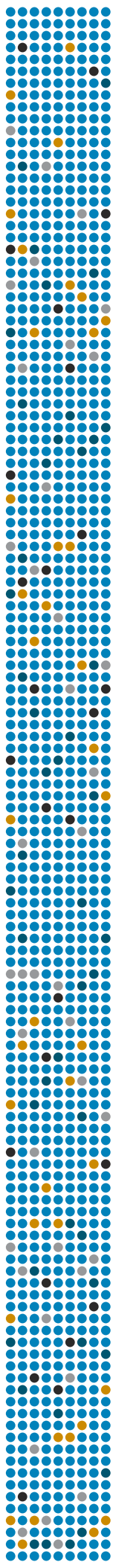




Senstar Symphony  
7.3.x  
User Guide



# Contents

---

Introduction.....	6
Network configuration.....	6
Getting started.....	7
Symphony Server.....	9
Log in to the server configuration interface.....	9
Symphony Server services.....	9
Devices.....	11
Cameras.....	11
Templates.....	17
Hardware.....	19
Integrations.....	19
Access control devices.....	23
Device tree.....	24
Carousels.....	25
Security.....	26
Users.....	26
Groups.....	28
Security profiles.....	29
Logins.....	39
Active Directory authentication.....	40
Security authentication.....	40
Watermarking.....	40
Rules.....	41
Create a rule.....	41
Edit a rule.....	42
Delete a rule.....	42
Events.....	42
Action sets.....	53
Schedules.....	61
Licenses.....	62
Refresh licenses.....	62
Show license XML.....	62
Settings.....	62
Servers.....	62
General.....	65
Notifications.....	72
Cloud services.....	73
Maintenance.....	73
Backup and restore.....	74
Analytics.....	75
Add a video analytic license to a camera.....	75
Draw a processing mask.....	76
Calibrate a camera.....	77
TCP Listener.....	78
Analog Video Signal Loss.....	78
Automatic License Plate Recognition.....	78

- Camera Tampering.....82
- Crowd Detection..... 83
- Image Stabilization..... 86
- Indoor People Tracking..... 86
- Left and Removed Item Detection..... 89
- Motion Detection..... 93
- Outdoor People and Vehicle Tracking..... 95
- PTZ Auto-Tracking..... 98
- Face Recognition.....98
- Symphony Client..... 102
  - Open command..... 102
  - View log files..... 102
  - View events..... 103
  - Lock times..... 103
  - Customize the toolbar..... 103
  - Disable single sign-on..... 103
  - Device tree..... 103
    - Search the device tree..... 104
    - Display a list of users viewing a camera..... 104
    - Suspending access to video..... 104
    - Create a camera tour..... 105
    - Change IO state..... 105
    - Link a camera view..... 105
  - Server list..... 106
    - Enable the server list..... 106
  - Camera view panels..... 106
    - View a camera..... 106
    - View a Thin Client..... 107
    - View picture in picture..... 107
    - View instant replay..... 107
    - Save a camera view..... 107
    - Load a camera view..... 108
    - Open a docked camera view..... 108
    - Open a floating camera view..... 108
    - Add a camera view panel..... 108
    - Add an alarm..... 108
    - Add an alarm indicator..... 109
    - Configure a camera view panel..... 109
    - Search..... 111
    - Export video to file..... 112
    - Export video to the cloud..... 112
    - View video by date..... 113
    - Record video manually..... 113
    - Open by address..... 113
    - View summary video..... 114
    - Video controls..... 114
    - PTZ controls..... 116
    - Camera controls..... 116
  - Timeline..... 117
    - Timeline colors..... 117

- Display the timeline..... 118
- Maps..... 118
  - Add a map..... 118
  - Add a GIS map..... 118
  - View a map..... 118
  - Add a device to a map..... 119
  - Map icons..... 119
  - Display field of view..... 120
- Messenger..... 120
  - Send a message..... 120
- Carousels..... 120
  - Add a carousel..... 121
  - Edit a carousel..... 121
  - Delete a carousel..... 121
- Settings..... 121
  - View camera activity..... 122
  - Customize the toolbar..... 122
  - Change timeline colors..... 122
  - Startup settings..... 123
  - Display settings..... 124
  - Alarms settings..... 126
  - Video settings..... 126
  - Customize settings..... 129
  - Sound settings..... 130
  - Regional settings..... 131
  - Global settings..... 132
  - Lock settings..... 132
  - Update settings..... 133
  - Advanced settings..... 134
- Bookmarks..... 135
  - Create a bookmark..... 135
  - Delete a bookmark..... 135
- Video wall..... 135
  - Register a client..... 135
  - Create a video wall..... 135
- Server configuration..... 136
  - Connect to a server..... 136
  - Disconnect from a server..... 136
  - Delete recorded video..... 136
  - Get information about the server..... 136
  - Manual Configuration Editor..... 137
  - Windows authentication..... 139
- Reports..... 139
  - Create an alarm report..... 140
  - Create an alarm statistics report..... 140
  - Create a Face Recognition report..... 141
  - Create a heat map image report..... 143
  - Create an LPR report..... 144
  - Create an object counts report..... 145
  - Create an object counts across a line report..... 146
  - Create an object statistics report..... 147

- Edit a report..... 148
  - Run a report..... 148
- Alarms..... 148
  - Disable alarms for a camera..... 148
  - Disable alarms for a server..... 149
  - Alarm console..... 149
- Visual tracking..... 151
  - Add a visual tracking link..... 151
- Symphony Web Client..... 153
  - Log in to the Web Client..... 153
  - Configure the Web Client..... 153
- Symphony Player..... 154
  - Install the Player..... 154
  - Enable watermark verification..... 154
  - Play a video file..... 154
- Legal information..... 156
  - Third-party attributions..... 156

# Introduction

---

Senstar Symphony is an award-winning, intelligent video surveillance software that offers a single, innovative, and open IP video platform for video management, video analytics, system integration, and alarm management.

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

Symphony comprises two main components: the Symphony Server and the Symphony Client. You can use the server configuration interface to configure the Symphony Server and the client interface to interact with the cameras connected to Symphony.

Symphony also includes the Symphony Web Client and the Symphony Player. The Web Client provides functionality similar to the Client, but in a Web browser and without requiring installed software. The Player allows you to play video files that you export from Symphony.

Related concepts

[Symphony Server](#) on page 9

[Symphony Client](#) on page 102

[Symphony Web Client](#) on page 153

[Symphony Player](#) on page 154

## Network configuration

The Symphony Server uses the network ports below 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	Mobile Bridge (mobile listening port)
8488	TCP	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	Mobile Bridge (mobile listening port)
8488	TCP	Mobile Bridge (video proxy listening port)
50000	TCP	HTTP web server for the web client
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

### Getting started

Task	Topic
I want to add a digital camera to Symphony.	Add a camera manually Add a camera automatically
I want to save video to a file.	Export video
I want to view video from a camera.	View a camera

Task	Topic
I want to add an alert to Symphony.	Create a rule
I want to view an event across different cameras.	View Camera Activity

#### Related tasks

[Add a camera manually](#) on page 12

[Add a camera automatically](#) on page 12

[View a camera](#) on page 106

[Export video to file](#) on page 112

[Create a rule](#) on page 41

[View camera activity](#) on page 122

# Symphony Server

The Symphony Server includes functionality to manage devices, security, rules, sites, and settings.

You configure the Symphony Server using the server configuration interface. You can access the server configuration interface directly in a browser or from the client interface.

Related concepts

[Introduction](#) on page 6

[Symphony Client](#) on page 102

[Symphony Web Client](#) on page 153

[Symphony Player](#) on page 154

## Log in to the server configuration interface

You can open the server configuration interface in a browser.

You can also access the **Web Client** from the server configuration interface.

1. In a browser, navigate to the IP address of your Symphony Server.
2. In the language list, select your language.
3. Type your username and password.
4. Click **Server Configuration**.

## Symphony Server services

The Symphony Server runs the following services.

Service	Function
AI Authentication Service	<ul style="list-style-type: none"> <li>• Performs single sign-on authentication</li> <li>• Log file prefix:                             <ul style="list-style-type: none"> <li>• sso</li> </ul> </li> </ul>
AI AxisPACSListener	<ul style="list-style-type: none"> <li>• Communicates with Axis access control devices</li> <li>• Optional service/Manual installation</li> <li>• Log file prefix:                             <ul style="list-style-type: none"> <li>• aacl</li> </ul> </li> </ul>
AI DataAccessService	<ul style="list-style-type: none"> <li>• Communicates with the Symphony database</li> <li>• Log file prefix:                             <ul style="list-style-type: none"> <li>• da</li> </ul> </li> </ul>
AI Enterprise Management Service	<ul style="list-style-type: none"> <li>• Communicates with the Enterprise Manager</li> <li>• Updates Symphony Server software automatically when using Enterprise Manager to make configuration changes</li> <li>• Log file prefix:                             <ul style="list-style-type: none"> <li>• fs</li> </ul> </li> </ul>

Service	Function
AI InfoService	<ul style="list-style-type: none"> <li>• Hosts the Symphony Web service that receives all requests from the Symphony Client</li> <li>• Hosts the Web server for the server configuration interface</li> <li>• Retrieves timeline data from footage storage</li> <li>• Log file prefixes:                             <ul style="list-style-type: none"> <li>• <code>is</code> (information service)</li> <li>• <code>isac</code> (access control)</li> <li>• <code>isbk</code> (automatic backup)</li> </ul> </li> </ul>
AI Mobile Bridge	<ul style="list-style-type: none"> <li>• Facilitates communication between mobile devices and the Symphony Server</li> <li>• Facilitates communication between Thin Client devices and the Symphony Server</li> <li>• Log file prefix:                             <ul style="list-style-type: none"> <li>• <code>mo</code></li> </ul> </li> </ul>
AI NetSendHist	<ul style="list-style-type: none"> <li>• Retrieves historical video from the footage storage</li> <li>• Streams video</li> <li>• Creates historical images</li> <li>• Log file prefix:                             <ul style="list-style-type: none"> <li>• <code>hs</code></li> </ul> </li> </ul>
AI OPCServer	<ul style="list-style-type: none"> <li>• Communicates with the OPC Server</li> <li>• Optional service/Manual installation</li> <li>• Log file prefix:                             <ul style="list-style-type: none"> <li>• <code>op</code></li> </ul> </li> </ul>
AI Scheduler	<ul style="list-style-type: none"> <li>• Polls hardware alarm inputs</li> <li>• Generates alarms</li> <li>• Generates reports</li> <li>• Removes expired video files</li> <li>• Retrieves search results (video and XML) from the NAS</li> <li>• Log file prefixes:                             <ul style="list-style-type: none"> <li>• <code>sc</code> (scheduler)</li> <li>• <code>scac</code> (actions)</li> <li>• <code>scax</code> (access)</li> <li>• <code>sccl</code> (cleaner)</li> <li>• <code>sccp</code> (CPU/memory)</li> <li>• <code>scis</code> (multicaster)</li> <li>• <code>scpm</code> (PTZ)</li> <li>• <code>scse</code> (searches)</li> </ul> </li> </ul>
AI SNMP Registry	<ul style="list-style-type: none"> <li>• Registers sub-agents</li> </ul>

Service	Function
AI Tracker	<ul style="list-style-type: none"> <li>Analyzes video</li> <li>Saves video to storage</li> <li>Log file prefix:                             <ul style="list-style-type: none"> <li>cs</li> </ul> </li> </ul> <p>The Symphony 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.</p>
AI Watchdog	<ul style="list-style-type: none"> <li>Monitors and starts Symphony services</li> <li>Log file prefixes:                             <ul style="list-style-type: none"> <li>hm (health monitoring)</li> <li>nu (health monitor)</li> </ul> </li> </ul>

## Devices

Symphony supports cameras, digital input/output devices, and access control devices.

You can configure devices on the Devices tab in the server configuration interface. The Devices tab includes the Cameras, Templates, Hardware, Access Devices, Device Tree, and Carousels tabs.

## Cameras

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

Symphony supports the following standards:

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

Symphony supports the most recent official firmware for cameras, as provided by camera manufacturers.

## Multicasting

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

Multicasting can reduce the load on both the Symphony Server and camera when a large number of Symphony Client instances need to display video from a camera. To use multicasting with Symphony, 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:

- Configure multicasting on the network switch.
- Configure multicasting on the camera.
- In the Symphony server configuration interface, add the camera and select Multicast as the transport for the camera.
- In the Symphony Client, set the camera connection mode to Connect directly, if the camera supports it.

Related tasks

[Add a camera automatically](#) on page 12

[Add a camera manually](#) on page 12

Related reference

[Video settings](#) on page 126

## Search for a camera

You can use filters in the server configuration interface to search for specific cameras.

You can filter the camera list using the following filters:

- camera ID (ID)
  - camera name (Name)
  - Symphony 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)
  - group to which the camera belongs (Group)
  - video analytic active on the camera (Add-on)
1. In the server configuration interface, click **Devices > Cameras**.
  2. Define the filter criteria.
  3. Click **Apply filter**.

## Add a camera manually

You can manually add cameras to Symphony 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**.

Related concepts

[Multicasting](#) on page 11

Related tasks

[Add a camera automatically](#) on page 12

Related reference

[Video settings](#) on page 126

## Add a camera automatically

Symphony 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**.

Related concepts

[Multicasting](#) on page 11

Related tasks

[Add a camera manually](#) on page 12

Related reference

[Video settings](#) on page 126

## Add a mobile camera

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



**Note:** Symphony video analytics do not support mobile cameras.

12. In the **Server** field, select the Symphony Server for the mobile camera.
13. Click **Add 1 Selected Camera**.
14. Configure the settings for the mobile camera.



**Note:** The resolution on the mobile device must match the resolution set in the server configuration interface to transmit video.

15. Click **Save**.

## Import cameras

You can import cameras from a CSV file.

You can create a CSV file of cameras by either exporting a list of 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**.

## Create a blank import file

You can create a blank `CSV` file to use for importing cameras to a Symphony 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**.

Symphony saves a file named `import.csv` to your download location.

## Export cameras

You can export the camera list from a Symphony 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 Symphony Server.

## Set a camera password

You can set a new password that Symphony 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 home page.

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.

## Edit a camera

You can modify camera settings in the server configuration interface.

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 **ID/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. Click **Save**.

### Related tasks

[Add an analytics stream](#) on page 15

[Configure a privacy mask](#) on page 16

[Configure video storage for a camera](#) on page 15

[Add a camera to a device group](#) on page 17

## Move a camera

You can move a camera to a different Symphony 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**.

## Add a stream

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

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 Symphony.
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 Symphony considers to be key frames.
10. In the **Recording Mode** list, select when Symphony records video from the stream.
11. In the **Schedule** list, select when the recording mode is active for the stream.
12. Click **Save**.

## Add an analytics stream

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

To add an analytics stream, you must configure a video analytic for the camera.

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

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 Symphony records video from the stream.
5. In the **Schedule** list, select when the recording mode is active for the stream.
6. Click **Save**.

## Configure video storage for a camera

You can set the video storage setting for individual cameras.

The camera setting takes precedence over the video storage settings for individual Symphony Server instances and the server farm.

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

3. To set the storage path for video from the camera, perform one of the following tasks in the **Storage Paths** section:
  - To use the storage path that the Symphony Server uses for video, select **Use storage paths set by server**.
  - To use a custom storage path, select **Use specific paths for this camera** and type the storage path.
4. To set the video retention policy for the camera, perform one of the following tasks in the **Video Storage** section:
  - To use the video retention policy that the Symphony Server uses for video, select **Use storage limit set by server**.
  - To use a video retention policy, select **Limit the number of days video is stored** and set the number of days to retain video.
5. To use a custom video retention policy for video associated with alarms, perform the following tasks:
  - a) Select **Protect Alarm Recordings**.
  - b) In the **Days** field, set the time (in days) for which the Symphony Server retains video associated with alarms.
  - c) In the **Pre Alarm** field, set the time (in seconds) before the alarm that the Symphony Server includes in the alarm video.
  - d) In the **Post Alarm** field, set the time (in seconds) after the alarm that the Symphony Server includes in the alarm video.
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 Symphony 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.

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) Symphony 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 Symphony applies the privacy mask.  
This setting only applies to dynamic privacy masks.
  - d) On the **Blur Amount** slider, select to what degree Symphony 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 **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**.

## 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 Symphony Client.

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**.

Related tasks

[Create a device group](#) on page 24

## Configure digital input and output

You can configure how digital inputs and outputs appear in the 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 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 client interface when clicking on the input or output activates it.
  - d) In the **Deactivate** field, type the text that appears in the 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**.

## 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.

## Template settings

### General

Setting	Description
Failover enabled	Select and specify whether failover is enabled or disabled.

Setting	Description
Support Direct Connect	Select whether the camera allows direct connections through a browser.
Enable Audio Input	Select whether the camera can record audio.
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 Symphony 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.
4. Configure the settings for the template.
5. Click **Save**.

## Hardware

Hardware can provide data Symphony can use data from digital input and output devices to trigger events.

Symphony supports the following manufacturers:

- Advantech ADAM
- Axis
- Phoenix Contact
- Gallagher
- JCI P2000
- Siemens SPC
- Software House

## Add a hardware device

You can add hardware devices to Symphony.

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.
4. In the **General** section, specify the settings for the hardware device.  
The settings are specific to the manufacturer.
5. Click **Save**.

## Integrations

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

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

## Symphony Access Control introduction

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

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

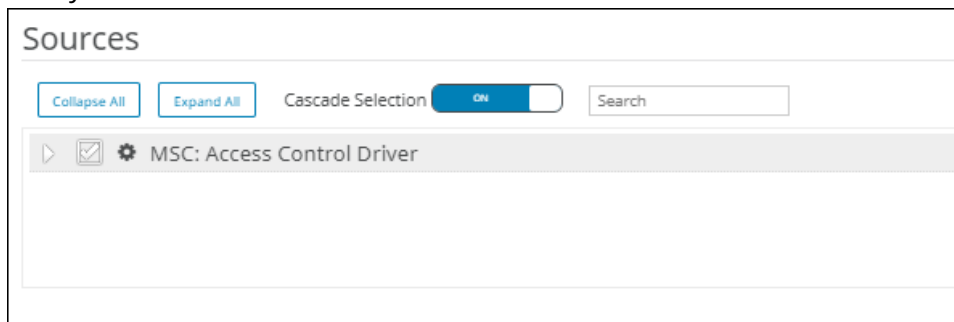
Related reference

[Symphony Access Control event settings](#) on page 47

## Connect to Symphony Access Control

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

1. In the Symphony 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 Symphony Access Control.  
This name will appear in the device list in the Symphony Server configuration interface and the device tree in the Symphony Client interface.
5. In the **Database Server** field, type the name of the computer that hosts the Symphony Access Control database.
6. In the **Database Name** field, type the name of the Symphony Access Control database.
7. In the **Username** field, type the username that the Symphony Server uses to access the Symphony Access Control database.
8. In the **Password** field, type the password that the Symphony Server uses to access the Symphony Access Control database.
9. Click **Connect to Device**.
10. In the **Sources** list, select the nodes that you want to add to the Symphony 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.



11. In the **Groups** list, select the device tree folder in which the Symphony Access Control appears.
12. Click **Save**.

### *Symphony Access Control settings*

#### General

Setting	Description
Name	Type a meaningful name for the 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.

Setting	Description
Database Server	Type the name of the computer that hosts the Symphony Access Control database.
Database Name	Type the name of the Symphony Access Control database.
Username	Type the username that the Symphony Server uses to access the Symphony Access Control database.
Password	Type the password that the Symphony Server uses to access the 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 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 Symphony Server. The Symphony Server supports the Senstar Network Manager 2.32 and later.

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

Related tasks

[Connect to Senstar Network Manager](#) on page 22

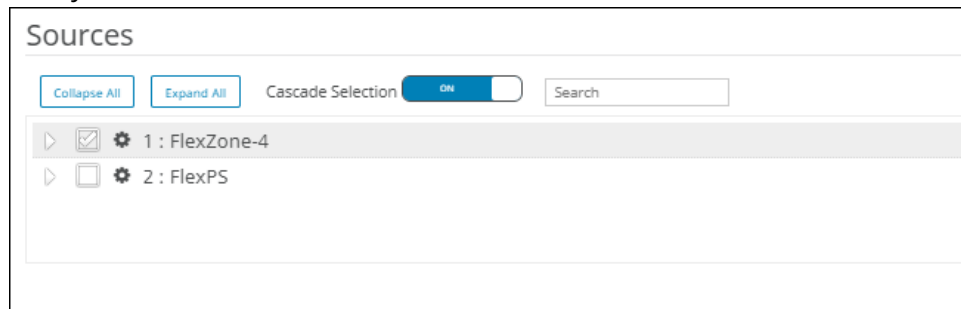
Related reference

[Senstar Network Manager event settings](#) on page 46

## Connect to Senstar Network Manager

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

1. In the Symphony 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 Symphony Server configuration interface and the device tree in the Symphony Client interface.
5. In the **IP Address** field, type the IP address of the Senstar Network Manager.
6. In the **Secondary IP Address** field, type the IP address of a secondary (redundant) Senstar Network Manager.
7. In the **Unit ID** field, type the ID of the Senstar Network Manager.
8. Click **Connect to Device**.
9. In the **Sources** list, select the nodes that you want to add to the Symphony 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.



10. In the **Groups** list, select the device tree folder in which the Senstar Network Manager appears.
11. 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.
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.

## Access control devices

Symphony can use data from access control devices to trigger events.

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

Symphony 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 Symphony.

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 Xnet for the manufacturer of the access control device.

1. In the server configuration interface, click **Devices > Access Devices**.
2. Click **Add Access Device**.
3. In the **Manufacturer** list, select the manufacturer of the access control system.
4. In the **Server** list, select the Symphony Server to which you want to add the access control device.
5. In the **IP Address** field, type the IP address of the access control system.
6. In the **Username** and **Password** fields, type the credentials for the access control system.
7. In the **Sources** list, select the devices in the access control system that can trigger events in Symphony.
8. Click **Save**.

## Device tree

The device tree organizes and displays devices in the client interface.

You can organize the devices in groups. In the server configuration interface, you can create, copy, edit, and delete groups. Changes that you make in the server configuration interface appear immediately in the 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.
3. Type a name for the group and press Enter.
4. Drag devices into the group.
5. Click **Save**.

Related tasks

[Add a camera to a device group](#) on page 17

## 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**.

## Carousels

Carousels are configurations for video panels in the 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 client interface displays video before moving to the next camera. The device tree in the client interface lists all available carousels. You can open a carousel in any video panel.

## 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 in Symphony 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 use Symphony.

### Add a user

You can add a user to allow someone to use Symphony.

1. In the server configuration interface, click **Security > Users**.
2. Click **Add**.
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**.

Related concepts

[Security authentication](#) on page 40

Related tasks

[Set the security profile permissions](#) on page 30

## 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.
4. Click **Save**.

## 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 Symphony Client. You can use this feature to ensure that two people are present when a user performs an operation in the 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**.

Related tasks

[Add a group](#) on page 28

[Add a user](#) on page 26

[Add a user to a group](#) on page 27

## Enable supervisor impersonation

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

1. Open the `acc.ini` file at `%appdata%\Senstar7`.

2. In the [Main] section, add the following text:

```
ShowTwoManRule=True
```

3. Save and close the `acc.ini` file.

The **Supervisor Logon** option is visible on the login page for the Symphony Client.

## Impersonate a supervisor

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

1. In the 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 Symphony 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 Symphony Server and Symphony Client.

Groups can contain users that you create and maintain in Symphony 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.

Related tasks

[Set the security profile permissions](#) on page 30

## 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**.

## 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 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 Symphony.

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 that you set for that security profile.

For example, you can create a default security profile and an emergency security profile. For normal operation, the default security profile is active and the permissions assigned to the users or user groups are also active. In the case of an emergency, you activate the emergency security profile and the permissions that you define for the users and user groups within the profile become active.

## Add a security profile

You can copy an existing security profile to add another security profile to Symphony.

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**.

## 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.

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 Symphony as long as the security profile is not active.

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

## Set the security profile permissions

You can set the security profile permissions for a user or group. When you activate the security profile, Symphony 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.

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.
5. In the permission list, set the permissions.
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 client interface.
Configure Maps	This permission allows a user to configure maps in the 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 client interface.
Export Video	This permission allows a user to export video from the client interface.
Get Logs	This permission allows a user to view and download logs in the client interface.
Manage Bookmarks	This permission allows a user to create and edit bookmarks in the client interface.
Manage Services	This permission allows a user to edit service settings in the server configuration interface.

Permission	Description
Play Sounds	This permission allows a user to play audio in the 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 server configuration interface.
Manage Alarms	This permission allows a user edit and delete alarms in the server configuration interface.
Mark Alarms	This permission allows a user to mark alarms as an alarm, false alarm, or real actionable in the client interface.
View Alarms	This permission allows a user to view alarms in the 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 client interface.

Permission	Description
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 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 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 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 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 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 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 Symphony 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 Symphony 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 Symphony client interface.

## Messenger

Permission	Description
Modify Pre-written Messages	This permission allows a user to edit the canned messages in the messenger in the Symphony client interface.

Permission	Description
Send Messages	This permission allows a user to send messages using the messenger in the Symphony client interface.

### Point of Sale

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

### Report

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

### Rule

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

### Search

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

### Security

Permission	Description
Activate Security Profile	This permission allows a user to activate security profiles in the Symphony server configuration interface.
Change Authentication Mode	This permission is not used.

Permission	Description
Edit Security	This permission allows a user to edit security settings in the Symphony server configuration interface.
Manage Security Profiles	This permission allows a user to add, edit, and delete security profiles in the Symphony server configuration interface.

### Subscription

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

### UI

Permission	Description
Change Carousels	This permission allows a user to edit camera carousels in the Symphony server configuration interface.
Lock UI	This permission allows a user to lock the Symphony client interface.
Manage Shared Views	This permission allows a user to edit and save shared views in the Symphony client interface.
View Carousels	This permission allows a user to view camera carousels in the Symphony client interface.

### User

Permission	Description
Add Users	This permission allows a user to create users in the Symphony server configuration interface.
Multiple Logins	This permission allows a user to log in to multiple Symphony client interfaces and server configuration interfaces concurrently.

### Video Wall

Permission	Description
Change Video Wall Client	This permission allows a user to configure video wall clients in the Symphony client interface.

Permission	Description
Control Video Walls	This permission allows a user to remotely control video wall clients in the Symphony client interface.
Create Video Walls	This permission allows a user to create video walls in the Symphony 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.
Configure Analytics	This permission allows a user to configure analytics for a device.
Delete	This permission allows a user to remove a device from Symphony.
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.

Permission	Description
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 client interface.
Trigger Manual Alarm	This permission allows a user to add an alarm to a camera timeline in the client interface.

## Audio

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

## LPR

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

## PTZ

Permission	Description
Calibrate PTZ Camera	This permission allows a user to calibrate a PTZ camera in the client interface.
Control PTZ	This permission allows a user to pan and tilt a PTZ camera using the client interface.
Control zoom via clients	This permission allows a user to zoom a PTZ camera using the client interface.
PTZ Presets	This permission allows a user to move a PTZ camera to a preset position using the client interface.

## Search

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

## Video

Permission	Description
Manage Recording	This permission allows a user to manage recordings.
Video 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 has been marked as private.
View Restricted Historical Video	This permission allows a user to view video that has been marked as restricted.

## User permissions

### General

Permission	Description
Terminate user session	This permission allows a user to end the session for another user.
View Group	This permission allows a user to view user groups.
View User	This permission allows a user to view users.

### Configuration

Permission	Description
Add Members	This permission allows a user to add users to user groups.
Delete Group	This permission allows a user to delete user groups.
Delete User	This permission allows a user to remove users from Symphony.
Edit Group Membership	This permission allows a user to modify the user groups to which user groups belong.
Edit Group Properties	This permission allows a user to modify the name, description, and Active Directory association of user groups.

Permission	Description
Edit Group Security	This permission allows a user to modify the security profiles of user groups.
Edit Membership	This permission allows a user to modify the users in user groups.
Edit Security	This permission allows a user to modify the security profiles of users.
Edit User Properties	This permission allows a user to modify the properties of users (phone number, email, description, etc.).
Remove Members	This permission allows a user to remove users from user groups.

## 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 Symphony.
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.

Permission	Description
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 Symphony server configuration interface.

### Configuration

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

## Shared view permissions

### General

Permission	Description
View Shared View	This permission allows a user to view shared views in the Symphony server configuration interface.

## Logins

The Logins page displays active and historical sessions for the Symphony Server.

### Stop an active session

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.

## Active Directory authentication

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

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

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

### Associate a group

If you use Active Directory authentication, you must associate groups that you create in 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**.
4. In the **Search For** box, type a group name and click **Search**.
5. Click the group and click **OK**.

## Security authentication

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

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

Related tasks

[Add a user](#) on page 26

## Watermarking

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

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

Related tasks

[Enable watermark verification](#) on page 154

[Enable watermarking](#) on page 41

## Enable watermarking

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

1. In the 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
```

4. Click **OK**.
5. Restart the Symphony services.

Related concepts

[Watermarking](#) on page 40

Related tasks

[Enable watermark verification](#) on page 154

## Rules

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

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 event triggers a rule. Examples include events from video analytics, camera inputs, and access devices.

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

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 Symphony to perform the actions defined in the rule's action set.

## Create a rule

You can create a rule to trigger actions in Symphony.

1. In the Symphony 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. Add an existing action set to the rule or create a new action set to add to the rule.

8. Add and existing schedule to the rule or create a new schedule to add to the rule.
9. Click **Save**.

Related tasks

[Create an event](#) on page 42

[Create an action set](#) on page 54

[Create a schedule](#) on page 61

## 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 from Symphony.

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

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

## Events

Events define the condition that must exist for a rule to trigger an alarm in Symphony.

### Create an event

You can create an event that triggers a rule in Symphony.

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

1. In the Symphony server configuration interface, click **Rules > Events**.
2. Click **New Event**.
3. Type a name for the event.
4. To add a device, perform the following tasks:
  - a) Click **Add Devices**.
  - b) Select the device.
  - c) Click **OK**.
5. Perform one of the following 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.
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 Symphony.

1. In the Symphony 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 Automatic License Plate Recognition 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 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 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 Crowd Detection 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.

Related reference

[Crowd Detection settings](#) on page 85

## Face Recognition event settings

Select video engine from those running on camera

Face Recognition ▼

Match Threshold  ▲▼

Max Spoof Score  ▲▼

Alarm type

Alarm on all real faces

Alarm only on real faces not in the list(s)

Alarm only on real faces in the list(s)

Alarm only on spoofing attacks

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 Left and Removed Item 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.
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.
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 Outdoor People and Vehicle Tracking 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 TCP Listener 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 Symphony Server.

Setting	Description
Activated	Select to trigger a rule on the Symphony Server when an output connected to the Senstar Network Manager is activated.
Deactivated	Select to trigger a rule on the Symphony Server when an output connected to the Senstar Network Manager is deactivated.
Alarm	Select to trigger a rule on the Symphony Server when an input connected to the Senstar Network Manager enters an alarm state.
Alarm Secure	Select to trigger a rule on the Symphony Server when an input connected to the Senstar Network Manager exits an alarm state.
Communication Fail	Select to trigger a rule on the Symphony Server when device connected to the Senstar Network Manager enters a communication failure state.
Communication Fail Secure	Select to trigger a rule on the Symphony Server when a device connected to the Senstar Network Manager exits a communication failure state.
Communication Fault	Select to trigger a rule on the Symphony 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 Symphony Server when a device connected to the Senstar Network Manager exits a communication fault state.
Diagnostic Warning	Select to trigger a rule on the Symphony 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 Symphony Server when a device connected to the Senstar Network Manager exits a diagnostic warning secure state.

Setting	Description
Diagnostic Fatal	Select to trigger a rule on the Symphony 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 Symphony Server when a device connected to the Senstar Network Manager exits a fatal diagnostic state.
Enclosure Tamper	Select to trigger a rule on the Symphony 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 Symphony Server when a device connected to the Senstar Network Manager exits an enclosure-tampered state.
Tamper	Select to trigger a rule on the Symphony Server when an input connected to the Senstar Network Manager enters a tampered state.
Tamper Secure	Select to trigger a rule on the Symphony Server when an input connected to the Senstar Network Manager exits a tampered state.
Trouble	Select to trigger a rule on the Symphony Server when an input connected to the Senstar Network Manager enters a trouble state.
Trouble Secure	Select to trigger a rule on the Symphony Server when an input connected to the Senstar Network Manager exits a trouble state.

Related concepts

[Senstar Network Manager](#) on page 21

## Symphony Access Control event settings

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

Some events are listed twice in the Symphony 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 Symphony Server when a door contact connected to the Symphony Access Control detects a door forced open.
Door Held Open	Select to trigger a rule on the Symphony Server when a door contact connected to the Symphony Access Control detects a door held open.

Setting	Description
Door is Closed	Select to trigger a rule on the Symphony Server when a door contact connected to the Symphony Access Control detects that the door is closed.
Door is Opened	Select to trigger a rule on the Symphony Server when a door contact connected to the Symphony Access Control detects that the door is open.
Request To Exit	Select to trigger a rule on the Symphony Server when a door contact or request to exit device connected to the Symphony Access Control detects a request to exit.
Request To Exit (Door Used)	Select to trigger a rule on the Symphony Server when a request to exit device connected to the 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 Symphony Server when a request to exit device connected to the Symphony Access Control detects a request to exit with the door not used.
Door is Locked	Select to trigger a rule on the Symphony Server when a door strike device connected to the Symphony Access Control detects that the door is locked.
Door is Unlocked	Select to trigger a rule on the Symphony Server when a door strike device connected to the Symphony Access Control detects that the door is unlocked.
Deadbolt Disengaged	Select to trigger a rule on the Symphony Server when a door strike device connected to the Symphony Access Control detects that the deadbolt lock is disengaged.
Deadbolt Engaged	Select to trigger a rule on the Symphony Server when a door strike device connected to the Symphony Access Control detects that the deadbolt lock is engaged.
Door Schedule is Disabled	Select to trigger a rule on the Symphony Server when a door strike device connected to the Symphony Access Control detects that the door schedule is disabled.
Door Schedule is Enabled	Select to trigger a rule on the Symphony Server when a door strike device connected to the Symphony Access Control detects that the door schedule is enabled.
Door is Momentarily Unlocked	Select to trigger a rule on the Symphony Server when a door strike device connected to the Symphony Access Control detects that the door is momentarily unlocked.
Double Locked	Select to trigger a rule on the Symphony Server when a door strike device connected to the 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	<p>Select to trigger a rule on the Symphony Server when a door strike device connected to the Symphony Access Control detects that a command to lock the door and set the reader mode to disabled is issued.</p> <p>This event applies to Assa Abloy wireless locks only.</p>
Locked Open	<p>Select to trigger a rule on the Symphony Server when a door strike device connected to the Symphony Access Control detects that a command to restore the door and reader to normal operation after a Locked Down event.</p> <p>This event applies to Assa Abloy wireless locks only.</p>
Control Point Deactivated	<p>Select to trigger a rule on the Symphony Server when a door sounder device connected to the Symphony Access Control detects that a control point is deactivated.</p>
Control Point Activated	<p>Select to trigger a rule on the Symphony Server when a door sounder device connected to the Symphony Access Control detects that a control point is activated.</p>
Control Point Pulse	<p>Select to trigger a rule on the Symphony Server when a control point device connected to the Symphony Access Control detects that the control point receives a command to momentarily activate a relay or output.</p>
Reader Mode: Disabled	<p>Select to trigger a rule on the Symphony Server when a reader device connected to the Symphony Access Control is disabled.</p>
Reader Mode: Unlocked	<p>Select to trigger a rule on the Symphony Server when a reader device connected to the Symphony Access Control is unlocked.</p>
Reader Mode: Locked (REX Only)	<p>Select to trigger a rule on the Symphony Server when a reader device connected to the Symphony Access Control is locked and can only be unlocked with a request to exit (REX).</p>
Reader Mode: Facility Code Only	<p>Select to trigger a rule on the Symphony Server when a reader device connected to the Symphony Access Control can only be unlocked when the facility code on a card matches the facility code in the system configuration.</p>
Reader Mode: Card Only	<p>Select to trigger a rule on the Symphony Server when a reader device connected to the Symphony Access Control is set to accept cards only.</p>
Reader Mode: PIN Only	<p>Select to trigger a rule on the Symphony Server when a reader device connected to the Symphony Access Control is set to accept PINs only.</p>
Reader Mode: Card and PIN	<p>Select to trigger a rule on the Symphony Server when a reader device connected to the Symphony Access Control is set to accept cards with PINs only.</p>

Setting	Description
Reader Mode: Card or PIN	Select to trigger a rule on the Symphony Server when a reader device connected to the Symphony Access Control is set to accept cards or PINs.
User Command Requested	Select to trigger a rule on the Symphony Server when a reader device connected to the Symphony Access Control detects that the terminal keypad requests a user code.
Reader Mode: Fingerprint Only	Select to trigger a rule on the Symphony Server when a reader device connected to the Symphony Access Control is set to accept fingerprints only.
Reader Mode: Card and Fingerprint	Select to trigger a rule on the Symphony Server when a reader device connected to the Symphony Access Control is set to accept cards with fingerprints only.
Reader Mode: Card or Fingerprint	Select to trigger a rule on the Symphony Server when a reader device connected to the Symphony Access Control is set to accept cards or fingerprints.
Reader Mode: Office First	Select to trigger a rule on the Symphony Server when a reader device connected to the Symphony Access Control is set to respond to the first person in situation.
Reader Mode: Blocked	Select to trigger a rule on the Symphony Server when a reader device connected to the 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 Symphony Server when a reader device connected to the Symphony Access Control enters the emergency locked state.
Reader Mode: Emergency Unlock	Select to trigger a rule on the Symphony Server when a reader device connected to the Symphony Access Control exits the emergency locked state.
Access Granted	Select to trigger a rule on the Symphony Server when a reader device connected to the Symphony Access Control grants access.
Access Denied: Level	Select to trigger a rule on the Symphony Server when a reader device connected to the Symphony Access Control denies access to a card because of an insufficient access level.
Access Denied: Time	Select to trigger a rule on the Symphony Server when a reader device connected to the 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 Symphony Server when a reader device connected to the Symphony Access Control denies access and locks the door.

Setting	Description
Access Denied: Card	Select to trigger a rule on the Symphony Server when a reader device connected to the Symphony Access Control denies access to a card.
Access Denied: Facility	Select to trigger a rule on the Symphony Server when a reader device connected to the Symphony Access Control denies access to a card because of an incorrect facility code.
Access Denied: Passback	Select to trigger a rule on the Symphony Server when a reader device connected to the Symphony Access Control denies access because of a card passback.
Access Denied: Issue Code	Select to trigger a rule on the Symphony Server when a reader device connected to the 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 Symphony Server when a reader device connected to the Symphony Access Control denies access because of a invalid card format.
Card Information Event	Select to trigger a rule on the Symphony Server when a reader device connected to the 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 Symphony Server when a reader device connected to the Symphony Access Control grants access and unlocks the door.
Access Granted: Door Not Used	Select to trigger a rule on the Symphony Server when a reader device connected to the Symphony Access Control grants access but the door was not used.
Access Granted: Door Used	Select to trigger a rule on the Symphony Server when a reader device connected to the Symphony Access Control grants access and the door was used.
Access Denied: Deactivated Card	Select to trigger a rule on the Symphony Server when a reader device connected to the Symphony Access Control denies access because of a deactivated card.
Access Denied: Before Activation Date	Select to trigger a rule on the Symphony Server when a reader device connected to the Symphony Access Control denies access because the card is not yet active.

Setting	Description
Access Denied: After Expiration Date	Select to trigger a rule on the Symphony Server when a reader device connected to the Symphony Access Control denies access because the card is expired.
Access Denied: Invalid PIN	Select to trigger a rule on the Symphony Server when a reader device connected to the Symphony Access Control denies access because the PIN is invalid.
Access Denied: 2nd Card not Presented	Select to trigger a rule on the Symphony Server when a reader device connected to the 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 Symphony Server when a reader device connected to the 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 Symphony Server when a reader device connected to the Symphony Access Control denies access because the area is not enabled.
Access Denied: Use Limit	Select to trigger a rule on the Symphony Server when a reader device connected to the 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 Symphony Server when a reader device connected to the Symphony Access Control denies access because duress code was used.
Access Denied: Duress (Door Used)	Select to trigger a rule on the Symphony Server when a reader device connected to the Symphony Access Control denies access because a duress code was used and the door was used.
Access Denied: Duress (Door Not Used)	Select to trigger a rule on the Symphony Server when a reader device connected to the 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 Symphony Server when a reader device connected to the 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 Symphony Server when a reader device connected to the 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 Symphony Server when a reader device connected to the Symphony Access Control grants access because the verification was confirmed.

Setting	Description
Access Denied: No Biometric Record	Select to trigger a rule on the Symphony Server when a reader device connected to the 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 Symphony Server when a reader device connected to the 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 Symphony Server when a reader device connected to the Symphony Access Control detects that the area is armed and is ready to alarm.
Intrusion Area: Disarmed	Select to trigger a rule on the Symphony Server when a reader device connected to the 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 Symphony Server when a reader device connected to the Symphony Access Control denies a disarm attempt because of insufficient permission.
Access Granted: Office First Door Unlocked	Select to trigger a rule on the Symphony Server when a reader device connected to the 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 Symphony Server when a reader device connected to the 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 Symphony Server when a reader device connected to the 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 Symphony Server when a reader device connected to the 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 Symphony Server when a reader device connected to the Symphony Access Control grants access on a card passback and the door was used.

Related concepts

[Symphony Access Control introduction](#) on page 19

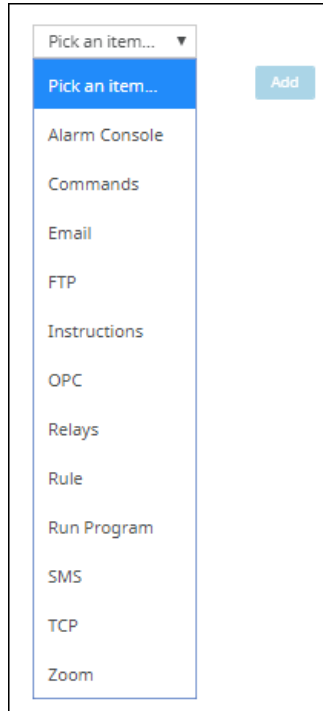
## Action sets

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

## Create an action set

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

1. In the Symphony server configuration interface, click **Rules > Action Sets**.
2. Click **New Action Set**.
3. Type a name for the action set.
4. In the **Alarm** list, select the cameras to view when an alarm occurs.
5. In the **Record** list, select the cameras that record footage when an alarm occurs.
6. To add other actions, perform the following tasks:
  - a) In the **Pick an item** list, select an action.



- b) Click **Add**.
  - c) Configure the settings for the action.
7. Click **Save**.

## Actions

### Commands

The Symphony Server can send commands to the Senstar Network Manager and the Symphony Access Control.

Setting	Description
Activate	Select to activate the output device.  This command works for both Senstar Network Manager devices and Symphony Access Control devices.

Setting	Description
Deactivate	Select to deactivate the output device. This command works for both Senstar Network Manager devices and Symphony Access Control devices.
Arm	Select to arm the input device. This command works for Symphony Access Control devices.
Disarm	Select to disarm the input device. This command works for Symphony Access Control devices.
Disable	Select to disable the reader device. This command works for Symphony Access Control devices.
Unlock	Select to unlock the reader device. This command works for Symphony Access Control devices.
Lock	Select to lock the reader device. This command works for Symphony Access Control devices.
Change reader mode to Facility Code	Select to change the reader device so that only the facility code can unlock the device. This command works for Symphony Access Control devices.
Change reader mode to Card Only	Select to change the reader device so that only cards can unlock the device. This command works for Symphony Access Control devices.
Change reader mode to PIN Only	Select to change the reader device so that only PINs can unlock the device. This command works for Symphony Access Control devices.
Change reader mode to Card and PIN	Select to change the reader device so that only both cards and PINs together can unlock the device. This command works for Symphony Access Control devices.
Change reader mode to Card or PIN	Select to change the reader device so that only cards or PINs can unlock the device. This command works for Symphony Access Control devices.
Mask Door Forced Open alarm	Select to change the door contact device to ignore door forced open alarms. This command works for Symphony Access Control devices.
Unmask Door Forced Open alarm	Select to change the door contact device to register door forced open alarms. This command works for Symphony Access Control devices.

Setting	Description
Mask Door Held Open alarm	Select to change the door contact device to ignore door held open alarms. This command works for Symphony Access Control devices.
Unmask Door Held Open alarm	Select to change the door contact device to register door held open alarms. This command works for Symphony Access Control devices.
Momentarily Unlock	Select to unlock the door strike device for a brief time. The time is configured on the door strike device. This command works for Symphony Access Control devices.

## Email

The Symphony Server can send email messages when an alarm occurs.

Setting	Description
Email Address	Type the email address to which the Symphony Server sends the email. You can type multiple email addresses by pressing Enter after typing an email address.
Only email if not acknowledged in	Select to only send an email if an the alarm remains unacknowledged for a specified time.
Minutes	Specify the number of minutes that the alarm must remain unacknowledged before the Symphony Server sends the email.

## FTP

The Symphony Server can capture images from cameras and post those images to an FTP server when an alarm occurs.

Setting	Description
FTP camera images on alarm	Select the cameras from which the Symphony Server collects images to post to the FTP server.
Server name	Type the IP address of the FTP server.
Port	Select the port that the FTP server uses.
Username	Type the username for accessing the FTP server.
Password	Type the password for accessing the FTP server.
Remote directory	Type the directory to which the Symphony Server posts the image files.
Transfer Multiple pictures	Select to make the Symphony Server post multiple images to the FTP server.

Setting	Description
Pre-alarm pictures	Select the number of images prior to the alarm that the Symphony Server posts to the FTP server.
Post-alarm pictures	Select the number of images after the alarm that the Symphony Server posts to the FTP server.
Interval between pictures	Select the number of milliseconds between each picture.
Show all Decorations	Select to include all decorations in the images. If you clear this selection, you can select specific decorations to include in the images.
Boxes	Select to include tracking boxes in the images.
Decorations	Select to include the camera name and description in the images.
Date	Select to include the date in the images.
Time	Select to include the time in the images.
Paths	Select to include tracking paths in the images.
Resize the transferred file	Select a size to which the Symphony Server scales images before posting them to the FTP server.
Rename the transferred file according to this pattern	Select to rename the images using the pattern that you define in the text field.  For example, %YYYY %MM %DD instructs the Symphony Server to rename the image file to 2018_01_01.jpg.
Use UTC date and time	Select to use the UTC date and time when the Symphony Server renames image files.

### Instructions

The Symphony Server can display a message or file to users in the Symphony Client interface when an alarm occurs. If you add a file to an alarm, you can zoom in or out on the file using the Ctrl key and the mouse scroll wheel.

Setting	Description
Display	Select whether to display the instructions for the alarm in text or in a file.
Enter what should be done in case of an alarm below	When adding instructions in text, type the text that the Symphony Client displays.

Setting	Description
Drag file here	<p>When adding instructions in a file, drag and drop the file that the Symphony Client displays in the pane. The Symphony Client supports the following file formats:</p> <ul style="list-style-type: none"> <li>• .doc</li> <li>• .docx</li> <li>• .epub</li> <li>• .htm</li> <li>• .html</li> <li>• .mht</li> <li>• .odt</li> <li>• .pdf</li> <li>• .rtf</li> <li>• .txt</li> </ul>

## OPC

Setting	Description
Alarm type	Specify the value that the Symphony Server sends to the item.
Stay for	Set how long that the Symphony Server sends the alarm type value.

## Relays

The Symphony Server can trigger a relay when an alarm occurs.

Setting	Description
Use the following hardware device	Select the relay to control.
Turn Relay On	Select to turn the relay on.
Turn Relay Off	Select to turn the relay off.
Toggle Relay	Select to change the state of the relay.
Relay #	Define the address on the relay board to control.
Restore state	Define when the relay remains in the state before resetting.

## Rule

Setting	Description
Enable rule	Select to enable a rule.
Disable rule	Select to disable a rule.

Setting	Description
Toggle rule	Select to toggle a rule.
Choose a rule	Select the rule.

## Run Program

The Symphony Server can run third-party applications when an alarm occurs.

Setting	Description
Working Directory	Specify the folder that contains the application or batch file. For example, <code>C:\Program Files\Senstar\Symphony\_bin</code> .
Executable Name	Specify the path of the application executable file (for applications) or the command prompt executable file (for batch files). For example, <code>C:\Windows\System32\cmd.exe</code> .
Arguments	Type <code>/C</code> and the batch file name. For example, <code>/C RecordToggle.bat</code> .

## SMS

The Symphony Server can send SMS messages when an alarm occurs. The modem that Symphony Server uses to send SMS messages must support protocol data unit (PDU) mode.

Setting	Description
COM Port	Specify the COM port that the Symphony Server uses to connect to the modem.
Baud Rate	Specify the baud rate for the connection to the modem.
Phone Numbers	Type the phone numbers to which the Symphony Server sends the SMS message. You can type multiple phone numbers by pressing Enter after typing a phone number.
Message	Type the message that the Symphony Server sends when the alarm occurs.

## TCP

The Symphony Server can send a TCP message when an alarm occurs.

Setting	Description
Address	Specify the IP address of the recipient of the TCP message.
Port	Specify the port that the recipient uses for TCP.
Message	Type the message that the Symphony Server sends.

## Zoom

The Symphony Server can send commands to PTZ cameras when an alarm occurs.

Setting	Description
Auto-tracking	Select to make the PTZ camera track the object that triggers the alarm.
Force a PTZ camera to a location	Select to force a PTZ camera to a specific camera.
Camera	Select the camera that move to the location.
Get the current location	Click to populate the Pan, Tilt, and Zoom fields with the current pan, tilt, and zoom from the camera.
Pan	Specify the pan for the camera.
Tilt	Specify the tilt for the camera.
Zoom	Specify the zoom for the camera.
Seconds to stay at location when auto-tracking is disabled	Specify how long the camera should stay at the location when auto-tracking is not active.
Minimum seconds between activations of this rule	Specify how much time must elapse before the Symphony Server can trigger this action when auto-tracking is active.

## Edit an action set

You can edit an action set to change what actions Symphony 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 Symphony.

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 Symphony server configuration interface, click **Rules > Action Sets**.
2. Select an action set.
3. Click **Delete**.
4. Click **Yes**.

## Schedules

Schedules determine when rules is active in Symphony.

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 Symphony.

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

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

## Licenses

License settings in Symphony 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 Symphony 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 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 licenses from Xnet, select .
  - 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

Settings in Symphony allow you to configure servers, general settings, email notifications, health monitoring, Enterprise Manager, updates, and backup and restore.

You access the settings on the Settings tab in the server configuration interface. The Settings tab includes the Servers, General Settings, Notifications, Cloud Services, Maintenance, and Backup & Restore tabs.

## Servers

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

## Configure video storage for a server

You can configure how a Symphony Server stores and maintains video footage.

You can configure where Symphony stores video footage, how much video footage Symphony stores, and under which conditions Symphony 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 Symphony 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**.  
Symphony attempts to save footage files to the first path in the list. If that path is not available, Symphony attempts to save footage files to the next path in the list.
  - d) To save footage files to all storage paths, select **Redundant**.
  - e) Select the path from which Symphony should read footage files in the **Force disk reads from**.
4. To specify a secondary (archive) storage path, complete the following tasks:
  - a) Select **Archive video to secondary storage path**.
  - b) Type the path to which Symphony should save footage files.  
You must type a secondary (archive) storage path for each of the primary storage paths.
  - c) In the **Days to store before archiving** field, set how many days must occur before Symphony 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.
5. 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.
6. To set the maximum number of days for which Symphony can retain footage files, select **Limit the number of days video is stored** and set the number of days.
7. To retain metadata after Symphony deletes footage files, select **Keep metadata longer** and set the number of days.
8. 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.
9. In the **Cameras** list, define any storage paths specific to cameras.  
By default, Symphony saves footage files from all cameras to the storage paths.
10. Click **Save**.

## Configure overload protection

You can configure a Symphony Server to move cameras to another server 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.
5. Set the CPU threshold (in percent).
6. Set the polling frequency (in seconds).
7. Set the maximum number of cameras to move to the new server.
8. Click **Save**.

## Server redundancy

Symphony supports server redundancy in server farms. If a Symphony Server stops responding, the camera and device processing moves to another Symphony Server.

A primary servers actively performs camera and device processing. When failover occurs, the primary server becomes a redundant server.

A redundant server does perform camera and device processing. There must be at least one redundant server available in the server farm at all times. When failover occurs, the redundant server becomes the primary server.

In addition, one server in the server farm is the master server. The master server performs the additional task of managing failover actions. If the master server is unavailable, Symphony designates another server as the master server.

Server redundancy works within redundancy groups.

## 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 an existing redundancy group, select **<New>**.
4. Click **Save**.

## Configure failover

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

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 Symphony to move cameras back to the primary server when it comes back online.

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

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 Symphony Server to a different Symphony Server in your server farm.

You can only move all cameras from one to 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. Select the server from which to move cameras.
3. Select the server to which to move the cameras.
4. Click **Swap Servers**

## General

The General Settings tab in the server configuration interface is the interface for configuring settings that apply to all of the Symphony Server instances in the server farm.

### Configure video storage for a server farm

You can set a global video storage setting for a Symphony Server farm.

The global setting takes effect when you do not configure video storage settings for individual Symphony Server instances.

1. In the server configuration interface, click **Settings > General Settings**.
2. In the **Video Storage** section, select **Limit the number of days video is stored**.
3. Set the maximum number of days to save video.
4. To keep video metadata after the video is deleted, select **Keep metadata longer**.
5. Set the maximum number of days to save video metadata.
6. Click **Save**.

### Configure SNMP

You can configure Symphony 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) Symphony updates the size of the footage.
5. Click **Save**.
6. Restart the Symphony services.
7. Configure the Windows SNMP Agent Service on the computer that hosts the Symphony Server.

### SNMP object identifiers

#### Server information

Object	Description
serverId	This object is the unique identifier of the Symphony Server.
serverName	This object is the name of the Symphony Server.

#### Version information

Object	Description
serverVersion	This object is the assembly version of the Symphony Server software.
webserviceVersion	This object is the version of the Symphony Web service protocol.
cameraMessageVersion	This object is the version of the Symphony camera message protocol.

Object	Description
<code>streamingVersion</code>	This object is the version of the Symphony streaming protocol.

### Client bandwidth

Object	Description
<code>connectedClientNumber</code>	This object is the number of Symphony Client instances that are connected to the Symphony Server.
<code>connectedClientIndex</code>	This object is the unique identifier of the Symphony Client.
<code>connectedClientIpAddress</code>	This object is the IP address of the Symphony Client.
<code>connectedClientUsername</code>	This object is the username that the Symphony Client uses to connect to the Symphony Server.
<code>connectedClientDuration</code>	This object is how long the Symphony Client has been connected to the Symphony Server.
<code>connectedClientDataReceived</code>	This object is how much data (in kilobytes) the Symphony Client has received from the Symphony Server.
<code>connectedClientCurrentBandwidth</code>	This object is the amount of data (in kilobytes per second) transmitted between the Symphony Client and the Symphony Server.

### Camera information

Object	Description
<code>cameraNumber</code>	This object is the number of cameras that are connected to the Symphony Server.
<code>cameraId</code>	This object is the unique identifier for the camera.
<code>cameraName</code>	This object is the name of the camera.
<code>footagePath</code>	This object is the storage path for footage from the camera.
<code>footageSize</code>	This object is the size (in bytes) of the footage at the storage path.

### Storage information

Object	Description
<code>storagePoolNumber</code>	This object is the number of storage pools that are connected to the Symphony Server.
<code>storagePath</code>	This object is the path of the storage pool.

Object	Description
storageCapacity	This object is the total capacity (in megabytes) of the storage pool.
storagePercentAvailable	This object is the available capacity (in megabytes) of the storage pool.
storageFootageSize	This object is the size (in megabytes) of the footage in the storage pool.
storageFootageFiles	This object is the number of footage files in the storage pool.

### Service information

Object	Description
infoServiceStatus	This object is the status of the AI InfoService service.
netSendHistStatus	This object is the status of the AI NetSendHist service.
schedulerStatus	This object is the status of the AI Scheduler service.
trackNumber	This object is the number of active AI Tracker services.
trackerId	This object is the unique identifier for the AI Tracker service.
trackerStatus	This object is the status of the AI Tracker service.

### Login monitor information

Object	Description
authorizedLoginNotif	This object is the notification sent when a login is successful. Trap
unauthorizedLoginNotif	This object is the notification sent when a login is unsuccessful. Trap
loginNotifyIpAddress	This object is the IP address of the Symphony Client.
loginNotifyUsername	This object is the username that the Symphony Client used to connect to the Symphony Server.
loginNotificationMessage	This object is the additional details about the login.

## Alarm monitor information

Object	Description
alarmNotif	This object is the notification sent when an alarm occurs. Trap
alarmNotifyCameraId	This object is the identifier of the camera that recorded the alarm.
alarmNotifyCameraName	This object is the name of the camera that recorded the alarm.
alarmNotifyUserId	This object is the identifier of the user who marked the alarm.
alarmNotifyUserName	This object is the name of the user who marked the alarm.
alarmNotifyMarkedDelay	This object is the time at which the alarm was marked.
alarmNotifyFalseAlarm	This object is whether the alarm is a false alarm.
alarmNotifyRuleId	This object is the identifier of the rule causing the alarm.
alarmNotifyRuleName	This object is the name of the rule causing the alarm.
alarmNotifyDBId	This object is the identifier of the alarm.
alarmNotifyComment	This object is the comment associated with that alarm.
alarmNotifyMSSinceChange	This object is the milliseconds between when the alarm occurred and when it was detected.

## Device Movement monitor information

Object	Description
devicesMovedNotif	This object is the notification sent when a device moves from one server to another server. Trap
sourceServerId	This object is the identifier of the server from which the device moved.
destinationServerId	This object is the identifier of the server to which the device moved.
numberDevicesMoved	This object is the number of devices that moved from the source server to the destination server.

## Health monitor information

Object	Description
healthMonitorFaultNotification	This object is the notification sent when the health monitor detects a fault. Trap
healthMonitorActionNotification	This object is the notification sent when the health monitor takes an action in response to a fault. Trap
healthMonitorName	This object is the name of the associated health monitor.
healthMonitorAction	This object is the action that the health monitor took in response to a fault.

## Configure mobile connections

You can configure Symphony to support connections with Symphony mobile applications on mobile devices.

The mobile connections functionality in Symphony replaces the Mobile Bridge standalone application. For more information on the Mobile Bridge standalone application, see the *Symphony Mobile Bridge Installation Guide*.

1. In the server configuration interface, click **Settings > General Settings**.
2. Navigate to the **Mobile Connections** section.
3. To select the SSL certificate, click **Change**, select the certificate, and click **OK**.
4. In the **Mobile Port** field, set the port that Symphony uses to listen for requests from mobile devices.
5. In the **Video Proxy Port** field, set the port that Symphony uses to stream video to and receive video from mobile devices.
6. To allow Symphony to send push notifications to iOS devices, select **Enable iOS Notifications**.
7. Click **Save**.

## General settings

### Video

Setting	Description
Time based video playback restriction applied at	This setting determines how long (in minutes) after video is recorded that a user can view the video in the Symphony Client.

### Video decorations

Setting	Description
Frame rate stats	This setting determines whether the frame rate (in frames per second) appears in video.

Setting	Description
Frame rate variance	This setting determines whether the frame rate variance decoration appears in the video. The frame rate variance decorations show how much the frame rate changes over the last 50 frames.
Overlay camera name on video	This setting determines whether the camera name appears in video.
Overlay camera ID on video	This setting determines whether the camera ID appears in video.
Overlay logo on video	This setting determines whether a custom logo appears in video.
Decoration Text Color	This setting determines the color of the text for decorations.
Background sensitive	This setting determines whether the text color for decorations automatically adjusts to the colors in the video to provide more contrast.
Decoration Text Background	This setting determines the color of the background for decoration text.
Transparency	This setting determines the transparency of the background for decoration text.

## Event log

Setting	Description
Enable Event Log	This setting determines whether Symphony logs events.
Never archive logs	This setting prevents Symphony from archiving event logs.
Archive logs weekly	This setting causes Symphony to archive event logs every week.
Event archive retention	This setting determines how long (in days) Symphony retains archived event logs.

## SNMP

Setting	Description
Enable SNMP	The setting determines whether SNMP is enabled.
Data polling rate	This setting determines how often (in seconds) the SNMP agent polls Symphony for data.
Footage size polling rate	This setting determines how often (in seconds) the SNMP agent polls Symphony for the size of video footage.

## Web Client

Setting	Description
Randomly redirect master server logins to other available servers in the farm	This setting determines if the master Symphony Server redirects users to other servers in the server farm. This provides load balancing for the Web Client.
Refresh rate	This setting determines how often the Web Client updates information from Symphony.
Use an ICE Server	This setting determines if you are using an ICE server with the Web Client.
Type	This setting determines what type of an ICE Server you are using, STUN or TURN.
URL	This setting is the URL of the ICE Server.
Username	This setting is the user name for the ICE Server.
Password	This setting is the password for the ICE Server.

## SMTP

Setting	Description
SMTP server	This setting is the URL of the SMTP server.
Use Secure Sockets Layer	This setting determines whether Symphony uses SSL for communication with the SMTP server.
Sender email account	This setting defines the email account that Symphony uses to send email.
SMTP server requires authentication	This setting determines whether the SMTP requires authentication.
Username	This setting is the user name that Symphony uses to authenticate with the SMTP server.
Password	This setting is the password that Symphony uses to authenticate with the SMTP server.
Send a test email to address	This setting allows you to test the SMTP settings. Type an email address and click Send Test to send a test email.

## User Connections

Setting	Description
Do not allow more than one concurrent connection per user	This setting determines if users can log in to more than one server configuration interface concurrently per server farm.

Setting	Description
Automatically log out inactive Server Configuration users	This setting determines if Symphony automatically logs users out of the server configuration interface after a period of inactivity.
Minutes of Inactivity	This setting determines the timeout period for the server configuration interface.

### Farm Location

Setting	Description
GPS Latitude	This is the latitudinal coordinate of the Symphony server farm.
GPS Longitude	This is the longitudinal coordinate of the Symphony server farm.

### Mobile Connections

Setting	Description
SSL Certificate	This setting displays the SSL certificate that Symphony uses to communicate with mobile devices.
Mobile Port	This setting determines the port that Symphony uses to communicate with mobile devices.
Video Proxy Port	This setting determines the port that Symphony uses for sending video to and retrieving video from mobile devices.
Enable iOS Notifications	This setting determines whether push notifications are enabled for iOS devices.

## Notifications

The Notifications tab in the server configuration interface is the interface for configuring event notifications from the server farm.

### Configure notifications

You can configure Symphony to send notifications when users perform specific action in the server configuration interface and client interface.

Before you begin:

- Configure SMTP for Symphony

These notifications are different from the notifications that events trigger.

1. In the server configuration interface, click **Settings > Notifications**.
2. For each event for which you want Symphony to send a notification, type an email address. To add multiple email addresses, separate each email address with a semi-colon (;).
3. Click **Save**.

## Cloud services

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

### Turn on health monitoring

If you purchased the Maintenance and Support option with your Symphony Server license, you can turn on health monitoring.

Health monitoring sends telemetry data from the Symphony Server to Xnet. You can log in to Xnet and view the status of all Symphony services.

1. In the server configuration interface, click **Settings > Cloud Services**.
2. Move the **Health Monitoring** toggle switch to **On**.

To turn off health monitoring, move the **Health Monitoring** toggle switch to **Off**.

### Manage Symphony with Enterprise Manager

You can manage your Symphony Server or server farm using Enterprise Manager.

**!** **Warning:** If you have created users or groups in Symphony, those users and groups are replaced with the users from Enterprise Manager when you add the Symphony Server to Enterprise Manager. This includes administrator users. We recommend that you back up your configuration settings or database before you manage your server or server farm with Enterprise Manager.

1. In the server configuration interface, click **Settings > Cloud Services**.
2. Move the **Enterprise Manager** toggle switch to **On**.
3. In the **Address** field, type the IP address of Enterprise Manager.
4. In the **Site Name** field, type a name for the site.  
Enterprise Manager uses this site name to identify the server or server farm.
5. In the **Organization Name** field, type your Enterprise Manager organization name.
6. In the **Passphrase** field, type your Enterprise Manager password.
7. Click **Save**.

## Maintenance

The Maintenance tab in the server configuration interface is the interface for configuring updates for the Symphony Client.

### Configure automatic server updates

The Symphony Server can perform automatic updates.

1. In the server configuration interface, click **Settings > Maintenance**.
2. In the **Server Updates** section, select **Enable automatic updates**.
3. Specify when to download and install the update.
4. Perform one of the following actions:
  - To update from a specific location, select **Update from the following location** and type the file path.
  - To update from the Internet, select **Update from product web site**.
5. Click **Save**.

## Check for server updates

In you have a standalone Symphony Server (single-server farm), you can manually check for software updates.

This feature is not available in multi-server farms.

1. In the server configuration interface, click **Settings > Maintenance**.
2. In the **Server Updates** section, click **Check for Updates**.
3. If there are updates and you want to apply the updates, click **Yes**. The Symphony Server starts downloading and installing updates.
4. Click **Close**.
5. Click **Close** again.
6. Wait 20 minutes and then log in to the server configuration interface.

## Configure client updates

You can configure when the Symphony Client applies updates.

1. In the server configuration interface, click **Settings > Maintenance**.
2. In the **Client Updates** section, select one of the following options:
  - To update the Symphony Client as soon as an update is available, select **Immediately**.
  - To update the Symphony Client at a specific time, select **During time frame** and set the time during which to apply the updates.
3. Click **Save**.

## Backup and restore

The Backup & Restore tab in the server configuration interface is the interface for configuring backing up and restoring configurations.

### Configure backups

You can back up the Symphony Server configuration.

By default, the Symphony Server creates a backup file automatically at 11:00 PM to the local backup path.

1. In the server configuration interface, click **Settings > Backup & Restore**.
2. In the **Backup configuration daily at** field, type the time at which you want the Symphony Server to create a backup file.
3. In the **Local backup path** field, type the path to which the Symphony Server saves the backup file.

For a server farm, type a network path that is available to all servers in the server farm.

4. To backup the server to Xnet, turn **Enable online backup** on.



**Note:** This feature requires a Maintenance & Support license.

5. To test your configuration, click **Test configuration**.
6. To create a backup, click **Back up now**.

### Restore from a local backup


You can restore configuration settings for a Symphony Server from the local backup path.

1. In the server configuration interface, click **Settings > Backup & Restore**.

2. To restore the configuration settings from a Symphony 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 Symphony Server from the Xnet.

 **Note:** 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 Symphony Server from a file.

1. In the server configuration interface, click **Settings > Backup & Restore**.
2. To restore the configuration settings from a Symphony 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**.

## Analytics

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 Symphony Server. Once installed, you can enable and configure the video analytic on a camera in the Symphony Server configuration interface.

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

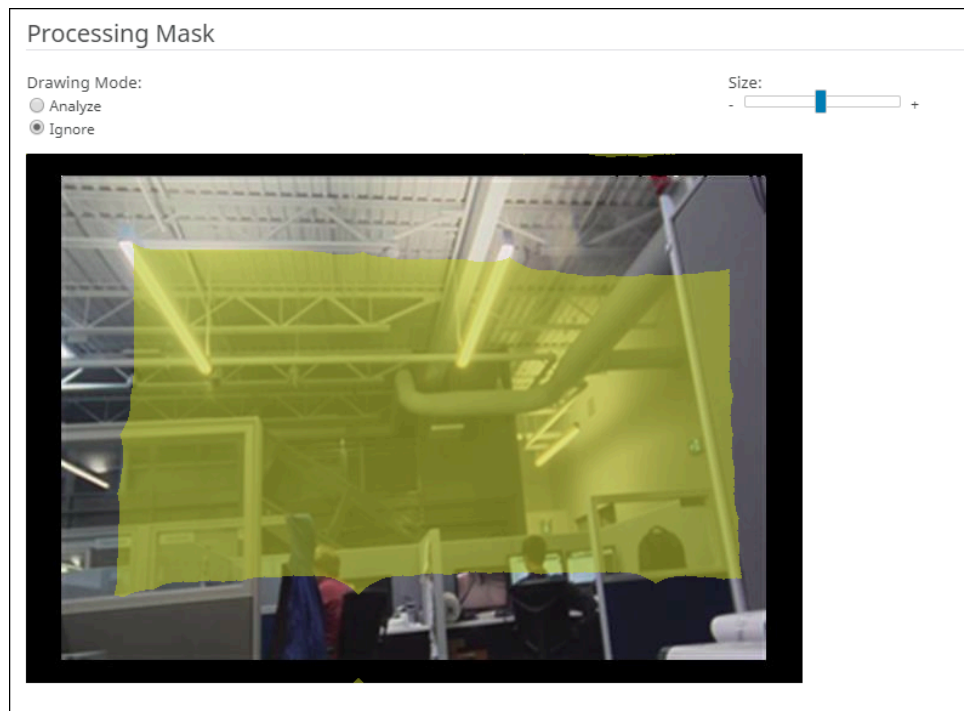
## Draw a processing mask

You can draw a processing mask for a video analytic in the Symphony 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 Symphony 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 Symphony 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**.

### Calibration

Type

Manually set the camera position and field of view information.

#### Instructions



Field of view (degrees)	<input type="text" value="40"/>
Pan (degrees)	<input type="text" value="0"/>
Twist (degrees)	<input type="text" value="0"/>
Height (meters)	<input type="text" value="4"/>
Distance (meters)	<input type="text" value="40"/>

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

### Enable the TCP Listener

1. In the Symphony 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 Symphony 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 Symphony 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 Symphony 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.

Setting	Description
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 the Automatic 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.
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.

- Warning:** 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.

Setting	Description
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 Symphony 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.
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 placed in front of a camera, or when the lights in the scene are turned off.

### Related tasks

[Configure Camera Tampering](#) on page 83

### Related reference

[Camera Tampering settings](#) on page 83

## Configure Camera Tampering

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

1. In the Symphony 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**.

Related reference

[Camera Tampering settings](#) on page 83

## 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.
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 include 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.

Related tasks

[Configure Crowd Detection](#) on page 84

[Calibrate a camera](#) on page 77

[Draw a processing mask](#) on page 76

Related reference

[Crowd Detection settings](#) on page 85

## Configure Crowd Detection

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

Related tasks

[Calibrate a camera](#) on page 77

[Draw a processing mask](#) on page 76

Related reference

[Crowd Detection settings](#) on page 85

## 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.

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
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.

Related reference

[Crowd Detection event settings](#) on page 43

## 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 Symphony 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 Symphony 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.

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

5. 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.

Setting	Description
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.

### 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.

Setting	Description
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

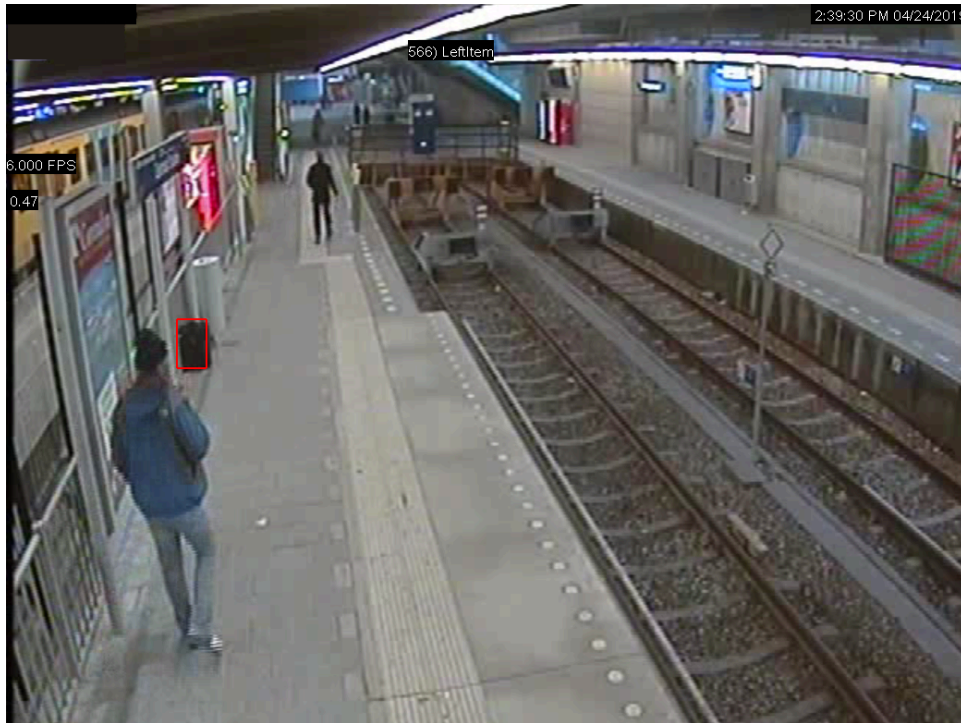
This section is only visible in simple mode.

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.
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 Symphony 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.

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

5. 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.

Setting	Description
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.

**Warning:** 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.

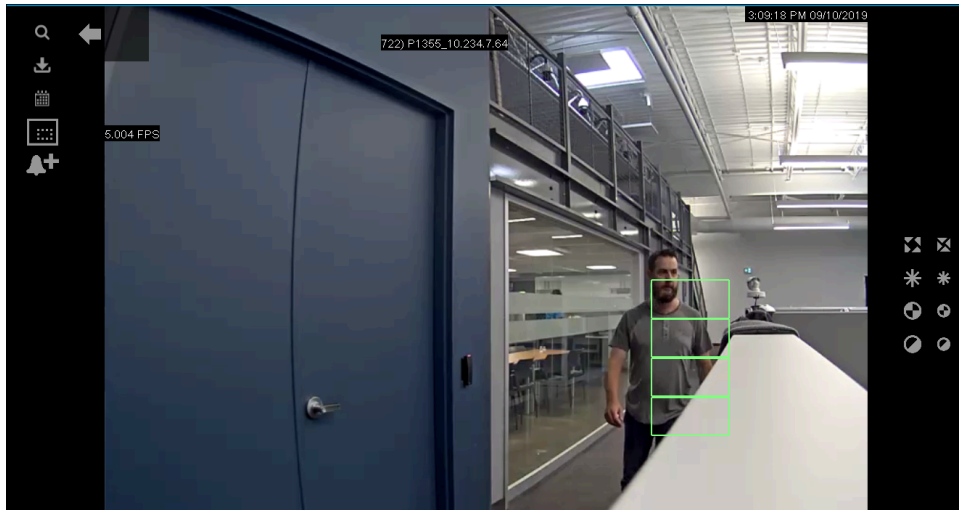
Setting	Description
Check for object drop-off	Select whether the Left and Removed Item Detection video analytic ignores items that a person picks up or drops off.  The default setting is selected.
Initial background model learn time	Set the time (seconds) that the Left and Removed Item Detection video 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.
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.

Setting	Description
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.
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

1. In the Symphony 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. Adjust the settings for the Motion Detection video analytic.
5. Click **OK**.

## 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.

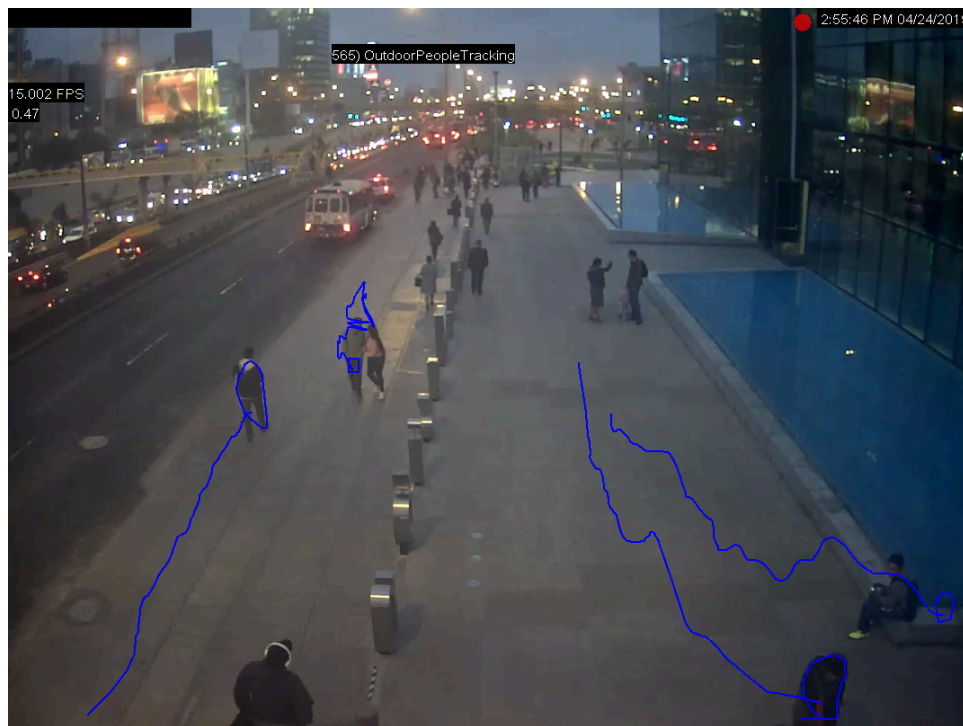
## Grid View

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 Symphony 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**.

- 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.

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

- Click **Save**.

Related tasks

[Calibrate a camera](#) on page 77

[Draw a processing mask](#) on page 76

## 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 in 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.

Setting	Description
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.
Shadow Suppression (Complex)	Select to use complex shadow suppression. Complex shadow suppression is effective when there are dark shadows in the scene.
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.

Related tasks

[Configure PTZ Auto-Tracking](#) on page 98

Related reference

[PTZ Auto-Tracking settings](#) on page 98

## Configure PTZ Auto-Tracking

1. In the Symphony 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 analytic for the camera.
4. In the **Add-Ons** list, turn PTZ Auto-Tracking on and click **Configure**.
5. Configure the video analytic.
6. Click **Save**.

Related reference

[PTZ Auto-Tracking settings](#) on page 98

## 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.

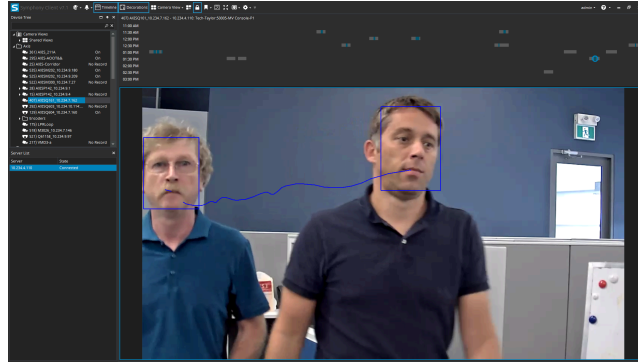
The Face Recognition video analytic uses profiles to represent individuals. Each profile can include multiple images of an individual's face. Use the Symphony Client interface to create profiles, add images of faces, and set whether the profile is blocked or allowed. When the Face Recognition video analytic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

**Note:** 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.

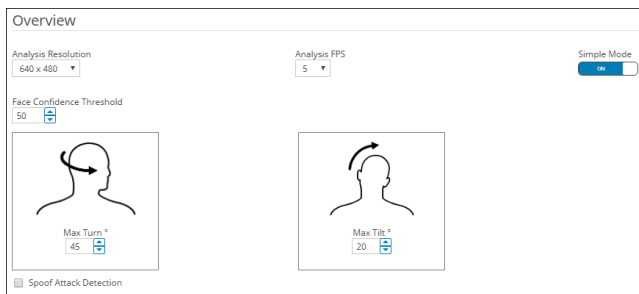
In the Symphony Client interface, a blue square surrounds a tracked face and a red square surrounds a tracked face that triggers an alarm.



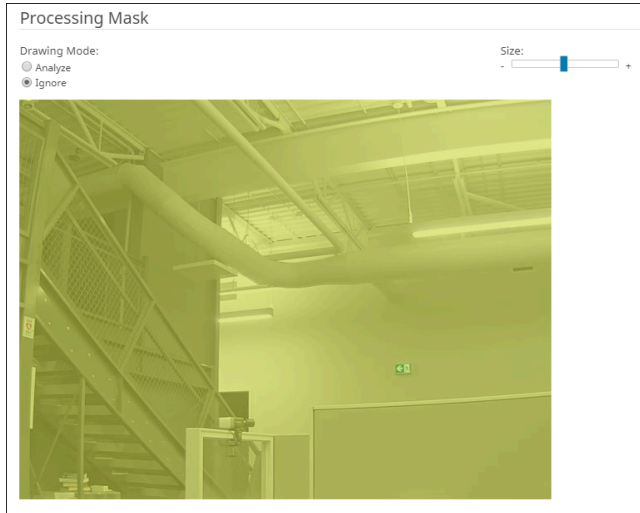
## Configure Face Recognition

Configure the settings for the Face Recognition video analytic in the Symphony Server configuration interface.

1. In the Symphony 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 parameters that Face Recognition uses when detecting faces.



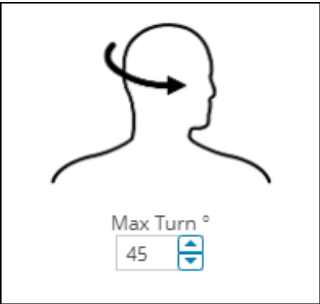
- In the **Processing Mask** section, set the areas in the image that the camera ignores or analyzes.

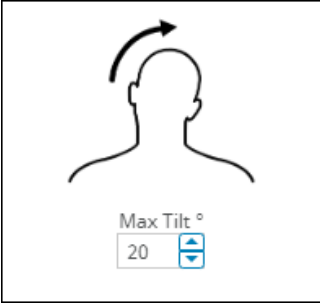


- Click **OK**.
- Click **Save**.

## 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. 

Setting	Description
Max Tilt	<p>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.</p> 
Spoof Attack Detection	<p>Select to enable spoofing attack detection. Spoof attack detection requires 15 frames for processing. So, if the Face Recognition video analytic is operating at 5 frames per second, it will take 3 seconds to generate an alarm.</p> <p>This setting is disabled by default.</p>

### 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.

# Symphony Client

---

The Symphony Client includes functionality to monitor cameras, manage video, generate reports, and configure alarms.

The Symphony Client is automatically installed with the Symphony Server, but you can also install the Client on additional computers and connect to the Symphony Server

You can use the client interface to access the Symphony Client.

Related concepts

[Introduction](#) on page 6

[Symphony Server](#) on page 9

[Symphony Web Client](#) on page 153

[Symphony Player](#) on page 154

## Open command

You can open the Symphony 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 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 Symphony Client and any Symphony Servers to which the Client connects.

1. In the 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**.

## View events

You can view and export events for the Symphony Client and any Symphony Servers to which the Client connects.

By default, the client interface displays the events for the current day.

1. In the client interface, click **Help > View Detailed Events**.
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**.

## Lock times

You can lock times on navigation in the 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 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 client interface, click **Lock Times On Navigation**.

## Customize the toolbar

You can change the icons that appear on the toolbar in the client interface.

1. In the 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**.

## Disable single sign-on

You can disable the single sign-on option when changing users and registering new farms in the Symphony Client.

When you disable single sign-on, the Windows Authentication check box is disabled when you change users or when you register a new Symphony Server farm.

1. Open the `acc.ini` file at `%appdata%\Senstar7`.
2. In the `[Main]` section, add the following text:

```
DisableWindowsAuthentication=True
```

3. Save and close the `acc.ini` file.

## Device tree

The device tree in the client interface lists the cameras, devices, and carousels available on the Symphony 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 Symphony 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 Symphony Server.

## 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 only includes devices that match your search term.

1. In the 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. 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 Symphony 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 **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

Symphony 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).

## 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 Symphony database.

1. In the server configuration 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 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
```

- d) Press Enter.
- e) Click **OK**.

Related tasks

[Add a group](#) on page 28

[Add a user to a group](#) on page 27

## Suspend access to video

You can suspend access to video (ban video) from a camera or camera group for a specific user group.

1. In the client interface, right-click a camera or camera group in the device tree.
2. Click **Ban Video**.

To resume access to video, click **Unban Video**.

## Create a camera tour

You can create a tour of preset locations for a PTZ camera to visit in the client interface.

1. In the **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 **client interface**.

1. In the **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, Symphony 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 **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**.

## Server list

The server list is an optional panel you can display in the Symphony client interface.

The server list displays the Symphony Server instances to which the Symphony Client connects.

Enabling the server list panel hides the server list in the toolbar.

## Enable the server list

You can display the service list as a panel in the client interface.

1. In the `acc.ini` file, set the `ShowFarmDropDown` value in the `Main` to `False`.
2. Save and close the `acc.ini` file.
3. Start the Symphony Client.
4. In the client interface, click **View > Server List**.

## Camera view panels

Camera view panels display live video, recorded video, and decorations from cameras.

Camera view panels can display overlays with controls for the camera. To hide the overlays, you can press and hold the Alt 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 client interface.

Before you begin:

- Add a camera to Symphony
- Open a floating or docked camera view

1. In the client interface, click a camera view.
2. In the device tree, click the camera that you want to view.

## View a Thin Client

You can view a Thin Client device in the client interface.

Before you begin:

- Add a Thin Client device to Symphony

When you view a Thin Client device in the client interface, the Thin Client device opens in a new floating view.

In the device tree, click the Thin Client device 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 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 Symphony Client.

You can select the instant replay duration on the Video Settings page in the Symphony Client settings.

1. In the server configuration interface, set the instant replay duration.
2. In a video pane in the client interface, click the **Instant Replay** icon.
3. View recorded video.

To end the instant replay, click the **Go to live view** icon.

Related reference

[Video settings](#) on page 126

## 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 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 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 client interface.

The Symphony Client includes camera views with 1, 4, 6, 9, 16, and 25 camera view panels.

1. In the 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 Symphony Client includes camera views with 1, 4, 6, 9, 16, and 25 camera view panels.

1. In the 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 client interface. A new camera view panel appears as a floating camera view panel, but you can dock it in the client interface.

1. In the client interface, click **Add Camera View Panel**.
2. Drag the camera view panel to the desired location.

## Add an alarm

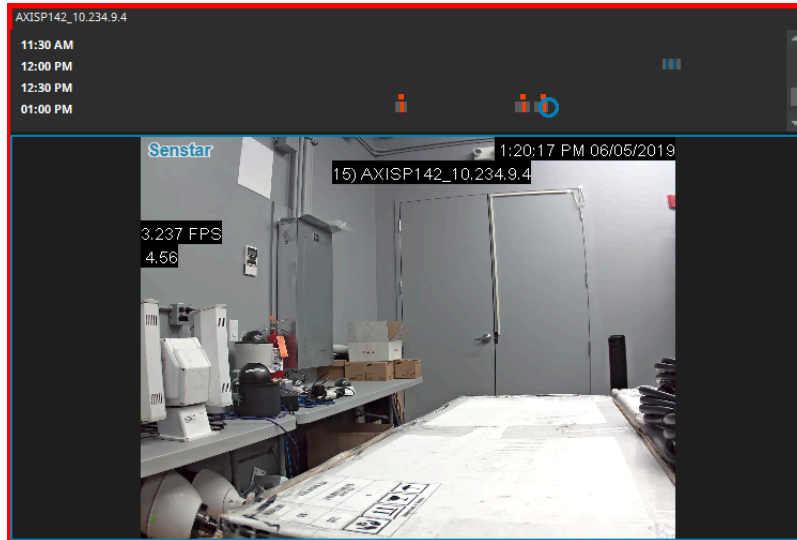
You can add a manual alarm to a camera in the Symphony Client.

You can use manual alarms to activate the action set associated with the manual rule.

1. In the 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 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 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**.

## 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.
Overlay Time	Select to display the time in the camera view panel.

Setting	Description
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.
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.
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.

Setting	Description
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 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.

- In the 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.
- In the **Class** pane, select the type of object for which to search.
- In the **Behavior** pane, select whether the object should be moving or loitering and for how long it should demonstrate the behavior.
- Select whether to define the search area by a mask or fences.
- 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.
- In the **Draw** pane, select whether to add or remove mask area or fences.
- 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.
9. In the **Add-Ons** pane (available if you search for any events), select the video analytic events to search.
10. In the **Rules** pane, select the rule events to search.
11. In the **Stream** list, select the stream to search.
12. Click **Search**.

## Export video to file

You can export video from the Symphony Client as `.aira` or `.avi` files.

1. In the client interface, perform one of the following tasks:
  - Right-click the camera view panel and click **Export**.
  - Hover over the camera view panel and click the Export icon.
  - Right-click the timeline to mark the export start and export end, and click **Export**.
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 **Local Disk** and specify the file location for the exported video.
4. In the **Format** field, select the file format to use for the video export.
5. To include the Symphony Player with the video export, select **Include Symphony Player**.  
You can use the Symphony Player to play `.aira` files.
6. To protect the video export files with a password, perform the following tasks:
  - a) Select **Password Protect**.
  - b) Type and confirm the password.
7. In the **Split Files at** field, select the maximum size (in MBs) for the video export files.  
Symphony divides the exported video into files no larger than the size that you specify.
8. Click **Export**.

## Export video to the cloud

You can export video from the Symphony 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 Symphony user account.

Symphony uploads the video files (as `.aira` files) to Xnet and sends an email with a link to download the video files to the email address associated with your Symphony user account. You can then forward the link to other recipients.

When exporting video to the cloud, Symphony 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 client interface, perform one of the following tasks:
  - Right-click the camera view panel and click **Export**.
  - Hover over the camera view panel and click the Export icon.
  - Right-click the timeline to mark the export start and export end, and click **Export**.

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. Click **Export**.

Symphony sends you an email that includes a link to manage your exported video. You can use the link to delete exported videos.

## 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 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.

For cameras that are not set to always record, you can manually start recording video.

1. In the 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.

The camera view panel displays an icon to show that Symphony 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 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.





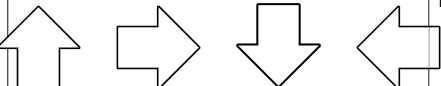



1. In the client interface, view video from a camera that is running a video analytic.
2. In the timeline, navigate to historical video.
3. Click the **Summarize Video** icon to play summary video.

## 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.

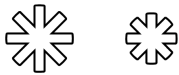


Control	Description
	Play video.
	Pause video.
	Go forward one frame.
	Go forward one second.
	Go forward ten seconds.
	Navigate to the next activity.
	Navigate to the next alarm.
	Navigate to the next bookmark.
	Show live video

## PTZ controls

Control	Description
	Move the PTZ camera to a preset location.
	Increase the zoom on the PTZ camera.
	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

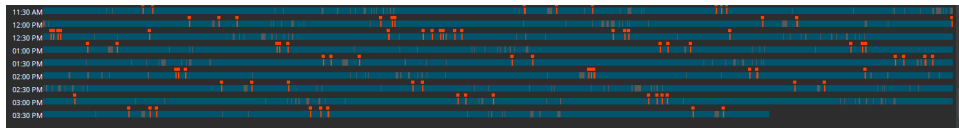
Control	Description
	Open or close the iris of the camera to adjust how much light enters the lens of the camera.

Control	Description
	Increase or decrease the brightness of the camera.
	Adjust the focus of the camera.
	Adjust the contrast of the camera.

## Timeline

Timelines display the activities and alarms for a camera in the client interface.

You can display a timeline for each camera in the client interface and the timeline spans the current day for that camera. You can click on the timeline to navigate to specific times or events in the footage. A purple circle indicates your current position on the timeline.



## Timeline colors

The 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
Transparent (#00FFFFFF)	No record

Color	Event
Light blue (#59CBE8)	Zoom

## Display the timeline

You can display a timeline for a camera in a video panel.

In addition, you can display a timeline for every camera in a video panel by clicking the Timeline button in the client interface.

1. In the client interface, right-click a video panel.
2. Click **Show Timeline**.

To hide a timeline, right-click the video panel and click Show Timeline again.

## Maps

Maps can display the location of cameras, camera views, digital inputs and output devices, links, and labels in the client interface.

A map can be an image file (*jpg, gif, or bmp* file) or a map provided by a GIS service. You can use the map editor in the client interface to add, edit, and delete maps.

You can add cameras and camera views to a map. Clicking on a device icon performs the following actions in the client interface:

- Clicking a camera icon displays the camera view in the active video panel.
- Clicking a camera view icon loads the camera view in the client interface.

You can add digital input and output devices to a map.

## Add a map

You can add an image file of a map to Symphony.

1. In the 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 Symphony.

1. In the 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 client interface.

You can navigate on the map by using the scroll bars or clicking and dragging the map.

1. In the 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, 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 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**.

## Map icons

Icon	Description
	Rule
	Digital input <ul style="list-style-type: none"> <li>• Activated: yellow background</li> <li>• Not activated: white background</li> </ul>
	Digital output <ul style="list-style-type: none"> <li>• Activated: yellow background</li> <li>• Not activated: white background</li> </ul>
	Camera <ul style="list-style-type: none"> <li>• Online camera: gray arrow</li> <li>• Offline camera: white arrow</li> <li>• Motion detected: blue arrow</li> <li>• Alarm: orange arrow</li> <li>• Selected camera: orange circle</li> </ul>
	PTZ camera <ul style="list-style-type: none"> <li>• Online camera: gray arrow</li> <li>• Offline camera: white arrow</li> <li>• Motion detected: blue arrow</li> <li>• Alarm: Orange arrow</li> </ul>

Icon	Description
	Access control device <ul style="list-style-type: none"> <li>• Access granted: green</li> <li>• Access denied: red</li> </ul>
	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 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 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**.

## Messenger

Symphony Messenger allows you to send messages to any user who is logged in to the Symphony Client or Symphony Web Client.

## Send a message

You can send messages to users or groups.

1. In the client interface, click **Setting > Messenger** to open the 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 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 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 client interface.
4. 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.
5. In the **Available Cameras on Servers** list, select the cameras to include in the carousel and click **Add Selected**.
6. 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.
7. 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**.

## Settings

You can use the Symphony Client settings to customize the 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 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.

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

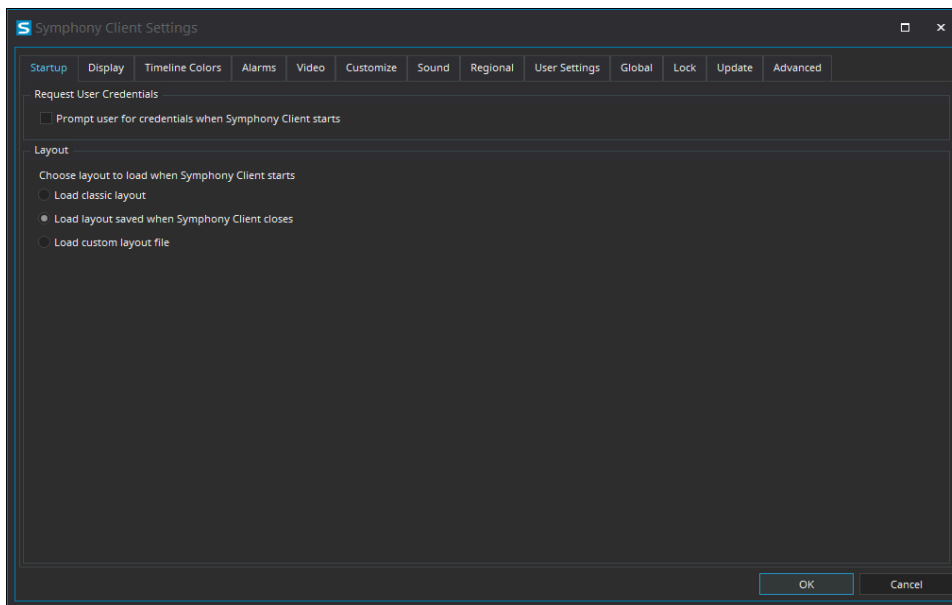
You can change the colors that the Symphony Client uses in the timeline.

When you change the timeline colors, you also change the colors that the Symphony Client uses for map icons.

1. In the 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 Symphony colors at any time or use the classic colors from Symphony 6.14.

## Startup settings



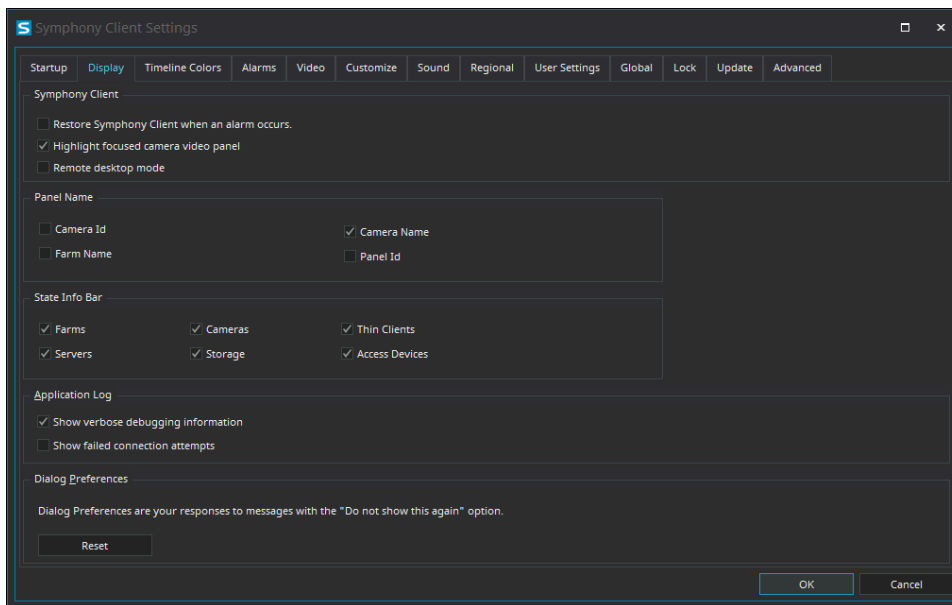
### Request User Credentials

Setting	Description
Prompt user for credentials when Symphony Client starts	Select to make users provide a valid username and password before using the Symphony Client.

### Layout

Setting	Description
Load classic layout	Select to load the default layout when the Symphony Client starts.
Load layout saved when Symphony Client closes	Select to load the layout from the last session when the Symphony Client starts.
Load custom layout file	Select to load the layout from a saved layout file when the Symphony Client starts.

## Display settings



### Symphony Client

Setting	Description
Restore Symphony Client when an alarm occurs	Select to restore the 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 Symphony Client. This setting removes the dependency of overlays and navigation controls in the 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.
Storage	Select to display warning messages for video storage in the notification bar.
Thin Clients	Select to display warning messages for Thin Client devices in the notification bar.
Access Devices	Select to display warning messages for access control devices in the notification bar.

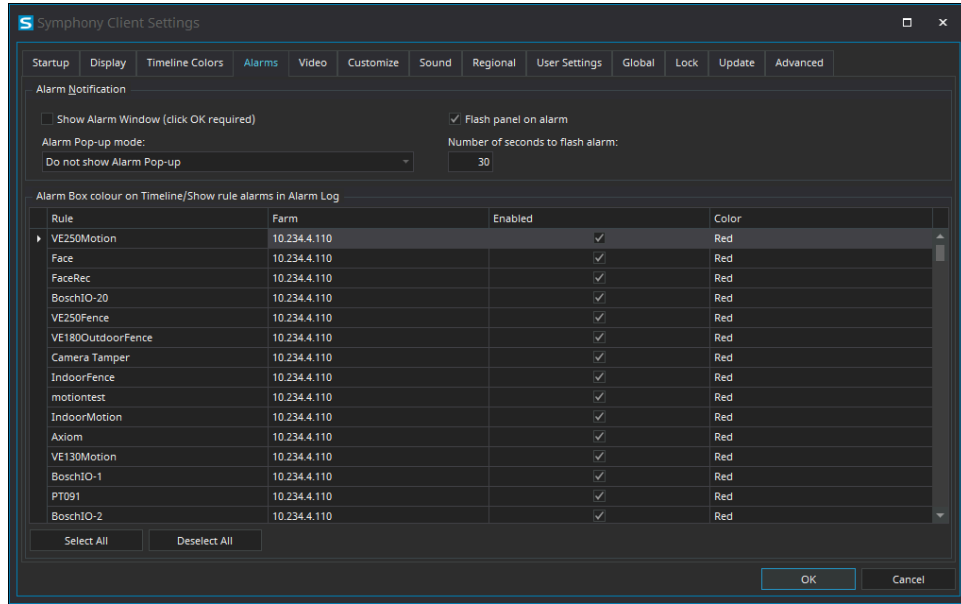
### Application Log

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 client interface.

## Alarms settings



Setting	Description
Show Alarm Window (click OK required)	Select to make the Symphony Client display a dialog box when an alarm occurs.
Alarm Pop-up mode	Select how the Symphony Client displays alarm dialog boxes.
Flash panel on alarm	Select to display an alarm indicator around camera view panels when cameras record alarms.
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 colour 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

### 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).

Setting	Description
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.
Messenger messages	Select to display messages from Messenger over the video in the camera view panel.
Seconds	Select how long the messages remain visible.
Video Retention	Select to display video retention capacity over the video in the camera view panel.
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.
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 Symphony 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 Symphony Client.

## Related concepts

[Multicasting](#) on page 11

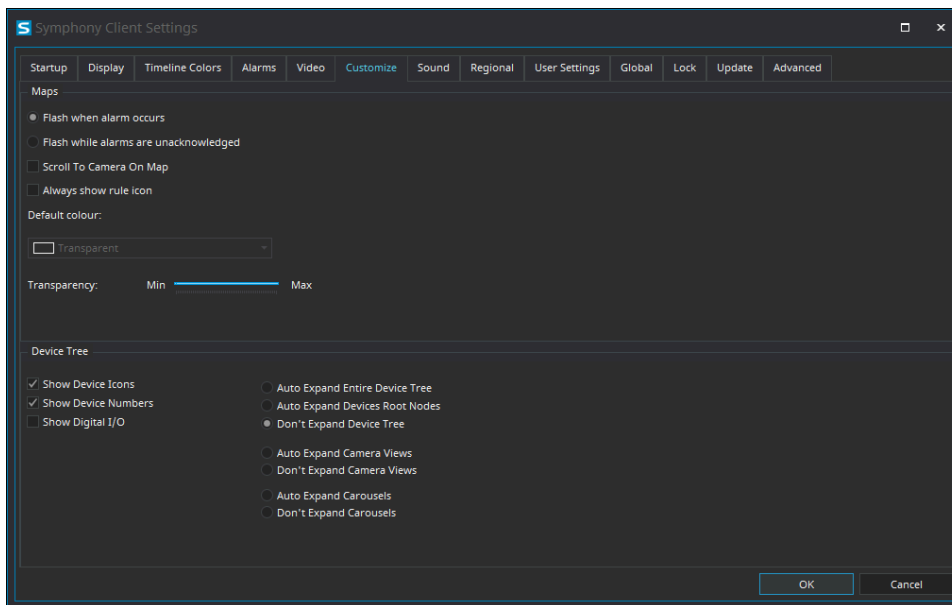
## Related tasks

[View instant replay](#) on page 107

[Add a camera automatically](#) on page 12

[Add a camera manually](#) on page 12

## Customize settings



### Maps

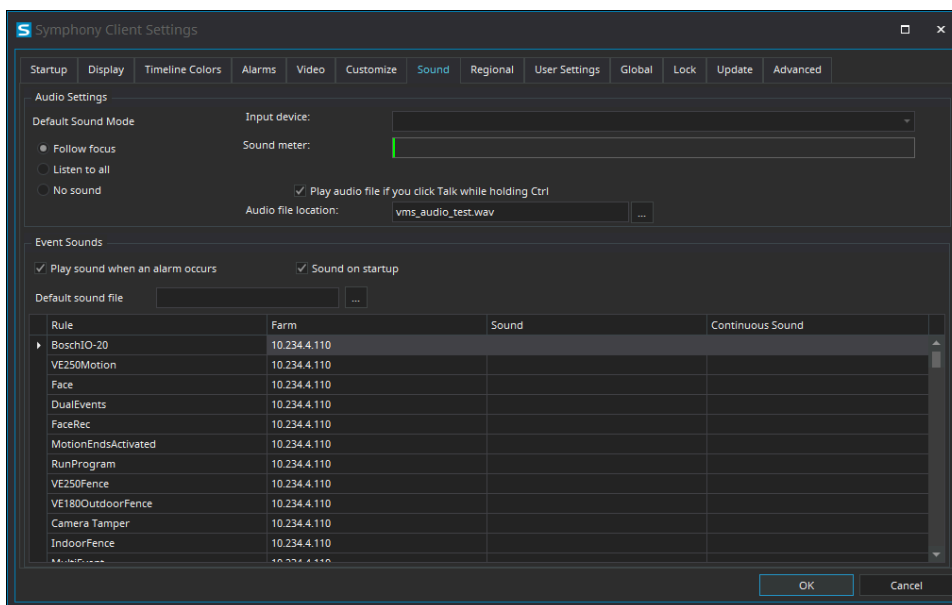
Setting	Description
Flash when alarm occurs	Select to flash the alarm icon when the alarm occurs.
Flash while alarms are unacknowledged	Select to flash the alarm icon while the alarm is unacknowledged.
Scroll To Camera On Map	Select to center the map on a camera when you click the camera in the Map Navigation pane of the 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 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 client interface starts.

Setting	Description
Auto Expand Devices Root Nodes	Select to expand the top level of the device tree when the client interface starts.
Don't Expand Device Tree	Select keep the device tree collapsed when the client interface starts.
Auto Expand Camera Views	Select to expand the camera views in the device tree when the client interface starts.
Don't Expand Camera Views	Select to keep the camera views collapsed in the device tree when the client interface starts.
Auto Expand Carousels	Select to expand the carousels in the device tree when the client interface starts.
Don't Expand Carousels	Select to keep the carousels collapsed in the device tree when the client interface starts.

## Sound settings



## Audio settings

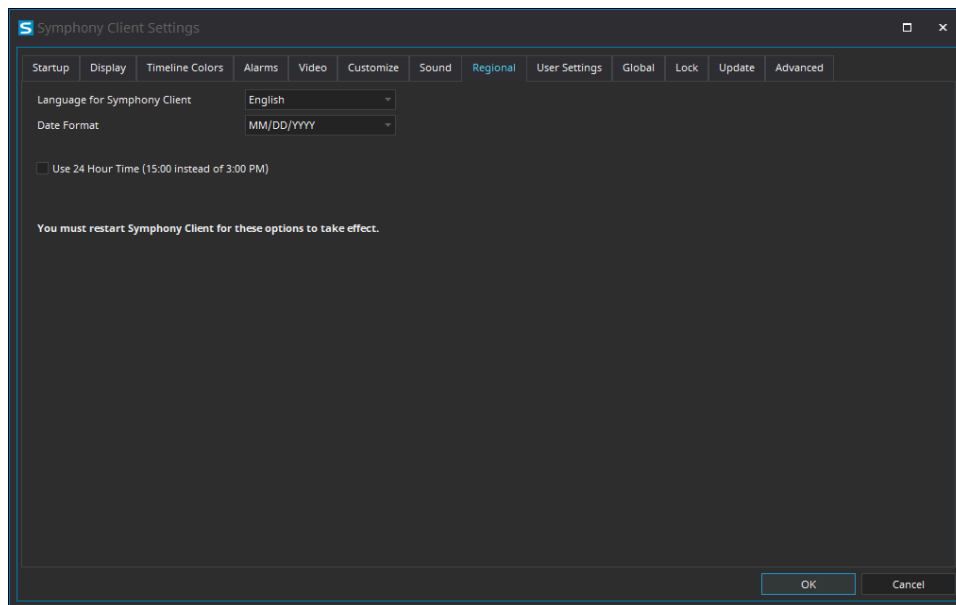
Setting	Description
Default Sound Mode	Set how the Symphony Client plays or mutes audio for video. Select Follow focus to play audio from the active video panel. Select Listen to all to play audio from all video panels. Select No sound to mute all audio.
Input device	Select the audio input device.

Setting	Description
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

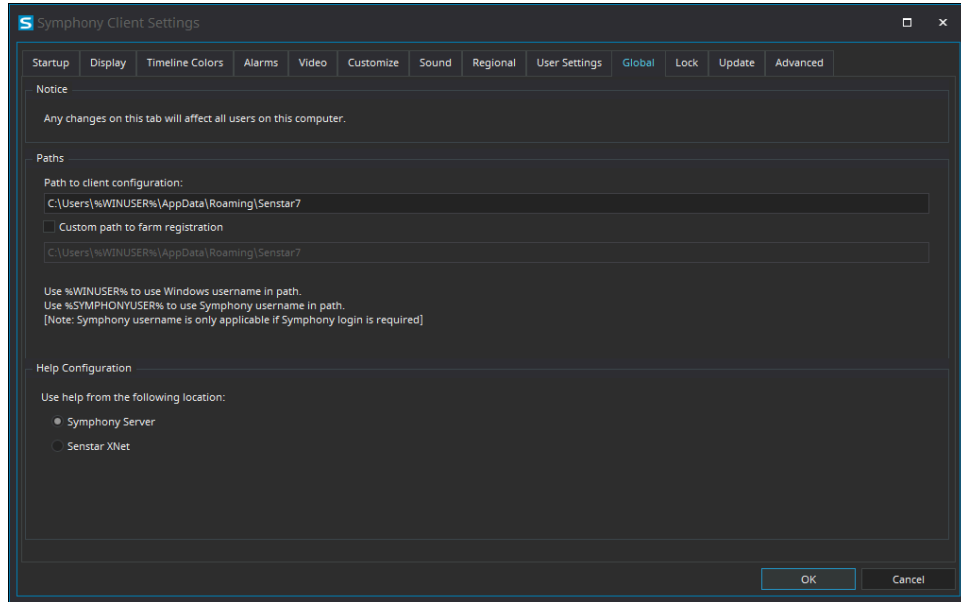
Setting	Description
Play sound when an alarm occurs	Select to play a sound when an alarms occurs. You can set both the alarm sound and the continuous sound for each rule.
Sound on startup	Select to play the default sound file when the Symphony Client starts.
Default sound file	Select the default audio file.

### Regional settings



Setting	Description
Language for Symphony Client	Select the language for the client interface.
Date Format	Select the format for dates in the client interface.
Use 24 Hour Time	Select to display time in the 24-hour format in the client interface.

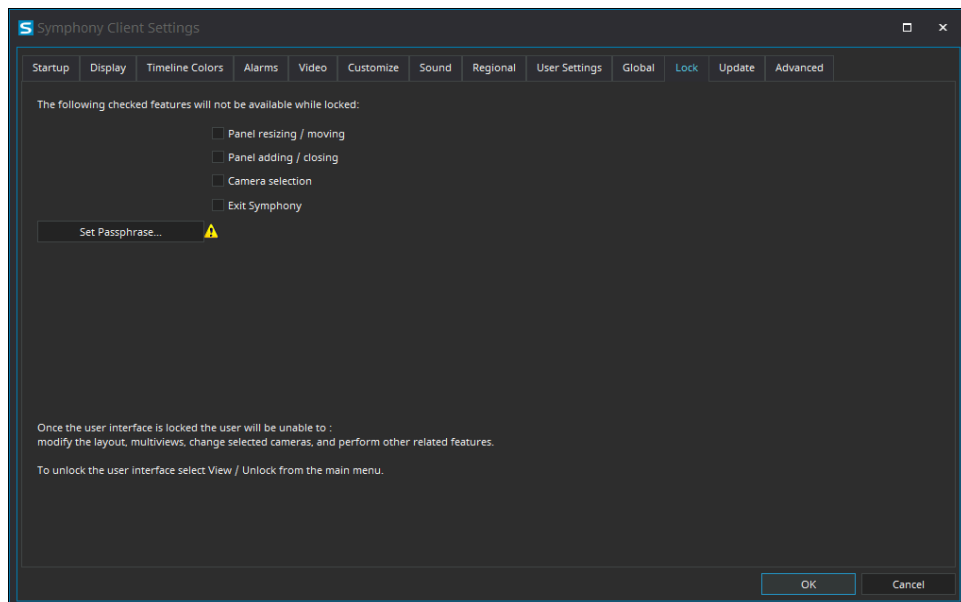
## Global settings



Setting	Description
Path to client configuration	Define the path to configuration data for the Symphony 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 Symphony Client opens help that is included with the Symphony Server or help from the Internet.

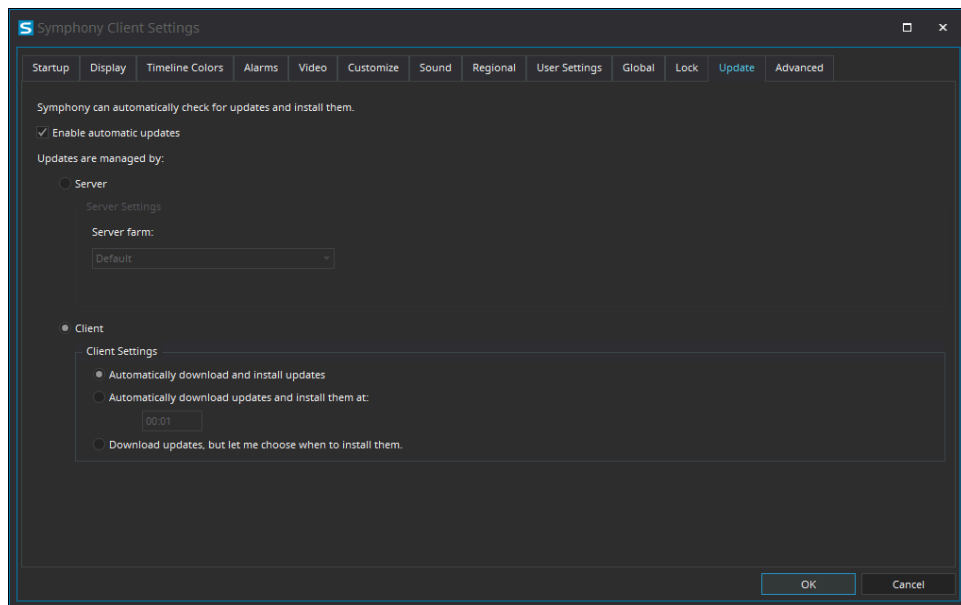
## Lock settings

The lock settings determine the functionality that is available to users when you lock the Symphony Client and allows you to set the passphrase for unlocking the Symphony Client.



Setting	Description
Panel resizing/moving	Select to prevent users from resizing and moving camera view panels.
Panel adding/closing	Select to prevent users from adding and closing camera view panels.
Camera selection	Select to prevent users from selecting different cameras.
Exit Symphony	Select to prevent users from closing the Symphony Client.
Set Passphrase	Click to set the passphrase that unlocks the Symphony Client.

## Update settings



Setting	Description
Enable automatic updates	
Updates are managed by	
Use help from the following location	Select whether the Symphony Client opens help that is included with the Symphony Server or help from the Internet.

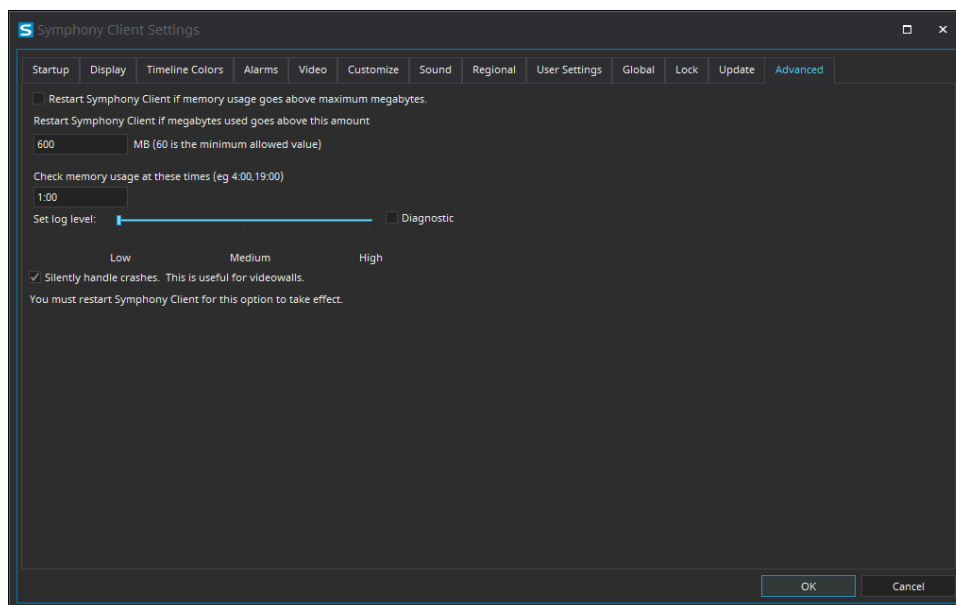
## Server settings

Setting	Description
Server farm	

### Client settings

Setting	Description
Automatically download and install updates	
Automatically download updates and install them at	
Download updates but let me choose when to install them	

### Advanced settings



Setting	Description
Restart Symphony Client if memory usage goes above maximum megabytes	
Restart Symphony Client if megabytes goes above this amount	
Check memory usage at these times	
Set log level	
Silently handle crashes	

## 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 client interface.

## Create a bookmark

You can create a bookmark to reference video from a specific time and camera.

You can share a bookmark so that other users can open the video that you mark.

1. In the 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 client interface, click **Bookmarks > Manage Bookmarks**.
2. Select **Delete** for the bookmark.
3. Click **OK**.

## Video wall

The video wall feature in Symphony can display footage from multiple cameras in the server farm on multiple monitors.

Any Symphony Client can act as a video wall client, and you can include any monitors connected to the computers that host the Symphony Client in the video wall.

## Register a client

Register each computer that hosts the Symphony Client that you want to include in the video wall.

1. In the Symphony 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 Symphony 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 Symphony Server in the server configuration interface, the client interface includes functionality to configure some settings on the Symphony Server.

### Connect to a server

You can connect a Symphony Client to multiple Symphony Server instances.

1. In the client interface, click **Server Configuration > New Symphony Server Registration**.
2. In the **Address** field, perform one of the following tasks:
  - Select the Symphony Server from the list of discovered servers.
  - Type the IP address of the Symphony Server.
  - Type the DNS name of the Symphony Server.
3. In the **Name** field, type a meaningful name for the Symphony Server. This name will appear in the Server List in the client interface.
4. To log in to the Symphony Server, perform one of the following tasks:
  - To use your Windows account to authenticate with the Symphony Server, select the **Windows Authentication** check box.
  - Type your username and password.
5. Click **OK**.

### Disconnect from a server

You can disconnect from a Symphony Server to remove the cameras associated with that server from the Symphony Client.

1. In the client interface, click **Server Configuration > Delete Symphony Server Registration**.
2. Select the server from which to disconnect.
3. Click **Remove**.

### Delete recorded video

You can delete recorded video for a specific time or delete all recorded video.

1. In the 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**.

### Get information about the server

You can gather information about the Symphony Servers to which the Symphony Client connects.

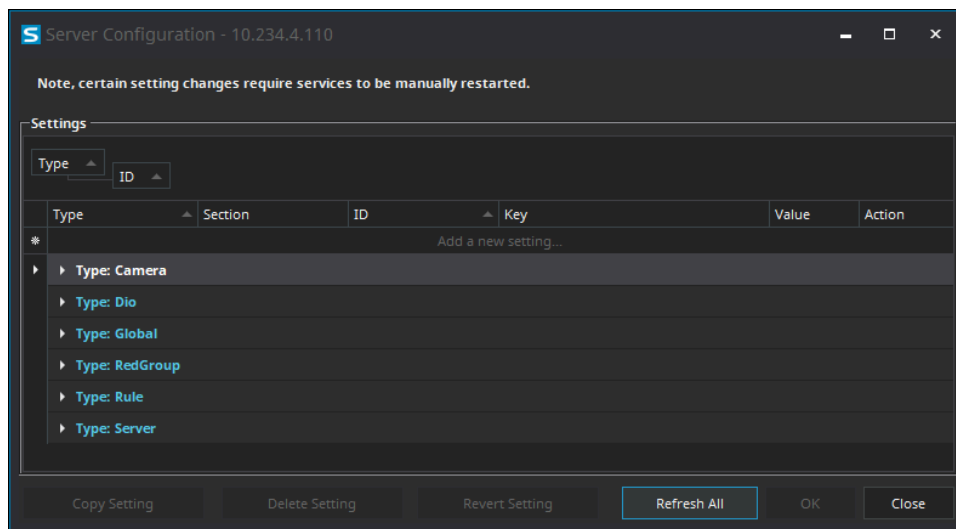
1. In the client interface, click **Server Configuration > Get Info**.
2. In the **Choose Server** list, select the server for which you want information.

3. To get additional information, select **Verbose**.  
The verbose information includes:
  - Hard drive information
  - Symphony 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 Symphony component that you can use to add and edit advanced settings in the Symphony Database.

You can access the Manual Configuration Editor from the Symphony Client or as a stand-alone application if you install the Symphony Server.



Each setting includes the following fields:

- Type
- Section
- ID
- Key
- Value
- Action

When you click OK after making changes, the Symphony Client sends the changes to the Symphony Server, which adds the changes to the Symphony Database.

## Add a setting

You can use the Manual Configuration Editor to add a setting to the Symphony Database.

Adding a setting to the Symphony Database is a way to add advanced functionality to the Symphony Server or Symphony Client.

1. In the Symphony 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.
3. Add the values to the setting.
4. Click **OK**.

## Copy a setting

You can use the Manual Configuration Editor to copy a setting in the Symphony Database.

Copying a setting is a quick way to add a new setting to the Symphony Database by using a similar existing setting as a template.

1. In the Symphony 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 [Copy] label in the **Key** field.

## Edit a setting

You can use the Manual Configuration Editor to edit a setting in the Symphony Database.

Editing a setting is a quick way to add a new setting to the Symphony Database by using a similar existing setting as a template.

1. In the Symphony 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 Symphony Database.

Reverting a setting returns the setting to the values in the Symphony Database before you save you changes. This only works if you have not yet clicked **OK** after making changes.

1. In the Symphony 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 Symphony Database.

1. In the Symphony 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 Symphony Database.

Refreshing the settings ensures that the settings in the Manual Configuration Editor match the current settings in the Symphony Database. This functionality is helpful if multiple people can make changes to the Symphony Database.

1. In the Symphony 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 Symphony Server and Symphony Client must be in the same security domain, and the user must use domain credentials to log in to the Symphony Client.

### Enable Windows authentication

1. In the client interface, right-click a Symphony Server in the **Server List**.
2. Click **Edit**.
3. Select **Windows Authentication**.
4. Click **OK**.

### Update the storage path

To use Windows authentication on all computers in the domain, you must save the farm registration information to a network location that is available to the computers.

1. In the client interface, click **View > Settings**.
2. Click the **Global** tab.
3. Select **Custom path to farm registration**.
4. Type a network location where registration information is stored for all roaming users.
5. Click **OK**.

## Reports

You can generate reports on the data from Symphony.

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, Symphony saves the report to the `\Data\Reports` path for the server (by default) or the path that you set when you install the Symphony Server.

Symphony includes the following reports:

- Alarm Report—a report that displays a list of and information about individual alarms
- Alarm Statistics—a report that summarizes all alarms for a specific time
- Face Recognition Report—a report that displays information about matched faces
- Heat Map Image—a report that displays a graphical representation of traffic patterns
- Object Counts—a report that summarizes the number of objects
- Object Counts Across a Line—a report that summarizes the object counts across a line
- Object Statistics—a report that compares traffic and dwell time

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.

## Create an alarm report

The alarm report displays a list of and information about individual alarms for a specific time.

1. In the client interface, click **Reports**.  
The Report Designer opens in a browser.
2. Log in to the Report Designer.
3. Click **New Report**.
4. Type a name for the report.
5. In the **Report Type** list, select **Alarm Report**.
6. To allow other users to run the report, select **Allow other users to run this report**.
7. Click **OK**.
8. 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**.
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 Symphony 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**.

## Create an alarm statistics report

The alarm statistics report summarizes alarms for a specific time.

1. In the client interface, click **Reports**.  
The Report Designer opens in a browser.
2. Log in to the Report Designer.
3. Click **New Report**.
4. Type a name for the report.

5. In the **Report Type** list, select **Alarm Statistics**.
6. To allow other users to run the report, select **Allow other users to run this report**.
7. Click **OK**.
8. 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**.
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 Symphony 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 **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**.

## Create a Face Recognition report

The Face Recognition report displays information about license plates 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 client interface, click **Reports**.  
The Report Designer opens in a browser.
2. Log in to the Report Designer.
3. Click **New Report**.

4. Type a name for the report.
5. In the **Report Type** list, select **Face Recognition**.
6. To allow other users to run the report, select **Allow other users to run this report**.
7. Click **OK**.
8. 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**.
9. 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**.
10. 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.
11. 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.
12. 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.
13. In the **Distribution** section, perform the following tasks to determine how Symphony 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.

14. 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.
15. Click **Save**.

## Create a heat map image report

The heat map image report displays a graphical representation of traffic patterns for a specific time.

1. In the client interface, click **Reports**.  
The Report Designer opens in a browser.
2. Log in to the Report Designer.
3. Click **New Report**.
4. Type a name for the report.
5. In the **Report Type** list, select **Heat Map Image**.
6. To allow other users to run the report, select **Allow other users to run this report**.
7. Click **OK**.
8. 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**.
9. 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.
10. 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.
11. 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.

12. 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.
13. In the **Distribution** section, perform the following tasks to determine how Symphony 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.
14. 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.
15. Click **Save**.

## Create an LPR report

The LPR report displays information about license plates for a specific time.

1. In the client interface, click **Reports**.  
The Report Designer opens in a browser.
2. Log in to the Report Designer.
3. Click **New Report**.
4. Type a name for the report.
5. In the **Report Type** list, select **LPR Report**.
6. To allow other users to run the report, select **Allow other users to run this report**.
7. Click **OK**.
8. 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**.
9. In the **Filter** section, select the plate lists on which to 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 Symphony 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**.

## Create an object counts report

The object counts report displays information about objects for a specific time.

1. In the client interface, click **Reports**.  
The Report Designer opens in a browser.
2. Log in to the Report Designer.
3. Click **New Report**.
4. Type a name for the report.
5. In the **Report Type** list, select **Object Counts**.
6. To allow other users to run the report, select **Allow other users to run this report**.
7. Click **OK**.
8. 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**.
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 it 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 Symphony 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**.

## Create an 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 client interface, click **Reports**.  
The Report Designer opens in a browser.
2. Log in to the Report Designer.
3. Click **New Report**.
4. Type a name for the report.
5. In the **Report Type** list, select **Object Counts Across a Line**.
6. To allow other users to run the report, select **Allow other users to run this report**.
7. Click **OK**.
8. 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**.
9. In the **Line** section, select the line across which to count objects.
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 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.

12. In the **Distribution** section, perform the following tasks to determine how Symphony 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.
13. 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.
14. 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.
15. Click **Save**.

## Create an object statistics report

The object statistics report displays information about objects traffic and dwell time for a specific time.

1. In the client interface, click **Reports**.  
The Report Designer opens in a browser.
2. Log in to the Report Designer.
3. Click **New Report**.
4. Type a name for the report.
5. In the **Report Type** list, select **Object Statistics**.
6. To allow other users to run the report, select **Allow other users to run this report**.
7. Click **OK**.
8. 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**.
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 it 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 Symphony 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**.

## Edit a report

You can make changes to an existing report in the Report Designer.

1. In the client interface, click **Reports**.  
The Report Designer opens in a browser.
2. Log in to the Report Designer.
3. Perform one of the following tasks:
  - Select a report and click **Edit**.
  - Double-click a report.
4. Make changes to the report.
5. Click **Save**.

## Run a report

You can manually generate a report at any time.

1. In the client interface, click **Reports**.  
The Report Designer opens in a browser.
2. Log in to the Report Designer.
3. Select a report.
4. Click **Run**.

## Alarms

Alarms occur when a video analytic running on a device detects the conditions of a rule.

In the client interface, alarms appear in the camera timeline.

## Disable alarms for a camera

You can disable the alarms for a camera in the Symphony Client.

1. In the 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 Symphony Server to which the Symphony Client is connected.

1. In the 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**.

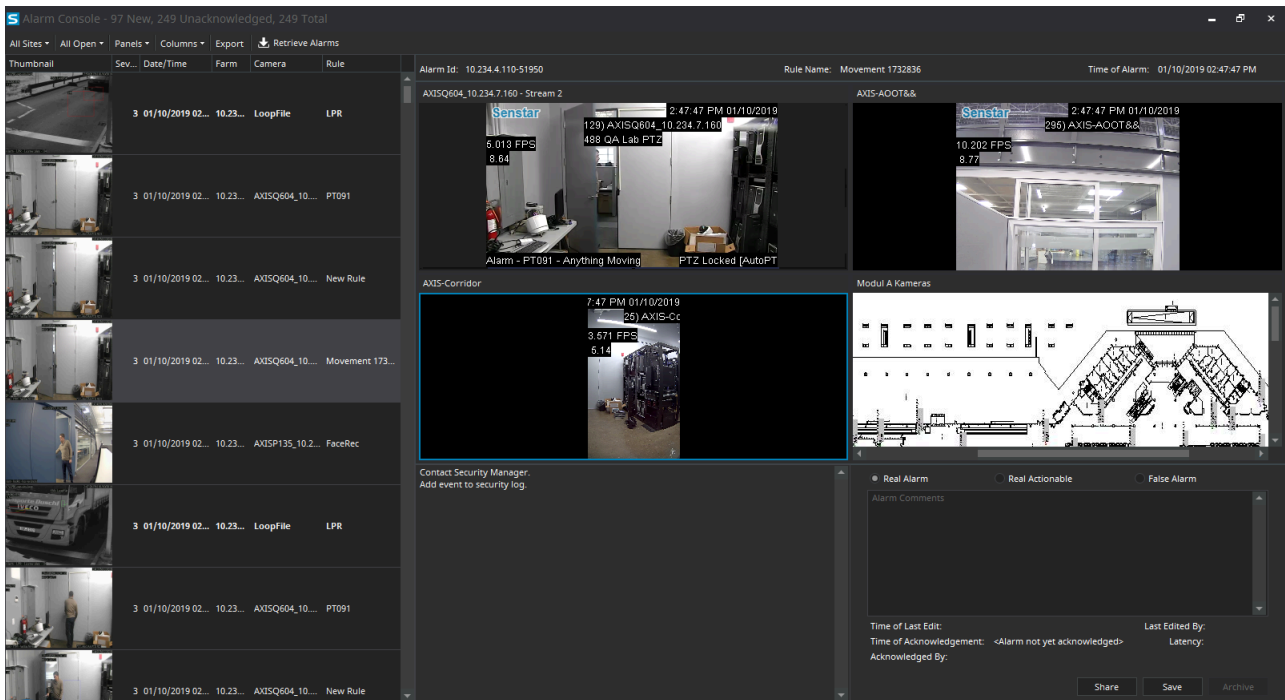
## Alarm console

The alarm console in the Symphony Client includes functionality to view and manage alarms.

The alarm console appears in the 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 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 client interface. The alarm console includes the following components:

- Alarm list
- View panels (display one to four in the Alarm Console section on the Action Sets page in the server configuration interface)
- Instruction pane (Instruction section on the Action Sets page in the server configuration interface)
  - 📄 **Note:** If you add a file, you can zoom on the file by hold the CTRL button and using the mouse scroll wheel.
- Acknowledgment pane



## Retrieve alarms

You can retrieve alarms for dates that are not included in the alarm list.

Depending on how you sort the alarm log, the alarms that you retrieve might not appear at the top of the list.

1. In the client interface, click **View > Alarm Log**.
2. Click **Retrieve Alarms**.
3. Select a date.

## Export an alarm list

You can export alarms from the client interface.

When exporting alarms, Symphony supports the following formats:

- PDF
- HTML
- MHT
- RTF
- XLS
- XLSX
- CSV
- Text
- Image

1. In the client interface, click **View > Alarm Log**.
2. Filter and sort the alarms until you get the list that you want to export.
3. Click **Print And Export To**.

The amount of time it takes Symphony to process the export file increases with the number of alarms you want to export.

4. In the **Preview** window, click **File > Export Document**.

5. Click the file format.
6. Specify the options for the output and click **OK**.

## Share an alarm

You can share an alarm with any user who is logged in to the Symphony Client.

When you share an alarm with a user, the Symphony Client displays a message for the user in the 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

1. In the alarm console sidebar, click **Advanced Mode**.
2. Select the alarm.
3. Select the type of the alarm.
  - Real Alarm
  - Real Actionable
  - False Alarm
4. Type any comments that you want to add to the alarm.
5. Click **Save**.

## 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 client interface.

1. In the 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.

# Symphony Web Client

---

The Symphony Web Client includes functionality to monitor cameras, manage video, generate reports, and configure alarms.

The Web Client is designed to mimic the Symphony Client as much as possible. Most core features of the Client are available in the Web Client. In addition, the Web Client includes the Report Designer.

Each Symphony Server has a dedicated Web Client.

Related concepts

[Introduction](#) on page 6

[Symphony Server](#) on page 9

[Symphony Client](#) on page 102

[Symphony Player](#) on page 154

## 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**.

1. In a browser, navigate to the IP address of your Symphony Server.
2. In the language list, select your language.
3. Type your username and password.
4. Click **Web Client**.

## Configure the Web Client

1. In the server configuration interface, click **Settings > General Settings**.
2. To use load balancing with the **Web Client**, select **Randomly redirect master server logins to other available servers in the farm**.
3. Set how often the Web Client refreshes the information on the Monitoring tab in the **Refresh rate** field.
4. To use an ICE server, complete the following tasks:
  - a) Select **Use an ICE Server**.
  - b) Select the type of the ICE server (either TURN or STUN).
  - c) In the URL field, type the IP address of the ICE server.
  - d) In the **Username** field, type the username that Symphony uses for authentication with the ICE server.
  - e) In the **Password** field, type the password that Symphony use for authentication with the ICE server.
5. Click **Save**.

# Symphony Player

---

The Symphony Player is an application that can view video files created in the Symphony Client.

The Player is a lightweight solution that allows you to view video and search results from Symphony. By default, the Player installs with the Client and the Server, but you can also install it as a standalone application.

Related concepts

[Introduction](#) on page 6

[Symphony Server](#) on page 9

[Symphony Client](#) on page 102

[Symphony Web Client](#) on page 153

## Install the Player

You can install the Symphony 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 Symphony Player to prevent the Player from playing tampered video.

1. Open the `acc.ini` file at `%appdata%\Senstar7`.
2. Add the following values:

```
[VideoRecvCTRL]
UseWatermarking=True
```

3. Save and close the `acc.ini` file.

Related concepts

[Watermarking](#) on page 40

Related tasks

[Enable watermarking](#) on page 41

## 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 Client.

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
<b>Play/Pause</b>	Play or pause the video.
<b>&lt; snippet</b>	Move backwards to the last activity in the video.
<b>&lt; frame</b>	Move backwards one frame.
<b>frame &gt;</b>	Move forwards one frame.
<b>snippet &gt;</b>	Move forwards to the next activity in the video.
Slider	Move the slider to navigate to the corresponding position in the video.

## Legal information

Copyright © 2019 Senstar Corporation and/or its Licensor(s). All rights reserved.

This material is for informational purposes only. Senstar makes no warranties, express, implied or statutory, as to the information in this document.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Senstar Corporation

Senstar may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Senstar, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

Portions of this software are based in part on the work of the Independent JPEG Group.

All other trademarks are the property of their respective owners.

## Third-party attributions

Component	Attribution
Boost Software	Copyright © 1998-2005 Beman Dawes, David Abrahams. Copyright © 2004-2007 Rene Rivera. Boost is licensed under the <a href="#">Boost Software License</a> .
OpenH264	Copyright © 2013, Cisco Systems. OpenH264 is licensed under this <a href="#">license</a> .
Crypto++	Copyright © 1995-2013 Wei Dai. All rights reserved. Crypto++ is licensed under the <a href="#">Boost Software License</a> .
CxImage	Copyright © 2001-2008 Davide Pizzolato. CxImage is licensed under this <a href="#">license</a> .
FFmpeg	Copyright © 2007 Free Software Foundation, Inc. FFmpeg is licensed under the <a href="#">GNU Lesser General Public License (LGPL) version 2.1</a> or later.
Dapper	Dapper is licensed under the <a href="#">Apache License 2.0</a> .
DirectShowNET Library	Copyright © 1991, 1999 Free Software Foundation, Inc. The DirectShowNET Library is licensed under the <a href="#">GNU Lesser General Public License (LGPL) version 2.1</a> .
excellibrary	The excellibrary is licensed under the <a href="#">GNU Lesser General Public License (LGPL)</a> .

Component	Attribution
gson	Copyright © 2008 Google Inc. google/gson is licensed under the <a href="#">Apache License 2.0</a> .
Jayrock	Copyright © Atif Aziz. All rights reserved. Jayrock is licensed under the <a href="#">GNU Lesser General Public License (LGPL)</a> .
Joda-Time	Copyright © 2002-2018 Joda.org. All Rights Reserved. Joda-Time is licensed under the <a href="#">Apache License 2.0</a> .
libcurl	Copyright © 1996-2018, Daniel Stenberg. All rights reserved. libcurl is licensed under this <a href="#">license</a> .
libjpeg	Copyright © 1991-2018 Thomas G. Lane, Guido Vollbeding.
Live555	Copyright © Live Networks, Inc. All Rights Reserved. Live555 is licensed under the <a href="#">GNU Lesser General Public License (LGPL)</a>
OpenCV	Copyright © 2018 OpenCV team. OpenCV is licensed under this <a href="#">license</a> .
OpenSSL	Copyright © 1998-2018 The OpenSSL Project. All rights reserved. OpenSSL is licensed under this <a href="#">license</a> .
RapidXML	Copyright © 2006, 2007 Marcin Kalicinski. RapidXML is licensed under the <a href="#">Boost Software License</a> .