CVEDIA

Publishing Date: January 27, 2025
Plugin version: 2024.2.5 and higher

CVEDIA-RT AI Analytics Plugin for Milestone XProtect

User Manual: Installation, Activation, Configuration, Update

Technical Support
Ask for help

Contact Sales
support@cvedia.com

CVEDIA-RT AI Analytics Plugin for Milestone XProtect

User Manual: Installation, Activation, Configuration, Update

The integration of CVEDIA-RT with the XProtect VMS solution from Milestone is facilitated through a VMS plugin and a Controller Service that can run on the Windows Operating System.

The CVEDIA-RT plugin enables powerful analytics capabilities in your Milestone XProtect system, enhancing the effectiveness of your surveillance operations.

Key Features

Key features of this integration include the detection of people, vehicles, and animals with a variety of associated analytics:

- Intrusion detection
- Area enter/exit
- Loitering
- Object guarding
- Object left behind
- Crowding
- Tailgating
- Line crossing
- Retrospective search by appearance (search by vehicle type and color; search by clothing color)

Surveillance operators can configure the analytics and create custom rules for triggering events within the XProtect VMS to leverage these alerts and make informed decisions in real-world situations.

This guide will take you through the process of setting up and using this integration.

Requirements

CVEDIA-RT Plugin

- Version 2024.2.5 or higher
- Appropriate licensing

Milestone XProtect

- XProtect Professional+, XProtect Expert, and XProtect Corporate version 2023 R2 or newer.
- All patches available installed.
- The CVEDIA-RT plugin utilizes one XProtect device license. This license is allocated for a Metadata Device that is created to stream bounding box data generated by the analytics.

Supported Decoders

- “video/h264” for H264 streams
- “video/hevc” for H265/HEVC streams

System Requirements

- Windows 10+ x64
- Check compatibility and requirements

Table of Contents

Section 1: Initial Setup Requirements

CVEDIA-RT plugin is compatible with XProtect Professional+, XProtect Expert, and XProtect Corporate version 2023 R2 or newer.

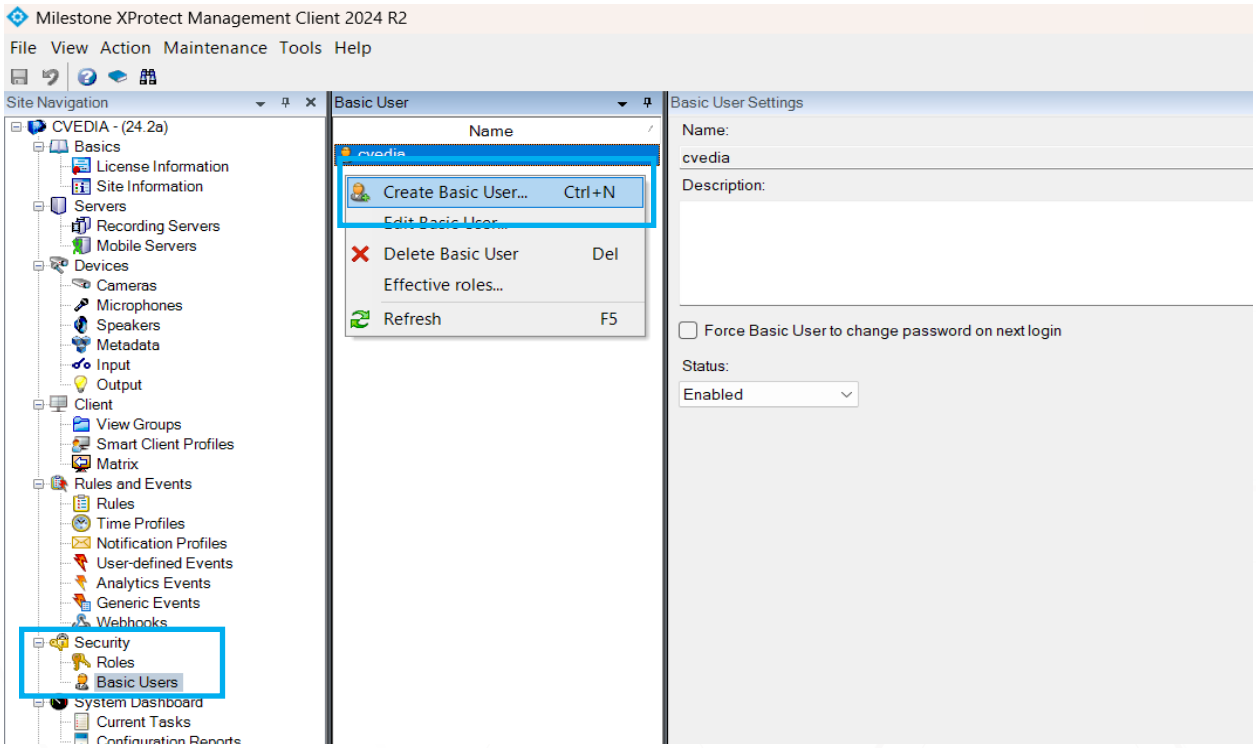
Before proceeding to further steps, please make sure you have a compatible version and license of XProtect software installed on your machine.

> **Notes**
>
> Please check https://www.milestonesys.com/products/software/xprotect-comparison/ to learn more about the different variants of Milestone XProtect software.

Create a Dedicated User

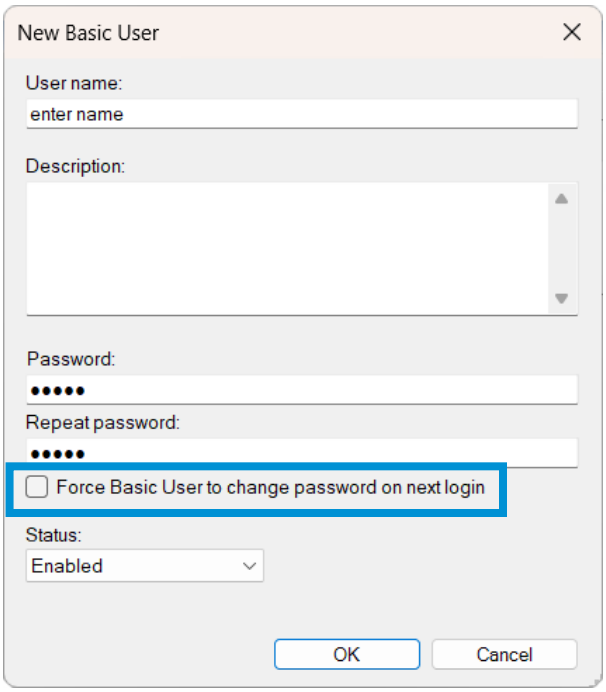
CVEDIA-RT AI Analytics integration requires a dedicated administration user account in Milestone XProtect VMS to communicate with CVEDIA analytics engine and to automate the configuration of the system.

1. On the target system, open the XProtect Management Client and sign in with administrator credentials. In the tree view on the left, choose Security > Basic Users and right-click on the Basic User view to bring up the context menu.

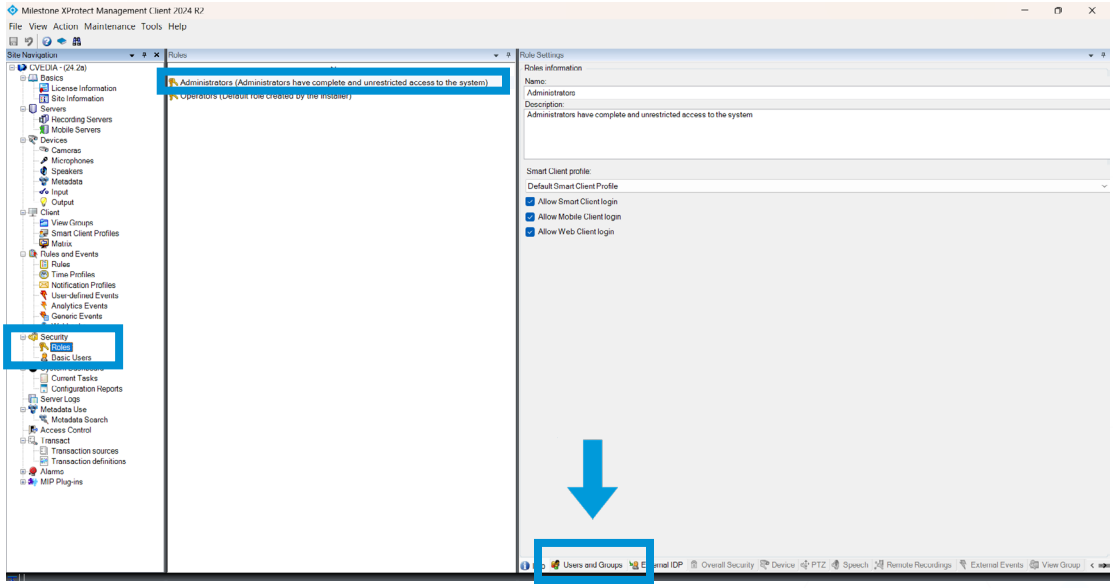


2 Choose Create Basic User and specify the user name and password.

Make sure the “Force Basic User to change password” checkbox is **NOT** checked.



3 Navigate to Security > Roles in the tree view on the left and select “Administrators” role. Press the “Users and Groups” button to view assigned users:



4 Press “Add” to select the previously created user and assign them to the Administrator role.

Once you complete these steps, you can proceed to install the CVEDIA-RT AI Analytics Plugin.

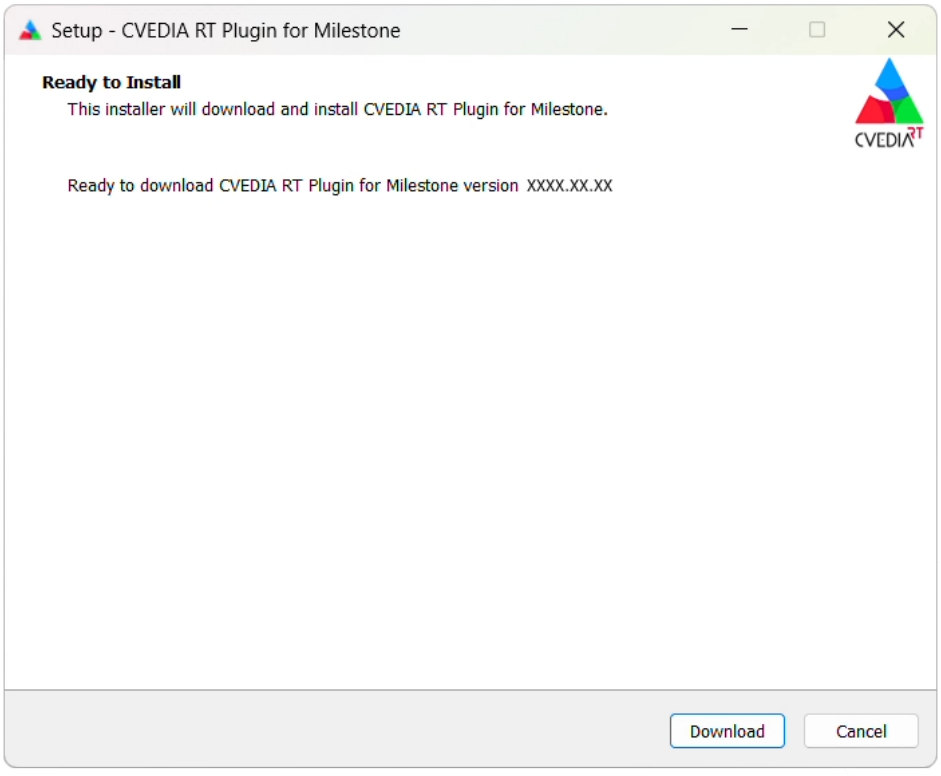
Section 2: Installation and Activation

Installation

1. Download the latest version of the CVEDIA-RT Plugin on the official website: https://rt.cvedia.com

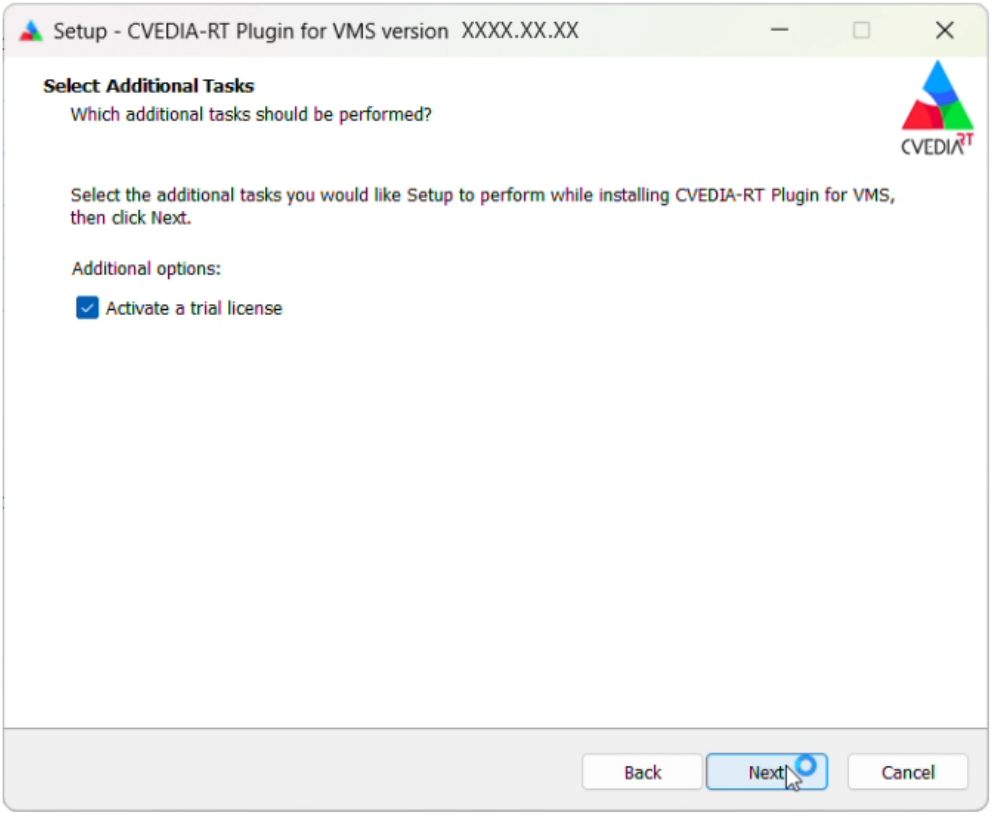
2. Launch the downloaded file: CVEDIA-RT-Plugin-Milestone-Downloader.exe

3. Press the “Download” button to start downloading the installation files.

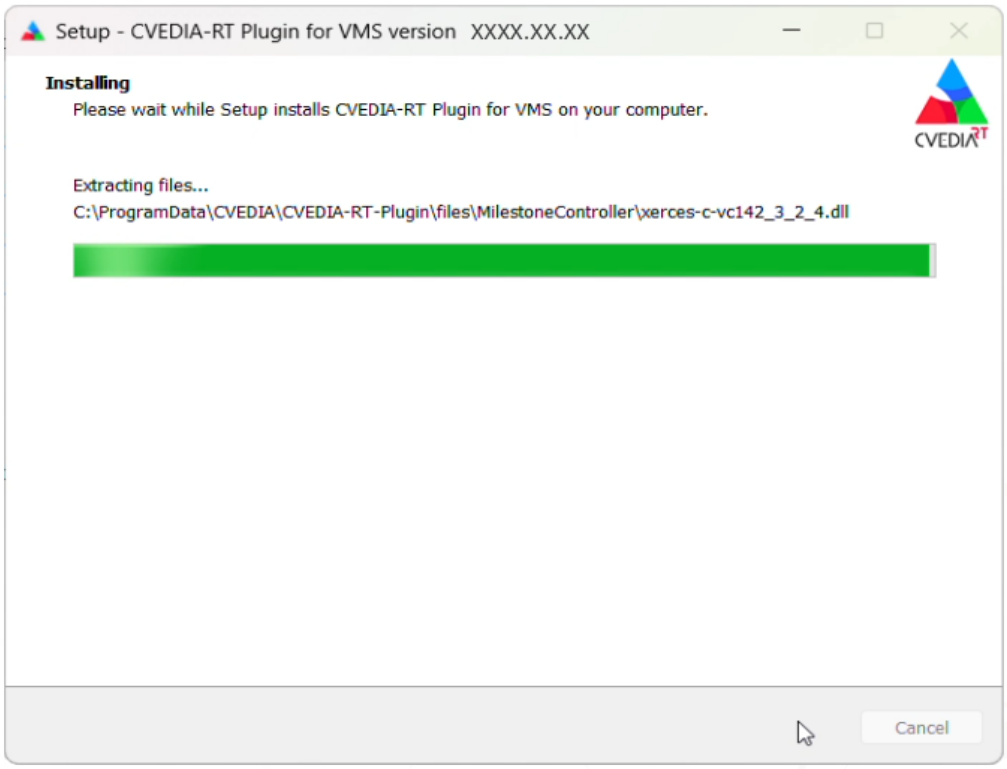


4. When prompted, accept the End User License Agreement.

5 (Optional): Activate the CVEDIA-RT trial license.



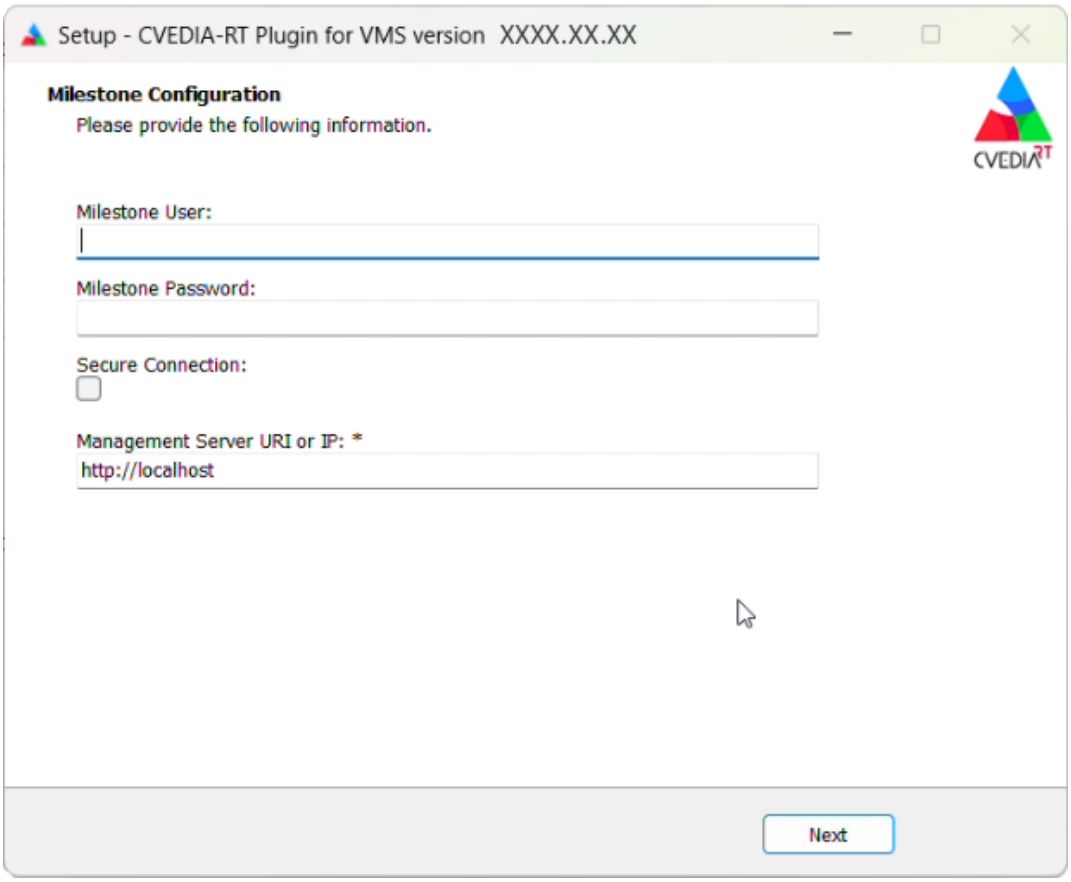
6 Congratulations! The installation process is ready to start: it will only take a few minutes.



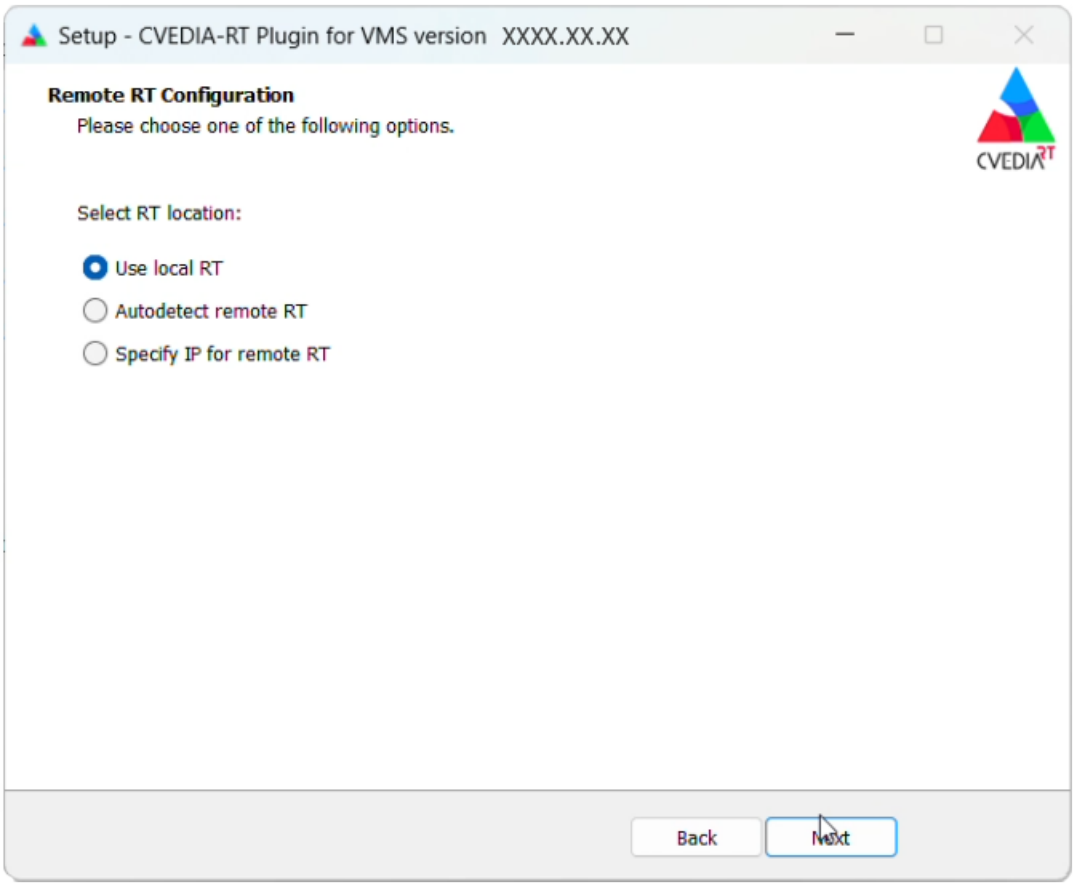
Notes

If you choose to activate the trial license, a pop-up will appear to inform you if the operation was successful.

7 Provide credentials for the dedicated Milestone XProtect user:



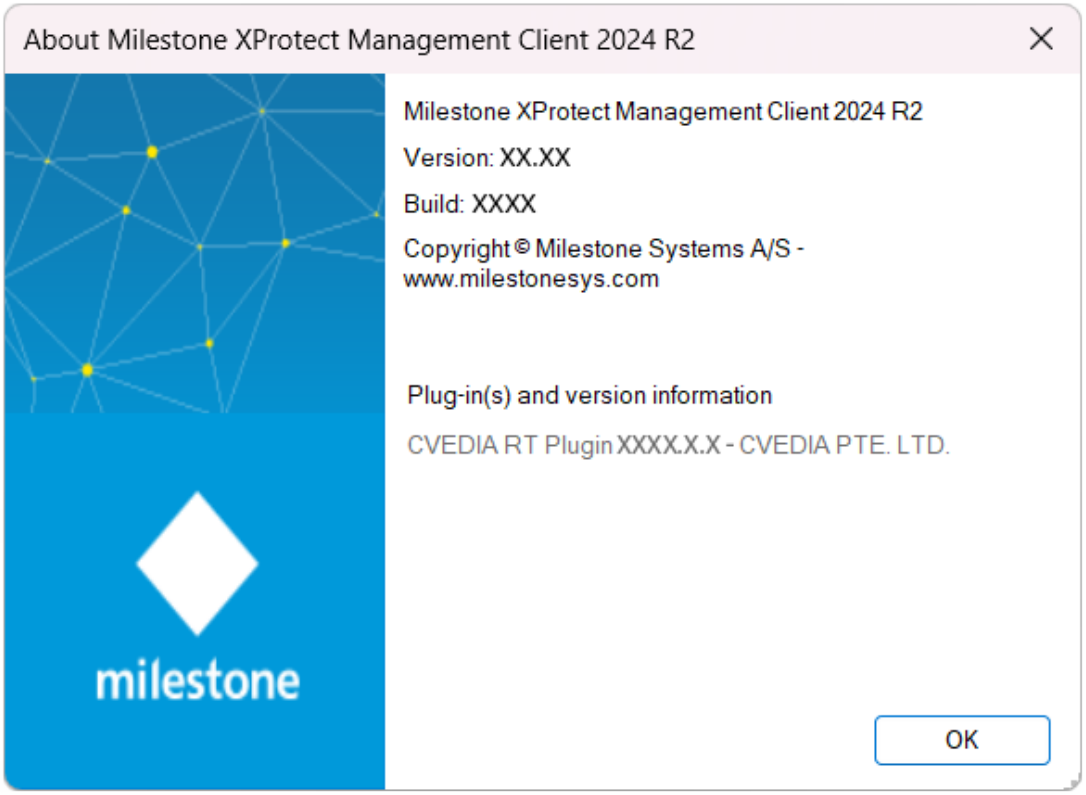
8 Choose “Use local RT” for an all-in-one setup.



Notes

The last step of the installation is to validate if the provided credentials are correct. If the validation is successful, the installation process will be complete.

9 Check the XProtect Management Client to see if the plugin was correctly loaded, by selecting Help / About.



Congratulations! You have successfully completed the installation process!

Important

The CVEDIA-RT plugin utilizes one XProtect device license. This license is allocated for a **Metadata Device** that is created to stream bounding box data generated by the analytics.

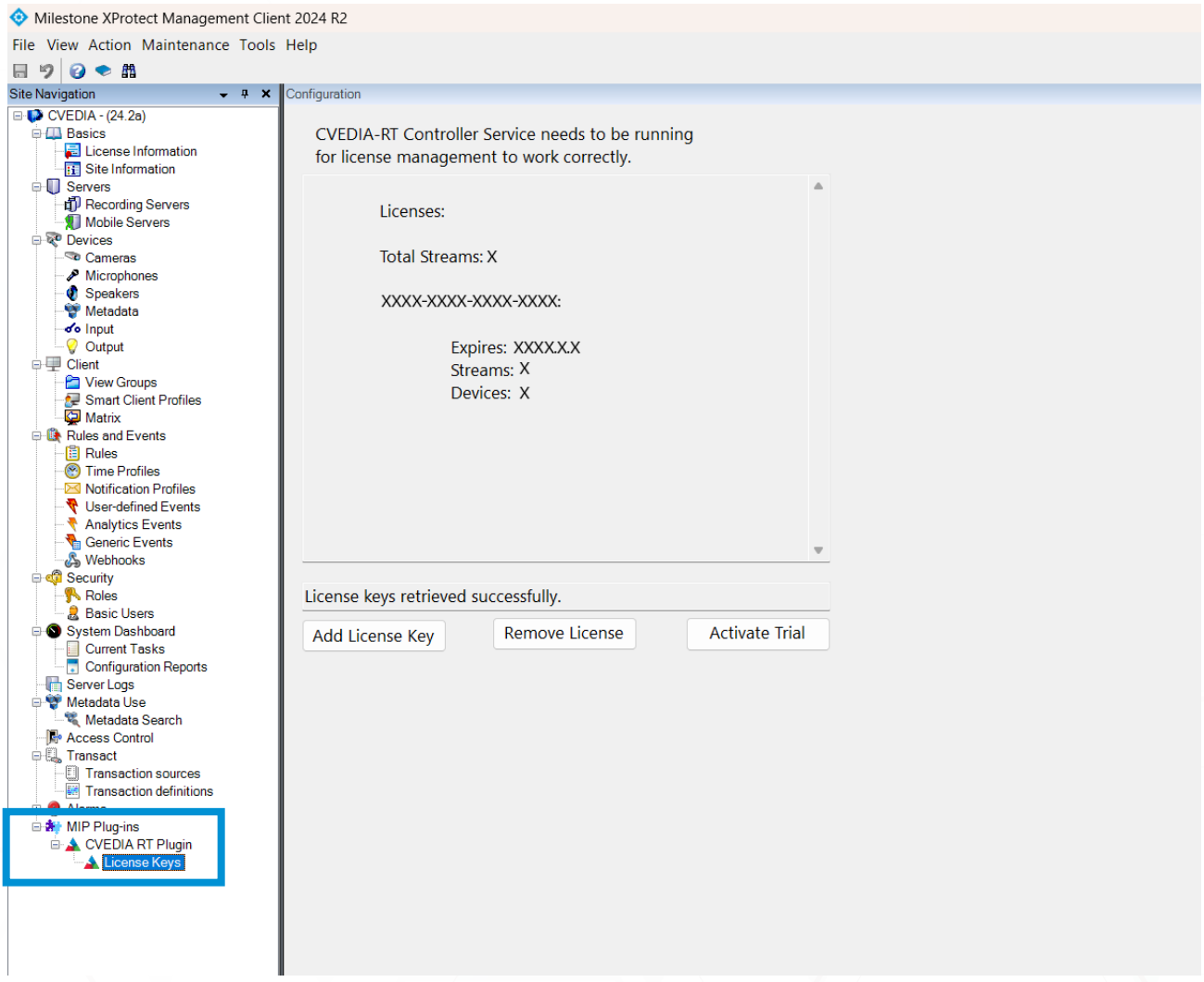
License Management

You can activate and deactivate new CVEDIA-RT licenses from within the XProtect Management Client by navigating to the MIP Plug-ins / CVEDIA RT Plugin page.

The operation of activating a new license key may require a few seconds. You can refresh the XProtect Management Client page by pressing F5 to check if the changes have been applied.

> **Notes**
>
> CVEDIA-RT Controller Service needs to be running for license management to work correctly. Check if the Service is running via Windows Services application".

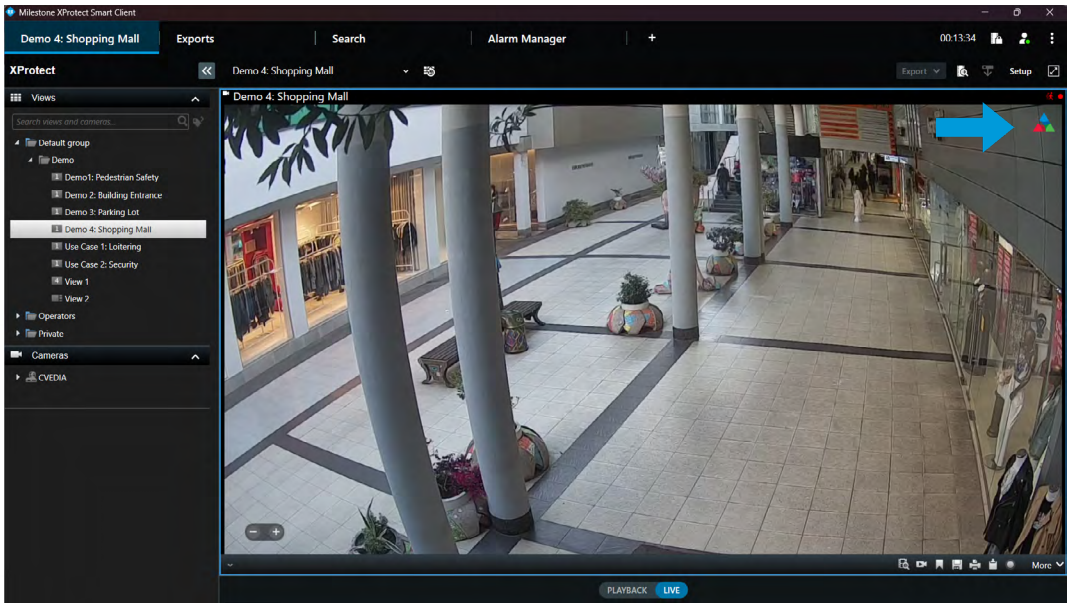
If you didn't choose to activate a trial license during installation, you can also do this here by clicking on the Activate Trial License button.



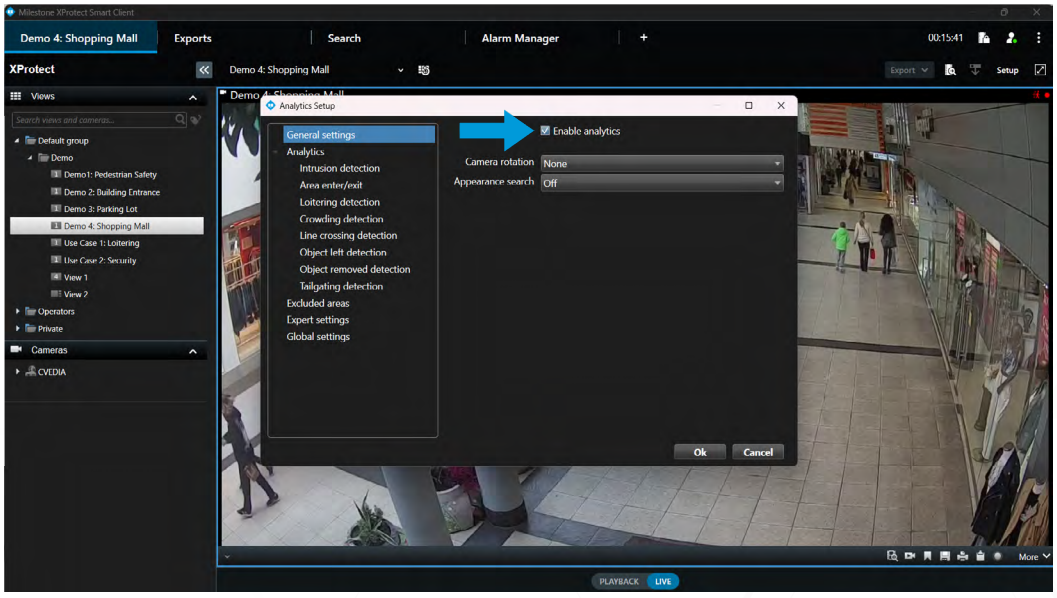
Enabling the Plugin

Once the initial setup is done, you can use the CVEDIA solution directly in XProtect Smart Client.

CVEDIA-RT analytics are available in all streams in your current view, and you can access the configuration menu by pressing the CVEDIA logo in the top right corner.



A new window will open, allowing you to configure analytics for the selected view. Detailed explanations of the available options and their functionalities are provided in the sections below.



Section 3: Analytics Configuration

Different types of analytics allow you to configure one or more detection areas or lines, choose the types of objects to detect, and select additional related parameters.

Notes

- Analytics are active only if at least one area or one line is defined.
- Please note that you can enable multiple analytics at the same time. This will not impact the performance of the system.
- Analytic events will be produced whenever a specified object class interacts with the zones and lines.

Key Features

Key features of this integration include the detection of people, vehicles, and animals with a variety of associated analytics:

- Intrusion detection
- Area enter/exit
- Loitering
- Object guarding
- Object left behind
- Crowding
- Tailgating
- Line crossing
- Retrospective search by appearance (search by vehicle type and color; search by clothing color)

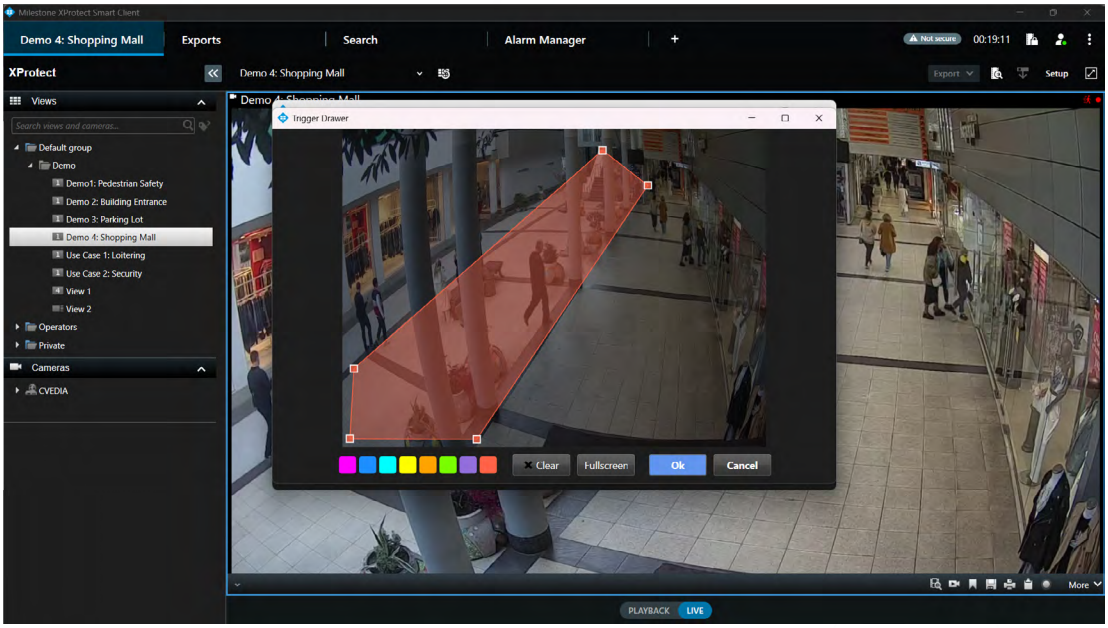
General Guidance

To define a zone of interest and configure the analytics, click on the stream's captured image to activate the zone drawing tool.

You can use the color palette buttons to select a color for the zone. This is particularly helpful when working with multiple zones within the same view for better differentiation.

Notes

- Trigger zones or lines must be configured for the AI analytics to function.
- CVEDIA-RT will not process any data until at least one trigger zone or line is placed. Ensure this step is completed for every stream where analytics are applied.



Creating Zones (Polygons)

Click on the image to place points to outline the shape of the polygon. To complete the polygon, click on the starting point.

Creating Virtual Lines

Click on the image to create points of the virtual line. To finalize the virtual line, click on the last point.

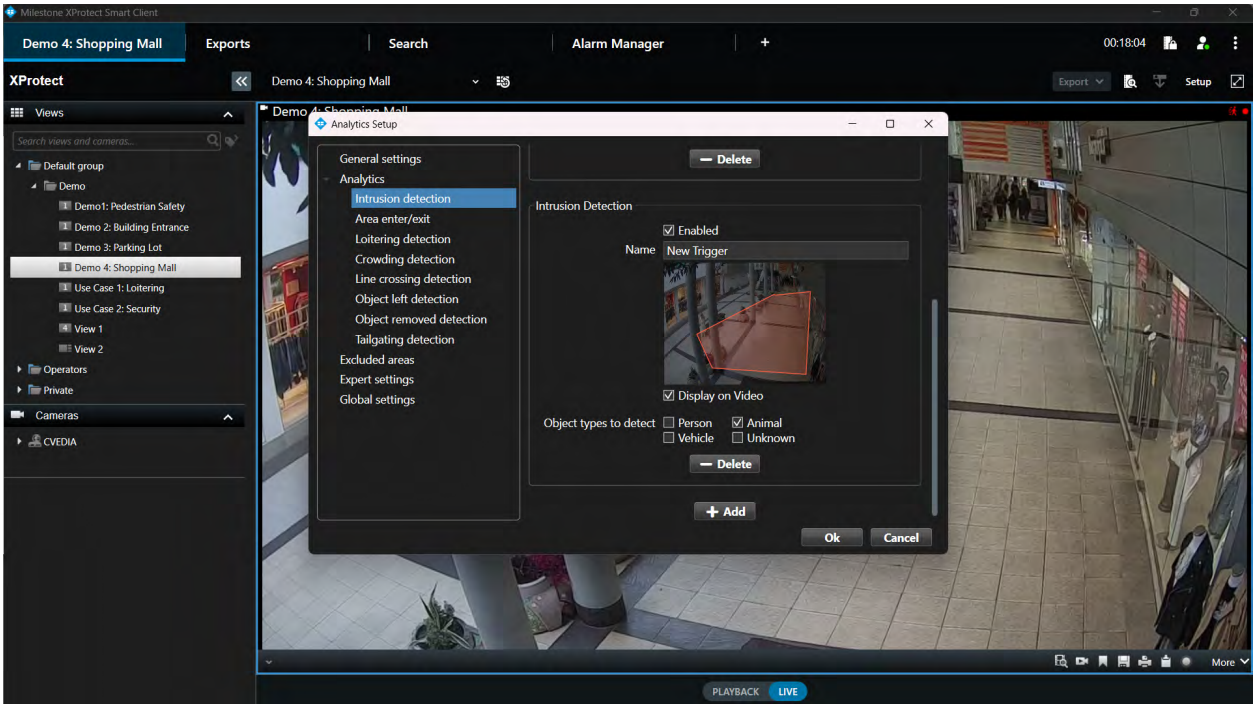
Editing Zones and Virtual Lines

After completing a zone, you can move the entire shape or adjust individual points; add new points by clicking the middle markers on segment lines; remove points by right-clicking on them.

Intrusion Detection

Definition

Detects objects that move inside a defined intrusion area. The event is triggered for any new target object (person, vehicle, animal) entering the area.



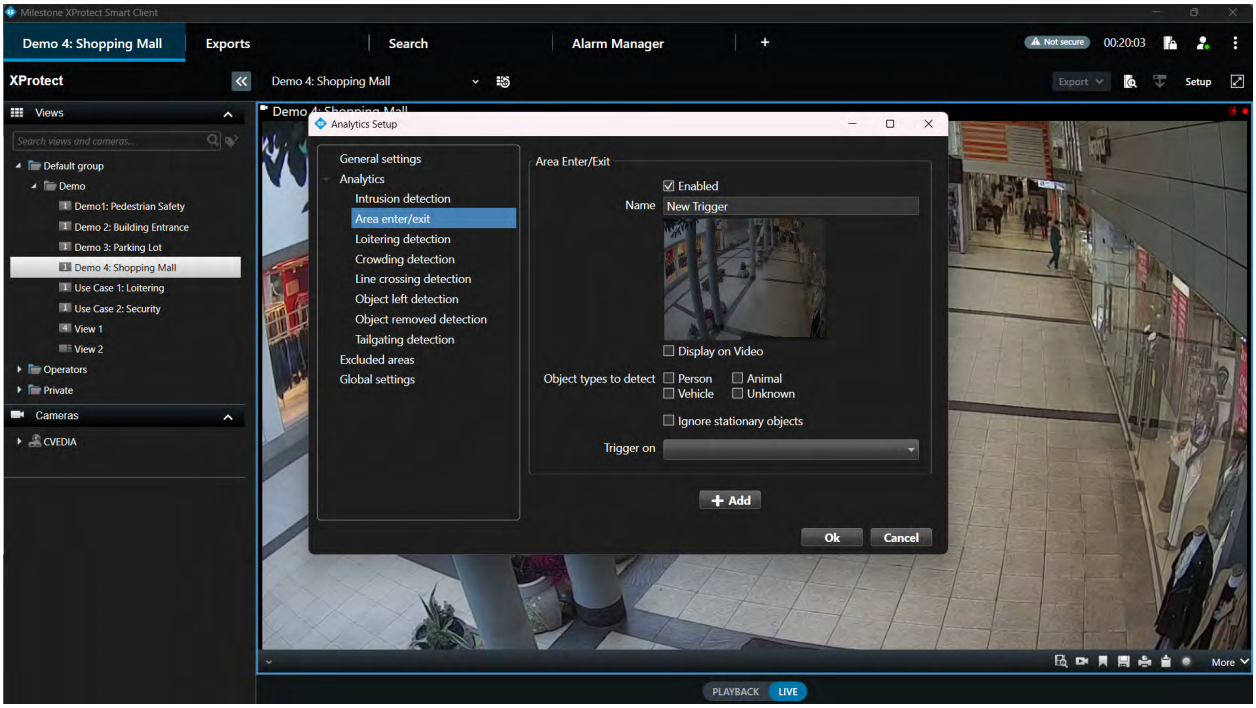
Configuration steps

- Open XProtect Smart Client.
- Click on the CVEDIA logo at the top right corner of a video stream.
- Click directly on the image under “New Trigger” to define the intrusion detection zone. Draw a custom polygon to encompass the area for intrusion detection.
- In the “Name” field, you can give a custom name to the zone of interest.
- Tick the “Display on Video” box to visualize the defined area on the live video stream.
- Select the different Object Types (person, vehicle, animal, unknown) that you would like to detect within each defined area.
- Additional zones can be defined by clicking “+ Add”.

Area Enter/Exit

Definition

Detects objects that enter/exit a defined area. This analytic can be employed to monitor objects detected in the area without triggering an intrusion event.



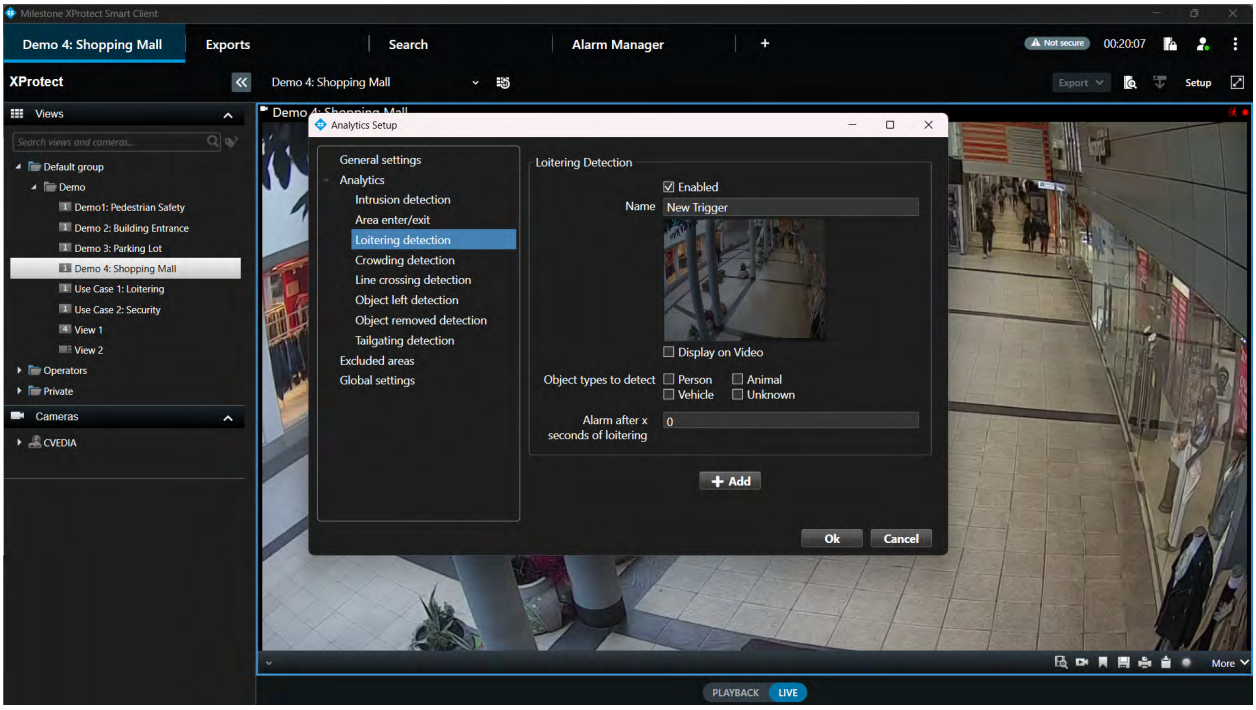
Configuration steps

- Open XProtect Smart Client.
- Click on the CVEDIA logo at the top right corner of a video stream.
- Click directly on the image under “New Trigger” to define the detection zone. Draw a custom polygon to encompass the area for detection.
- In the “Name” field, you can give a custom name to the zone of interest.
- Tick the “Display on Video” box to visualize the defined area on the live video stream.
- Select the different Object Types (person, vehicle, animal, unknown) that you would like to detect within each defined area.
- Select which event to trigger: Enter & Exit, Enter Only & Exit Only.
- Additional zones can be defined by clicking “+ Add”.

Loitering Detection

Definition

Detects objects that stay in the defined area longer than a specified time. An event will be triggered when a target object remains in the area for a duration of x seconds.



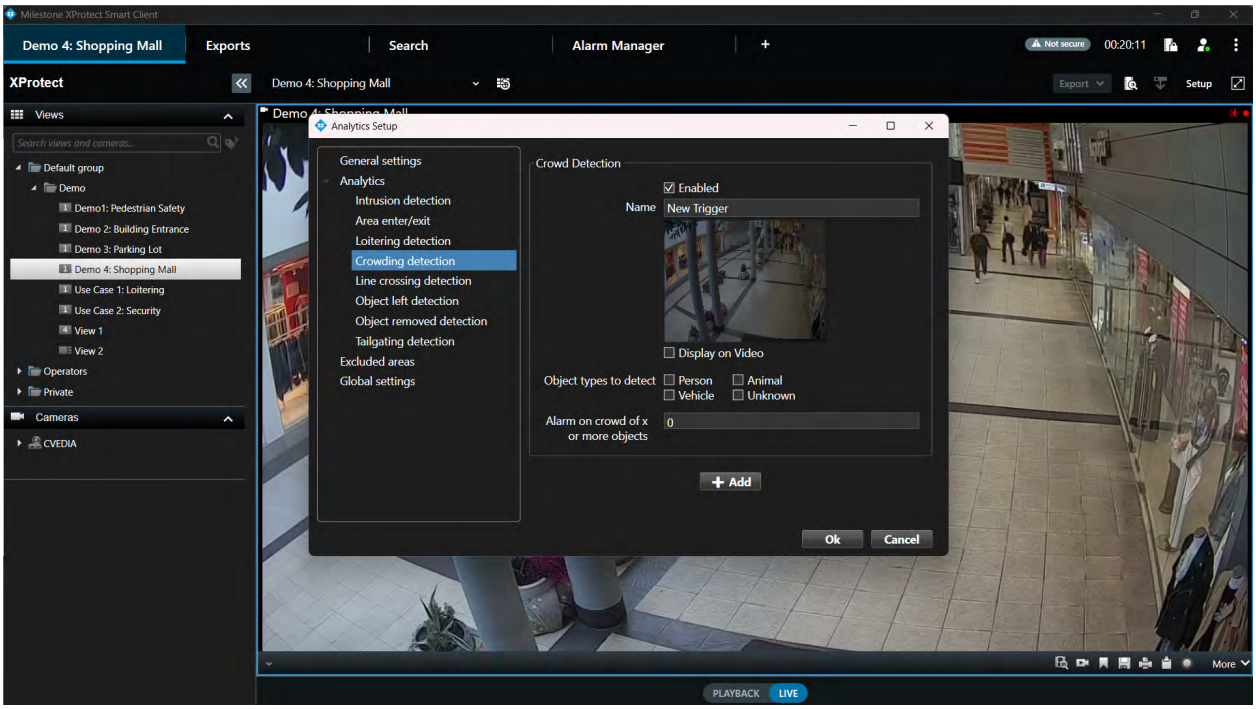
Configuration steps

- Open XProtect Smart Client.
- Click on the CVEDIA logo at the top right corner of a video stream.
- Click directly on the image under “New Trigger” to define the detection zone. Draw a custom polygon to encompass the area for detection.
- In the “Name” field, you can give a custom name to the zone of interest.
- Tick the “Display on Video” box to visualize the defined area on the live video stream.
- Select the different Object Types (person, vehicle, animal, unknown) that you would like to detect within each defined area.
- Set the duration threshold for triggering events.
- Additional zones can be defined by clicking “+ Add”.

Crowding Detection

Definition

Detects when the number of objects within a defined area at any given time reaches a set threshold. For instance, it could be a useful feature to detect a sudden increase of people in a queue in front of an ATM or in a commercial environment.



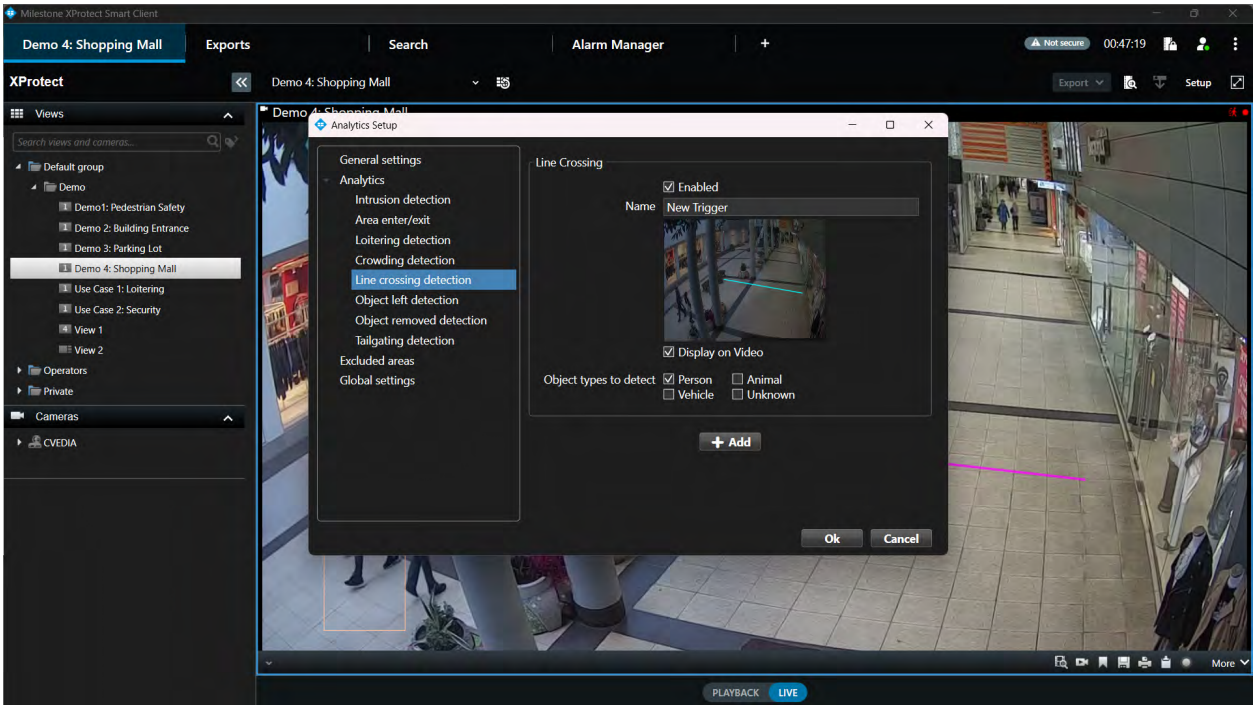
Configuration steps

- Open XProtect Smart Client.
- Click on the CVEDIA logo at the top right corner of a video stream.
- Click directly on the image under “New Trigger” to define the detection zone. Draw a custom polygon to encompass the area of interest.
- In the “Name” field, you can give a custom name to the zone of interest.
- Tick the “Display on Video” box to visualize the defined area on the live video stream.
- Select the different Object Types (person, vehicle, animal, unknown) that you would like to detect within each defined area.
- Specify the minimum number of objects required to trigger an event.
- Additional zones can be defined by clicking “+ Add”.

Line Crossing

Definition

Detects objects that cross a defined line. You have the option to create a multi-segment virtual line. This feature allows you to select the direction in which you intend to monitor the movement of objects.



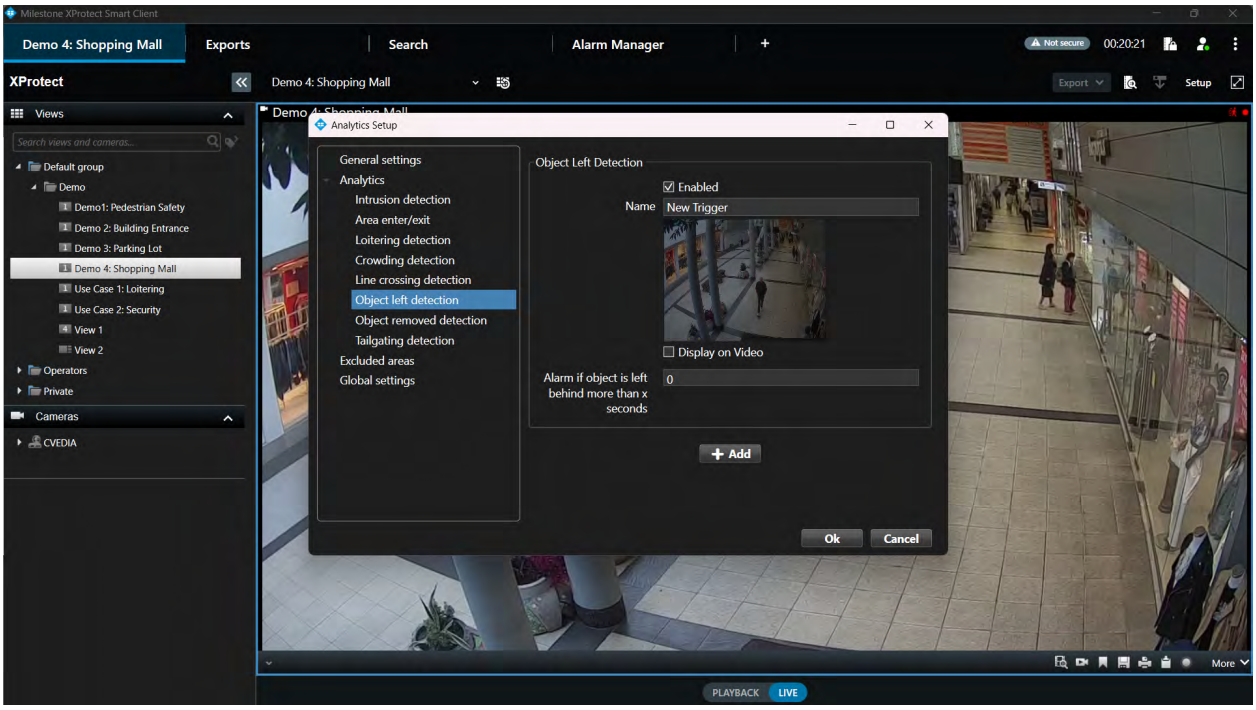
Configuration steps

- Open XProtect Smart Client.
- Click on the CVEDIA logo at the top right corner of a video stream.
- Click directly on the image to create a virtual line.
  - » Click once to create new points of the line, then click on the last point to end it.
  - » Define the direction of movement for object tracking. Click on the Arrows to choose which direction you would like to use to trigger events.
- In the “Name” field, you can give a custom name to the zone of interest.
- Tick the “Display on Video” box to visualize the virtual line on the live video stream.
- Additional lines can be defined by clicking (+ Add).

Object Left Detection

Definition

Detection of objects being left in a specified area, indicating potential delivery or object abandonment.



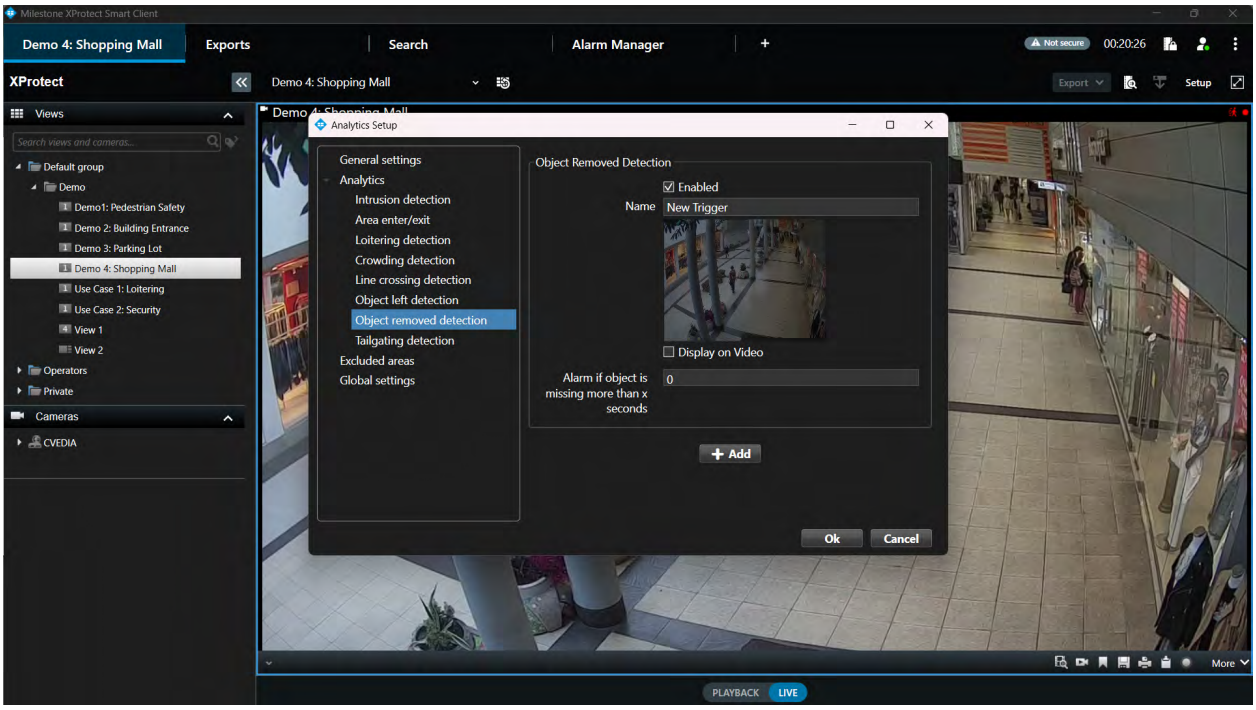
Configuration steps

- Open XProtect Smart Client.
- Click on the CVEDIA logo at the top right corner of a video stream.
- Click directly on the image under “New Trigger” to define the zone of interest. Draw a custom polygon to encompass the area for detection.
- In the “Name” field, you can give a custom name to the zone of interest.
- Tick the “Display on Video” box to visualize the defined area on the live video stream.
- Set the duration threshold for triggering events.
- Additional zones can be defined by clicking “+ Add”.

Object Removed Detection

Definition

Detection of objects being removed from a specified area, indicating potential theft.



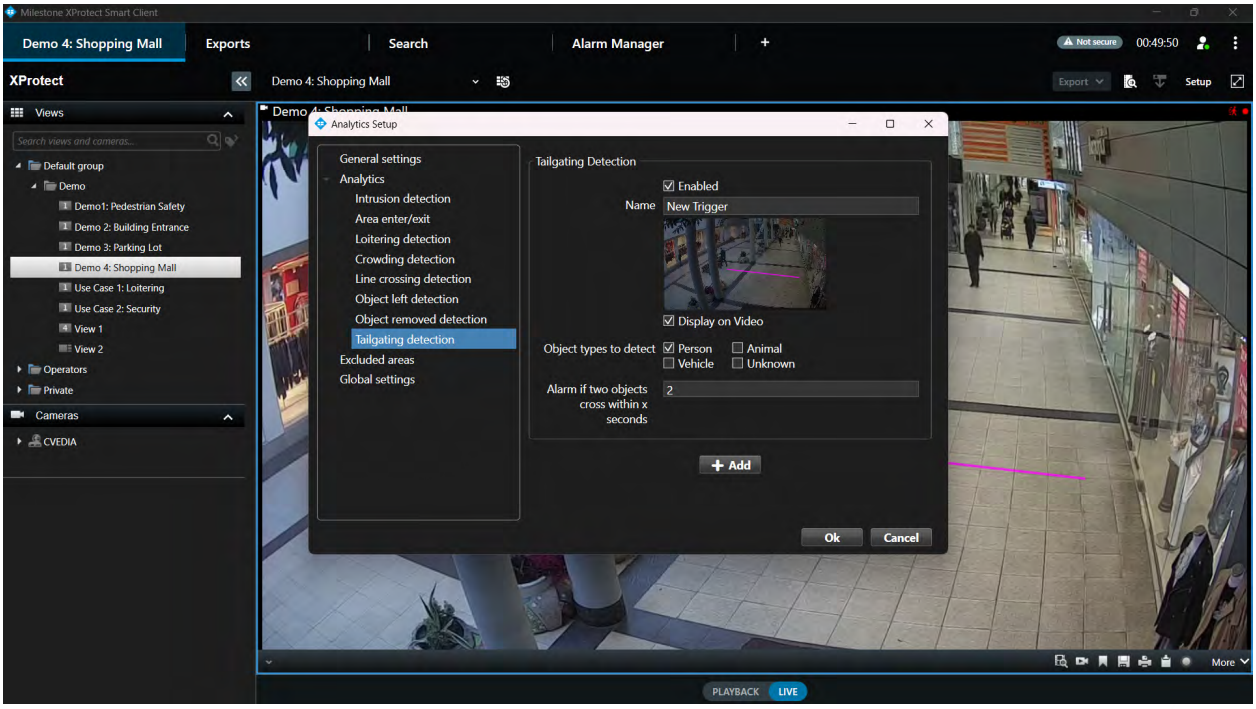
Configuration steps

- Open XProtect Smart Client.
- Click on the CVEDIA logo at the top right corner of a video stream.
- Click directly on the image under “New Trigger” to define the zone of interest. Draw a custom polygon to encompass the area for detection.
- In the “Name” field, you can give a custom name to the zone of interest.
- Tick the “Display on Video” box to visualize the defined area on the live video stream.
- Set the duration threshold for triggering events.
- Additional zones can be defined by clicking “+ Add”.

Tailgating Detection

Definition

The tailgating feature detects if more than one object crosses a virtual line during a predefined time interval. This feature could be useful for detection of multiple individuals or vehicles following each other in close proximity to gain access to a secured area.



Configuration steps

- Open XProtect Smart Client.
- Click on the CVEDIA logo at the top right corner of a video stream.
- Click directly on the image under “New Trigger” to define the zone of interest. Draw a custom polygon to encompass the area for detection.
- In the “Name” field, you can give a custom name to the virtual line.
- Tick the “Display on Video” box to visualize the virtual line on the live video stream.
- Set the duration threshold for triggering events.
- Additional zones can be defined by clicking “+ Add”.

Smart Events

Once the analytics are set up on at least one stream, events will start appearing in the Milestone XProtect system. To view these events, use the search feature in the XProtect Smart Client:

1. Navigate to the “Search” tab.
2. Select the cameras with CVEDIA-RT analytics enabled.
3. Click the “Search for..”. button and choose “Smart Events” to locate CVEDIA-RT events.
4. Specify a timeframe to display all analytics-generated events within that period.

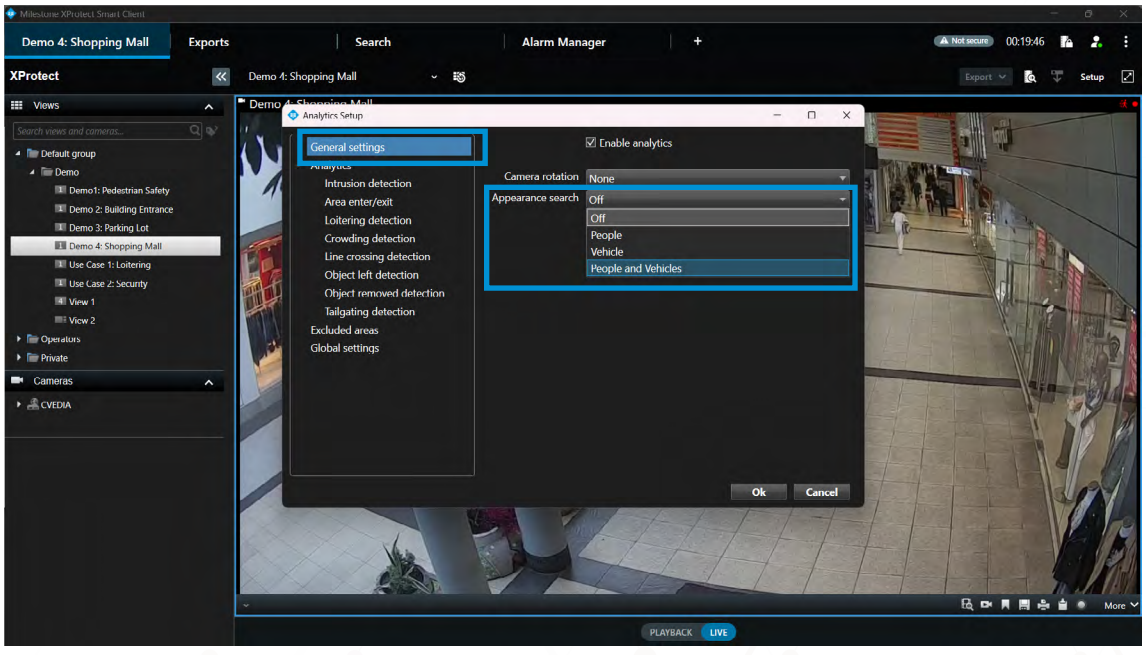
To narrow down the results, use the filtering options. These allow you to search for specific object classes or focus on particular analytics.

Retrospective Search by Appearance

Appearance Search feature allows users to leverage Smart events feature within Milestone XProtect to identify objects matching search parameters based on clothing color and vehicle type and/or color. This feature simplifies the process of locating specific individuals or vehicles within extensive video archives.

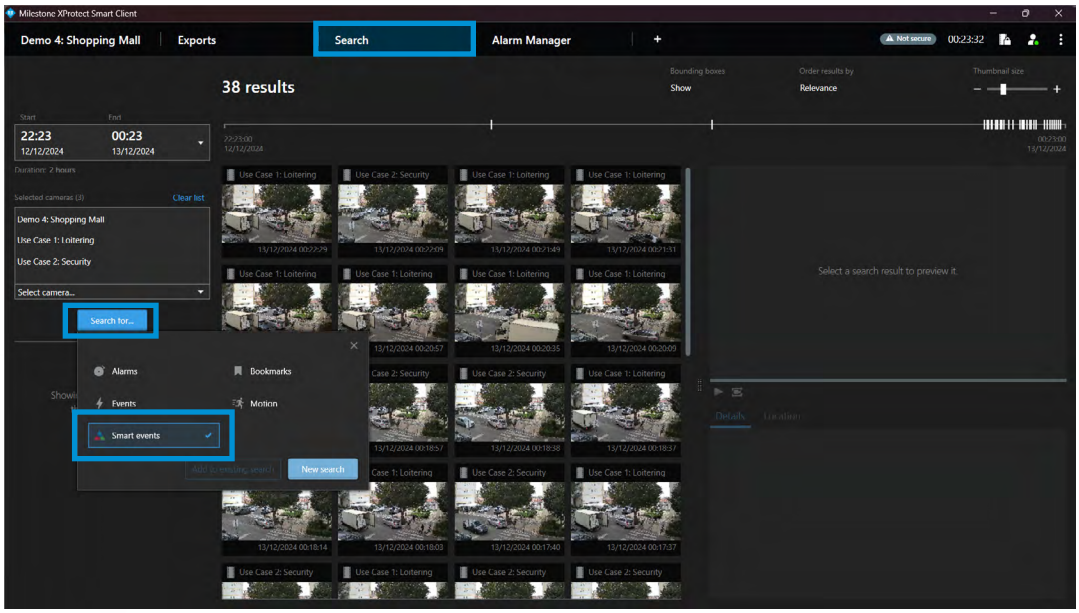
To enable Appearance Search feature:

- Open XProtect Smart Client.
- Click on the CVEDIA logo at the top right corner of a video stream.
- Open the “General settings” menu.
- In the “Appearance search” field, enable the feature by selecting one of the options from the dropdown menu: Person, Vehicle, or Person & Vehicle.

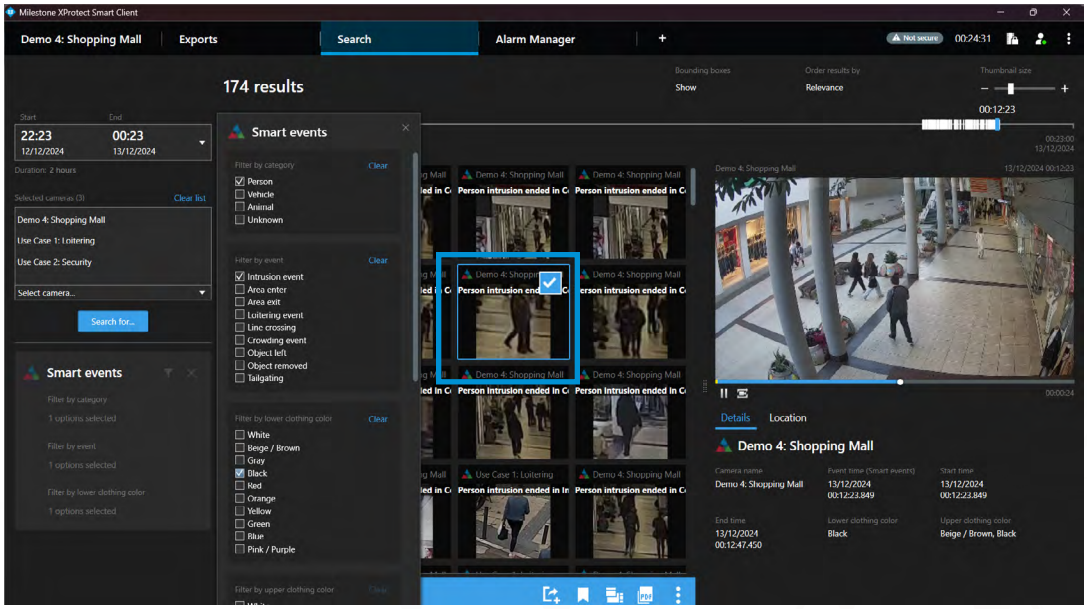


Once the Appearance Search feature is enabled, you can leverage Smart events functionality to filter out objects within existing detections based on vehicle type/color and clothing color.

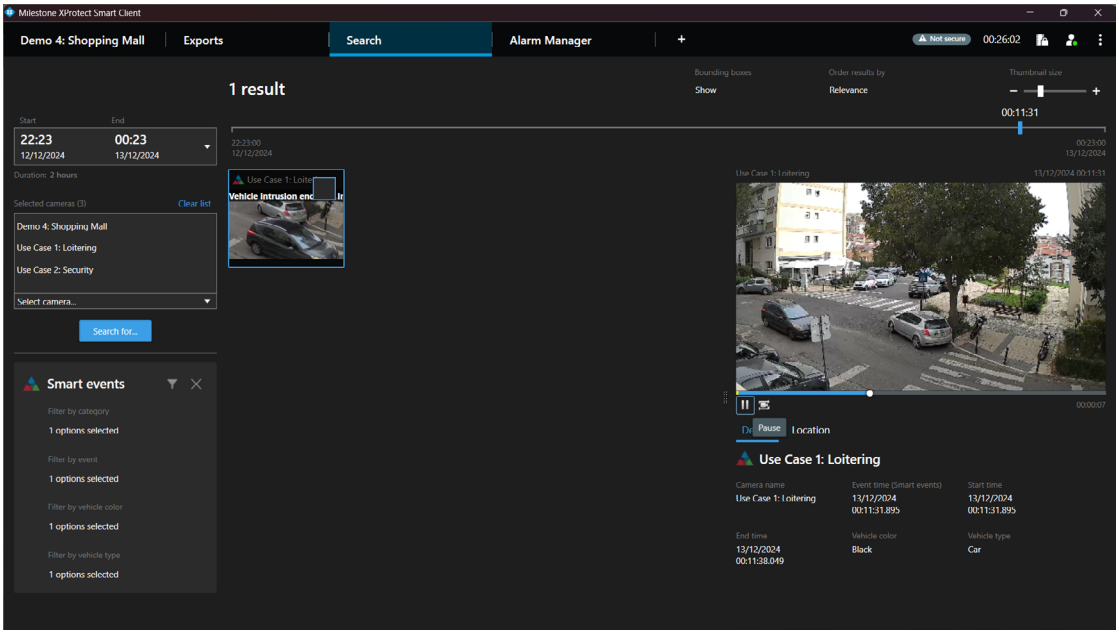
- Go to the “Search” tab of the XProtect Smart Client.
- On the left side of the window, click on the “Search for” button, select “Smart events” and click “New search”.



- In the “Smart events” section multiple filters will be available for selection.

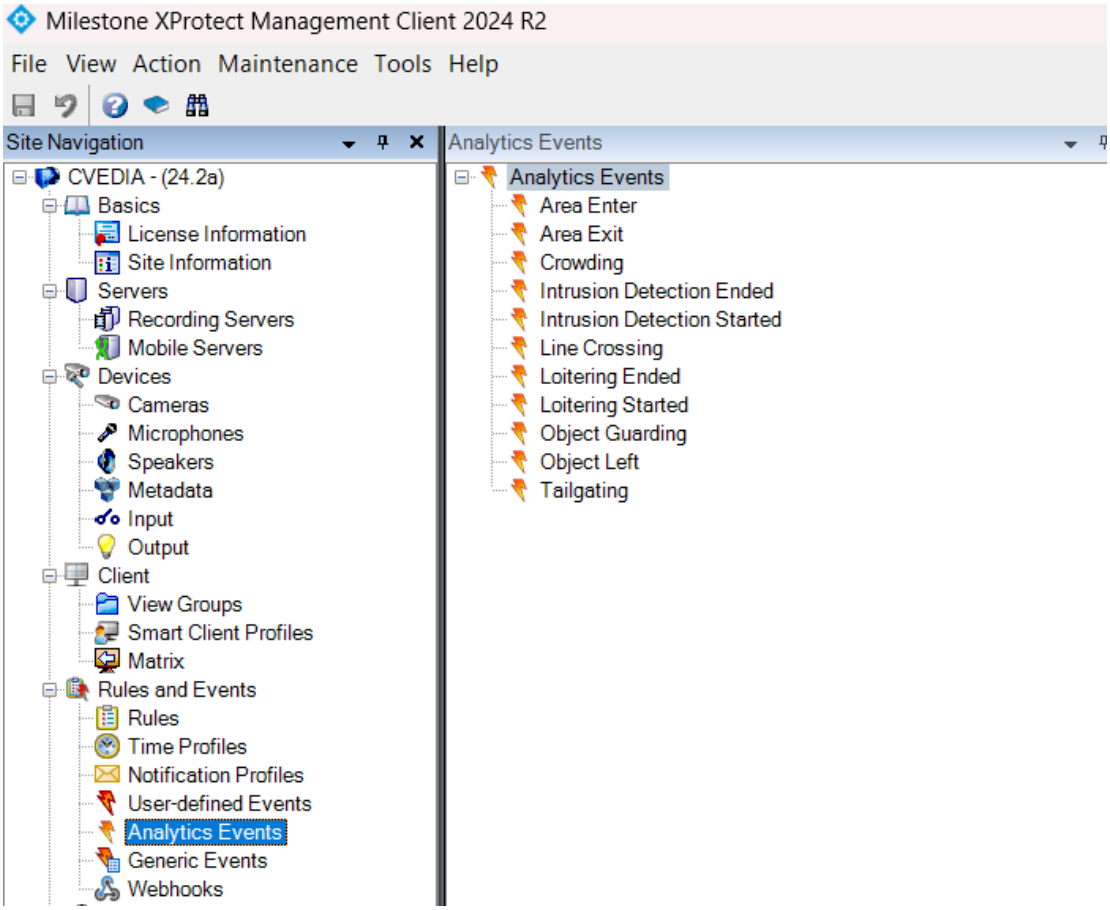


- Select a thumbnail of the target object, and watch the preview on the right side of the window.



Creating Rules

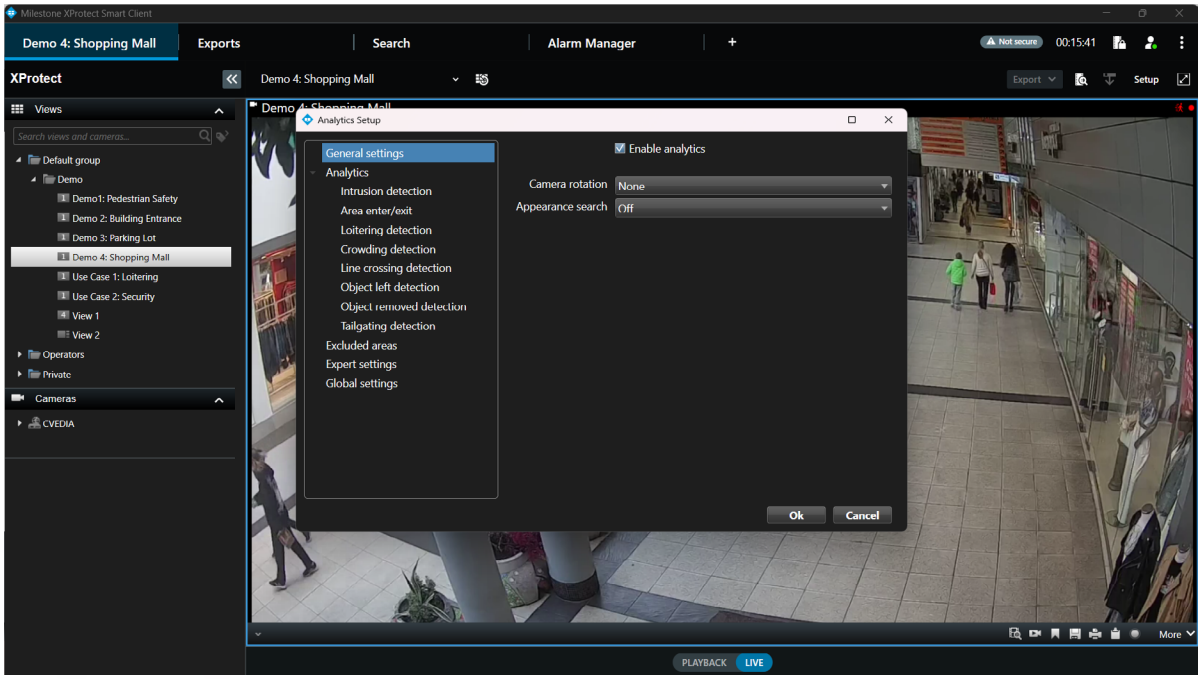
Using the XProtect Management Client, you can configure new rules triggered by CVEDIA-RT Analytic Events. Below is a list of the available events you can incorporate into your rule configurations.



Section 4: Plugin Settings

General Settings

The general settings section contains the options that apply to all analytic scenarios for this camera stream.



Check the “Enable analytics” box to activate the analytics on a given stream.

Notes

- This operation will increase the number of active AI channels.
- If the “Enable analytics” checkbox is unchecked, the stream is ignored and not counted toward the limits of the license.

Camera Rotation

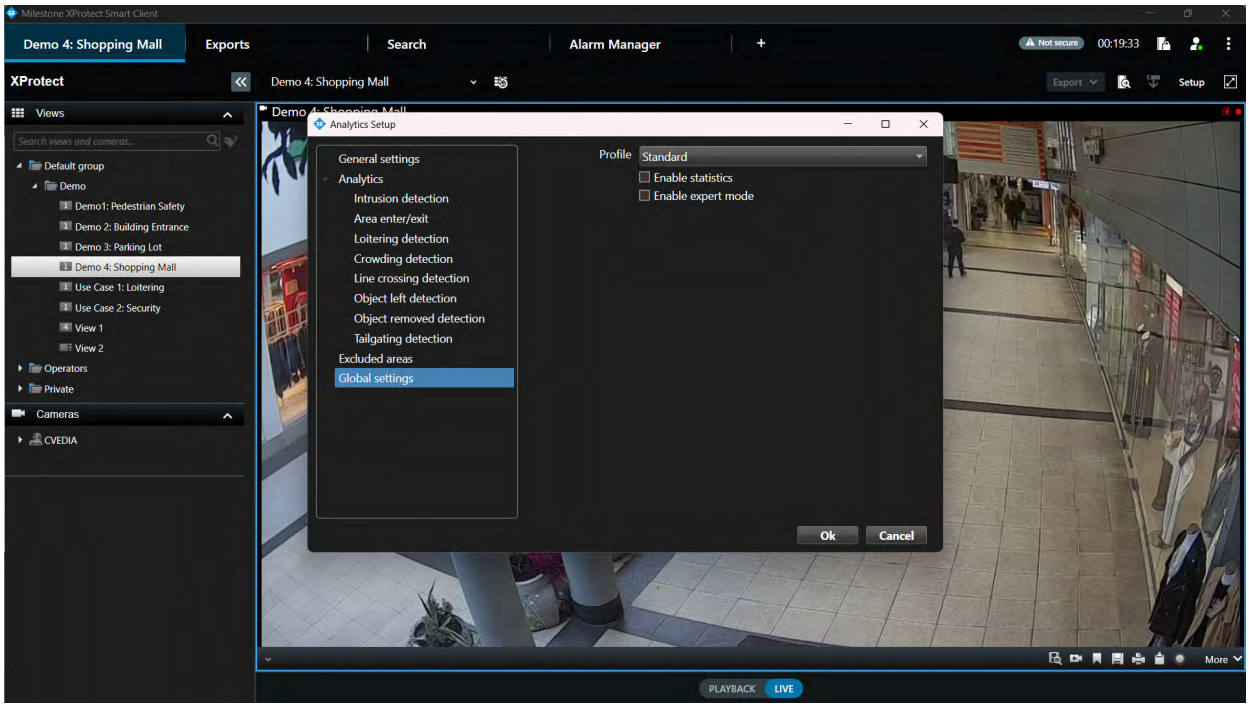
The camera rotation feature lets you adjust the orientation of the stream to match the physical rotation of the camera (e.g., when the camera is installed at an angle or upside down).

Appearance Search

The “Appearance Search” dropdown menu enables you to activate appearance analytics, allowing detection and analysis for people, vehicles, or both.

Global Settings

Global settings are applied universally to all channels where analytics are activated.



Profile Selection

The **Profile** dropdown menu allows users to switch between the **Standard** and **Hi-Res** profiles:

Standard Profile

- Default and recommended setting.
- Uses the secondary camera stream to provide optimal performance while maintaining high accuracy for typical security analytics.
- Offers a balanced approach to system performance and detection precision.

Hi-Res Profile

- Utilizes the primary camera stream and a larger AI model.
- Designed for detecting smaller or distant targets and handling crowded environments.
- Recommended only when the Standard profile does not meet detection requirements.

Enable Statistics

Displays detailed, real-time analytics information as an overlay in the top-left corner of the camera view.

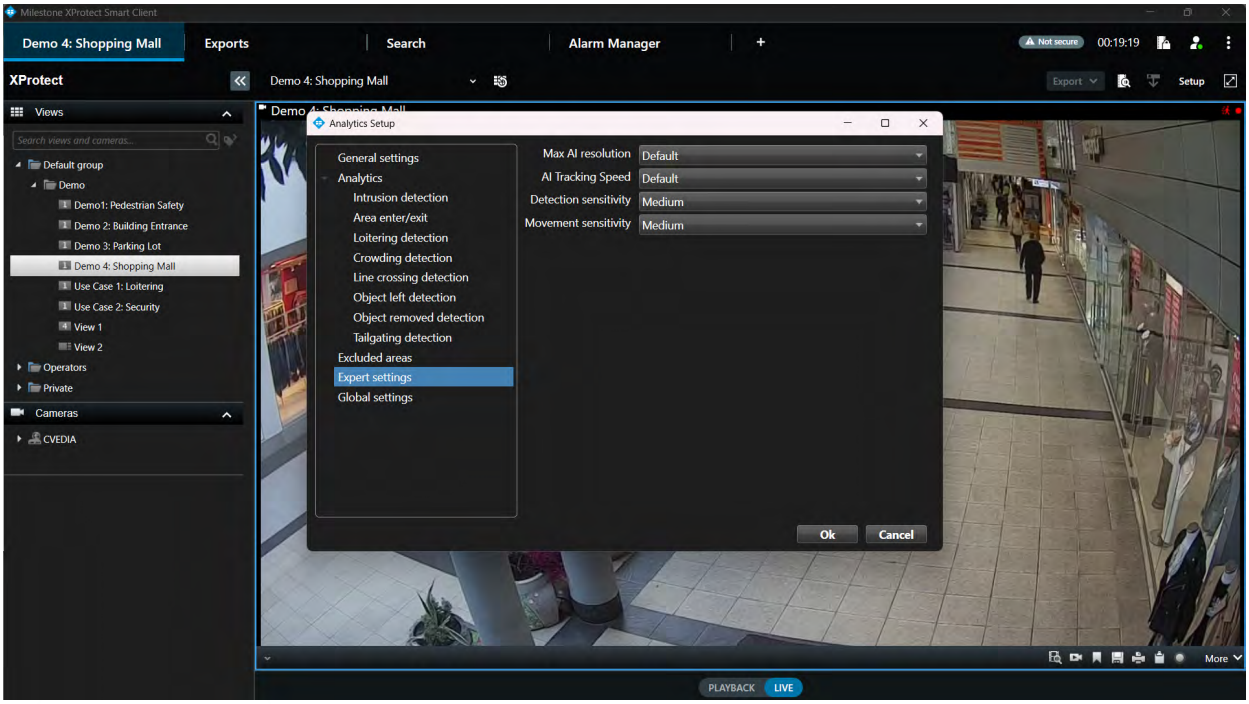
Statistics Info Includes:

- Engine version
- Plugin version
- Solution version
- Milestone Version
- Plugin run time
- Plugin Mode
- Camera input
- AI input
- Codec
- Frame time
- Input queue
- Dropped frames
- Instance run time
- # frames processed
- Dispatcher occupancy
- Decoder
- Accelerator
- AI models
- Active licenses

Enable Expert Mode

Reveals the Expert Settings menu in the left panel for advanced configuration.

Expert settings



Max AI Resolution

The Max AI Resolution setting allows you to define the maximum resolution that the AI processes. By default, this value is determined by the profile specified in the Global Settings, but it can be adjusted to meet specific requirements.

- If a resolution higher than the camera's native resolution is set, the plugin will automatically default to the camera's maximum supported resolution.
- Increasing the resolution can improve the detection of smaller targets.

Important

Only increase the resolution if absolutely necessary, as higher resolutions may significantly impact system performance.

AI Tracking Speed

The AI Tracking speed feature enables users to adjust the frame rate at which the AI processes data.

Modifying this from the default setting may impact server performance and reduce the number of AI streams that can run simultaneously on the same device.

Default:	5 FPS	Optimized for most of the security surveillance use cases.
Fast:	10 FPS	Optimized for tracking faster moving targets (e.g. cyclists).
Very Fast:	15 FPS	Optimized for capturing targets that move very fast (e.g. electric scooters).

Choose the appropriate speed based on the tracking requirements and the server's capacity to handle the additional load.

Detection Sensitivity

Increasing detection sensitivity improves the ability to detect challenging targets (e.g., smaller, occluded, or affected by lens noise) but may lead to more False Positives. Change "Detection Sensitivity" settings to "High" if the system misses events involving small objects or in busy scenes.

Movement Sensitivity

The Movement Sensitivity setting determines how the system detects motion within the camera's view. This setting can be adjusted to account for environmental factors such as rain, snow, camera noise, or light reflections, which might trigger false motion detections.

Low Sensitivity

- Reduces false motion detections caused by environmental conditions.
- Suitable for minimizing noise in challenging environments.

High Sensitivity

- Improves detection of fast-moving objects or objects that are visible for only a short duration.
- May increase False Positives under certain environmental conditions.

Section 5: Advanced Configuration

This section provides details about advanced configuration options designed for XProtect system administrators. While these settings are not necessary if the installation and initial configuration have been successfully completed, they can be useful for addressing specific or specialized use cases.

User Credentials

If you need the integration to use a different XProtect user, you can update the credentials directly through the command line without editing any configuration files.

Follow these steps:

1. Stop the CVEDIA-RT Controller Service:
Ensure the CVEDIA-RT Controller Service is stopped via the Windows Services application before proceeding.

2. Open an Administrative Command Prompt:

- Navigate to the folder where the integration is installed: ***C:\ProgramData\CVEDIA\CVEDIA-RT\files\MilestoneController.***
- Open a command prompt session with administrative privileges in this directory.

3. Run the Controller Executable:
Use the following command format to update the credentials:
.\RTController.exe -c -u <username> -p <password> -a <method> -s -m <server_uri> -r -i <remote_ip>

Parameters Explanation:

- ***-u <username>:*** The new XProtect username.
- ***-p <password>:*** The new XProtect password.
- ***-a <method>:*** Authentication method.
- ***-s:*** Indicates secure communication.
- ***-m <server_uri>:*** The XProtect server URI.
- ***-r:*** Enables remote login mode.
- ***-i <remote_ip>:*** The remote IP address.

4. Verify and Save:
The controller will attempt to log in to the XProtect system using the specified credentials. If the login is successful, the new settings will be saved and used automatically in future sessions.

Parameters Reference Table

The following table provides details about the parameters used with the ***RTController.exe*** command to update XProtect user credentials.

Parameter	Required	Description
-c	YES	Runs the controller executable in credential-setting mode.
-u <username>	YES	Specifies the new username to be used.
-p <password>	YES	Specifies the password for the new user.
-a <method>	YES	Authentication method for logging into XProtect. The integration requires **Basic user authentication** (refer to the installation guide for more details).
-m <server_uri>	YES	Specifies the URI of the XProtect server (e.g., ***http://localhost***).
-s	NO	Optional. Enforces secure connection when connecting to XProtect. Use this parameter if required by your system configuration for successful login.
-r	NO	Optional. Enables CVEDIA-RT remote mode. Use this only if CVEDIA-RT is running on a different server.
-i <remote_ip>	NO	Optional. Specifies the IP address of the remote CVEDIA-RT server. This is used in combination with the ***-r*** parameter. If not specified, the server is auto-discovered.

Example: Changing Credentials for Local Setup

Below is an example command to configure the system to use the basic XProtect user ***TestUser***, with both the XProtect server and CVEDIA-RT running on the local machine:

RTController.exe -c -u TestUser -p Password123! -a Basic -m http://localhost

Final Step: Restart the Controller Service

If you manually stopped the **CVEDIA-RT Controller Service** in the Windows Services application during the process, ensure that you restart the service for the changes to take effect.

Section 6: Updating

- Check for new plugin versions on the official website:

  https://rt.cvedia.com/Milestone

- Download the new version.
- Before running the installer to update to a new release of the CVEDIA-RT Plugin, make sure to close the Smart Client and the Management Client, and stop the Management Server.
- All configured settings and applied licenses will be preserved.

Section 7: Uninstalling

- Close the Smart Client and the Management Client, and stop the Management Server.
- Open Settings: press Windows key + I or click the Start menu.
- Go to Apps: click on Installed Apps and find CVEDIA-RT Plugin for VMS in the list.
- Uninstall the Plugin: select CVEDIA-RT Plugin for VMS and click Uninstall. Confirm if prompted.
- If prompted, restart your computer to complete the process.
- Done! The Plugin is now uninstalled.

Learn More
Access online documentation

Technical Support
Ask for help

Contact Sales
support@cvedia.com