Corsight for Milestone XProtect

Installation, Setup and User Guide

Product Version: v1.1.2

Date: 04/07/2024

Table of Contents

1 Prerequisites

1.1 Software and Licensing

1.1.1 Microsoft System Requirements

- Microsoft® Windows® 10 Pro and Enterprise (64 bit)
- Microsoft® Windows® 10 Enterprise LTSB 2016 (version 1607 or later)
- Microsoft® Windows® 10 IoT Enterprise, version 1803 or later (64 bit), IoT Core
- Microsoft® Windows® 11 Pro and Enterprise (64 bit)

- Microsoft® Windows® Server 2016 (64 bit): Essentials, Standard and Datacenter
- Microsoft® Windows® Server 2019 (64 bit): Essentials, Standard and Datacenter
- Microsoft® Windows® Server 2022 (64 bit): Essentials, Standard and Datacenter

1.1.2 Milestone XProtect System Requirements

- XProtect Essential+, XProtect Express+, XProtect Professional+, XProtect Expert, XProtect Corporate [2023 R1 (23.1a) or above]

- XProtect Event Server
    - The XProtect Event Server is included as part of your XProtect installation. ***Note*** ***If this component has not been installed with your version follow the steps found in troubleshooting at the end of this document.***

- XProtect Device Licenses applied to your XProtect Base License.
    - Device license is required for each video channel used for XProtect,
    - Any licensed XProtect video channel can be used with the Corsight service.
    - Below figure shows product SKU effective of XProtect 2021-R2.

LICENSES

SKU ID	Name
XPEXPLUSDL	XProtect Express+ Device License (DL)
XPPPLUSDL	XProtect Professional + Device License (DL)
XPETDL	XProtect Expert Device License (DL)
XPCODL	XProtect Corporate Device License (DL)

Open the XProtect Management Client and ensure that you have spare XProtect Device Licenses associated with the installed XProtect version before the installation of a ORBNET software trial.

1.1.3 ORBNET Systems

Part of this installation will include the Streaming Engine plugin for XProtect. This enables video feeds from XProtect to be shared with the Corsight AI service. There are license requirements for this product.

- License – When you first install the Streaming Engine you will get a 30-day trial license, following this you will need to update to a full license. Corsight will provide this license, subject to the payment terms and conditions that Corsight and the customer have agreed upon.

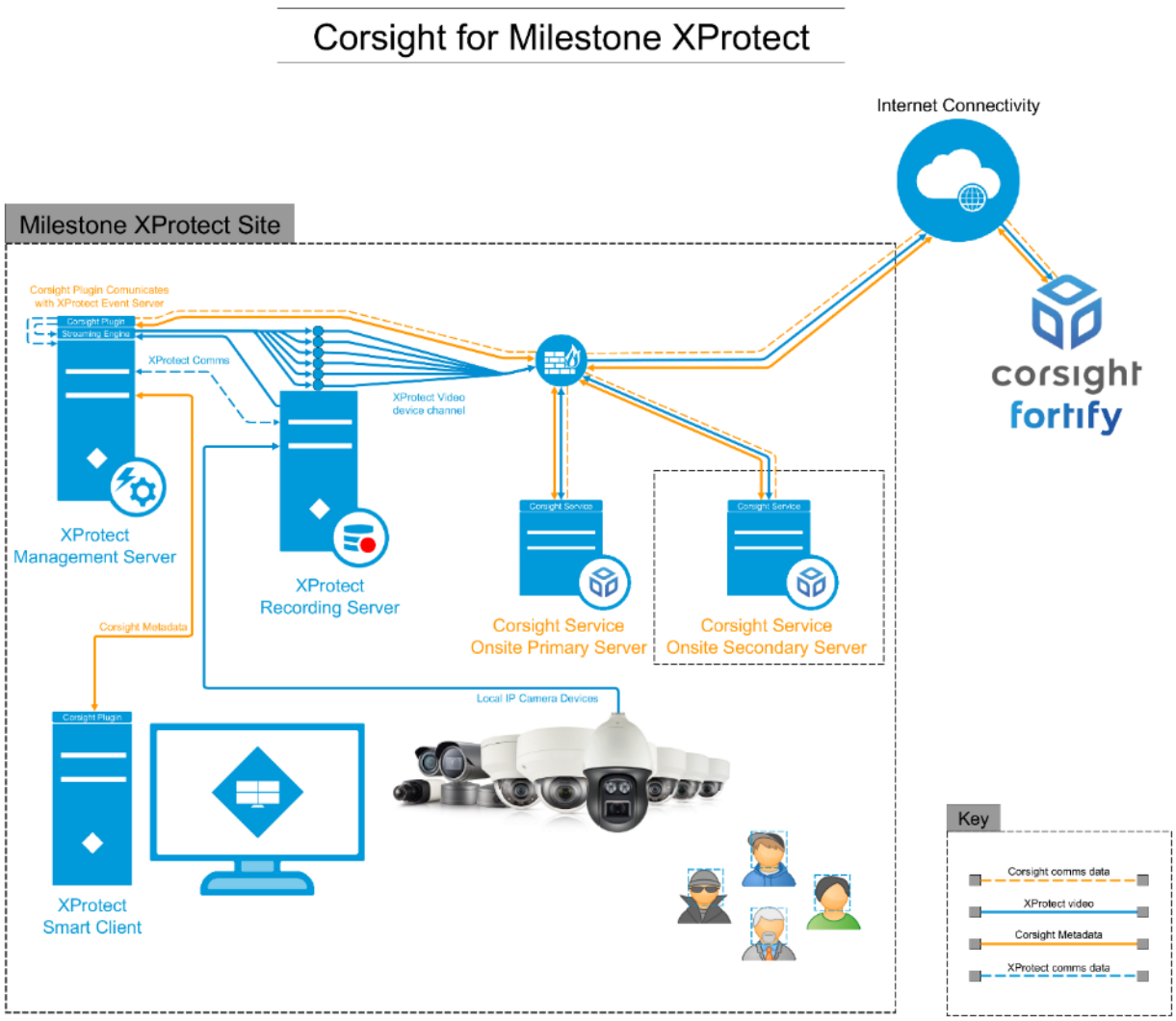
1.1.4 Corsight Service Requirements

- Corsight AI Service installed on local or hosted server.
    - Single server or multi-server

- Installers – Available to download from Corsight Partner Portal.
    - `'Corsight XProtect Plugins Installer v*.*.* EN.msi'`
    - `'ORBNET Streaming Engine Service Setup v*.*.* EN.msi'`
    - `'ORBNET Streaming Engine Plugins Setup v*.*.* EN.msi'`

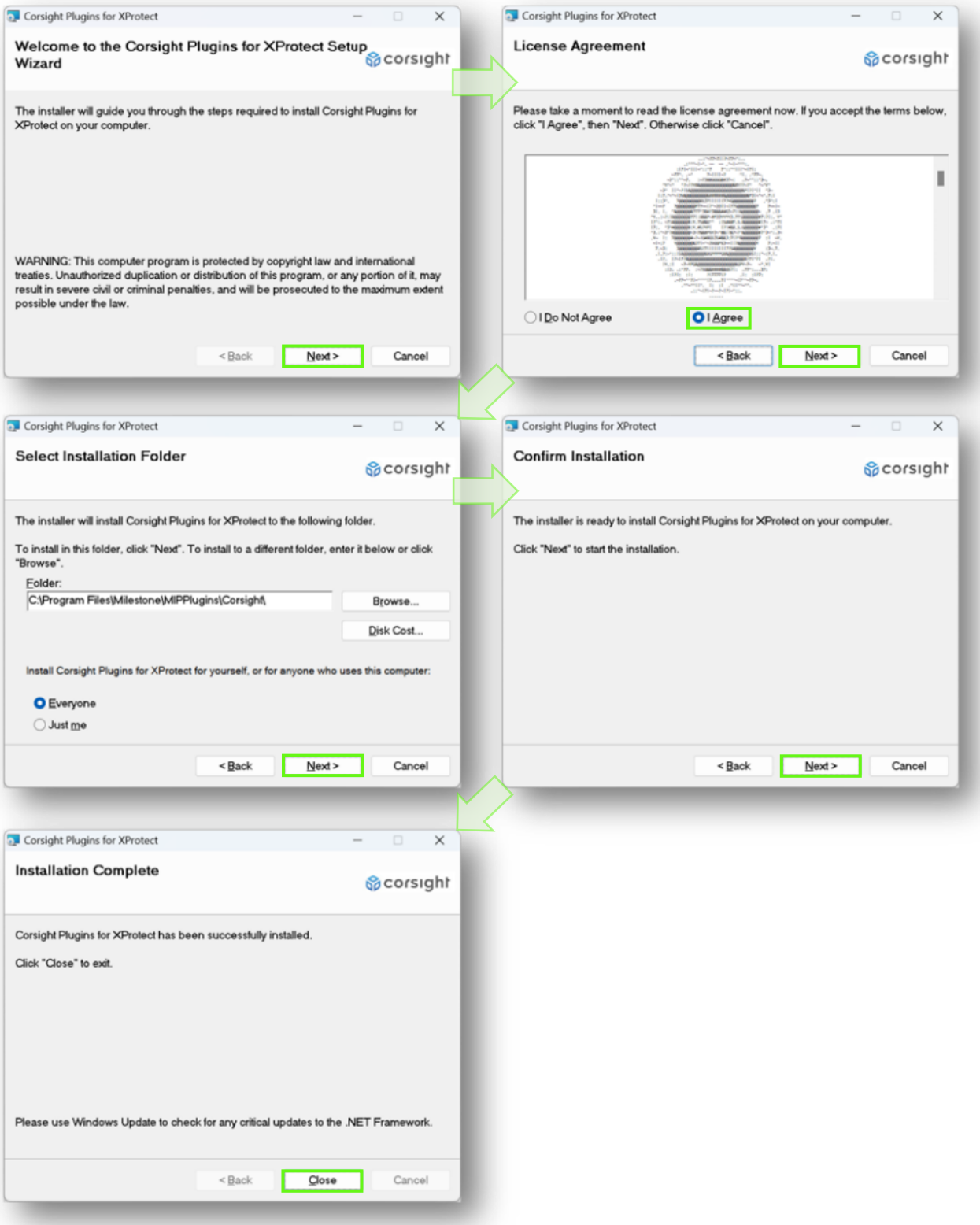
1.1.5 Copyright, trademarks, and disclaimer

2 Software Schematic with Installation Example

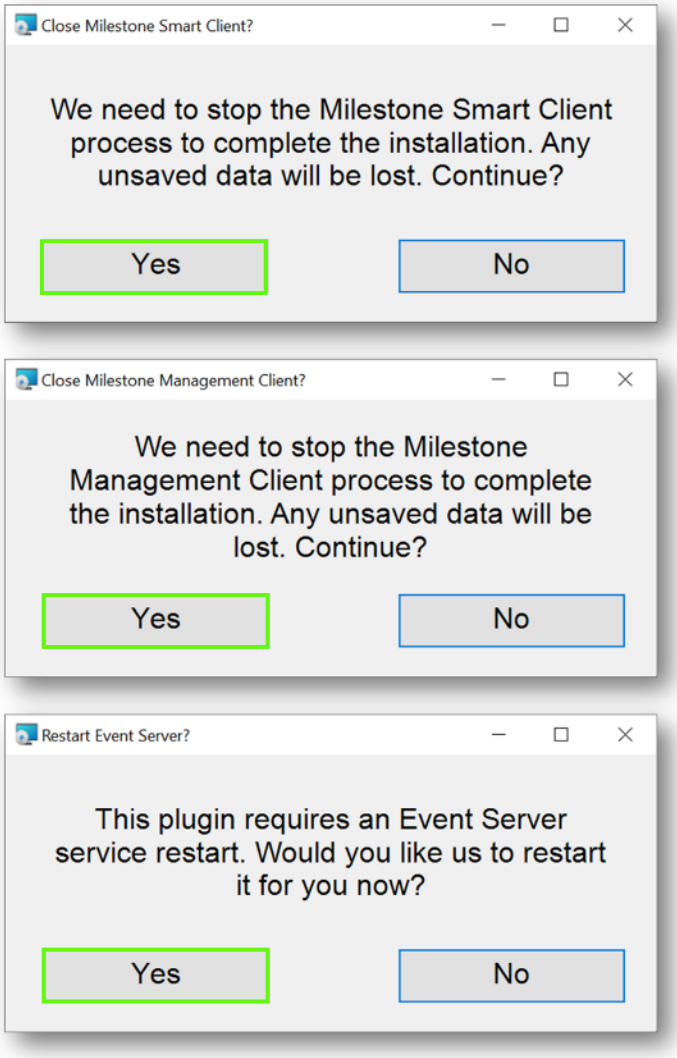


3 Installation of Corsight plugin for XProtect

Begin with the server/machine running the XProtect Management Server. Place the **'Corsight Plugin for XProtect Installer.msi'** in a folder on the desktop and double click to start the Install. The installer will prompt you to stop the XProtect Event Server service before installing.



It is possible some of these messages will show during the installation. Press **Yes** to close or restart the required installation dependant to complete the installation.

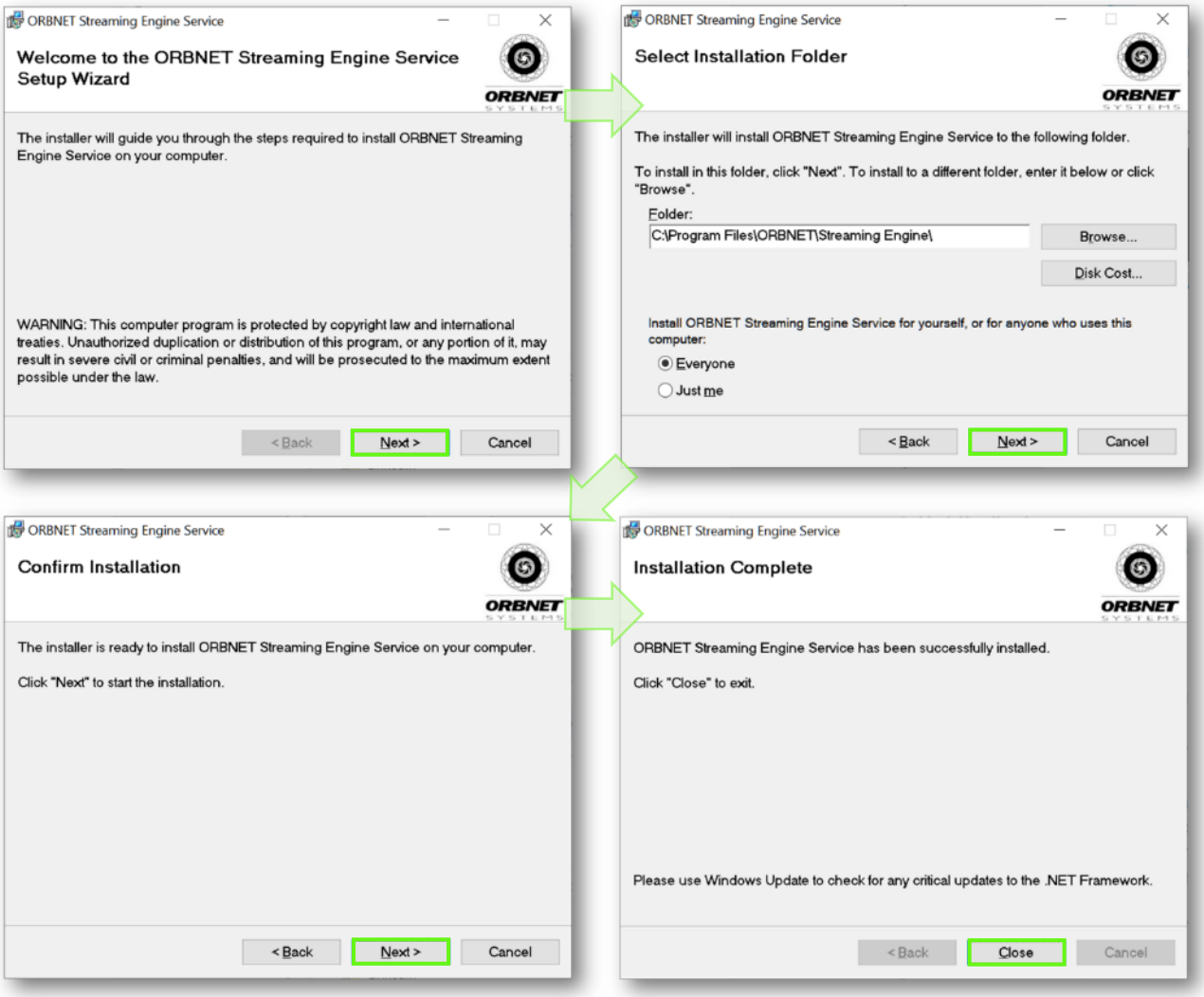


Follow the XProtect Management Server installation with any client machines that will be used for Corsight management. Both XProtect Management Clients and XProtect Smart Clients need this plugin installed. This one installer is used for both clients and servers.

4 Installation of Streaming Engine for XProtect

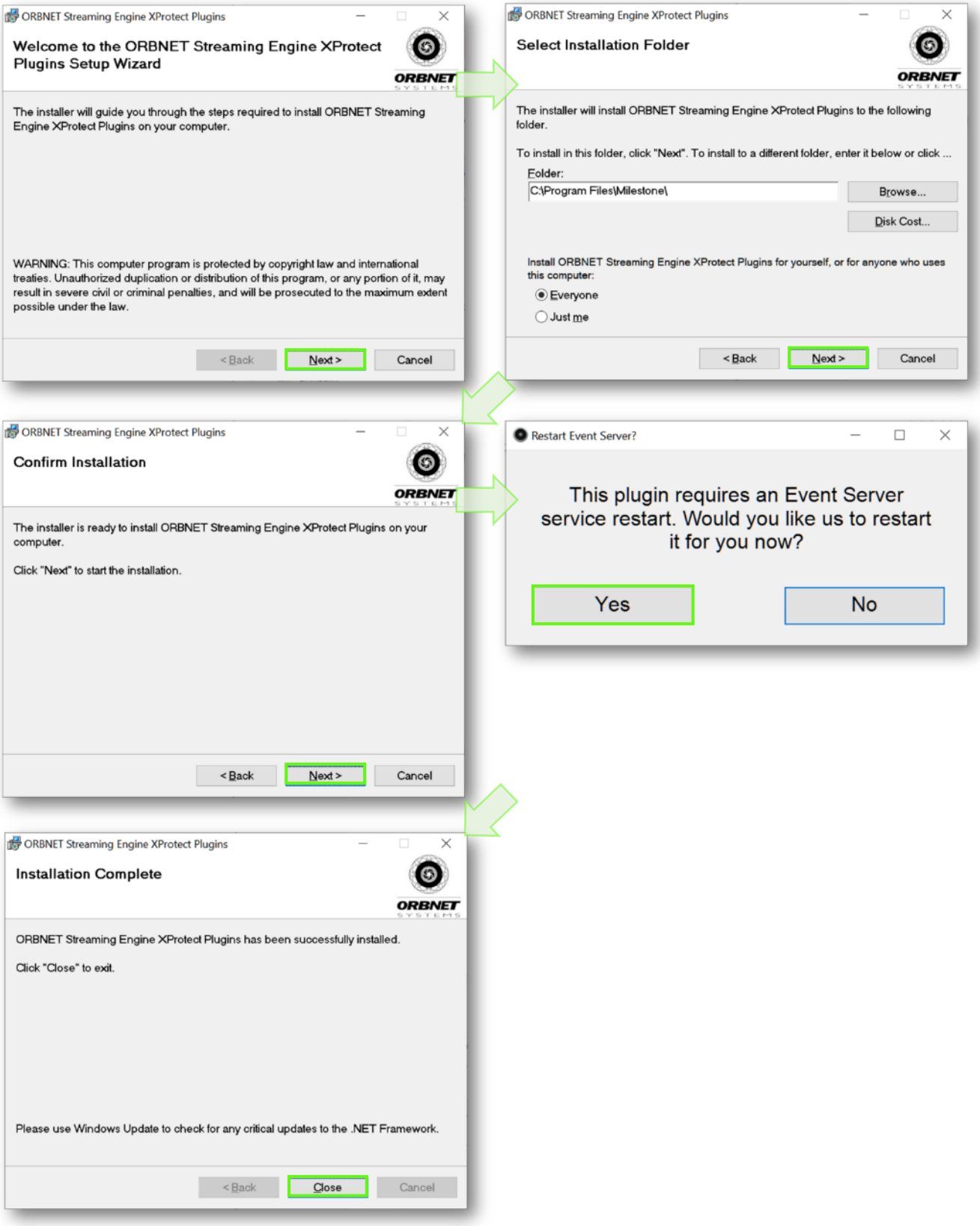
Begin with the server/machine running the Milestone XProtect Management, Event services and any machines with a Management Client that will need access to Streaming Engine settings.

Run the '`ORBNET Streaming Engine Service Setup.msi`'



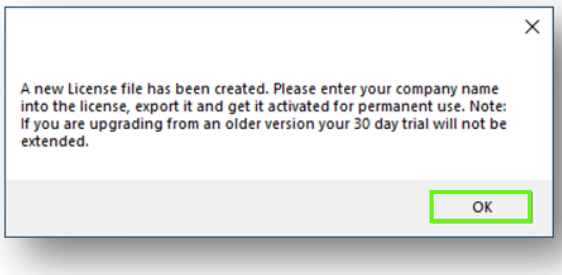
Follow with the server/machine selected to be used for the Streaming Engine service.

Run the '`ORBNET Streaming Engine Plugins Setup.msi`'



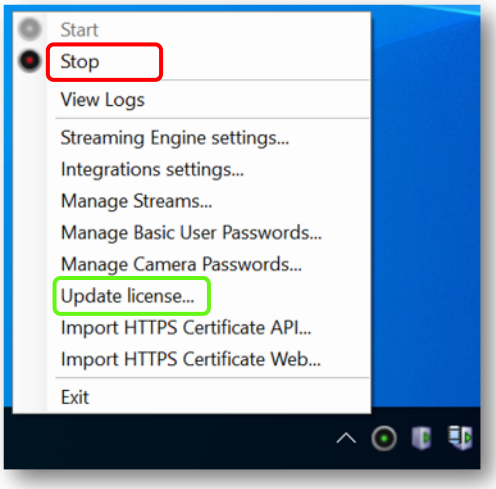
4.1 License Activation

When you first install the Streaming Engine, you will get a 30-day trial license, following this you will need to update to a full license. Corsight will provide this license, subject to the payment terms and conditions that Corsight and the customer have agreed upon.

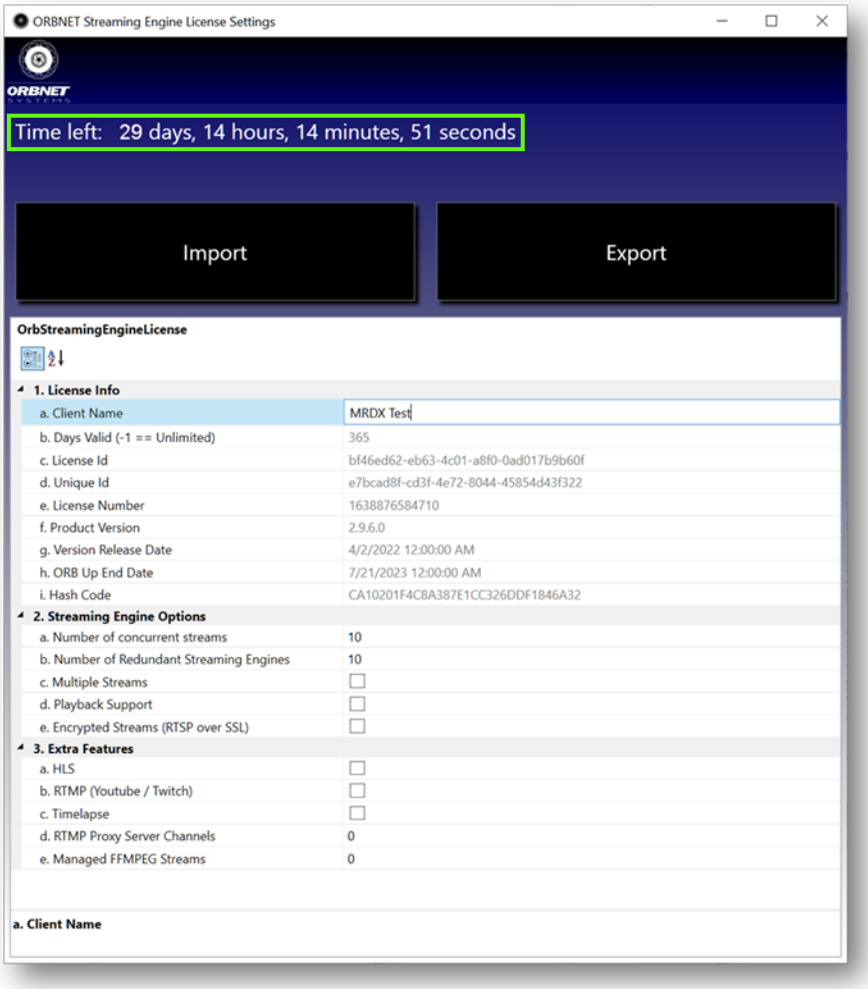


The Streaming Engine License information can be accessed from the Streaming Engine system tray icon. `Stop` the Streaming Engine service first.

Then right click again and you can then select `Update license`…



This window will initially show the default license values with just the trial license countdown at the top.



Use `Import` and `Export` buttons for license requests and software activation.

When making a license request, please complete the fields in bold.

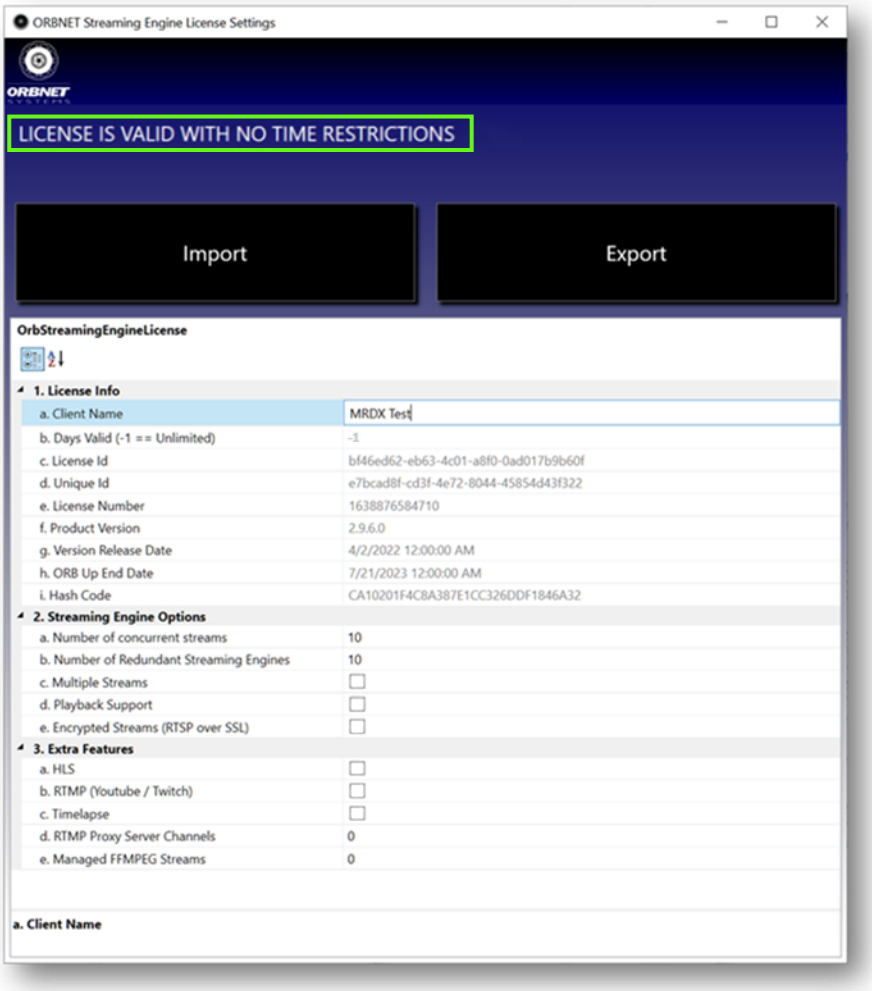
- 1. License Info
  - Enter the Client Name

- 2. Streaming Engine Options
  - Increment the values of the options and disable all checkboxes
    Number of concurrent streams

- 3. Extra Features
  - Increment the values of the options and enable the required checkboxes
    None required

Use the `Export` license request button to generate a license request file. This will be required to be included in an email to Corsight when requesting your activated product license.

On completion of an order alongside a license request file a valid license will be sent back. This can be imported by using the `Import` valid license button.
This will now show an unlimited (Days Valid = -1) time frame associated to the Streaming Engine instance at the top.



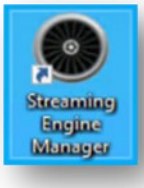
4.2 Initial connection to XProtect

Ensure you have either have a XProtect Basic User account created or a Windows service account ready and assigned to a Security Role in XProtect to be used for the Streaming Engine service.

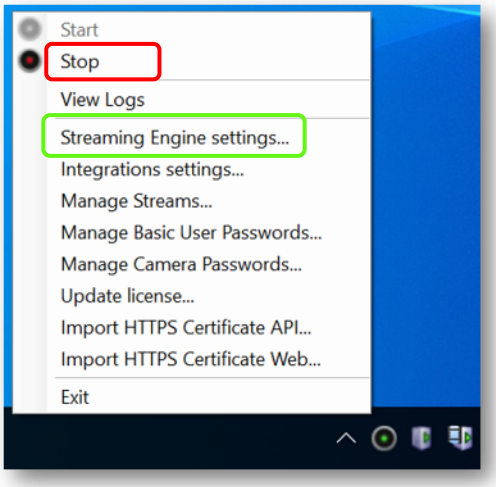
See **Basic User Setup** or **Changing a service account**

After installation, the Streaming Engine service will not be connected to the XProtect system.

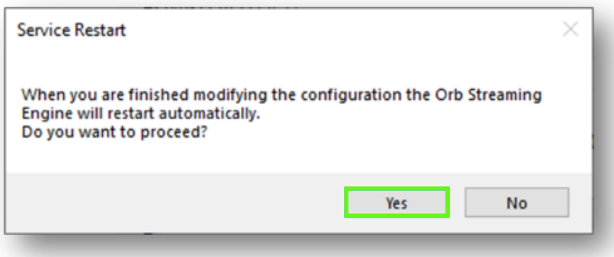
The Streaming Engine Manager will show in the system tray a red cross to indicate a problem. If the task icon is not showing, check that it is not hidden in the system tray or run from the desktop shortcut.



`Right click` the tray icon and select `Stop`, then `right click` again, and select `Change settings`…



Service Restart confirmation, Click `Yes`



From Streaming Engine Settings two XProtect user options are available.

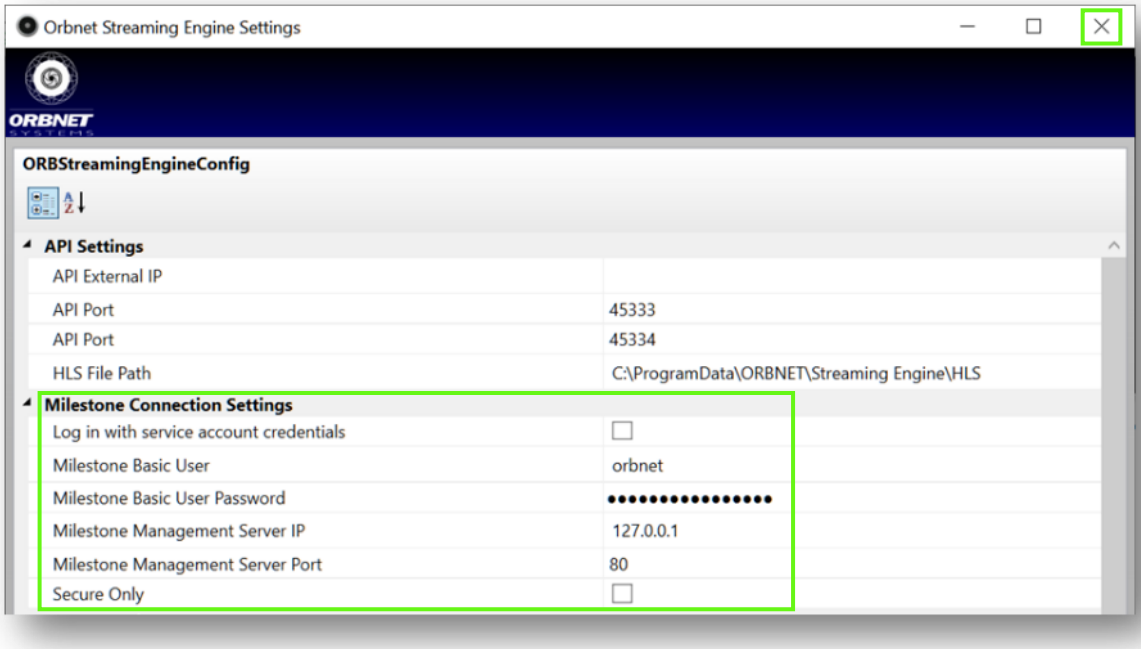
1. Log in with service account credentials

[Uses the windows account that is running the "ORBNET Streaming Engine" service to login to XProtect. If set to true, you must change the service user from "Network Service" to a domain service account of your choosing and add the service account to XProtect Security Roles.]

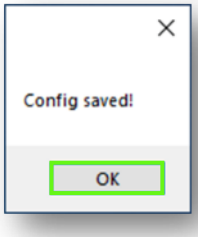
2. XProtect Basic User

[This is a uses a XProtect created basic user account, the account needs to be added to a relevant XProtect Security Role. Only works if "Log in with service account" is set to false.]

- Fill out the correct XProtect Management Server IP address and port.
- Tick Secure Only if you have installed XProtect using an SSL certificate on the XProtect Management Server.



Finish your configuration changes then exit with the close window `cross` at the top right of this window. You will get a message "`Config saved!`". Check that the Streaming Engine service is started from the system tray icon.

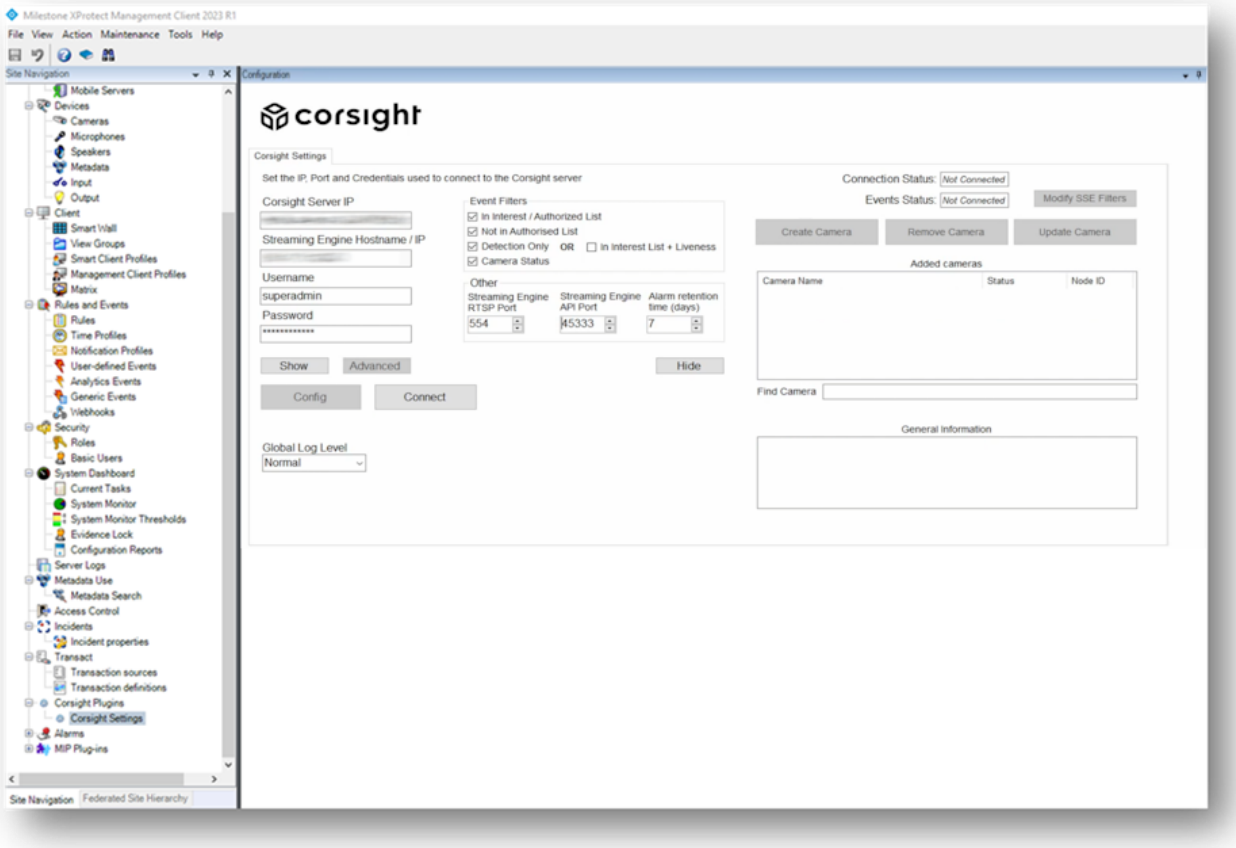


5 Configuration

5.1 XProtect Management Client

5.1.1 Connect Corsight device

From the Site Navigation window select `Corsight Plugins` then `Corsight Settings`.



5.1.2 Corsight Settings

From this window Set the IP, Port and Credentials used to connect to the Corsight Server.

- **Corsight Settings**
  - Corsight Server IP – IP address or hostname of your local or hosted Corsight Server
  - Streaming Engine Hostname/ IP – External IP address for Streaming Engine
  - Username – This is for the Corsight Server
  - Password – This is for the Corsight Server

Modify SSE Filter (Press button to display these settings)

Using this option means it is possible to update the filter settings without closing the connection to the Corsight AI service.

- **Corsight SSE Event Filters** (Server-Sent Events allows servers to push real-time client updates over a single HTTP connection.)
  - In Interest / Authorized List
  - Not in Authorized List
  - Detection Only **OR** In Interest List + Liveness
  - Camera Status

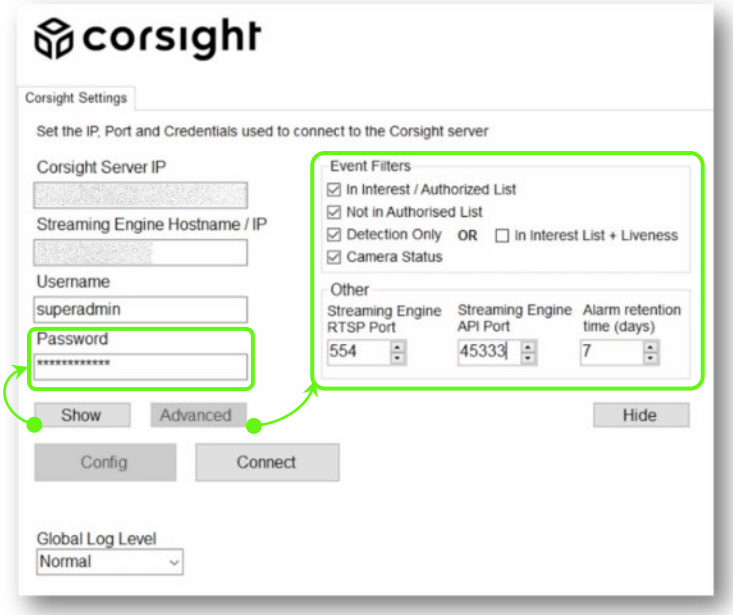
These options are used in the XProtect Smart Client to show or hide the default filter options for Corsight AI events. How the filters are shown in the XProtect Smart Client is directly synchronize with the setting changed here.

Advanced (Press button to display these settings)

- **Other**
  - Streaming Engine RTSP Port – Default: 554
  - Streaming Engine API Port – Default: 45333
  - Alarm retention time (days) – Number of days after which old alarms will no longer display in the “Alarms” Section of the plugin in Smart Client

The Streaming Engine is a third-party application provided by ORBNET Systems. This is used to stream video from XProtect to the Corsight AI service.

NEW for v1.1.2, more information is provided in
Debug logs to assist with any required troubleshooting.



Show – Show or hide the password in clear text.

Advanced – Show or hide ports config

Config – Once connected the configuration is greyed and not editable. Press `Config` to make changes. This will also disconnect from the Corsight Service plus client users.

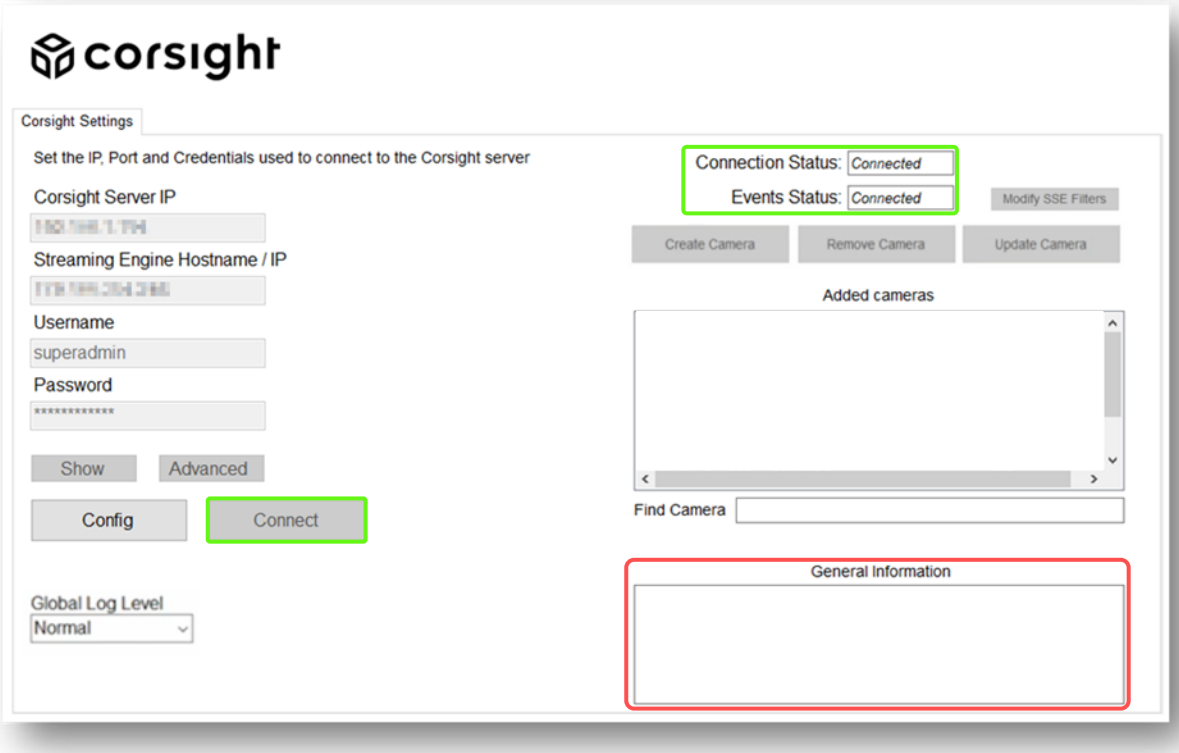
Connect – Once the Corsight Server settings are filled out, press the Save icon (top left) and then `Connect` to make the first connection.

Global Log Level – Change log level if asked by support for troubleshooting. `Normal, Debug, Trace`

Hide – Remove the config and filter menu from being visible.

Corsight Connection

With the Corsight settings filled press **Save** in the top toolbar first then **Connect**. The Connection Status and Event Status will update to show if the service is Connected. If the Connection Status remains as Not Connected. Further information will be shown in General information.

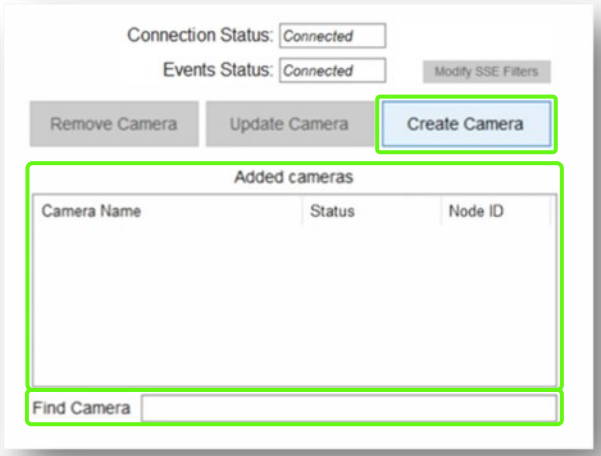


General Information – This section will provide text-based information on the status of connections to the Corsight service. Use this to troubleshoot if connections are not working.

5.1.3 Corsight add XProtect video camera

In this side of the Corsight menu, XProtect Cameras can be added to the Corsight service.

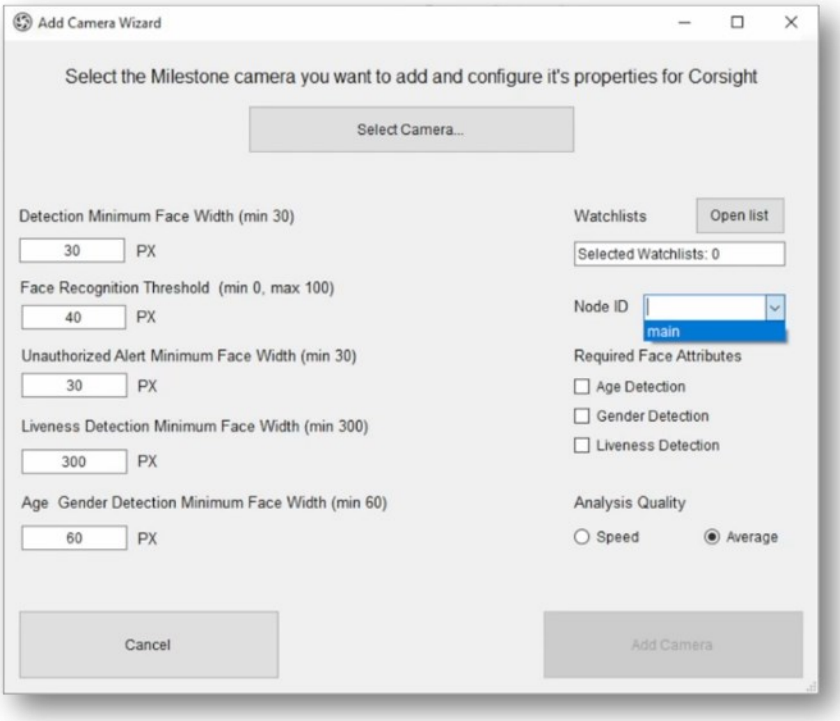
To add a video camera from XProtect to the Corsight service press `Create Camera`.



Added cameras – Once added cameras show in this list along with the Corsight AI processing status.

Find Camera – Use this to search list by Camera Name, input text to start a search.

Next a pop-up window. Add Camera Wizard will be shown, where a camera, watchlist and other Corsight settings can be updated. First use Select Camera



Select Camera... – Press to open camera picker.

Watchlists – Press `Open list` to select the relevant Watchlist/s.

Selected Watchlists number will update based number of watchlist selected.

Node ID - Additional processing nodes will show here. Select the one to be used.

Face Attributes – Use the tick boxes to select detection types.

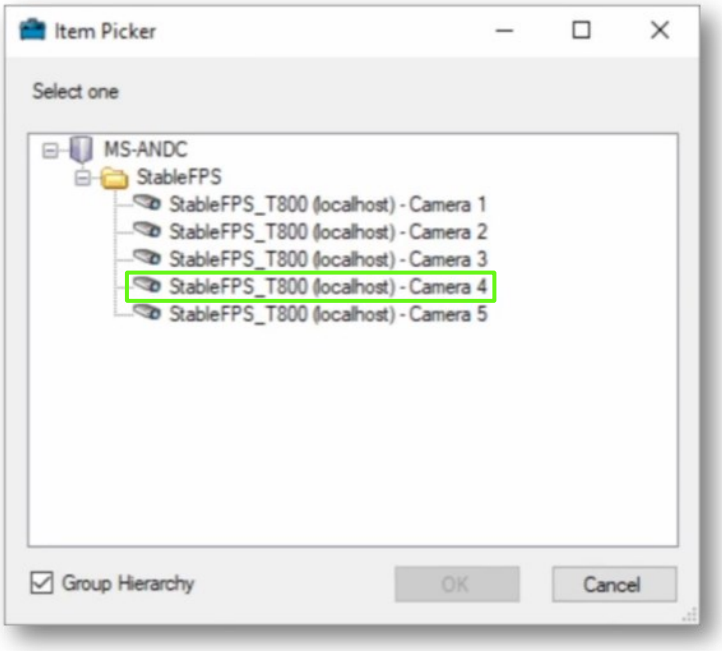
Analysis Quality – Select `Speed` or `Average` detection mode.

Corsight Pixel Thresholds – Set the pixel thresholds for each detection mode.

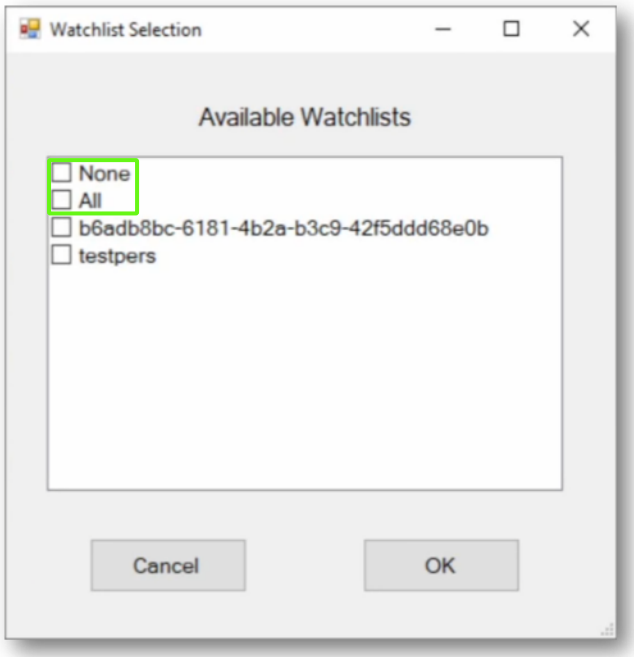
Cancel – Close this window.

Add Camera – Add to Corsight

From `Select Camera`… the Camera Item Picker will show. Pick the relevant camera to be added to the Corsight service.



From `Open list` the Watchlist Selection window will be shown. `Tick` one or many options for the relevant camera that is being added.



None – Default Watchlist helper option. This will untick all other selected watchlists.

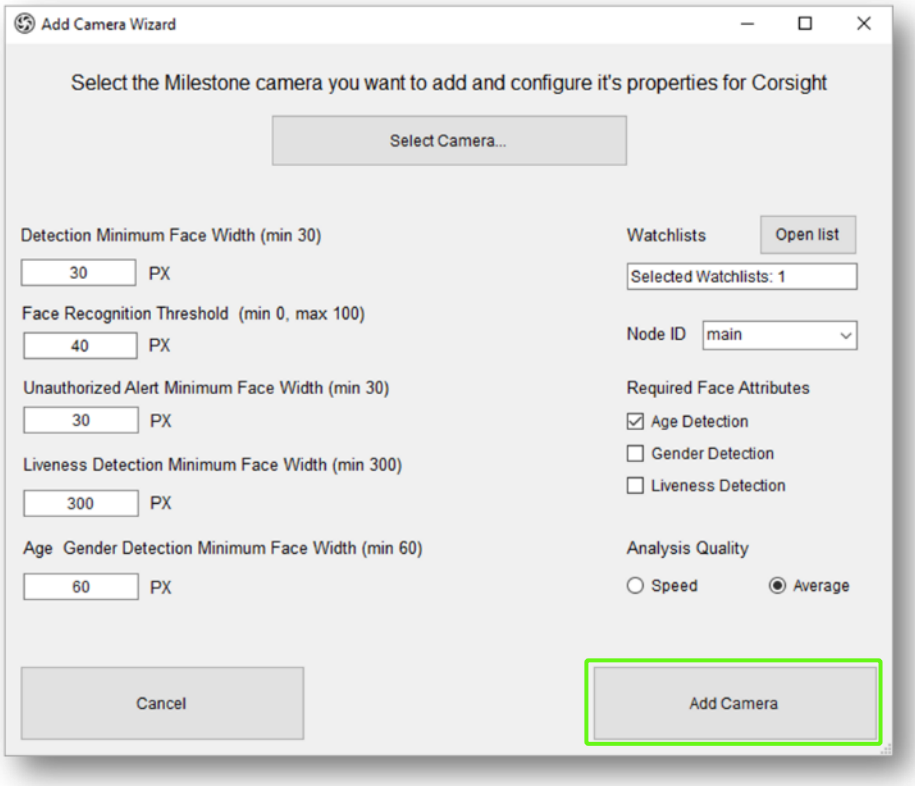
All - Default Watchlist helper option. This will tick all other unselected watchlists.

Other Named Watchlists options are shown below None and All. These are user defined watchlist.

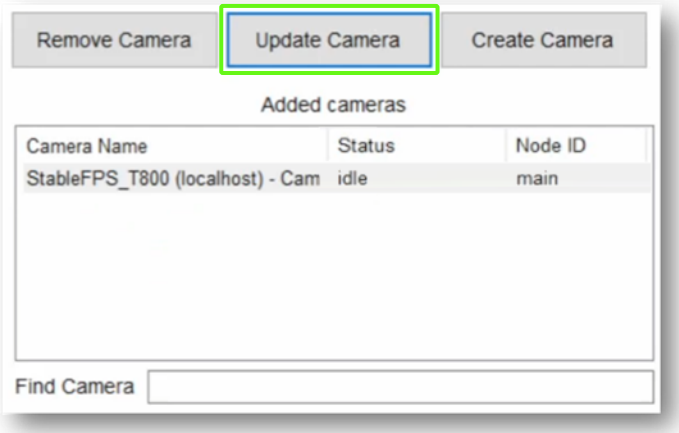
Run a final check of the settings for this window "Add Camera Wizard". Check all of these elements have been selected or updated.

1. Camera
2. Watchlist (If required)
3. Node ID
4. Detection mode (If required)
5. Corsight Pixel Thresholds

Now the XProtect camera can be added with the `Add Camera` button.



Once added the camera appears in Added cameras list with its Corsight status alongside.



Remove Camera – Remove the selected camera.

Update Camera – Press to open the Add Camera Wizard to edit settings.

Create Camera – Use to add new camera to Corsight service.

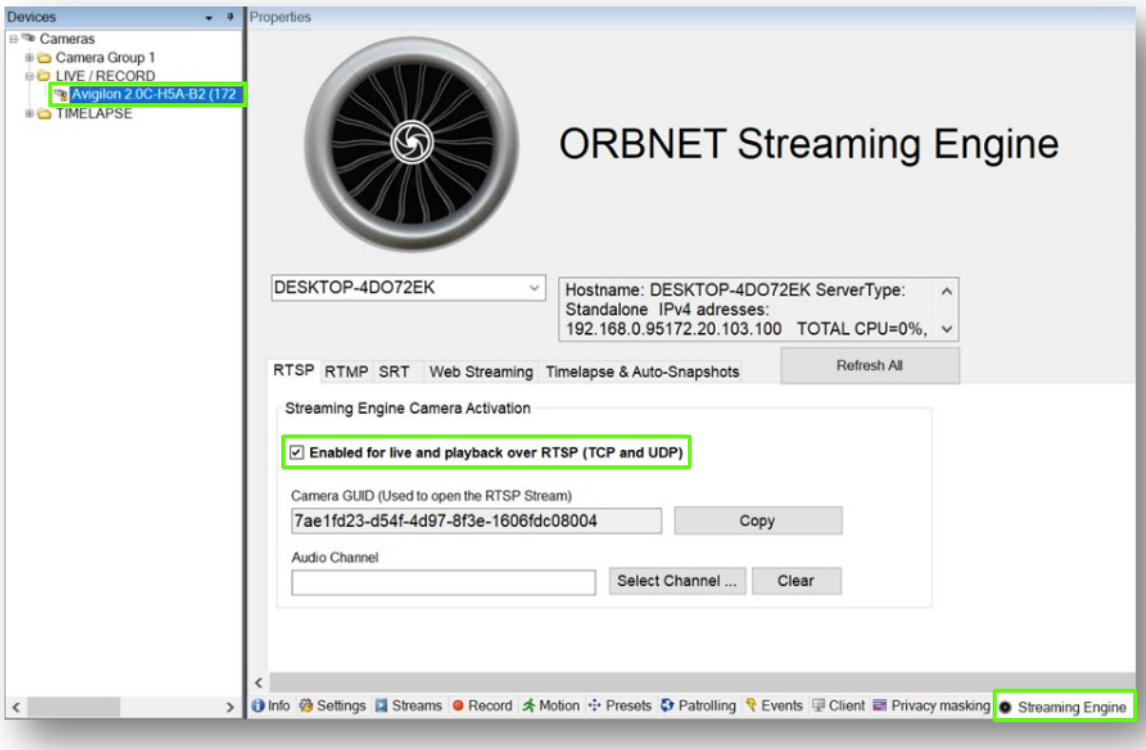
Find Camera - Use this to search list by Camera Name, input text to start a search.

5.1.4 Streaming Engine Integration

The Streaming Engine (made by ORBNET Systems) provides a method of streaming XProtect video to the Corsight Service.

Any of the devices added to the Corsight camera list will also need to have streaming enabled to be sent to the Corsight AI Service.

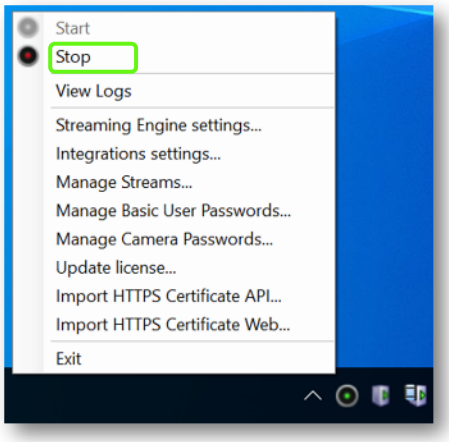
From the XProtect Management Client `go to` Site Navigation `select` Devices, Cameras. Find any camera devices used with the Corsight AI Service. `Go to` the Streaming Engine tab and `tick` Enable for live and playback over RTSP (TCP and UPD).



5.1.4.1 Enable All XProtect video streams for RTSP

For sites with a high number of camera devices used with the Corsight Service from XProtect. Instead of manually needing to go into each device and enable the RTSP stream in the Streaming Engine tab, there is an enable all option in the Streaming Engine configuration.

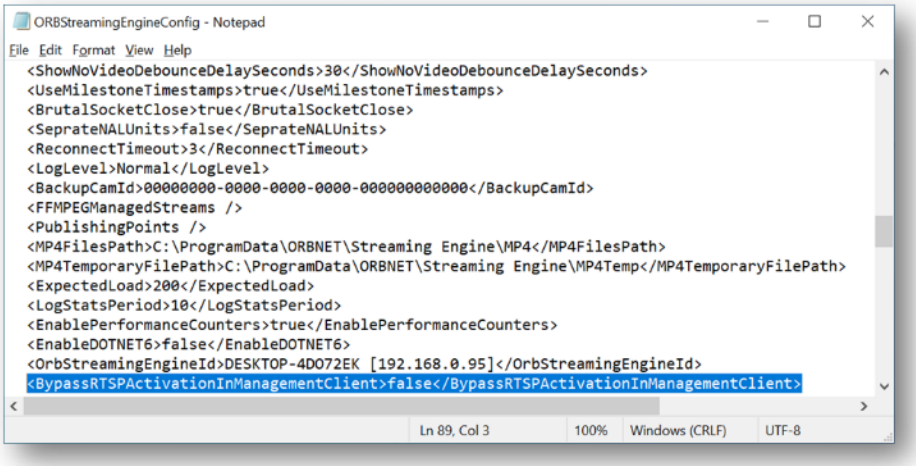
`Right click` the tray icon and select `Stop` to stop the Streaming Engine Service.



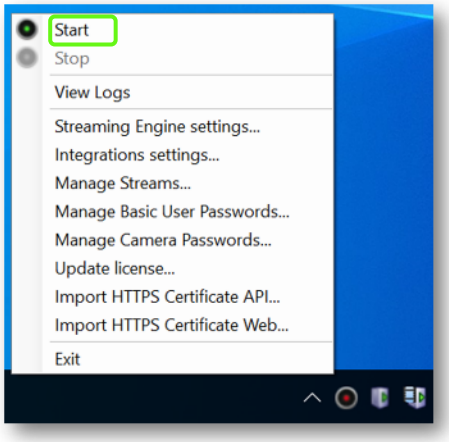
Navigate to `C:\ProgramData\ORBNET\Streaming Engine\` and open `ORBStreamingEngineConfig.xml` with Notepad.

Find the line with `<BypassRTSPActivationInManagementClient>`

Update from `false` to `true` and save this file.



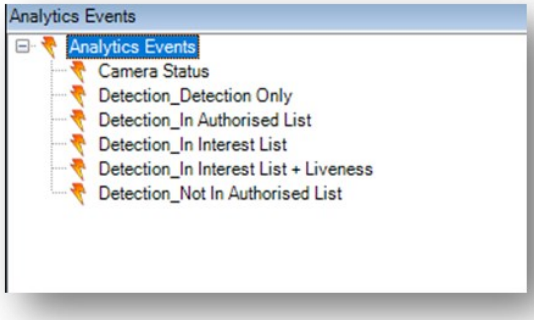
`Restart` the Streaming Engine from the system tray icon.



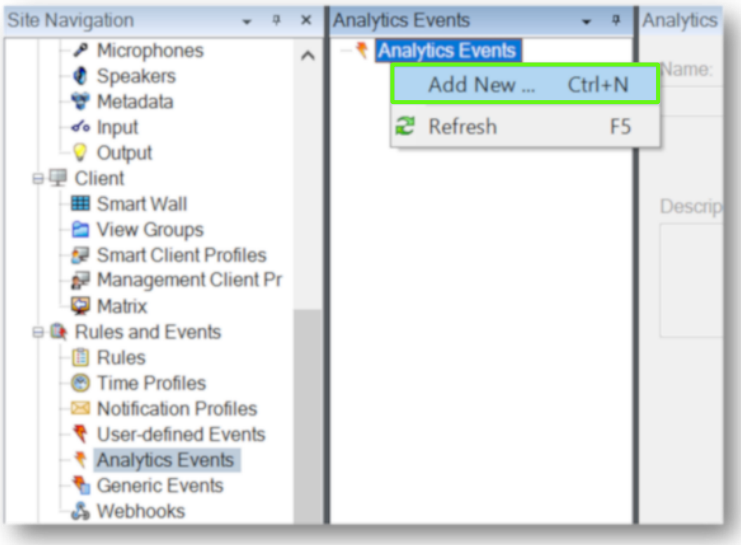
5.1.5 XProtect Analytics Events

From the XProtect Management Client Analytics Events need to be created manually to bring Corsight Service Events into XProtect. This plugin listens for these events that will use the below text and associated video device to trigger an event.

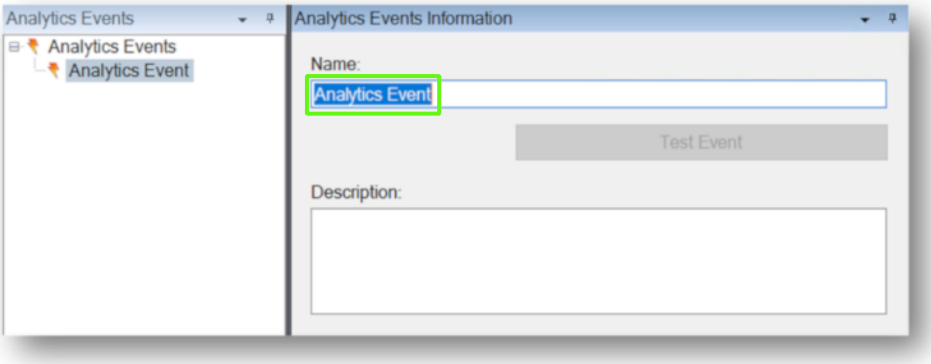
These events need to be created **exactly** as shown with capitals and underscores where shown. Otherwise, the event will not be triggered in XProtect.

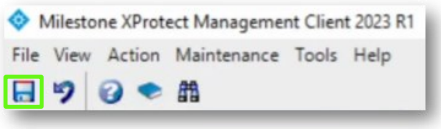


XProtect Management Client under Site Navigation find `Rules and Events` > `Analytics Events`. `Right click` Analytics Events and click `Add New`...



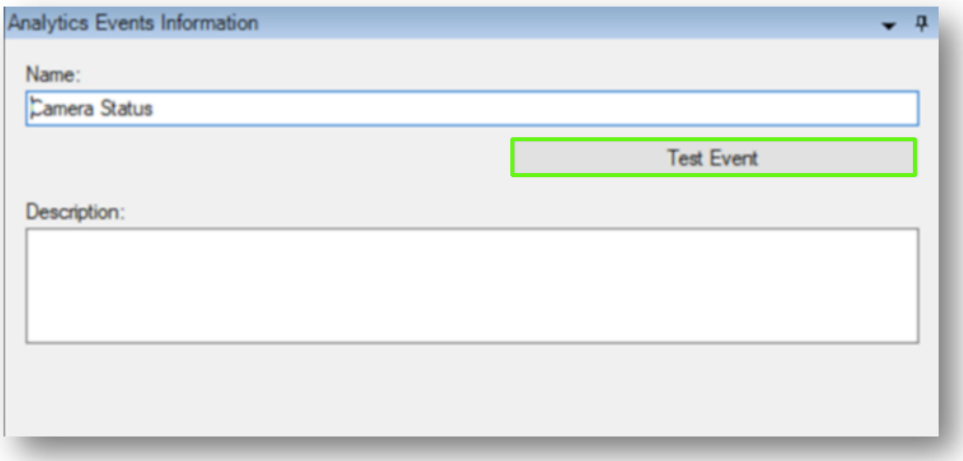
Copy the Analytics Event Name exactly as shown below. Once the Name is added use the toolbar `Save` button to confirm.






```
Camera Status
Detection_Detection Only
Detection_In Authorised List
Detection_In Interest List
Detection_In Interest List + Liveness
Detection_Not In Authorised List
```

After saving the Test Event button is now available, used this to confirm Rules and Alarms are working in XProtect. The next steps in this manual will go through Rules and Alarms.



5.1.6 Rules and Events Setup

5.1.6.1 Events

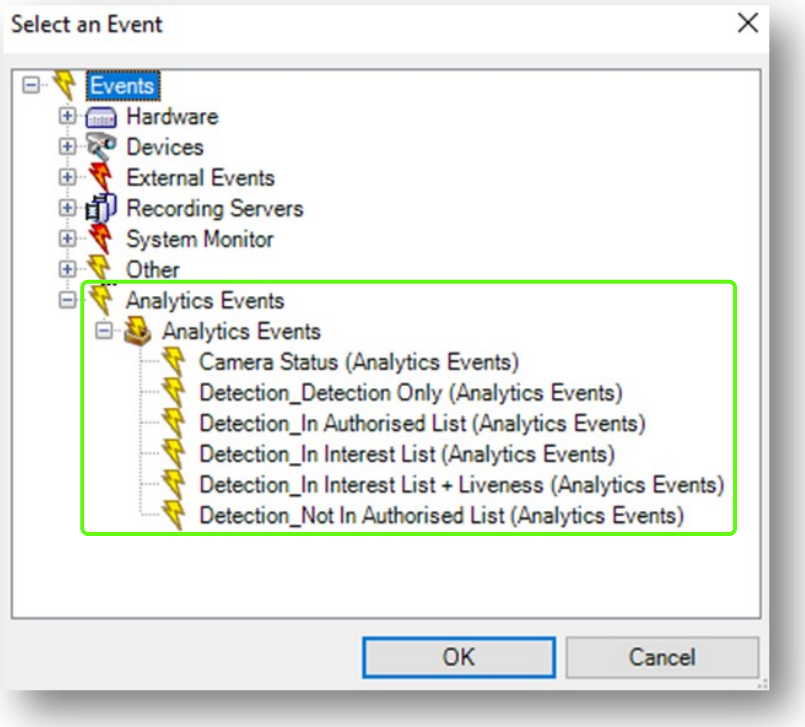
With the Analytics Events created they can now be used for Rules in XProtect.

XProtect Management Client under Site Navigation find `Rules and Events` > `Rules`.

`Right click` Rules and click `Add Rule`…

Use Perform an action on `event` then select the relevant Analytics Event. Refer to 5.1.6 XProtect Analytics Events for more information.

For `device/recording server/management server` select the relevant video device this Rule is related to.



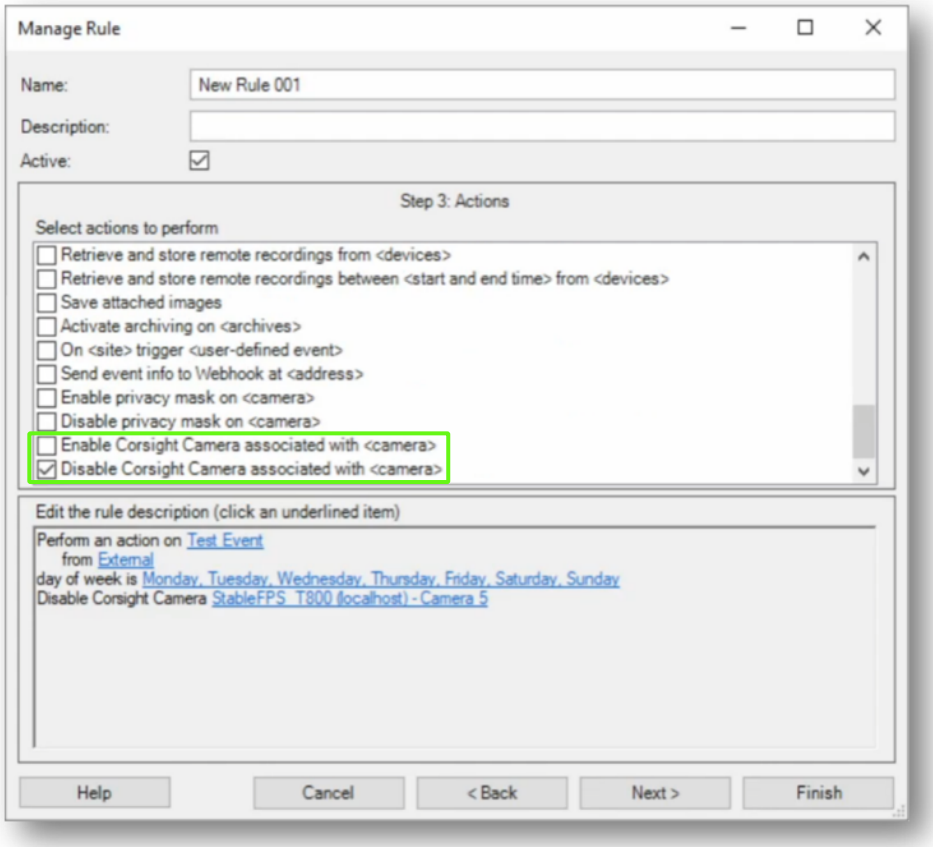
5.1.6.2 Actions

Actions that can be triggered from a Rule.

- Enable Corsight Camera associated with `<camera>`
- Disable Corsight Camera associated with `<camera>`

These actions enable or disable the Corsight service on the selected device. In a rule an Event of a Time Profile can be used to trigger this.

Use a time profile to enable Corsight service only in office hours for internal cameras.



5.1.7 Alarm Definitions

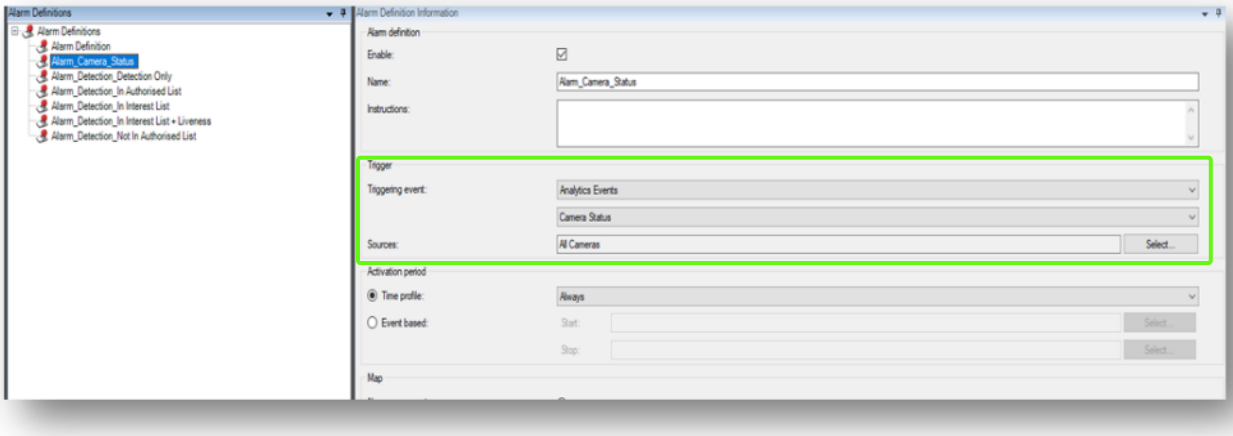
With the Analytics Events created they can now be used for Alarms in XProtect.

XProtect Management Client under Site Navigation find `Alarms` > `Alarm Definitions`.

`Right click` Alarm Definitions and click `Add New` …

For the Triggering Event use `Analytic Events` then select the relevant Event that is in the list that follows. Refer to 4.1.6 XProtect Analytics Events for more information.

For Sources select the relevant video device/s this Alarm is related to.



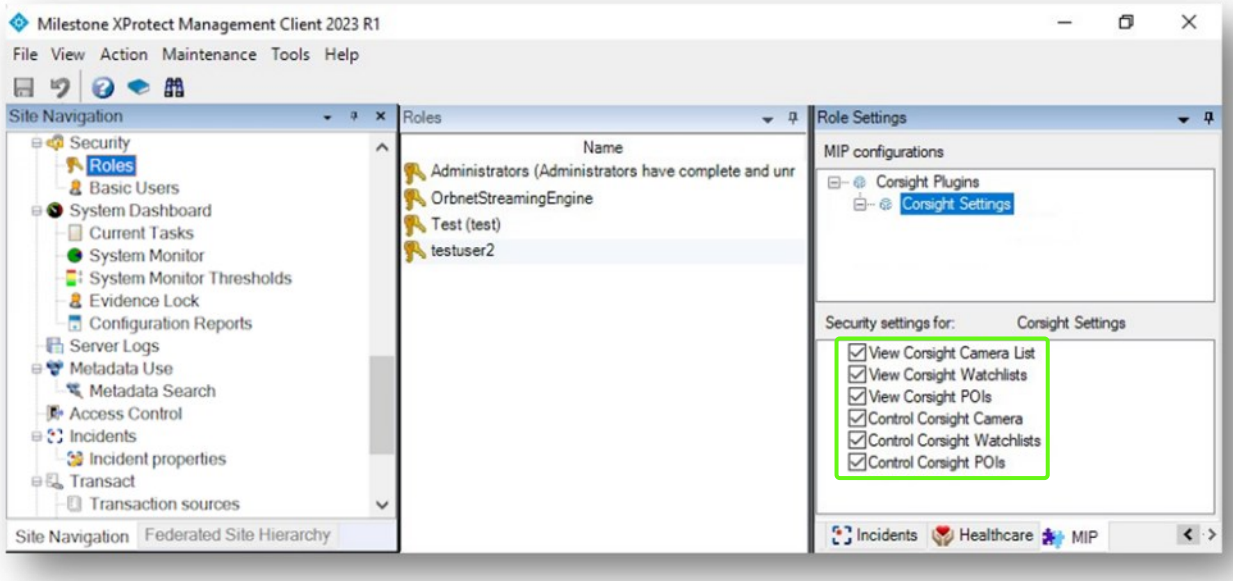
5.1.8 User Security Management

It is possible to add or remove security rights to the Corsight Plugin in Roles

XProtect Management Client under Site Navigation find `Security` > `Roles`.

`Select` the relevant Role you wish to update. Navigate to the `MIP` tab, then to `Corsight Plugin` > `Corsight Settings`.

There are security settings available for View and Control of the Corsight Camera List, Watchlist and POI.



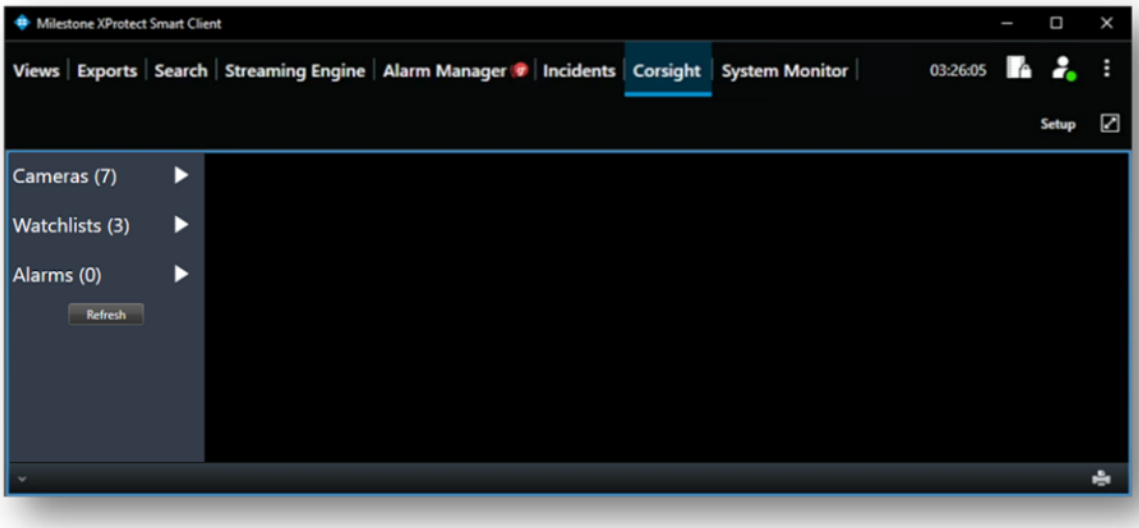
6 User Guide

6.1 XProtect Smart Client

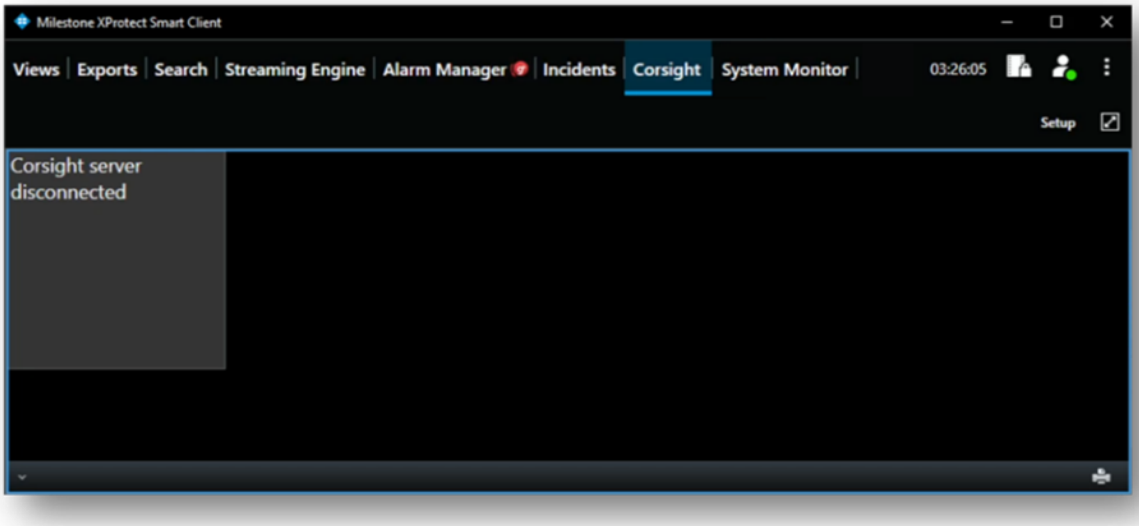
6.1.1 Corsight Plugin Tab

From the XProtect Smart Client select the `Corsight` Tab. Below shows the default layout when first opened.

- Cameras – Shows list of cameras connected to Corsight Service
- Watchlists – Shows Corsight Service Watchlists
- Alarms – Shows Corsight Service Alarms

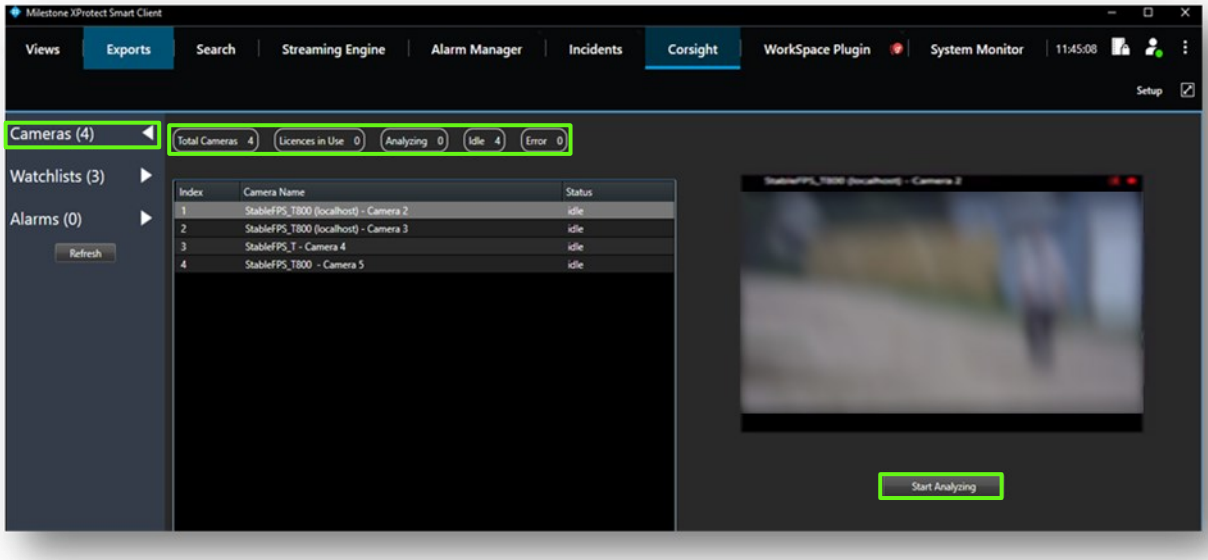


If not connected to the Corsight Service, the Corsight Plugin tab will show the below screen.



6.1.1.1 Cameras

Select `Cameras`, then select a camera from the list. The live camera image will display for this device.



Corsight Server Displayed Counts (Shown above Camera List)

Total Cameras – Total number of cameras connected to Corsight Service
Licenses in Use – Number of Corsight Service licenses in use
Analyzing – Number of XProtect video channels being analyzed
Idle – Number of XProtect video channels ready for processing
Error – Number of devices not working with Corsight Service

Corsight Camera Table

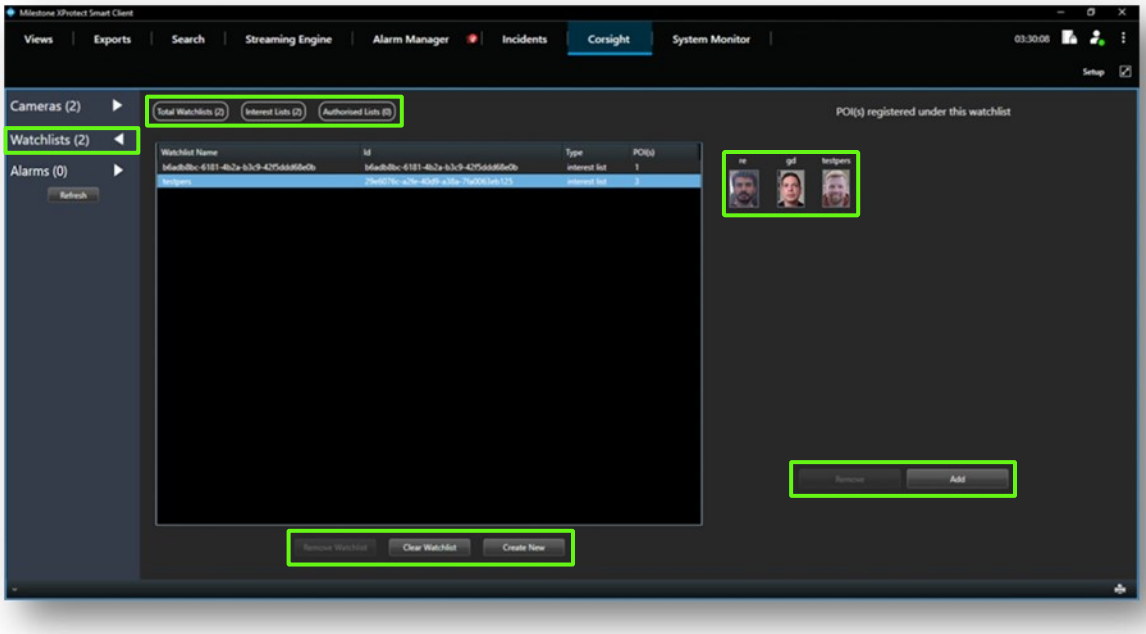
Camera Name - Camera Name as it is in XProtect.
Status - Current camera state (**idle**, **active**).

Live video display (Shown below video tile)

Start Analyzing – Start Corsight Service processing.
Stop Analyzing – Stop Corsight Service processing.

6.1.1.2 Watchlists

Select `Watchlists`, then select a watchlist from the list shown. The POI(s) included in the list will display on the right-hand side.



Corsight Server Displayed Counts (Shown above Watchlists)

Total Watchlist – Total number of Watchlists assigned to Corsight Server.
Interest List – Number of Watchlists related to Unauthorised Persons of Interest (deny list).
Authorised List – Number of Watchlists related to Authorised Persons of Interest (allow list).

Corsight Camera Table

Watchlist Name - Watchlist Name as in Corsight.
id - Watchlist ID as in Corsight.
Type - Watchlist type (**Interest**, **Authorised**).
POI(s) - Person of Interest, total number in Watchlist.

Watchlist action buttons (Shown below Watchlist)

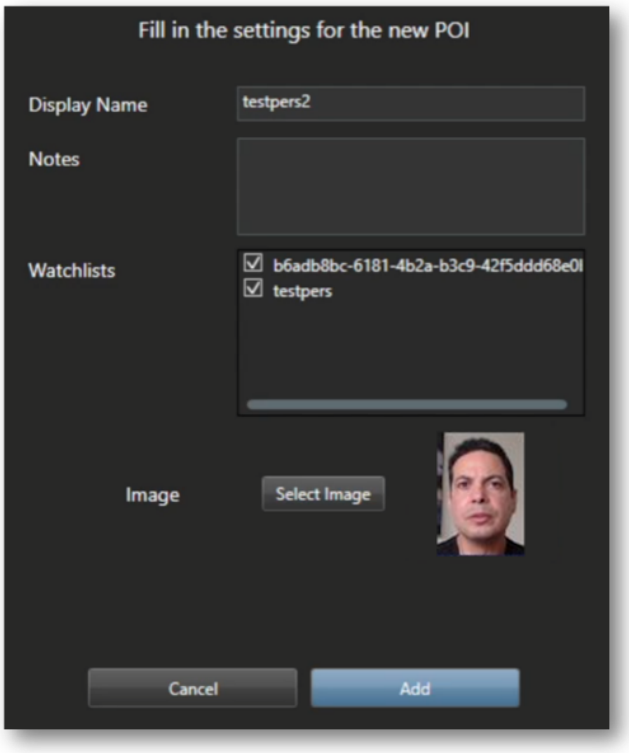
Remove Watchlist – Press to remove selected Watchlist. Available only if no POI(s) are registered.
Clear Watchlist – Press to remove all POI(s) from Watchlist.
(Confirmation will be requested, followed by if you wish to also remove POI(s) from the database)
Create New – Press to create a new Watchlist.

POI(s) registered under this watchlist

Shows each POI with the defined name and thumbnail.

Remove – Press to remove selected POI from list.
Add – Press to add new POI to list.

Add new POI form



Display Name – Relevant name used for POI.

Notes – Any further information to be used for POI.

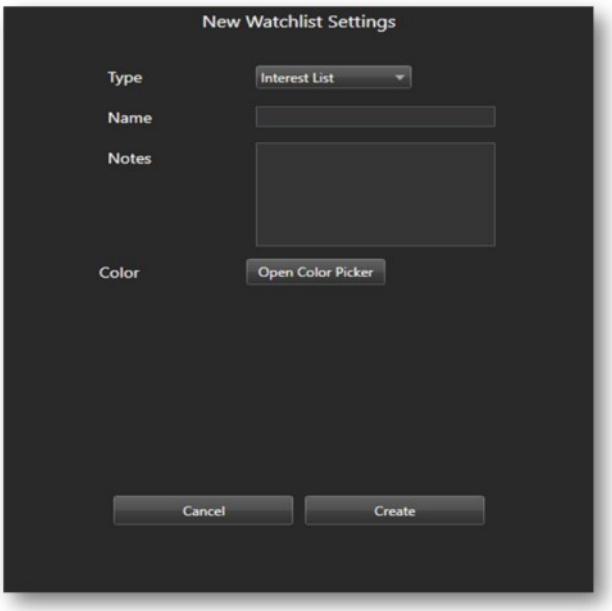
Watchlists – Select the Watchlists relevant to this user. The watchlist you started from is always selected

Image – Use `Select Image` to navigate to a relevant image on the XProtect Smart Client machine for this POI.

Cancel – Close this process and do not save.

Add – Commit to add POI to Watchlist.

Add new Watchlist form



Type – Can be either Interest or Authorised List

Name – Name of the new watchlist

Notes – Additional notes can be added.

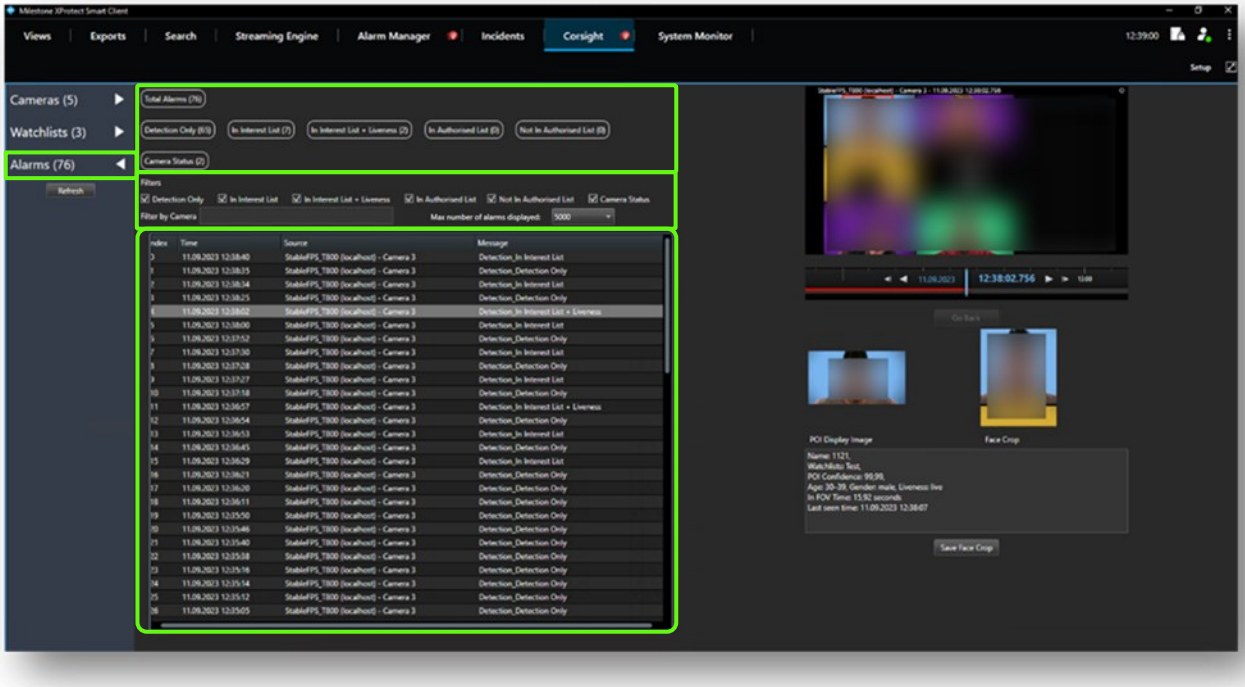
Color – Color of the bounding box displayed on matches for this watchlist.

Cancel – Press to close this process.

Create – Press to save a create this watchlist.

6.1.1.3 Alarms

Alarms in the plugin workspace are different from Alarms in the XProtect Alarm Manager. Although connected (as shown in the next section), these contain much more information and are updated in real-time.



Total Alarms – Total number of alarms generated by Corsight Service.
All types of alarms that can be generated by Corsight Service are listed below that and incremented as they appear.

Filters – Alarms can be filtered by event type or by camera name. All filters are additive, meaning that, for example, you can search for all "In Interest List" alarms that came from particular camera only.
(Selected filters are prefilled on startup in the XProtect Smart Client based on the last choice.)

Filter by Camera – Type search field
Max number of alarms displayed: (Default 5000)

The filter options are directly synchronized with the options made available in the XProtect Management Client under Corsight Plugins, Corsight Settings. `Select` Modify SSE Filter to update filters. This allows changes without closing the Corsight AI plugin connection.

Alarm List – Filtered list of alarms that were generated by Corsight Service. This is filtered by the filters above and also by the retention time setting set in the plugin settings in XProtect Management Client.

- Time: the time of the last update generated by Corsight Service. This time is the moment the video stops at and matches the bounding box and face crop.
- Source: the camera that generated the event

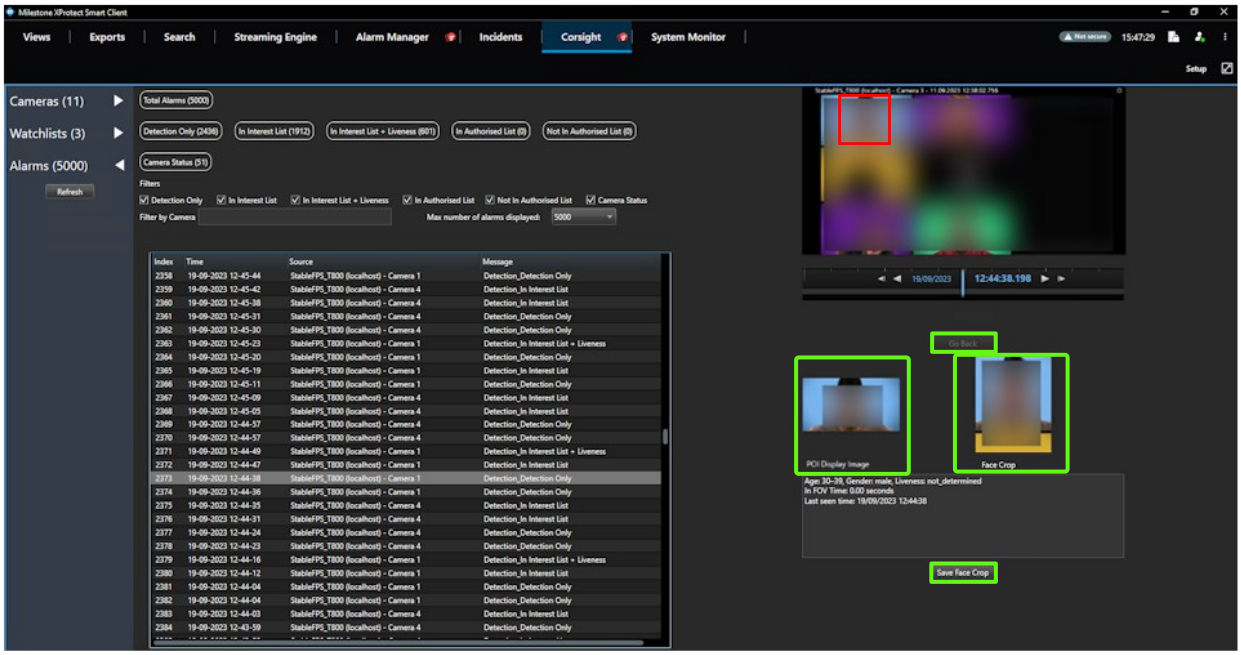
- Message: the type of the detection

This list is constantly refreshed, and new alarms will always appear on the top. There is a maximum limit of 5,000 alarms and when that is reached the oldest will be overwritten in order of creation.

The information is stored on disk (Program Data/Corsight) every minute so in case there is an issue with the XProtect Event Server connection the alarm list will be retrieved on start-up, but all alarms generated since the last save will be lost. This does not affect the alarms in the Alarm Manager, so in the situation described above, there could be a mismatch where there are more alarms in Alarm Manager than in the plugin workspace.

If a hard refresh is required, all files from that folder can be deleted and that will delete all stored alarms in the plugin Workspace. It will not affect the alarms in the Alarm Manager, but their face crops will be missing.

In case you want to view an old alarm that is no longer displayed in the list, you can adjust the retention time setting in the plugin settings in Alarm Manager. If there were more than 20,000 alarms generated in the meantime however, this will not work.



Bounding Box on video – Bounding box generated by the Corsight Service that matches the location of the face crop. The display colon matches the color of the watchlist for that particular POI (if it was a match). Green (no match) or red (not in an authorised list) are also possible.

Go Back – Press to go back to the moment of the alarm to return to the start of the alarm event. When playback has been used.

POI Display Image – Reference photo taken from Corsight database.
Face Crop – Latest update of the face crop generated by Corsight for that POI

Textbox

- Name: POI Name.
- Watchlist: Watchlist connected to trigger.
- Confidence: Shown as a percentage, match confidence level.
- Age, Gender, Liveness: Defined if selected as option for camera device.
- In FOV time: Time that POI remained in the camera's FOV
- Last seen time: The time that POI was last seen

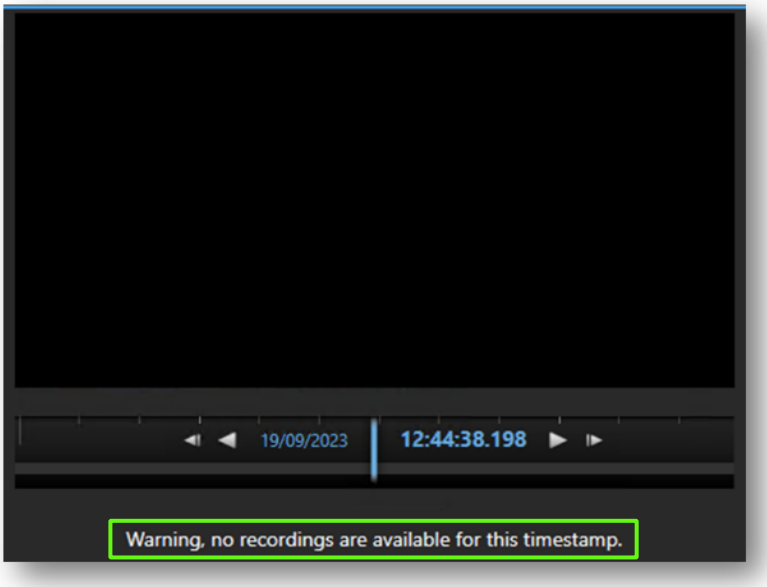
Save Face Crop – Press to save current recorded face crop to client machine.

XProtect records with motion detection by default, but in some cases an appearance can be picked by the Corsight Service without triggering the motion detection in XProtect.

Depending on the use case, the user can adjust the camera settings to avoid missing important events and recordings. One option is to enable motion recording and lower the motion detection threshold to start recording earlier. Another option is to choose continuous recording for some cameras.

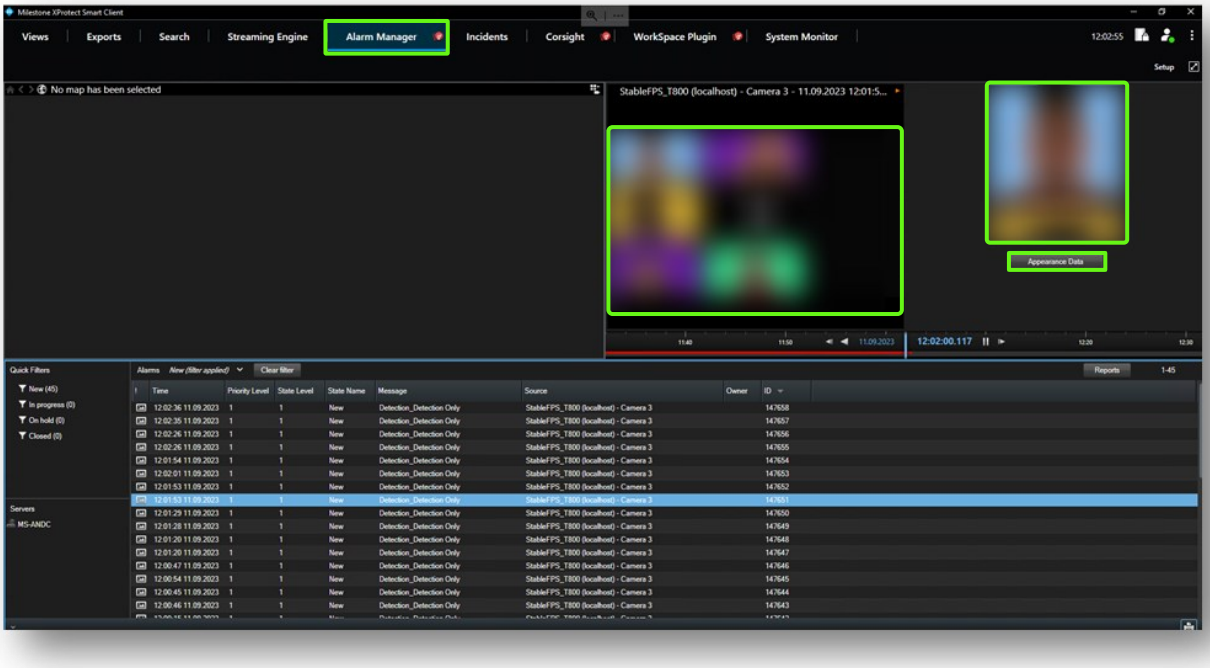
For further details see the troubleshooting section 7.3 Warning, no recordings are available for this timestamp

Where no recordings are available the video dialogue will display a warning message.
"Warning, no recordings are available for this timestamp."



6.1.2 Alarms in Alarm Manager

From the XProtect Smart Client select the `Alarm Manager` Tab. Below shows an example alarm generated by the Corsight Plugin. Refer to 5.1.8 Alarm Definitions for the setup of these alarms.



In the above Alarm example, we see the face crop of the POI taken from the Corsight system. The video shows the camera feed from XProtect at the moment the alarm is registered. Bellow the face crop is the `Appearance Data` button that will take you to the corresponding Alarm displayed in the Alarms section of the Corsight plugin workspace.

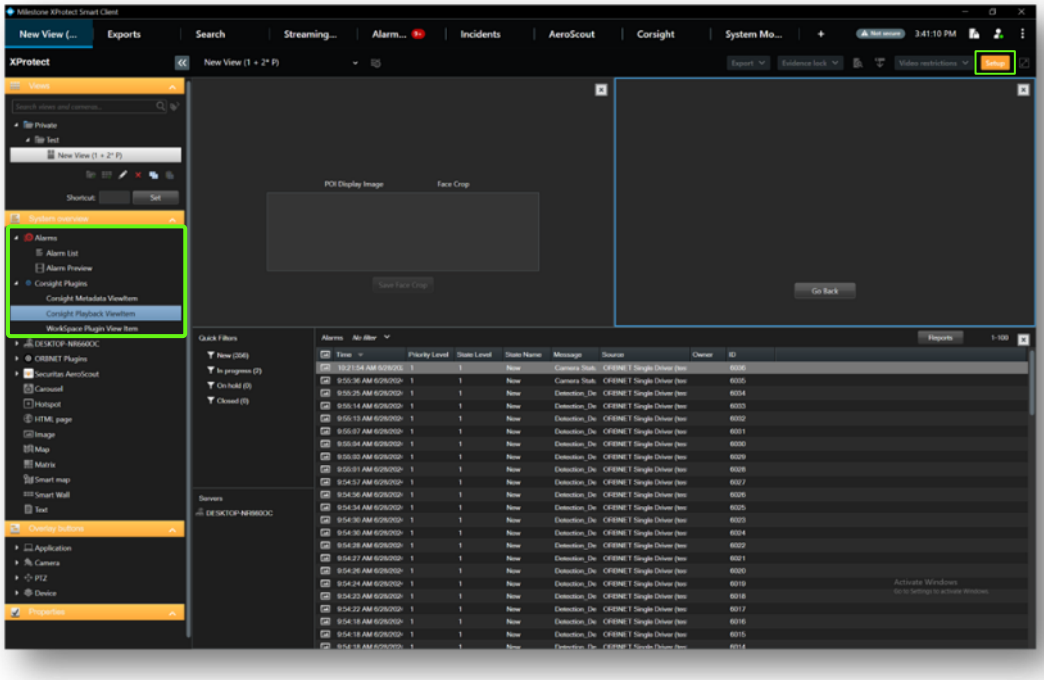
Alarms in the Alarm Manager are not updated with the latest face crop or analytics that can be provided by Corsight. They are tiggered as soon as a detection takes place. This is why it's necessary to click on the `Appearance Data` button to see the latest info in the Corsight plugin workspace. Once you do that that alarm will automatically enter the In Progress state and will now be found under that category in the Alarm Manager.

6.1.3 Create a Custom View

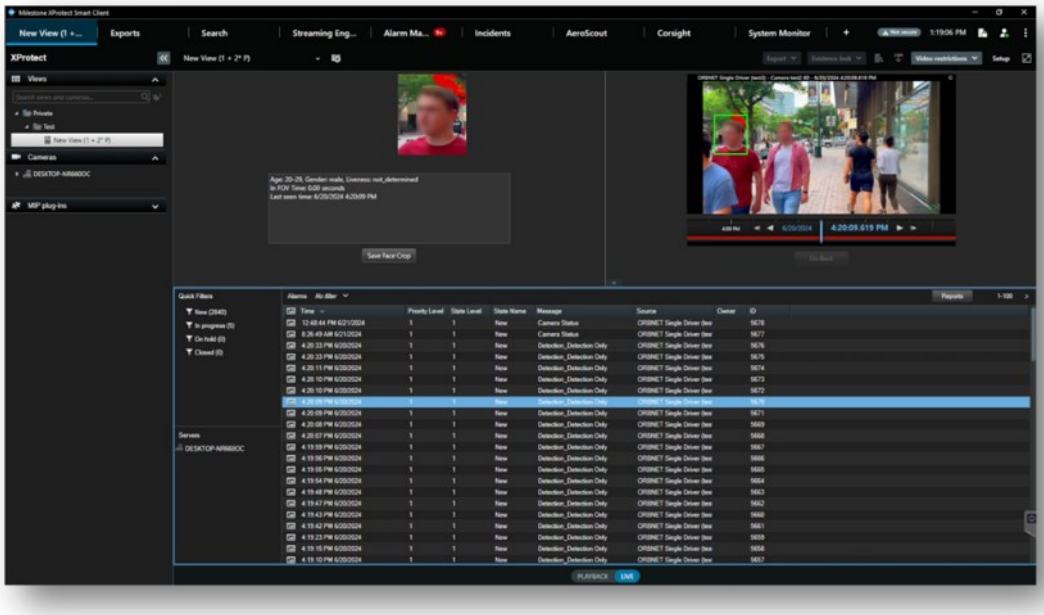
Within this plugin there is the option to create custom views with the Corsight AI view items.

In this example we have used the View (1 + 2* P), go to `Setup` then drag in Corsight Metadata View Item (Left) and Corsight Playback View Item (Right). Below use the XProtect Alarms, Alarm List.

An alternative option is a one tile view WorkSpace Plugin View Item, this is the same as is shown in the Corsight tab.



As shown out of Setup mode.



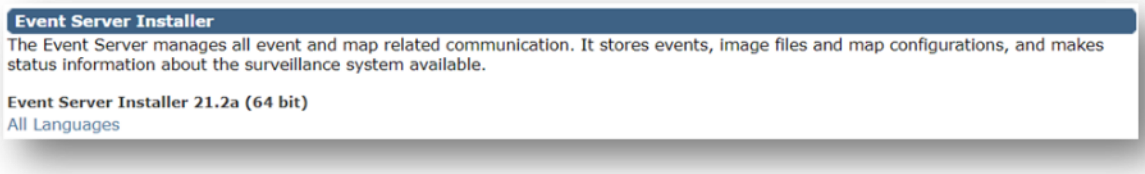
7 Troubleshooting

7.1 XProtect Event Server Installation

If XProtect was installed via a custom installation, the XProtect Event Server service may not have been included, as it is not always required.

From the server/machine with the XProtect Management Server service navigate to http://localhost/installation/admin/default-en-US.htm

This will provide a XProtect installation page where you will be able to run the installer for the XProtect Event Server. This must be installed so the ORBNET plugin can communicate with XProtect MIP SDK.



7.2 Corsight Plugin Logs

This location has logs related to all plugins. Search for Corsight in the log file.
C:\ProgramData\Milestone\XProtect Event Server\logs\MIPLogs\

Logs related to the Streaming Engine.
C:\ProgramData\ORBNET\Streaming Engine\ORBNET Streaming Engine\Logs\

7.3 Warning, no recordings are available for this timestamp

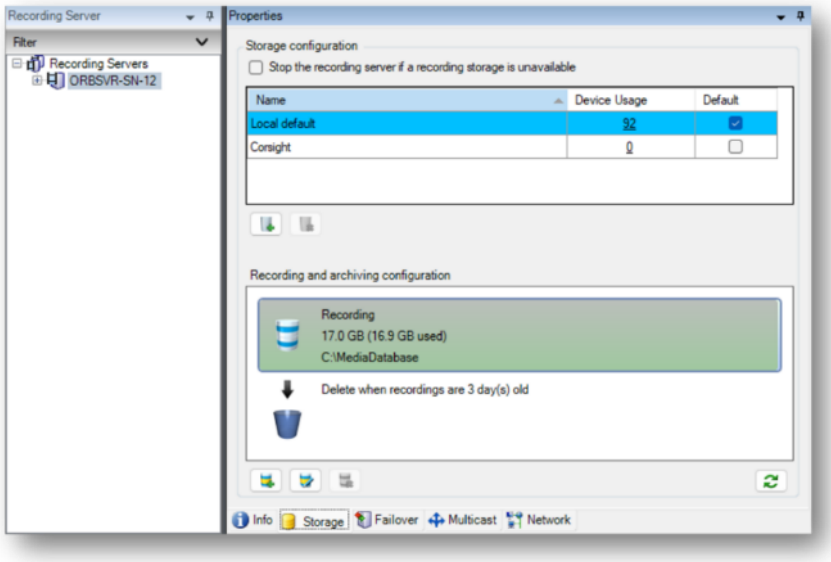
This error is shown when recordings are not made available from the XProtect system for the event timestamp request by the Corsight AI plugin. Generally, this will be related to the default XProtect recording settings. Below we will cover the general troubleshooting to ensure recordings are available for Corsight AI event.

The recommendation for recording when using the Corsight AI plugin is for recording to be always on. However, we are aware that in different user cases this would not always be possible or feasible.

Recording retention days

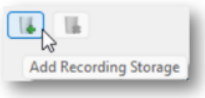
Select the relevant Recording Server followed by the Storage tab. Here you will see the recording retention for a recording profile. In the below example recordings are erased once they are 3 day(s) old.
If the Corsight AI plugin event view window shows events that are older than the recording retention timeframe the warning of no recordings being available will show for these events.

This window shows the used storage in the allocated storage area. Whenever the available space is below 1GB, XProtect is erasing video footage before the set number of retention days. This is to maintain the integrity of the video database.



If you would like all cameras relate to the Corsight AI plugin to have a separate recording profile to other cameras in your system, this can be done by creating a new recording profile.

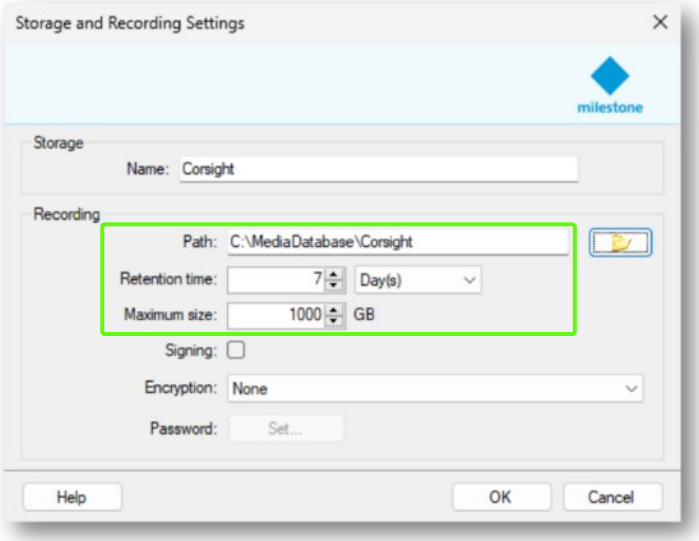
Select `Add Recording Storage`



Update the fields in this pop-up window in relation to your required system settings. Key points are the Path, Retention time and Maximum size.

- Path – This can be the same storage area as other storage configurations or another storage location.
- Retention time – This will erase the recording after a set timeframe. However, this requires a calculation based on the number of cameras, how much space they use and the available storage.

- Maximum size – This is the maximum size that XProtect can use for this storage area. If shared with another profile, ensure these are spaced accordingly for the total disk space (Generally allowing 10-20% free space buffer for performance).



The retention timeframe is ignored if the storage area is full. In this case once the Maximum size is reached XProtect will erase the oldest recordings to maintain a recording buffer for new recordings.

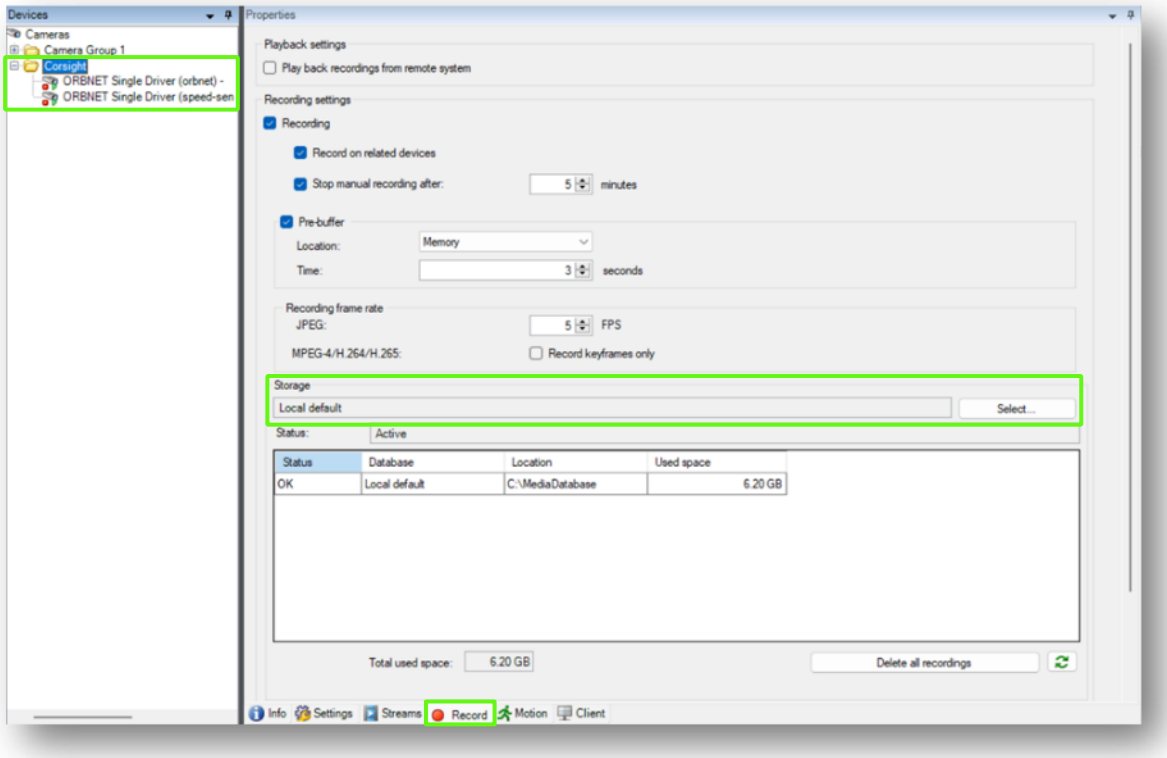
If the retention timeframe was 30-days but the system had only space for 25-days, you would only see 25-days of recordings available.

Confirm recording retention, per camera.

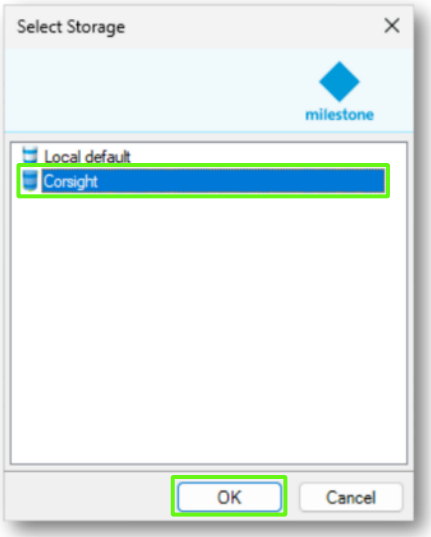
Use the XProtect Smart Client in a playback window to show when the last available recordings are available on your XProtect system for a camera. `Go to` a view with the camera you wish to check, `Select` the camera tile and `press` the First Sequence ⏮ button. Check the date shown.

Create a Camera Group for the cameras that will fall under this new recording profile, add the relevant cameras to this group, using **Edit**.

Select the **Record** tab for this group, under the Properties, see the settings for Storage, use **Select** to update the storage profile.



Select the new recording profile and press **OK**.

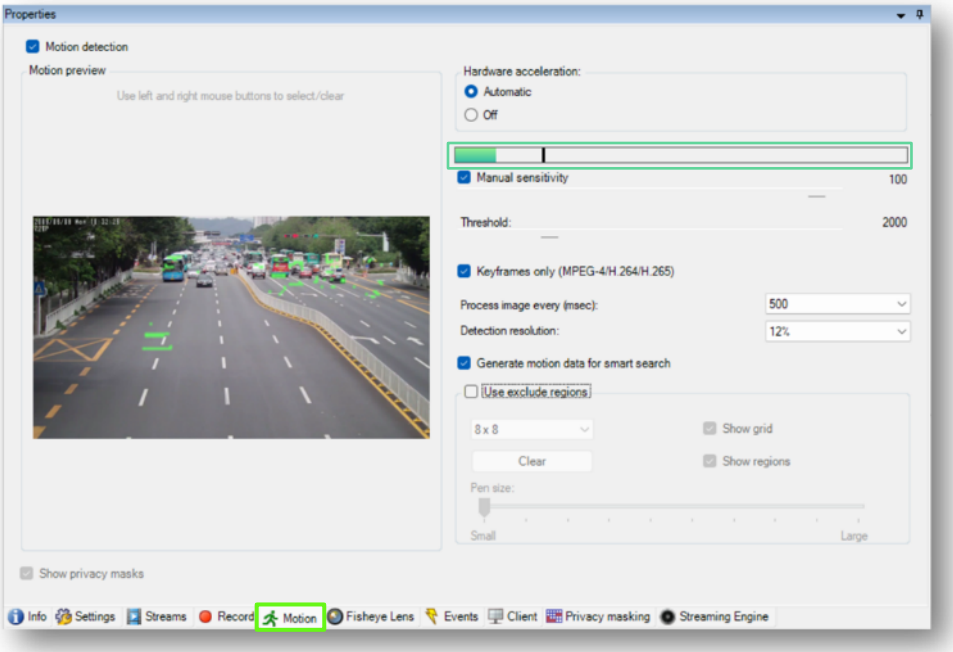


Motion Detection

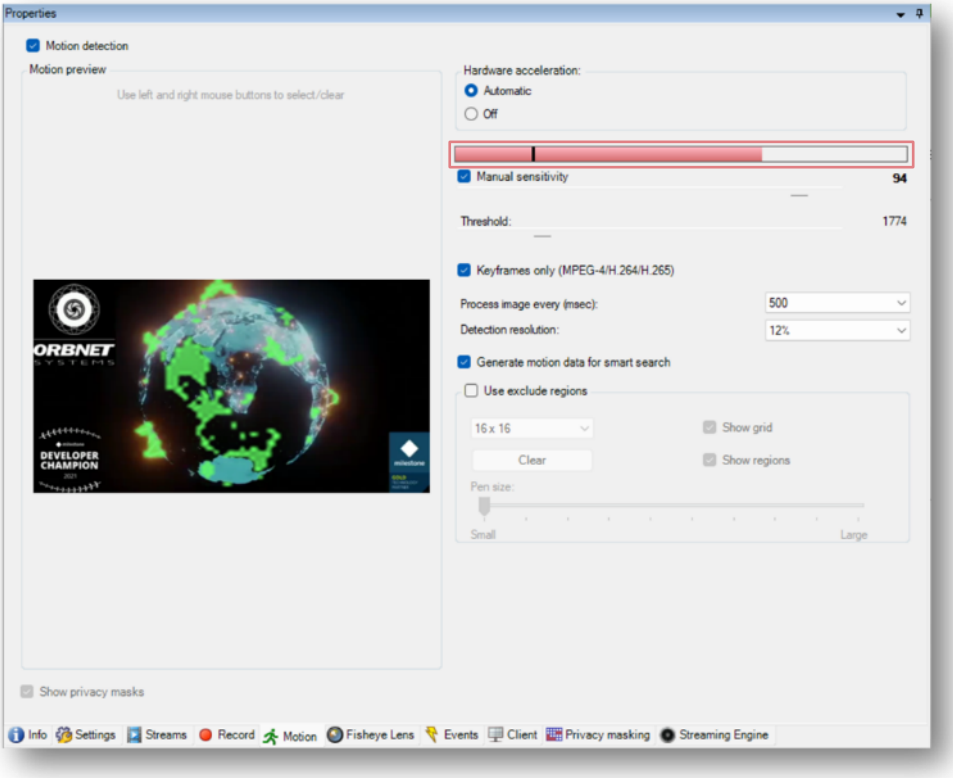
As default in a XProtect system, recordings are set to record only on motion detection. In the below example the motion detection threshold has not been reached so there will be no recordings at this time. Whenever the motion bar shows in green there is not enough motion to trigger the Motion Started event. Green in the motion bar can also mean the Motion Stopped event has been triggered.

Motion Settings

- Manual sensitivity – In newer XProtect systems, post 2020 dynamic motion sensitivity is used as default. With dynamic sensitivity, the system calculates and optimizes the sensitivity level automatically and suppresses the motion detections that come from noise in the images. This improves motion detection at nighttime, where the noise in the images often triggers false motion.
- Sensitivity (When Manual sensitivity is ticked) - The sensitivity setting determines how much each pixel in the image must change before it is regarded as motion. Value from 0-100, 0 being the most sensitive, 100 being the least.
- Threshold - The motion detection threshold determines how many pixels in the image must change before it is regarded as motion. Value in pixels from 0-10000.
- Keyframes only – As default this option is selected, in most cases H.264 or H265 would be used. Depending on the camera make this could have a default, anything from 1-4 seconds for a keyframe. Motion will only be processed on keyframes for H.264 or H265. This could affect the overall sensitivity of motion detection. Disabling this option could use far more system resources as the video has to be decoded to process the I-frames and P-frames.
- Process image every (msec) – Video images are processed for motion based on the timeframe set. This option is ignored if Keyframes only is enabled.
- Detection resolution - Specify whether the full image or a selected percentage of the image should be analyzed. For example, by specifying 25%, every fourth pixel is analyzed instead of all pixels, reducing the system resources used but also offering less accurate motion detection.
- Generate motion data for smart search – This option is unrelated to Motion started; Motion stopped events.
- Use excluded regions – These are selected areas within the video image that are selected to be excluded from motion detection. If too much of the image is covered with these areas, it may prevent motion from being triggered.



When the motion bar changes from green to red (as below), the Motion Started event is trigged.

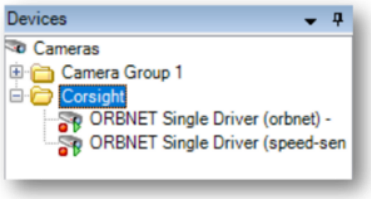


Camera Status

In the XProtect Management Client within Cameras, the cameras display status on the camera icon itself.

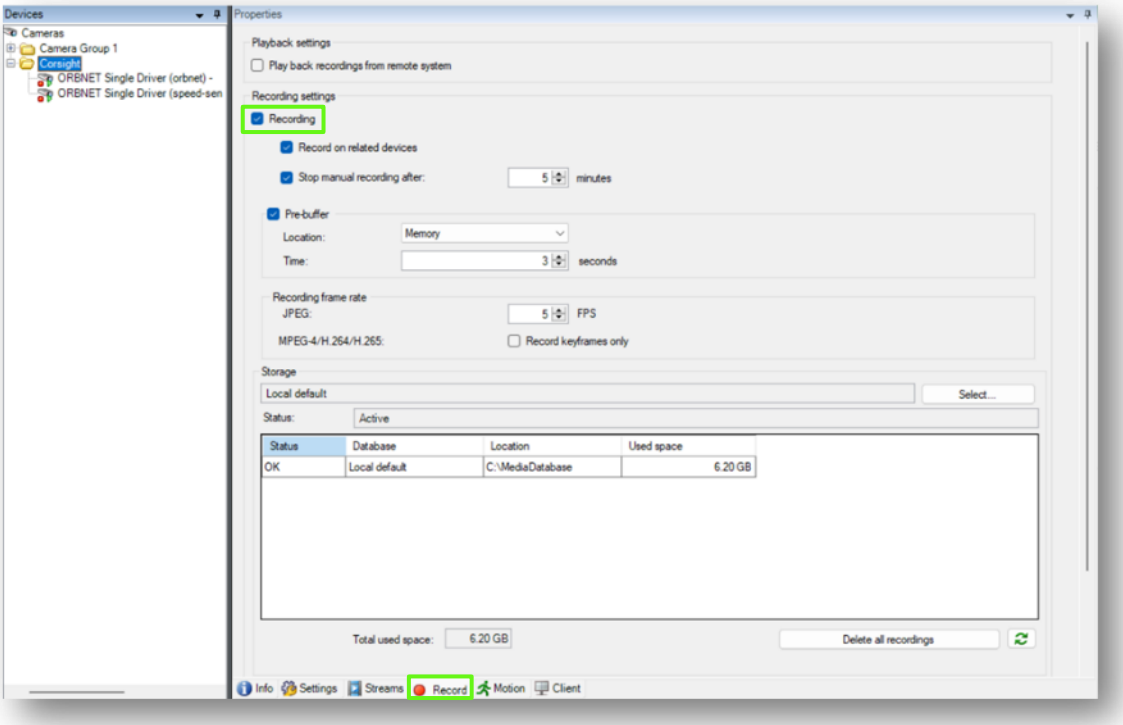
- - **Device enabled and retrieving data**: The device is enabled, and you retrieve a live stream.
- - **Device recording**: The device is recording data on the system.
- - **Device temporarily stopped or has no feed**: When stopped, no information is transferred to the system. In this state you cannot view live video, there will be no recordings.
- - **Devices disabled**: Cannot be started automatically through a rule and cannot communicate with the recording server. If a camera is disabled, you cannot view live or recorded video.
- - **Device requires attention**: The device does not function correctly.
- - **Device live and Recording**: This is the ideal combined camera state for Corsight AI connected camera devices.

Example shown under Devices, Cameras.



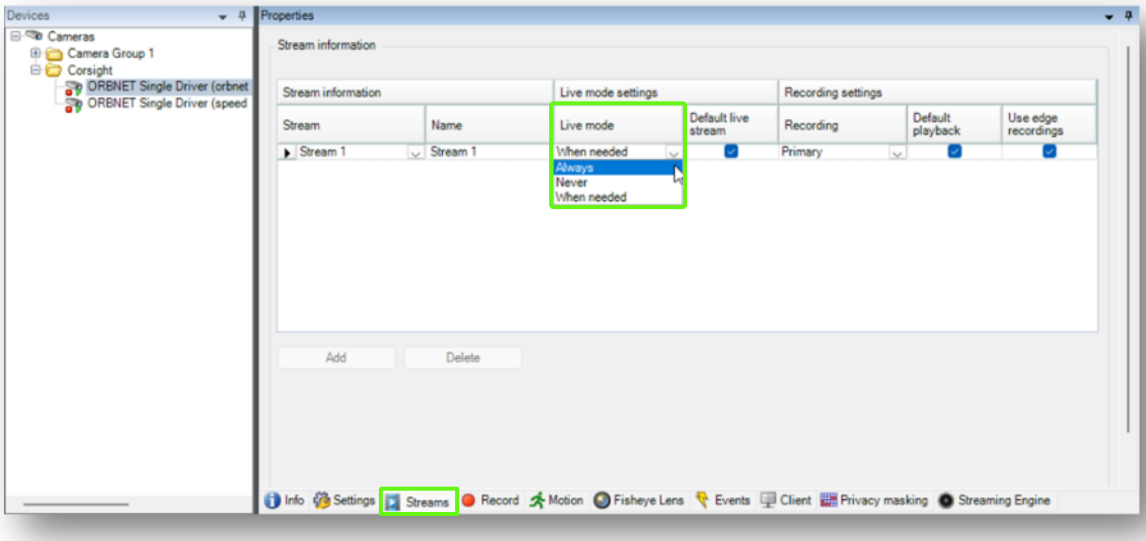
Recording and Stream Settings

`Select` a Camera or Camera Group, `select` the Record tab. From this tab confirm that Recording is ticked as enabled. Without this option ticked no recordings will be available for this camera device.



When using motion only recording or recording on a schedule in some cases the live video can go into a standby mode. This can cause the Streaming Engine to lose connection to the camera. In turn the Corsight AI plugin would lose connection to the video stream for processing. This is related to the priority of video delivered over the XProtect API.

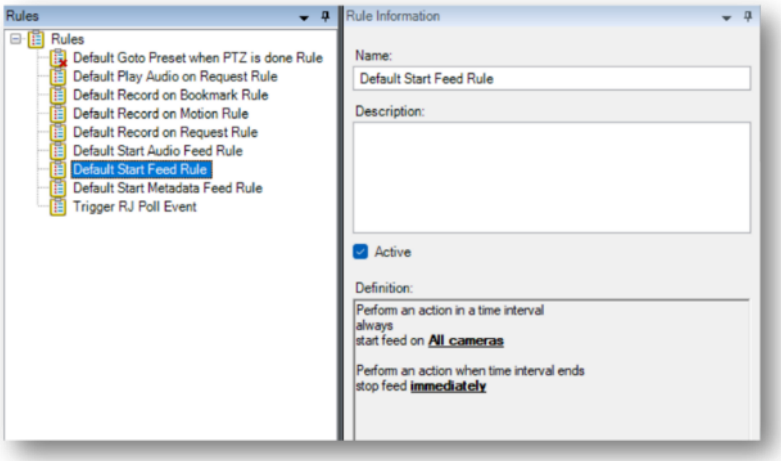
If this is the case, we recommend changing the Live mode setting for the used video stream from the default of When needed to Always.



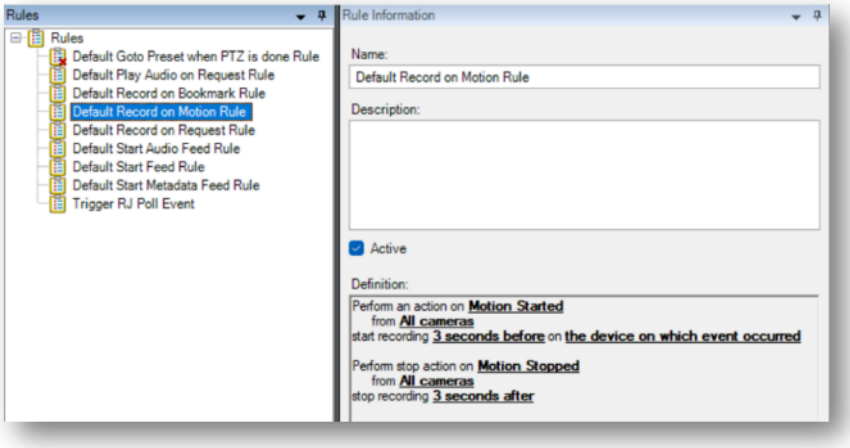
Recording Rules

XProtect uses rules to start camera video streams and record. As default all cameras are included in the Default Start Feed Rule. This means that camera video streams are available for live viewing.

- - **No feed**: When stopped, no information is transferred
- - **Device enabled and retrieving data**: The device is enabled, and you retrieve a live stream.



The Default Record on Motion Rule enables recoding pre and post a Motion Started and Motion Stopped event. Outside of these triggers there is no recording.

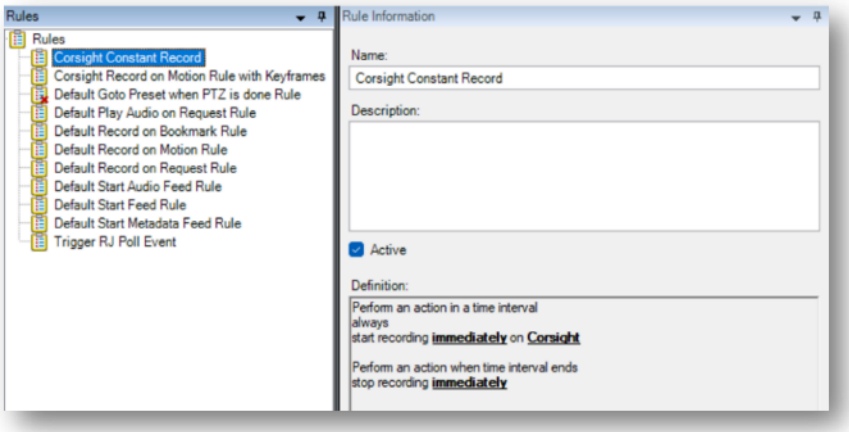


Alternative Rules;

Constant Record

This is the simplest rule to enable constant recording on the Corsight camera group.
Create a new rule, `right click` and Add Rule.

Step 1: Perform action in time interval:
Step 2: Always
Step 3: Start Recording on <devices> (`Select` the Corsight Camera Group)
Step 4: Perform an action when time interval ends
Step 5: Stop recording immediately



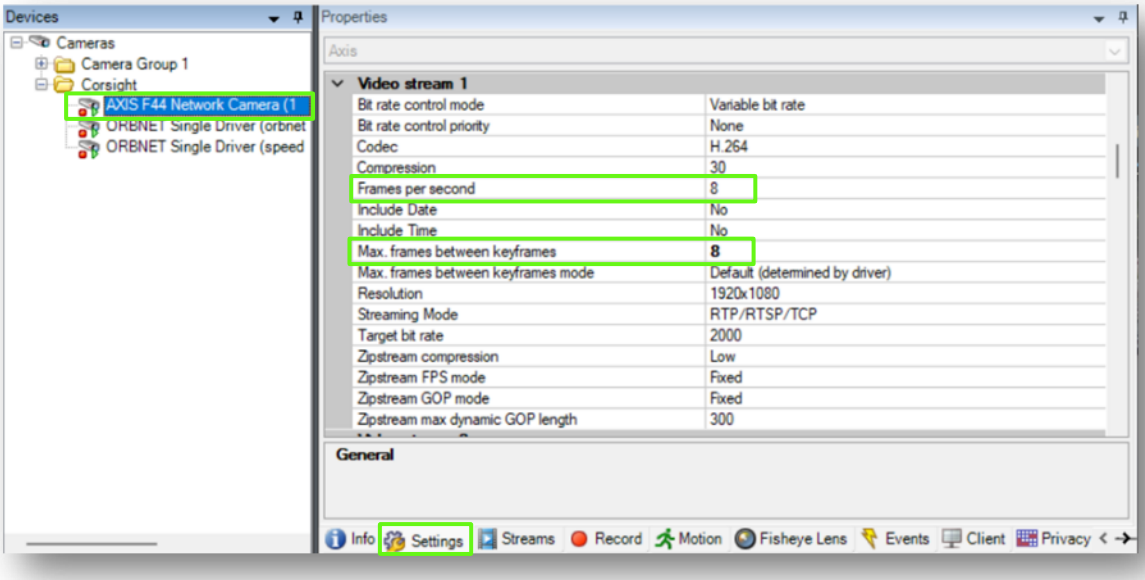
Constant Keyframe Record, All Frames on Motion

This rule will record constantly on keyframes. When motion detection is triggered, it will increase to the full framerate.

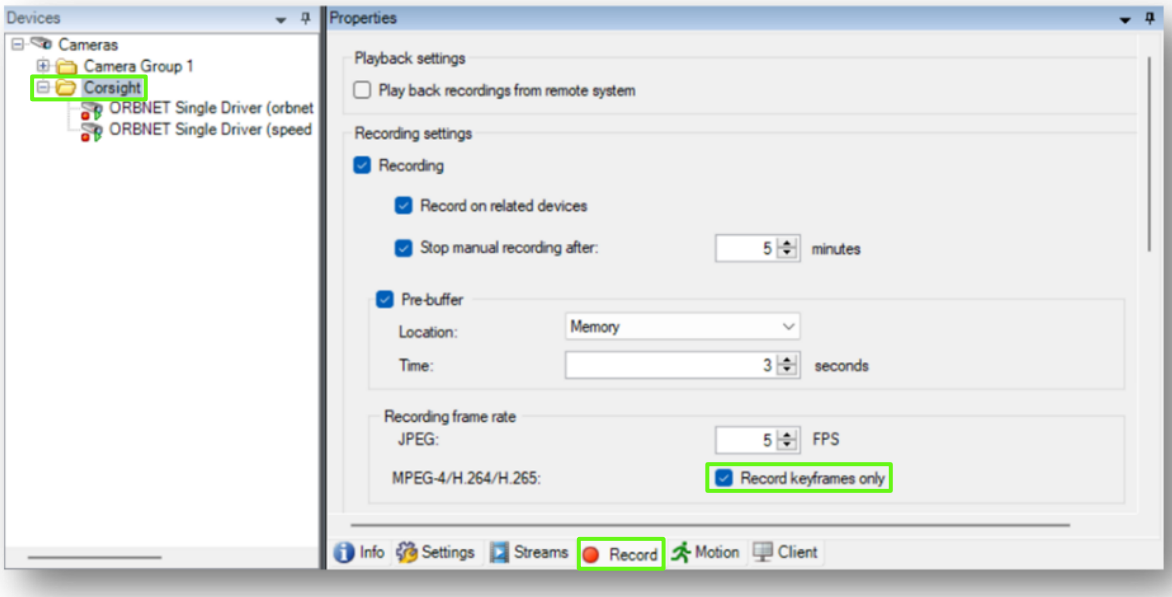
This rule requires a camera setting change.

Check the camera device settings, in this example we have an Axis camera.
Under Devices, `select` Cameras and the Corsight Camera Group. `Select` the Settings tab.
For Video Stream 1, see Frames per Second and Max. frames between keyframes.

For Max, frames between keyframes as default for the Axis camera this is 30. This would mean there would only be a keyframe every 3 75 seconds. When using keyframe recording 1 second between keyframes is ideal. Match the Frames per second and Max. frames between keyframes to achieve this.



`Go to` the Record tab.
`Tick` Record keyframes only.



Create a new rule, `right click` and Add Rule.

Step 1: Perform action on <event> (Motion Started)
Step 2: (Skip)
Step 3: Start Recording on <devices> (`Select` the Corsight Camera Group),
Set recording frame rate to all frames for MPEG-4/H.264/H.265 on the device which event occurred
Step 4: Perform an action on <event>
Step 5: (Automatic)Stop recording, Restore default recording rate.