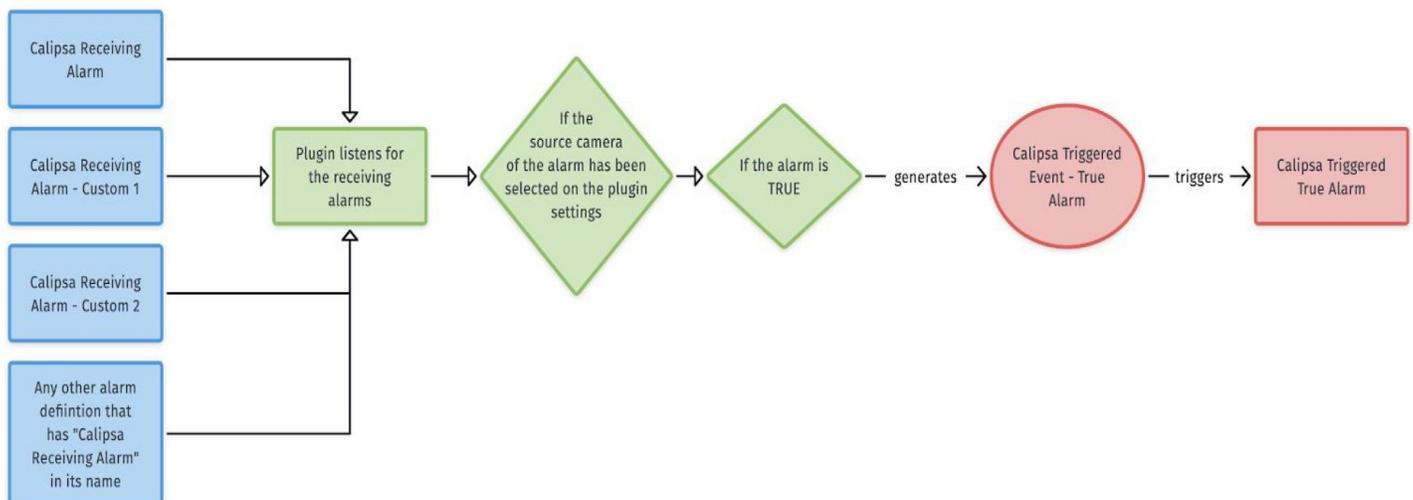


Calipsa Milestone Plugin Integration

Welcome! This guide walks you through the process of installing the Calipsa Milestone Plugin

How It Works

- The plugin will listen to any alarms generated by XProtect that have **Calipsa Receiving Alarm** as a substring of their name. This alarm definition, which is created by default, listens to **XProtect's Motion Detected system event**.
- If Calipsa marks the alarm as true, it'll generate the **Calipsa Triggered Event - True Alarm** analytics event that the plugin created itself. This event will, in turn, trigger the **Calipsa Triggered True Alarm** alarm (this can be verified by looking at the triggers of the Calipsa Triggered True Alarm definition).
- The definition of **Calipsa Receiving Alarm** basically controls what kinds of events (system, analytics, device events, etc) the plugin listens for. Hence, by extending/updating this definition (for example changing the default Motion Detection trigger to some camera in-built device event) we can change what Calipsa responds to and what it discards.



- **Calipsa Triggered Event - True Alarm** and **Calipsa Triggered True Alarm** can also be viewed in the **Smart Client**; via **rules and triggers**, various actions can also be executed when they occur.

Prerequisites

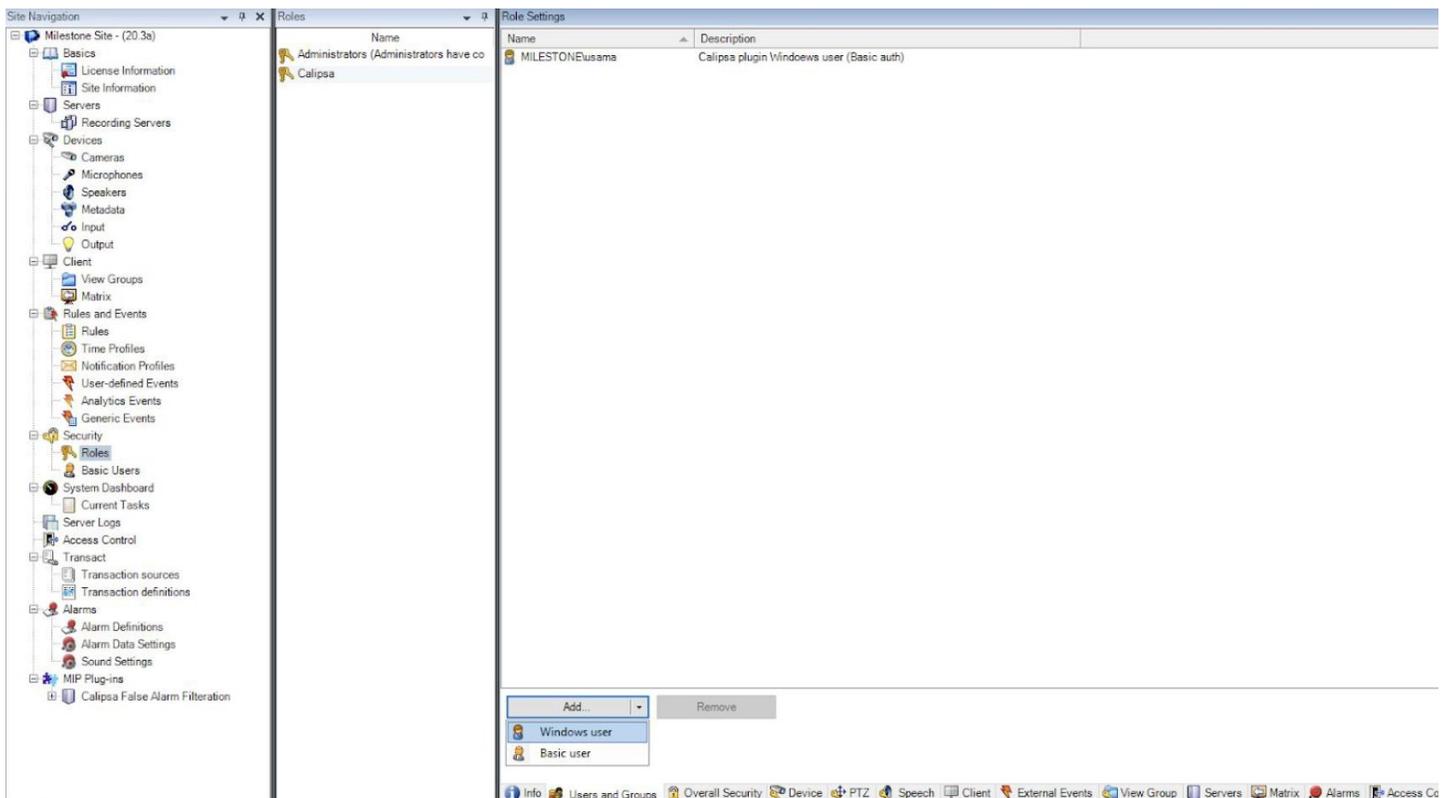
Remote Access

- Calipsa requires the Management Server, Image Server and Analytics Events to be remotely accessible in order to fetch images and post true alarms.
- These services run, by default, on local ports **80**, **7563** and **8888** for a standard XProtect installation.
- The following IPs will be used to make the requests for fetching the images and posting true alarms back into XProtect. Hence they should be allowlisted:

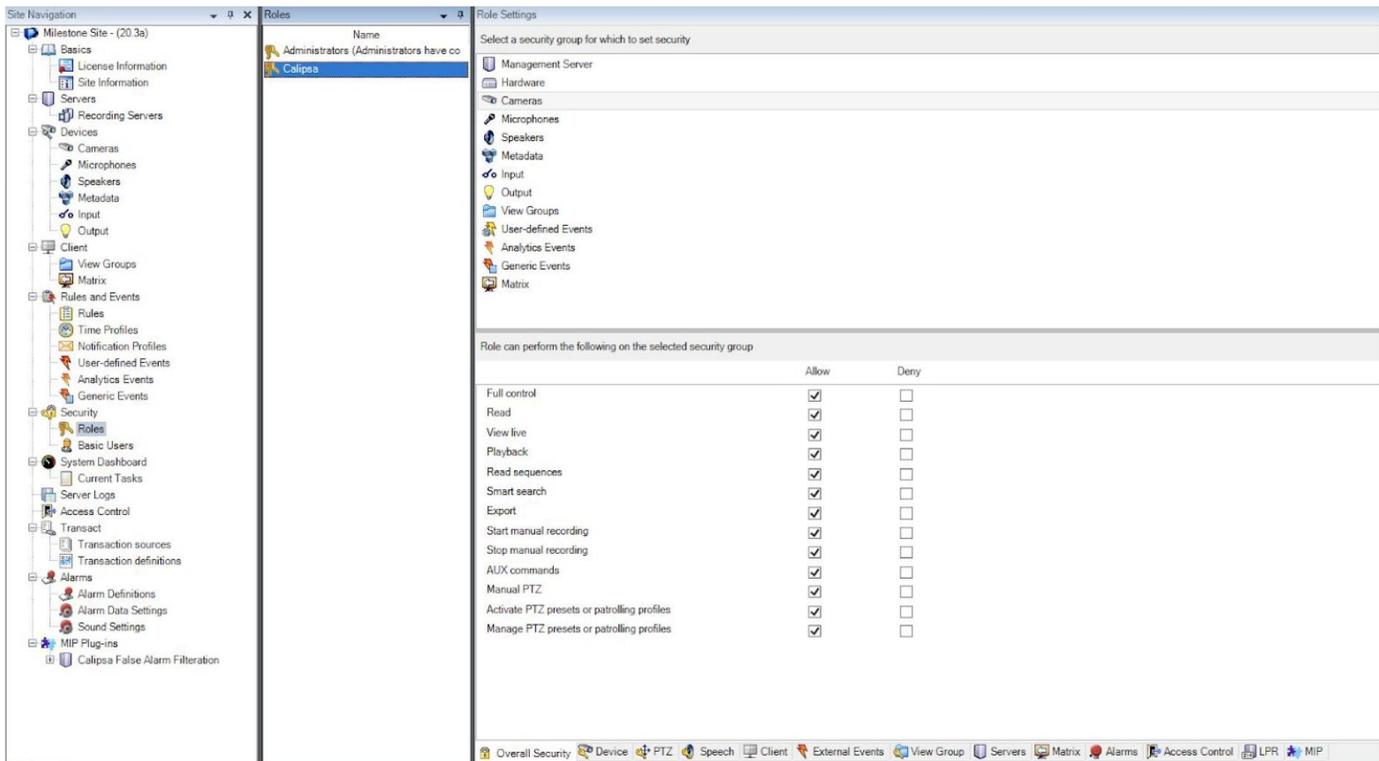
52.19.32.51 | 34.250.135.186 | 63.32.238.104 | 52.212.236.183

Windows User With XProtect Access

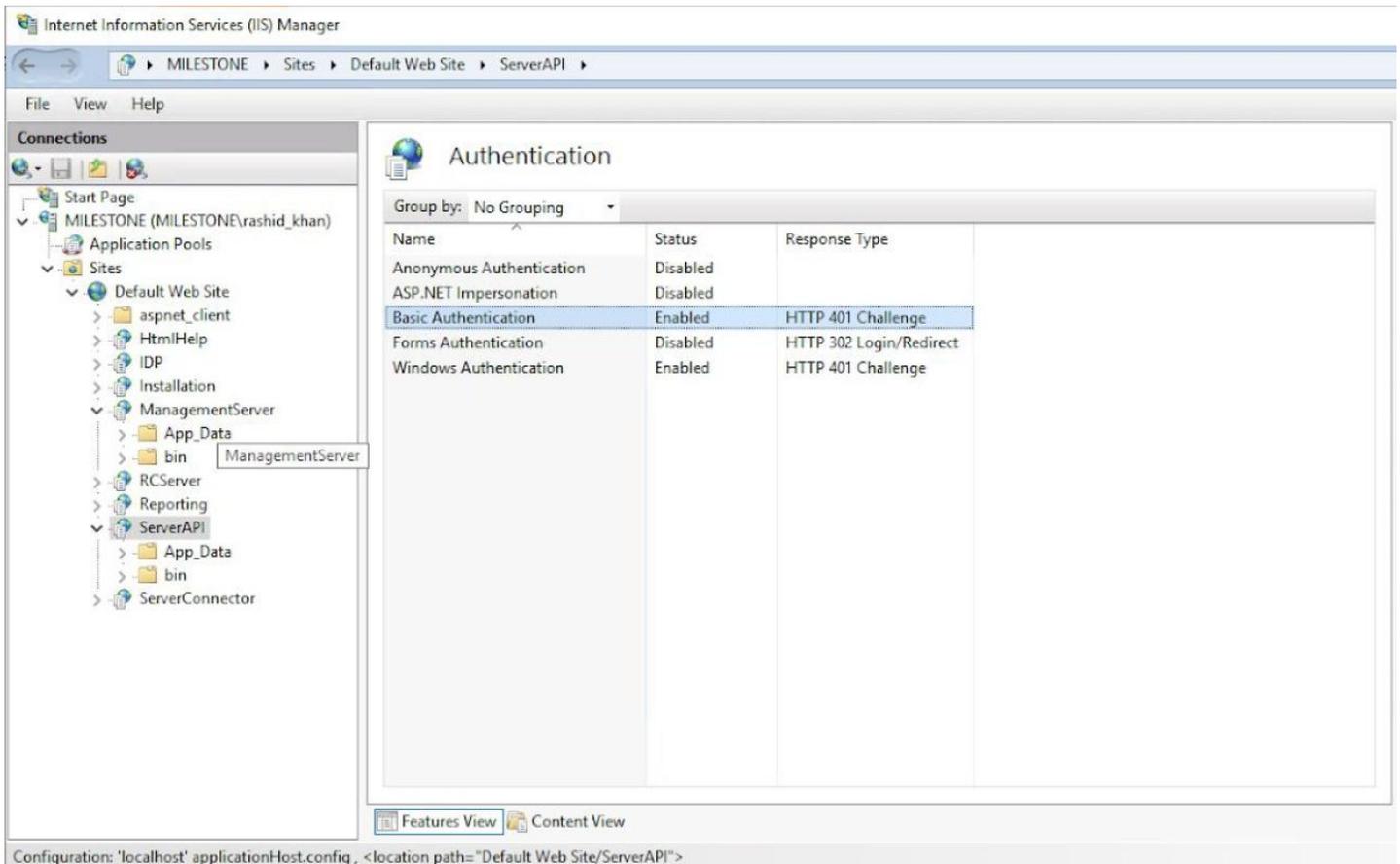
- We suggest creating a dedicated Windows user on the machine on which XProtect is installed, and then adding this user via the Management Client to a new, dedicated role that essentially gives it access to camera footage and allows remote logins.
- Having a dedicated Windows user solely for the integration with a dedicated role is considered good practice since it allows isolating access and not exposing information on existing accounts:



The screenshot displays the XProtect Management Client interface. On the left is the 'Site Navigation' tree, with 'Roles' selected under the 'Security' section. The main area is split into two panes: 'Roles' and 'Role Settings'. The 'Roles' pane shows a list of roles: Administrators (Administrators have co...), Calipsa, and MILESTONEusama. The 'Role Settings' pane shows the configuration for the selected role, MILESTONEusama, with a description of 'Calipsa plugin Windows user (Basic auth)'. At the bottom of the 'Role Settings' pane, there is an 'Add...' button and a 'Remove' button. The 'Add...' button is active, showing a list of users: 'Windows user' and 'Basic user'. The bottom status bar includes various system icons and labels like 'Info', 'Users and Groups', 'Overall Security', 'Device', 'PTZ', 'Speech', 'Client', 'External Events', 'View Group', 'Servers', 'Matrix', 'Alarms', and 'Access Co'.



- o Also make sure that **Basic** and **Windows authentication** is enabled for **ServerAPI** and **ManagementServer**. This can be done from the **Microsoft IIS Manager**:

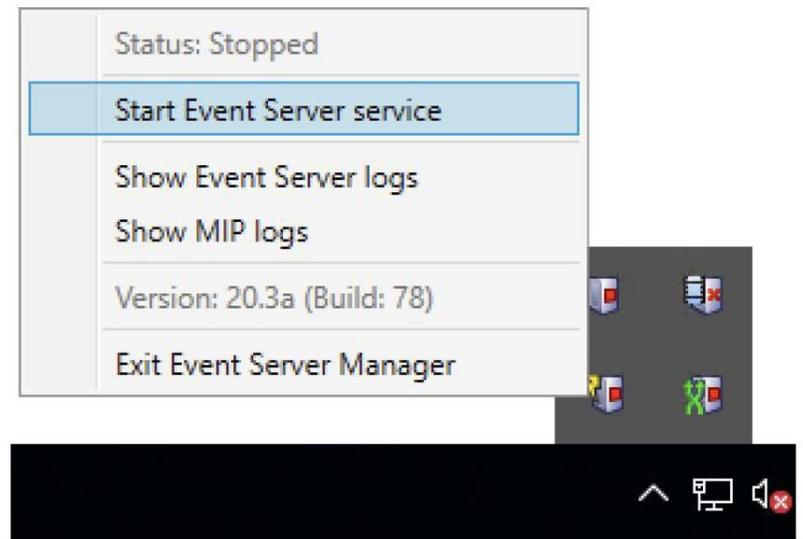
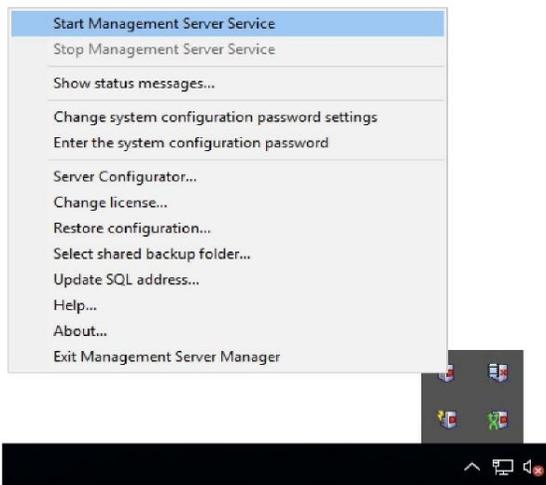


Installation

- Calipsa will provide a zipped file containing the plugin installation libraries. This should be unzipped, and the extracted folder should be copied to the **MIPPlugins** folder inside the **Milestone installation folder**:

C:\Program Files\Milestone\MIPPlugins

- Please stop and then restart the **Management Server** and the **Event Server** services again to load the newly added plugin:



Activation

 milestone | XProtect®

Calipsa False Alarm Filtration



Configure your plugin with Calipsa's false alarm filtering platform

Calipsa Server Address	<input type="text" value="https://milestone.calipsa.io"/>	Management Server IP	<input type="text"/>
Calipsa Server Port	<input type="text" value="443"/>	Management Server Port	<input type="text" value="80"/>
Calipsa Authentication Token	<input type="text"/>	Username	<input type="text"/>
		Password	<input type="text"/>
Number of tries	<input type="text" value="2"/>	Image Server IP	<input type="text"/>
Timeout (seconds)	<input type="text" value="5"/>	Image Server Port	<input type="text" value="7563"/>
Snapshot count	<input type="text" value="3"/>	Analytics Events Host	<input type="text" value="http://"/>
Gap between images (ms)	<input type="text" value="1000"/>	Analytics Events Port	<input type="text" value="8888"/>
		<input type="checkbox"/> Use TLS?	
	<input type="button" value="Save Settings"/>	<input type="button" value="Commit Credentials to Calipsa"/>	
	<input type="button" value="Select Cameras"/>		
	0 cameras connected		

1. After restarting the **Management Client**, you'll find the **Calipsa False Alarm Filtration** plugin under the **MIP Plug-ins** leaf within the **Site Navigation panel** on the left-hand side of the screen
2. Enter the **Management Server**, **Image Server**, **Windows user**, and **Analytics Events** information. The **username** and **password** will be the ones for the Windows user referred to earlier. Click **Commit Credentials to Calipsa**. If successful, the information will be saved with Calipsa.
3. Create a **Calipsa Authentication Token** via the following method:
 - a. Log into the **Calipsa Dashboard**
 - b. Click **Settings**
 - c. Click the **...** symbol next to **Integrations**
 - d. Click **Milestone**
 - e. Click **Create new token...**
 - f. Copy the token presented within the Calipsa window into the **Calipsa Authentication Token** text field within Milestone
 - g. Click **Save Settings**

4. Choose the cameras to be watched by Calipsa using the **Select Cameras** item picker. After selecting the cameras you want to add Calipsa analytics to, they will also appear within the Calipsa dashboard.
5. Under the **Alarms → Alarm Definitions** leaf in the **Site Navigation** panel, please verify that two new definitions were created by the plugin: **Calipsa Receiving Alarm** and **Calipsa Triggered True Alarm**
6. Under **Rules and Events → Analytics Events** a new analytics event named **Calipsa Triggered Event - True Alarm** will be seen