Windows Client connects.

1. In the Windows Client interface, click Server Configuration > Get Info.
2. In the Choose Server list, select the server for which you want information.
3. To get additional information, select Verbose. The verbose information includes:
    - Hard drive information
    - Server version information
    - System information
    - Up-time information
    - Task list information
    - IP configuration information
    - License information
    - Network statistics
    - Services information
4. Click Get Info. The

Get Info

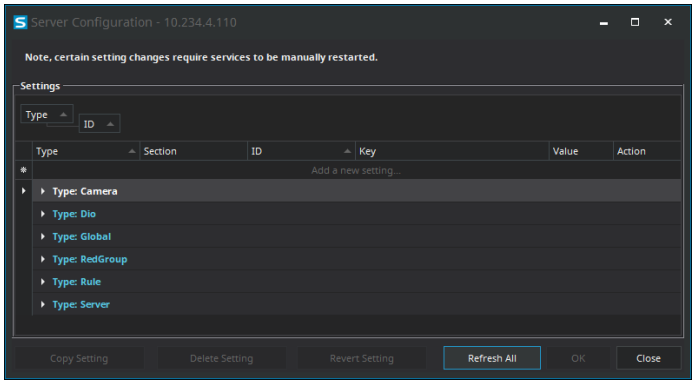
button also refreshes the information.

Manual Configuration Editor

The Manual Configuration Editor is a Senstar Symphony component that you can use to add and edit advanced settings in the Senstar Symphony Database.

You can access the Manual Configuration Editor from the Windows Client or as a stand-alone application if you install the Server.

+



+

Each setting includes the following fields:

- Type
- Section
- ID
- Key
- Value
- Action

When you click OK after making changes, the Windows Client sends the changes to the Server, which adds the changes to the Senstar Symphony Database.

Add a Setting

You can use the Manual Configuration Editor to add a setting to the Senstar Symphony Database.

Adding a setting to the Senstar Symphony Database is a way to add advanced functionality to the Server or Windows Client.

1. In the Windows Client interface, click Server Configuration > Manual Configuration Editor.
2. Click Add a new setting. The

Add a new setting

is a label in a blank line. You can click anywhere in the blank line to activate the data fields.

1. Add the values to the setting.
2. Click OK.

Copy a Setting

You can use the Manual Configuration Editor to copy a setting in the Senstar Symphony Database.

Copying a setting is a quick way to add a new setting to the Senstar Symphony Database by using a similar existing setting as a template.

1. In the Windows Client interface, click Server Configuration > Manual Configuration Editor.
2. Select the setting that you want to copy.
3. Click Copy Setting.

The copied setting appears at the bottom of the applicable setting list with the

label in the

Key

field.

Edit a Setting

You can use the Manual Configuration Editor to edit a setting in the Senstar Symphony Database.

Editing a setting is a quick way to add a new setting to the Senstar Symphony Database by using a similar existing setting as a template.

1. In the Windows Client interface, click Server Configuration > Manual Configuration Editor.
2. Select the setting that you want to edit.
3. Click Edit Setting.

Revert a Setting

You can use the Manual Configuration Editor to revert a setting to the values in the Senstar Symphony Database.

Reverting a setting returns the setting to the values in the Senstar Symphony Database before you save you changes. This only works if you have not yet clicked OK after making changes.

1. In the Windows Client interface, click Server Configuration > Manual Configuration Editor.
2. Select the setting that you want to edit.
3. Click Revert Setting.

Delete a Setting

You can use the Manual Configuration Editor to delete a setting in the Senstar Symphony Database.

1. In the Windows Client interface, click Server Configuration > Manual Configuration Editor.
2. Select the setting that you want to delete.
3. Click Delete Setting.

Refresh Settings

You can use the Manual Configuration Editor to refresh the settings to retrieve changes in the Senstar Symphony Database.

Refreshing the settings ensures that the settings in the Manual Configuration Editor match the current settings in the Senstar Symphony Database. This functionality is helpful if multiple people can make changes to the Senstar Symphony Database.

1. In the Windows Client interface, click Server Configuration > Manual Configuration Editor.
2. Click Refresh All.

Windows Authentication

Windows authentication, or single sign-on, uses domain identities to authenticate users.

To use Windows authentication, the Server and the Windows Client must be in the same security domain, and the user must use domain credentials to log in to the Windows Client interface.

Enable Windows Authentication

1. In the Windows Client interface, right-click a Server in the Server List.
2. Click Edit.
3. Select Windows Authentication.
4. Click OK.

Reports and Logs

You can generate reports on the data from the Server.

You can distribute reports as emails or save reports to files. You can schedule reports to run automatically or manually generate a report at any time. When you run a report, the Server saves the report to the \Data\Reports path for the server (by default) or the path that you set when you install the Server.

Available Reports

Report	Description
Alarm Report	Displays a list of and information about individual alarms
Alarm Statistics	Summarizes all alarms for a specific time
Face Recognition Report	Displays information about matched faces
Heat Map Image	Displays a graphical representation of traffic patterns
Object Counts	Summarizes the number of objects
Object Counts Across a Line	Summarizes the object counts across a line
Object Statistics	Compares traffic and dwell time

Run a report

You can manually generate a report at any time.

1. In the Windows Client interface, click Reports. The

Report Designer

opens in a browser.

1. Log in to the Report Designer.
2. Select a report.
3. Click Run.

Edit a report

You can make changes to an existing report in the Report Designer.

1. In the Windows Client interface, click Reports. The

Report Designer

opens in a browser.

1. Log in to the Report Designer.
2. Perform one of the following tasks:
   - Select a report and click Edit.
   - Double-click a report.
3. Make changes to the report.
4. Click Save.

To run reports, a user must have the Connect and Execute Report permissions. To run the Heat Map Image report, the user must additionally have the Search permission.

View Events

You can view and export events for the Windows Client and any Server to which the Windows Client connects.

Events are stored in the audit log in the Senstar Symphony Database. By default, the Windows Client interface displays the events for the current day.

1. In the Windows Client interface, click Help > View Audit.
2. Select the start date and time and the end date and time.
3. Click Reload.
4. To group the events, drag a column
5. To export the events as a CSV file, click Export.

Alarm Report

The alarm report displays a list of and information about individual alarms for a specific time.

1. In the Windows Client interface, click Reports. The

Report Designer

opens in a browser.

1. Log in to the Report Designer.
2. Click New Report.
3. Type a name for the report.
4. In the Report Type list, select Alarm Report.
5. To allow other users to run the report, select Allow other users to run this report.
6. Click OK.
7. In the Cameras section, perform the following tasks to add the cameras that provide information for the report:
   a. Click Add Cameras.
   b. Select one or more cameras. You can search for cameras by camera name.
   c. Click OK.

8. In the Date Range section, perform the following tasks to determine the data that the report includes:
    a. In the Start including data from section, define the start of the data.
    b. In the Stop including data after section, define the end of the data.
    c. To use data from a specific time range from each day, select Use custom time range for data collection and specify the time range.
9. In the Schedule section, perform the following tasks to run the report automatically:
    a. Select Schedule Enabled.
    b. In the Recurrence section, set when the report runs.
    c. In the Schedule start section, set when the report starts running automatically.
    d. In the Schedule finish section, set when the report stops running automatically.
10. In the Distribution section, perform the following tasks to determine how the Server distributes reports:
    a. To send the report attached to an email, select Send report in email, specify the email addresses of the recipients, and select the file formats for the reports.
    b. To save the report as a file, select Save report to file, specify the path, define the file name, and select the file formats.
11. In the Table Layout section, perform the following tasks to determine the appearance of the table in the report:
    a. In the Columns list, select the information that will appear in the columns of the report.
    b. In the Grouping section, select how the information is grouped in the report.
    c. In the Sorting section, select how the information is sorted in the report.
12. Click Save.

Alarm Statistics Report

The alarm statistics report summarizes alarms for a specific time.

1. In the Windows Client interface, click Reports. The

Report Designer

opens in a browser.

1. Log in to the Report Designer.
2. Click New Report.
3. Type a name for the report.
4. In the Report Type list, select Alarm Statistics.
5. To allow other users to run the report, select Allow other users to run this report.
6. Click OK.
7. In the Cameras section, perform the following tasks to add the cameras that provide information for the report:

   a. Click Add Cameras.
   b. Select one or more cameras. You can search for cameras by camera name.
   c. Click OK.
8. In the Date Range section, perform the following tasks to determine the data that the report includes:
   a. In the Start including data from section, define the start of the data.
   b. In the Stop including data after section, define the end of the data.
   c. To use data from a specific time range from each day, select Use custom time range for data collection and specify the time range.
9. In the Schedule section, perform the following tasks to run the report automatically:
   a. Select Schedule Enabled.
   b. In the Recurrence section, set when the report runs.
   c. In the Schedule start section, set when the report starts running automatically.
   d. In the Schedule finish section, set when the report stops running automatically.
10. In the Distribution section, perform the following tasks to determine how the Server distributes reports:
   a. To send the report attached to an email, select Send report in email, specify the email addresses of the recipients, and select the file formats for the reports.
   b. To save the report as a file, select Save report to file, specify the path, define the file name, and select the file formats.
11. In the Graph section, perform the following tasks to determine the appearance of the graph in the report:
   a. In the Default Graph list, select the alarm type to display.
   b. In the Graph Type list, select whether the graph is a line or bar graph.
   c. In the Graph Size list, select the size of the graph.
12. In the Table Layout section, perform the following tasks to determine the appearance of the table in the report:
   a. In the Columns list, select the information that will appear in the columns of the report.
   b. In the Grouping section, select how the information is grouped in the report.
   c. In the Sorting section, select how the information is sorted in the report.
13. Click Save.

Face Recognition Report

The Face Recognition report displays information about faces for a specific time.

For the Face Recognition report to be available, you must have the Face Recognition video analytic installed.

When creating this report, you must select different cameras as the entrance and exit cameras.

1. In the Windows Client interface, click Reports. The

Report Designer

opens in a browser.

1. Log in to the Report Designer.
2. Click New Report.
3. Type a name for the report.
4. In the Report Type list, select Face Recognition.
5. To allow other users to run the report, select Allow other users to run this report.
6. Click OK.
7. In the Entrance Cameras section, perform the following tasks to add the cameras that provide information for the report:
   a. Click Add Cameras.
   b. Select one or more cameras. You can search for cameras by camera name.
   c. Click OK.
8. In the Exit Cameras section, perform the following tasks to add the cameras that provide information for the report:
   a. Click Add Cameras.
   b. Select one or more cameras. You can search for cameras by camera name.
   c. Click OK.
9. In the Face Recognition section, perform the following tasks to
   a. To exclude faces that are observed by an exit camera first and then by an entrance camera, select Remove exit-to-entrance matches.
   b. In the Minimum confidence for report field, select how confident that the Face Recognition video analytic must be for it to report on the face.
   c. In the Reporting block size field, select the time (in seconds) from which the Face Recognition video analytic chooses the best face match.
   d. In the Number of blocks to check after current field, set how many blocks of time that the Face Recognition video analytic searches for a face match.
   e. In the Timeout for first match in block field, set the time before which the Face Recognition video analytic must detect a face entering the scene for the face to be eligible for a match.
   f. In the Hours to run report list, select the times at which the Face Recognition video analytic generates data for the report.
10. In the Date Range section, perform the following tasks to determine the data that the report includes:
    a. In the Start including data from section, define the start of the data.
    b. In the Stop including data after section, define the end of the data.
    c. To use data from a specific time range from each day, select Use custom time range for data collection and specify the time range.

11. In the Schedule section, perform the following tasks to run the report automatically:
    a. Select Schedule Enabled.
    b. In the Recurrence section, set when the report runs.
    c. In the Schedule start section, set when the report starts running automatically.
    d. In the Schedule finish section, set when the report stops running automatically.
12. In the Distribution section, perform the following tasks to determine how the Server distributes reports:
    a. To send the report attached to an email, select Send report in email, specify the email addresses of the recipients, and select the file formats for the reports.
    b. To save the report as a file, select Save report to file, specify the path, define the file name, and select the file formats.
13. In the Table Layout section, perform the following tasks to determine the appearance of the table in the report:
    a. In the Columns list, select the information that will appear in the columns of the report.
    b. In the Grouping section, select how the information is grouped in the report.
    c. In the Sorting section, select how the information is sorted in the report.
14. Click Save.

Heat Map Image Report

The heat map image report displays a graphical representation of traffic patterns for a specific time.

1. In the Windows Client interface, click Reports. The

Report Designer

opens in a browser.

1. Log in to the Report Designer.
2. Click New Report.
3. Type a name for the report.
4. In the Report Type list, select Heat Map Image.
5. To allow other users to run the report, select Allow other users to run this report.
6. Click OK.
7. In the Cameras section, perform the following tasks to add the cameras that provide information for the report:
    a. Click Add Cameras.
    b. Select one or more cameras. You can search for cameras by camera name.
    c. Click OK.
8. In the Zone Selection section, perform the following tasks to determine which zones in the camera view generate data for the report:
    a. Click Add Zone.

b. Move or reshape the zone.
c. To rename the zone, click Rename Zone, type a new name, and click OK.
d. Repeat to add another zone.

9. In the Sensitivity section, perform the following tasks to set how sensitive the heat map is to events:
   a. To set the number of intersections that must occur before the heat map starts registering intersections for a zone, select Minimum intersections and type the value.
   b. To set the number of intersections that must occur before the heat map stops updating the value for a zone, select Maximum Intersections and type a value.
   c. To set how long an object must remain stationary before the heat map starts registering dwelling objects for a zone, select Minimum Dwell Time and set the time.
   d. To set how long an object remains stationary before the heat map stops updating the value for a zone, select Maximum Dwell Time and set the time.
   e. To set how long an object must be stationary before it is considered as dwelling, select Dwell Threshold, and set the time.
10. In the Date Range section, perform the following tasks to determine the data that the report includes:
    a. In the Start including data from section, define the start of the data.
    b. In the Stop including data after section, define the end of the data.
    c. To use data from a specific time range from each day, select Use custom time range for data collection and specify the time range.
11. In the Schedule section, perform the following tasks to run the report automatically:
    a. Select Schedule Enabled.
    b. In the Recurrence section, set when the report runs.
    c. In the Schedule start section, set when the report starts running automatically.
    d. In the Schedule finish section, set when the report stops running automatically.
12. In the Distribution section, perform the following tasks to determine how the Server distributes reports:
    a. To send the report attached to an email, select Send report in email, specify the email addresses of the recipients, and select the file formats for the reports.
    b. To save the report as a file, select Save report to file, specify the path, define the file name, and select the file formats.
13. In the Table Layout section, perform the following tasks to determine the appearance of the table in the report:
    a. In the Columns list, select the information that will appear in the columns of the report.
    b. In the Grouping section, select how the information is grouped in the report.
    c. In the Sorting section, select how the information is sorted in the report.
14. Click Save.

Automatic License Plate Recognition Report

The LPR report displays information about license plates for a specific time.

1. In the Windows Client interface, click Reports. The

Report Designer

opens in a browser.

1. Log in to the Report Designer.
2. Click New Report.
3. Type a name for the report.
4. In the Report Type list, select LPR Report.
5. To allow other users to run the report, select Allow other users to run this report.
6. Click OK.
7. In the Cameras section, perform the following tasks to add the cameras that provide information for the report:
   a. Click Add Cameras.
   b. Select one or more cameras. You can search for cameras by camera name.
   c. Click OK.
8. In the Filter section, select the plate lists on which to report.
9. In the Date Range section, perform the following tasks to determine the data that the report includes:
   a. In the Start including data from section, define the start of the data.
   b. In the Stop including data after section, define the end of the data.
   c. To use data from a specific time range from each day, select Use custom time range for data collection and specify the time range.
10. In the Schedule section, perform the following tasks to run the report automatically:
    a. Select Schedule Enabled.
    b. In the Recurrence section, set when the report runs.
    c. In the Schedule start section, set when the report starts running automatically.
    d. In the Schedule finish section, set when the report stops running automatically.
11. In the Distribution section, perform the following tasks to determine how the Server distributes reports:
    a. To send the report attached to an email, select Send report in email, specify the email addresses of the recipients, and select the file formats for the reports.
    b. To save the report as a file, select Save report to file, specify the path, define the file name, and select the file formats.
12. In the Table Layout section, perform the following tasks to determine the appearance of the table in the report:
    a. In the Columns list, select the information that will appear in the columns of the report.

b. In the Grouping section, select how the information is grouped in the report.
c. In the Sorting section, select how the information is sorted in the report.

13. Click Save.

Object Counts Report

The object counts report displays information about objects for a specific time.

1. In the Windows Client interface, click Reports. The

Report Designer

opens in a browser.

1. Log in to the Report Designer.
2. Click New Report.
3. Type a name for the report.
4. In the Report Type list, select Object Counts.
5. To allow other users to run the report, select Allow other users to run this report.
6. Click OK.
7. In the Cameras section, perform the following tasks to add the cameras that provide information for the report:
   a. Click Add Cameras.
   b. Select one or more cameras. You can search for cameras by camera name.
   c. Click OK.
8. In the Date Range section, perform the following tasks to determine the data that the report includes:
   a. In the Start including data from section, define the start of the data.
   b. In the Stop including data after section, define the end of the data.
   c. To use data from a specific time range from each day, select Use custom time range for data collection and specify the time range.
9. In the Schedule section, perform the following tasks to determine when the report runs and what information is contains:
   a. Select whether to run the report manually or on a schedule.
   b. If you select to run the report on a schedule, set the schedule.
   c. Specify the time from which to collect data for the report. You can set a relative time based on the report or select specific times.
   d. Select how to group the data.
10. In the Distribution section, perform the following tasks to determine how the Server distributes reports:
    a. To send the report attached to an email, select Send report in email, specify the email addresses of the recipients, and select the file formats for the reports.

b. To save the report as a file, specify the path, define the file name, and select the file formats.

11. In the Graph section, perform the following tasks to determine the appearance of the graph in the report:
    a. In the Default Graph list, select the alarm type to display.
    b. In the Graph Type list, select whether the graph is a line or bar graph.
    c. In the Graph Size list, select the size of the graph.
12. In the Table Layout section, perform the following tasks to determine the appearance of the table in the report:
    a. In the Columns list, select the information that will appear in the columns of the report.
    b. In the Grouping section, select how the information is grouped in the report.
    c. In the Sorting section, select how the information is sorted in the report.
13. Click Save.

Object Counts Across a Line Report

The object counts across a line report displays information about objects crossing a line for a specific time.

1. In the Windows Client interface, click Reports. The

Report Designer

opens in a browser.

1. Log in to the Report Designer.
2. Click New Report.
3. Type a name for the report.
4. In the Report Type list, select Object Counts Across a Line.
5. To allow other users to run the report, select Allow other users to run this report.
6. Click OK.
7. In the Cameras section, perform the following tasks to add the cameras that provide information for the report:
    a. Click Add Cameras.
    b. Select one or more cameras. You can search for cameras by camera name.
    c. Click OK.
8. In the Line section, select the line across which to count objects.
9. In the Date Range section, perform the following tasks to determine the data that the report includes:
    a. In the Start including data from section, define the start of the data.
    b. In the Stop including data after section, define the end of the data.
    c. To use data from a specific time range from each day, select Use custom time range for data collection and specify the time range.

10. In the Schedule section, perform the following tasks to determine when the report runs and what information is contains:
    a. Select whether to run the report manually or on a schedule.
    b. If you select to run the report on a schedule, set the schedule.
    c. Specify the time from which to collect data for the report. You can set a relative time based on the report or select specific times.
    d. Select how to group the data.
11. In the Distribution section, perform the following tasks to determine how the Server distributes reports:
    a. To send the report attached to an email, select Send report in email, specify the email addresses of the recipients, and select the file formats for the reports.
    b. To save the report as a file, specify the path, define the file name, and select the file formats.
12. In the Graph section, perform the following tasks to determine the appearance of the graph in the report:
    a. In the Default Graph list, select the alarm type to display.
    b. In the Graph Type list, select whether the graph is a line or bar graph.
    c. In the Graph Size list, select the size of the graph.
13. In the Table Layout section, perform the following tasks to determine the appearance of the table in the report:
    a. In the Columns list, select the information that will appear in the columns of the report.
    b. In the Grouping section, select how the information is grouped in the report.
    c. In the Sorting section, select how the information is sorted in the report.
14. Click Save.

Overhead People Count Report

The overhead people count report displays information about the number of people counted by an overhead camera.

1. In the Windows Client interface, click Reports. The

Report Designer

opens in a browser.

1. Log in to the Report Designer.
2. Click New Report.
3. Type a name for the report.
4. In the Report Type list, select Overhead People Count.
5. To allow other users to run the report, select Allow other users to run this report.
6. Click OK.
7. In the Cameras section, perform the following tasks to add the cameras that provide information for

the report:

a. Click Add Cameras.

b. Select one or more cameras. You can search for cameras by camera name.

c. Click OK.

8. In the Line section, select the line across which to count people.
9. In the Date Range section, perform the following tasks to determine the data that the report includes:
   a. In the Start including data from section, define the start of the data.
   b. In the Stop including data after section, define the end of the data.
   c. To use data from a specific time range from each day, select Use custom time range for data collection and specify the time range.
10. In the Schedule section, perform the following tasks to determine when the report runs and what information is contains:
    a. Select whether to run the report manually or on a schedule.
    b. If you select to run the report on a schedule, set the schedule.
    c. Specify the time from which to collect data for the report. You can set a relative time based on the report or select specific times.
    d. Select how to group the data.
11. In the Distribution section, perform the following tasks to determine how the Server distributes reports:
    a. To send the report attached to an email, select Send report in email, specify the email addresses of the recipients, and select the file formats for the reports.
    b. To save the report as a file, specify the path, define the file name, and select the file formats.
12. In the Graph section, perform the following tasks to determine the appearance of the graph in the report:
    a. In the Default Graph list, select the alarm type to display.
    b. In the Graph Type list, select whether the graph is a line or bar graph.
    c. In the Graph Size list, select the size of the graph.
13. In the Table Layout section, perform the following tasks to determine the appearance of the table in the report:
    a. In the Columns list, select the information that will appear in the columns of the report.
    b. In the Grouping section, select how the information is grouped in the report.
    c. In the Sorting section, select how the information is sorted in the report.
14. Click Save.

Object Statistics Report

The object statistics report displays information about objects traffic and dwell time for a specific time.

1. In the Windows Client interface, click Reports. The

Report Designer

opens in a browser.

1. Log in to the Report Designer.
2. Click New Report.
3. Type a name for the report.
4. In the Report Type list, select Object Statistics.
5. To allow other users to run the report, select Allow other users to run this report.
6. Click OK.
7. In the Cameras section, perform the following tasks to add the cameras that provide information for the report:
   a. Click Add Cameras.
   b. Select one or more cameras. You can search for cameras by camera name.
   c. Click OK.
8. In the Date Range section, perform the following tasks to determine the data that the report includes:
   a. In the Start including data from section, define the start of the data.
   b. In the Stop including data after section, define the end of the data.
   c. To use data from a specific time range from each day, select Use custom time range for data collection and specify the time range.
9. In the Schedule section, perform the following tasks to determine when the report runs and what information is contains:
   a. Select whether to run the report manually or on a schedule.
   b. If you select to run the report on a schedule, set the schedule.
   c. Specify the time from which to collect data for the report. You can set a relative time based on the report or select specific times.
   d. Select how to group the data.
10. In the Distribution section, perform the following tasks to determine how the Server distributes reports:
    a. To send the report attached to an email, select Send report in email, specify the email addresses of the recipients, and select the file formats for the reports.
    b. To save the report as a file, specify the path, define the file name, and select the file formats.
11. In the Graph section, perform the following tasks to determine the appearance of the graph in the report:
    a. In the Default Graph list, select the alarm type to display.
    b. In the Graph Type list, select whether the graph is a line or bar graph.
    c. In the Graph Size list, select the size of the graph.

12. In the Table Layout section, perform the following tasks to determine the appearance of the table in the report:
    a. In the Columns list, select the information that will appear in the columns of the report.
    b. In the Grouping section, select how the information is grouped in the report.
    c. In the Sorting section, select how the information is sorted in the report.
13. Click Save.

Appendix

Reference information for the Windows Client.

In This Section

Open Command

You can open the Windows Client using a command in the command line. In addition, you can add arguments to the command that open specific cameras and, in the case of PTZ cameras, specific camera presets.

In custom application development, you can associate this command with a control to open the Windows Client from another application.

```
ae.exe ai://server/camera/preset
```

Where:

- server is the address of the server
- camera is the ID of the camera
- preset is the preset for the PTZ camera

View Log Files

You can view, search, and download log files for the Windows Client and any Server to which the Windows Client connects.

1. In the Windows Client interface, click Help > View Detailed Logs.
2. In the Date field, select the date for which you want to view log files.
3. Select a server or the client.
4. Select the log file to view.
5. To copy the visible log file, click Copy to Clipboard.
6. To download log files, perform the following tasks:
    a. Click Download.

b. Select the start and end date, or select Download all logs from server.
c. Click Download.

7. To search the visible log file, perform the following tasks:
   a. In the text field, type the search text.
   b. Click Find Next.

Disable Single Sign-On

You can disable the single sign-on option when changing users and registering new farms in the Windows Client.

When you disable single sign-on, the Windows Authentication check box is disabled when you change users or when you register a new Server farm.

1. Open the acc.ini file at %appdata%\Senstar8.
2. In the `[Main]` section, add the following text:

```
DisableWindowsAuthentication=True
```

1. Save and close the acc.ini file.

Configure the SSL Certificate Timeout

You can set how long the Windows Client waits for a valid certificate before it falls back to a non-SSL connection.

The default timeout for the SSL certificate is 15000 milliseconds.

1. Open the acc.ini file at %appdata%\Senstar8.
2. Ad the following text to the acc.ini file:

```
[Connectivity]
ReceiveTimeoutInMilliseconds=timeout
```

Where timeout is how long the Windows Client waits for a valid SSL certificate.

1. Save and close the acc.ini file.

Web Client

The Web Client includes functionality to monitor cameras, manage video, generate reports, and configure alarms.

The Web Client mimics the Windows Client as much as possible. Most core features of the Windows Client are available in the Web Client. In addition, the Web Client includes the Report Designer.

Each Server has a dedicated Web Client. For information on configuring which Symphony server is used, see General Settings: Web Client.

Log in to the Web Client

You can open the Web Client in a browser.

You can also access the Server configuration interface from the Web Client interface.

1. In a browser, navigate to the IP address of your Server.
2. In the language list, select your language.
3. Type your username and password.
4. Click the Web Client button.

Player

The Player is an application that can view video files created in the Windows Client.

The Player is a lightweight solution that allows you to view video and search results from the Server. By default, the Player installs with the Windows Client and the Server, but you can also install it as a standalone application.

Install the Player

You can install the Player as a standalone application.

1. Download and run the installer.
2. Select the language and click OK.
3. Review the license terms and conditions, select I accept the terms in the License Agreement, and click Next.
4. Select the installation location.
5. Select whether to install the Remote Support Tool.
6. Click Next.
7. Click Install.
8. Click Close.

Enable Watermark Verification

You can enable watermark verification for the Player to prevent the Player from playing tampered video.

1. Open the acc.ini file at %appdata%\Senstar8.
2. Add the following values:

```
[VideoRecvCTRL]
UseWatermarking=True
```

1. Save and close the acc.ini file.

Play a Video File

You can play video from a file or a URL.

You can export a video file from camera view panels or search results in the Windows Client interface.

You can generate a video URL by exporting search results by exporting search results as an email link. To play video from a URL, the computer hosting the Player must be on the same network as the Server.

1. In the Player, perform one of the following tasks:
   - To play video from a file, click File > Play From File, navigate to the file, and click Open.
   - To play video from a URL, click File > Play From URL, type the URL, and click OK.

2. To show decorations, click Decorations and select or clear decorations.
3. To zoom, click Zoom and either Zoom In or Zoom Out.
4. To set the playback speed, move the Speed slider to the desired speed.
5. To navigate through the video, use the following controls:

Option	Description
Play/Pause	Play or pause the video.
< snippet	Move backwards to the last activity in the video.
< frame	Move backwards one frame.
frame >	Move forwards one frame.
snippet >	Move forwards to the next activity in the video.
Slider	Move the slider to navigate to the corresponding position in the video.

Appendix

In This Section

Release Notes

Release 8.12.0 (July 2026)

New Features

Summary	Description
Protected footage	Security guards and administrators can mark footage from a camera or camera group as protected for a defined time range so it is not deleted by the retention engine, with permission-based protect/unprotect, audit logging, and a management view of protected footage.
OnGuard integration	Senstar Symphony now offers a complete, event-driven OnGuard 8.3/8.4 integration
SNMP v3 support	Added SNMP v3 support with authentication and encryption options for enhanced cybersecurity, alongside existing SNMP v1/v2 support.
Video Display Engine toggle in Startup	Added a toggle in Startup allowing users to switch to the new GPU-powered Display Engine, with a notice that audio output is not yet supported.
External metadata injection	The API offers a simple way to inject metadata such as parcel packages or any data into any camera for Advanced Search.
Protected footage storage warning	Administrators can configure warning and alarm thresholds that trigger a login banner when protected video exceeds a set percentage of disk space.
Camera connect/disconnect audit report	Added a report showing user and camera connect/disconnect sessions with aggregated totals by hour, day, week, or month, and CSV export.
Flashing panel borders on Advanced Alarm Console	The video panel border flashes when an unacknowledged alarm occurs on the Advanced Alarm Console, in both single-panel and quad view.
MP4 export	Operators can export recorded video to the local disk in MP4 format.
New alarm for camera/server fail-over and fallback	Alarm can be used to trigger actions in Rule Engine.
Plain text mode for TCP Action	The TCP Action can send plain text messages with escape character support, instead of the default XML-wrapped format.
Editable permissions for SEM-connected farms	Permissions not managed by Senstar Enterprise Manager (SEM) can now be changed through Server Configuration when a farm is connected to SEM.
Door status indicators on maps	Maps show a permanent open/closed indicator for integrated doors instead of a temporary flash.
Disable failover option	Administrators can temporarily disable failover across all groups from server configuration for a set duration, then re-enable it.

Improvements

Summary	Description
Protected footage metadata retention	Metadata cleanup now correctly accounts for protected footage, preventing metadata from being retained longer than necessary.
Protected footage banner server identification	The protected footage storage warning banner now identifies which server it applies to in multi-server environments.
Synchronized playback speed limits	Added an acc.ini option to set minimum and maximum playback speed while synchronized playback is enabled.
New video display engine handling of edge storage gaps	The display engine now skips gaps in footage from edge storage cameras instead of displaying a connection error for the full length of the gap.
Higher resolution stream on maximize/full screen	Panels now switch to the higher-resolution stream when a panel is maximized or switched to full screen.
Consistent metadata injection decoration order	Injected metadata decorations are now displayed in a consistent order.
API access for actions	Added a REST API, secured by an API key, to trigger existing action sets and individual actions from external systems.
Retention report improvements	The Resource Recording Log report now shows who generated it, the full camera IP/DNS name, and clearer integrity calculations.
Timelines refresh after failover	Timelines now refresh after a server fails over or back so operators see up-to-date signal data.
Accurate camera server time on timelines	Timelines now use the time of the server associated with each camera instead of the currently selected farm's time.
Timeline color loads correctly	Timelines no longer briefly display an incorrect placeholder color before loading actual activity data.
Reliable settings updates	Fixed a rare timing issue that could cause the settings poller to miss an update.
HeatMap scheduled report reliability	HeatMap scheduled reports no longer fail when a sensitivity element is missing attributes.
Gallagher integration hostname support	The Gallagher integration's Server field now accepts hostnames and FQDNs in addition to IP addresses.
OnGuard reauthenticate option	Certain OnGuard connection errors now surface a non-error state with a manual Reauthenticate option in the Authentication Status node.
Faster AMAG integration startup	The AMAG integration now uses a single connection during initialization, reducing startup time for farms with many devices.
LDAPS support	Added support for secure LDAP (LDAPS) authentication for environments that require encrypted directory connections.
CSV camera import validation	CSV camera import now validates that all required fields are present before adding devices.
Configurable service shutdown timeout	The timeout before a service is forcibly terminated during shutdown is now configurable, with a higher 10-second default.
Reduced database load from web service requests	Reduced SQL server contention caused by frequent Thin Client camera requests and session renewal updates on large farms.
License Plate Log midnight rollover	The License Plate Log now continues updating without interaction and correctly displays the last 24 hours across midnight.
Fiber Cut Alarm details on maps	Senstar Symphony Client Map now displays "fiber cut" alarm details, including the zone polyline and meter location, similar to zone intrusion alarms.
New DIO activated/deactivated map icons	Administrators can select new green (activated) and red (deactivated) icons when configuring DIO devices on a map.

Summary	Description
Improved error message security	Error messages in the Configuration Manager and web application no longer expose stack traces or other sensitive configuration details.
Encrypted report URLs	Report URLs generated by Configuration Manager are now served over HTTPS instead of unencrypted HTTP.
Faster rule editing in web configuration	Improved performance when adding or editing rules in the web configuration interface, especially on farms with many rules.
Accurate online backup restore messages	Restoring an online backup now displays the actual message returned by Xnet instead of a generic error.
Larger client title bar icons	Increased the size of icons in the Senstar Symphony Client title bar to match the rest of the standard delivery.
Optimized Overhead People Counting (OPC) report performance	Improved OPC report processing speed through pre-calculated path and line-crossing data.
Improved AI object counting accuracy	Refined the AI Object Detection and Tracking overhead algorithm to improve the accuracy of vehicle counting reports and counting lines.

Fixes

Summary	Description
Synchronized playback stability	Fixed multiple issues that could cause synchronized playback panels to drift out of sync, freeze on pause, or briefly show a black panel during normal playback, gap skipping, and restarts.
Playback speed and scrubbing	Fixed issues where the playback speed slider could reset unexpectedly, scrubbing and reverse playback of high-resolution or H.265 video did not work smoothly, and a panel could switch back to the old Display Engine after being blanked and the client restarted.
Edge storage download and timeline gap handling	Fixed several issues with edge storage video downloads and timeline gap display, including incorrect download start times, inconsistent gap reporting between the display engine and signals, mis-colored timeline sections, and the inability to play video directly from an edge camera.
New Video Display Engine (VDE) decoration and overlay fixes	Fixed multiple issues with the new VDE's decorations and controls, including missing or misapplied watermark, timestamp, and metadata decorations, decorations overlapping in multi-view layouts, and VDE control icons and transparency not displaying correctly.
Video Display Engine and client stability	Fixed numerous crashes, freezes, hangs, and memory or CPU usage issues affecting the VDE, Historical Video, and the Senstar Symphony Client during normal use, panel switching, and extended operation.
Timeline display and loading reliability	Fixed several issues where panel or consolidated timelines failed to load, displayed incorrectly, or fell out of sync with event data, including a Daylight Saving Time issue on Sundays.
Alarm display and permission fixes	Fixed several issues with alarm handling, including alarm markers and log entries not respecting rule or map permissions, unreliable alarm navigation, and pre-event buffer signals not drawing in real time for IO-triggered alarms.
Device model propagation fixes	Fixed device model propagation (ChangeMethod) issues, including newly added cameras not appearing until a service restart and polling-based propagation not functioning in rare situations.
Camera status and ONVIF discovery fixes	Fixed incorrect offline camera status in the device tree and timeline, and ONVIF discovery issues that mislabeled or failed to detect certain camera models.
Map fixes	Fixed multiple issues with maps, including highlighted lines not clearing, incorrect default styles when dragging output nodes, indistinguishable rule button elements, missing text outlines, and maps not responding correctly to clicks or drags.

Summary	Description
Tracking links fixes	Fixed tracking links (maps and browsers) that could not be added to a camera panel or would stop updating the device tree selection.
OnGuard integration reliability	Fixed several reliability issues with the OnGuard integration, including nodes not detecting as offline, aux inputs failing to receive status changes, and keep-alive heartbeat failures not recovering.
AMAG integration recovery	Fixed the AMAG integration not recovering after its communication channel faulted.
Reporting fixes	Fixed several reporting issues, including scheduled reports created by a deleted user failing to send, inconsistent layout between exported PDF and emailed reports, extra invalid rows in the Recording Detailed Log, and retention report columns that could not be hidden.
Server reliability fixes	Fixed a SQL deadlock that could prevent a Senstar Symphony Server from failing back, and fixed Mobile Bridge multicast messages not working with a non-default internal base port.
Device tree and client settings fixes	Fixed several issues where the device tree did not update or load correctly, including after permission changes, denied folder access, and server removal, without requiring a client restart.
RpcBridge.dll error launching Aira player files	Fixed an error stating "RpcBridge.dll was not found" when launching a downloaded .aira file after installing the Player.
Current VDE copy/paste camera	Fixed the Copy/Paste Camera option not working for cameras in the current VDE.
MP4 export internal server error	Fixed an internal server error that caused MP4 export to fail.
Digital zoom permission bypass	Fixed an issue where a user without the "Control zoom via clients" permission could still use the digital zoom box.
Metadata injection concurrency	Fixed an issue preventing multiple metadata injections from being performed at the exact same time.
PTZ preset permission	Fixed an issue preventing users with only the PTZ preset permission from using presets when PTZ control was denied.
Mobile Bridge camera ID	Fixed Mobile Bridge alarms retrieved from history returning a null camera ID.
License plate reading through I/O input	Fixed digital inputs configured under Integrations not triggering license plate reads.
HTTP Request action headers	Fixed an issue preventing headers from being added to the HTTP Request action.
Client/server version compatibility	Fixed incorrect camera status and timeline updates when connecting an older Windows Client to a newer Server.
Ctrl+audio playback	Fixed audio file playback not working while holding the Ctrl key.
Locale-dependent playback speed	Fixed a locale-dependent parsing issue that could set video playback speed to 0 on non-English Windows locales.
Untranslated Search Faces radio buttons	Fixed untranslated radio button text in the Search Faces window.
Axis keyboard and jogdial support	Fixed support for the Axis T8312 Keyboard and T8313 Jogdial (and the newer TU9002/TU9003).
Panel title date label	Fixed the panel title showing "Yesterday" when the day before yesterday was selected.

Glossary

Action set

An ordered set of actions that the Server runs when a rule fires. Typical actions include recording video, raising an alarm, sending an email, toggling a digital output, and calling an integration endpoint. See Action Sets.

Alarm

A high-priority event that requires an operator response. An alarm is created when a rule whose action set includes the "create alarm" action fires. Alarms have a lifecycle: triggered, displayed, acknowledged, resolved, archived. See Managing Alarms.

(Video) analytic

Software that analyses a camera's video stream to detect or classify what is happening in the scene. Examples: motion detection, outdoor people and vehicle tracking, face recognition. Analytics produce events that rules can act on. See Video Analytics.

Carousel

A view panel configuration that cycles through a set of cameras automatically, displaying each for a configured duration. Useful when one operator must monitor more cameras than fit on screen. See Carousels.

Windows Client

The Windows application operators use to view video, respond to alarms, and generate reports. Installed on the Server host and on workstations. See Windows Client.

Device

Any piece of hardware configured in the Server: cameras, access control readers, digital input/output hardware, intrusion sensors, video-wall endpoints. The device tree organises them for operators.

Device tree

The hierarchical list of devices shown in the Windows Client. Administrators control its structure through device groups.

Event

A discrete, time-stamped thing that happened in the system: motion started, a face was recognised, a door was opened, a digital input went high. Events are the raw material that rules consume. See Events.

Server farm

Two or more Server instances that share a configuration and present themselves as a single system. Cameras, rules, users, and security profiles are defined once and apply across the farm. See Settings.

Field of view (FoV)

The area of a scene a camera can actually see, given its lens and mounting. A shape displayed on site maps, where it is used to show coverage and gaps. See Display Field of View.

Integration

A first-class connection between the Server and a third-party system (access control, perimeter sensors, specialty hardware). The integration maps the third party's events into Senstar Symphony events, where rules can act on them. See Add Integration Hardware.

Processing mask

A shape (or set of shapes) drawn on a camera's frame that tells a video analytic which pixels to ignore. Used to exclude regions where the analytic would produce noise (moving foliage, passing traffic, time overlays).

Retention

The maximum age of recorded video before the Server deletes it. Set per camera, per server, or per farm, with per-camera taking precedence. See Configure Video Storage for a Camera.

Rule

The unit of automation in Senstar Symphony. A rule has an event (trigger), an action set (what to do), a schedule (when to be active), and a severity. See Rules.

Schedule

A recurring time window during which a rule is active. Schedules are reusable across rules. See Schedules.

Security profile

A reusable bundle of permissions. Profiles attach to groups, and users inherit them through group membership. See Security Profiles.

Server

The core service of a Senstar Symphony deployment. Records video from cameras, runs the rules engine, stores events and alarms, enforces permissions. See Server.

Site

A logical grouping of cameras and devices that represents a physical location (a building, a campus, a perimeter section). Used for permissions, reports, and map organisation.

State

The specific actionable or operational condition of a sensor or device, such as Alarm, Mask, Supervision, or Normal (secure).

Template

A saved collection of camera configuration settings that can be applied to other cameras to avoid repeating the same setup. See Templates.

User group

A container for users. Security profiles attach to groups; users inherit permissions from the groups they belong to. A user can belong to multiple groups; permissions are the union. See Groups.

View panel

A rectangular region in the Windows Client workspace that shows one source of content — live video, recorded video, a map, a browser, a carousel, or an alarm view. See View Panels.

Web Client

A browser-based client that provides functionality similar to the Windows Client without requiring installed software. See Web Client.

Network Ports

The Server software uses the following network ports by default.

Single-server Network Configuration

Port	Protocol	Description
80	TCP	HTTP web server that forwards to HTTPS on port 443 for server configuration
443	TCP	HTTPS secure web server for server configuration
8433	TCP	Senstar Symphony Mobile Bridge (mobile listening port)
8434	TCP	Senstar Symphony Mobile Bridge (event listening port)
8488	TCP	Senstar Symphony Mobile Bridge (video proxy listening port)
50000	TCP	HTTP web server for the web client
50001	TCP	Web service (control and notification port)
50010	TCP	RTSP live and historical video
50014	TCP	HTTPS secure web server for the web client (if configured)

Server Farm Network Configuration

Port	Protocol	Description
80	TCP	HTTP web server that forwards to HTTPS on port 443 for server configuration
443	TCP	HTTPS secure web server for server configuration
1433	TCP	Outbound rule for SQL server on the SQL server firewall
1434	UDP	Port for SQL communication
5045	UDP	Port for health checks
8433	TCP	Senstar Symphony Mobile Bridge (mobile listening port)
8488	TCP	Senstar Symphony Mobile Bridge (video proxy listening port)
50000	TCP	HTTP web server for the web client

Port	Protocol	Description
50001	TCP	Web service (control and notification port)
50004	TCP	Port for server sub-services
50010	TCP	RTSP live and historical video
50014	TCP	HTTPS secure web server for the Web Client (if configured)

Additional Network Configuration

Port	Protocol	Description
5041	TCP	Access control
50002	TCP	SSO authentication requests
50005	TCP	Video wall
50015	TCP	SSO authentication requests and cryptography

Legal Information

Senstar Symphony Third-Party Attributions

Component	Attribution
ARH Carmen ANPR/LPR	Copyright © 1993-2015. All rights reserved. EULA
Boost Software	Copyright © 1998-2005 Beman Dawes, David Abrahams. Copyright © 2004-2007 Rene Rivera. Boost is licensed under the Boost Software License.
Crypto++	Copyright © 1995-2013 Wei Dai. All rights reserved. Crypto++ is licensed under the Boost Software License.

Component	Attribution
CxImage	Copyright © 2001-2008 Davide Pizzolato. CxImage is licensed under this license.
Cybertec Patroni	Copyright © 2000–2021 CYBERTEC PostgreSQL International GmbH.
Dapper	Dapper is licensed under the Apache License 2.0.
DevExpress WinForms	Copyright © 1998-2021 Developer Express Inc. EULA
DirectShow.NET Library	Copyright © 1991, 1999 Free Software Foundation, Inc. The DirectShow.NET Library is licensed under the GNU Lesser General Public License (LGPL) version 2.1.
excellibrary	The excellibrary is licensed under the GNU Lesser General Public License (LGPL).
FFmpeg	Copyright © 2007 Free Software Foundation, Inc. FFmpeg is licensed under the GNU Lesser General Public License (LGPL) version 2.1 or later.
gson	Copyright © 2008 Google Inc. google/gson is licensed under the Apache License 2.0.
Intel Integrated Performance Primitives	Copyright © Intel Corporation. EULA
Jayrock	Copyright © Atif Aziz. All rights reserved. Jayrock is licensed under the GNU Lesser General Public License (LGPL).
Joda-Time	Copyright © 2002-2018 Joda.org. All Rights Reserved. Joda-Time is licensed under the Apache License 2.0.
libcurl	Copyright © 1996-2018, Daniel Stenberg. All rights reserved. libcurl is licensed under this license.
libjpeg	Copyright © 1991-2018 Thomas G. Lane, Guido Vollbeding.
Live555	Copyright © Live Networks, Inc. All Rights Reserved. Live555 is licensed under the GNU Lesser General Public License (LGPL)
Microsoft .NET Library	Copyright © 2021 Microsoft EULA
OpenH264	Copyright © 2013, Cisco Systems. OpenH264 is licensed under this license.
OpenCV	Copyright © 2018 OpenCV team. OpenCV is licensed under this license.
OpenSSL	Copyright © 1998-2018 The OpenSSL Project. All rights reserved. OpenSSL is licensed under this license.

Component	Attribution
PaddlePaddle/Paddle	Copyright © 2016 PaddlePaddle Authors. All rights reserved. PaddlePaddle/Paddle is licensed under the Apache License 2.0.
PostgreSQL	Copyright © 1996-2021 The PostgreSQL Global Development Group. PostgreSQL is licensed under The PostgreSQL Licence.
RapidXML	Copyright © 2006, 2007 Marcin Kalicinski. RapidXML is licensed under the Boost Software License.