

INSTALLATION AND CONFIGURATION USER MANUAL

MILESTONE VMS

iSENTRY

POWERED BY **IntellexVision**

2019 / VER 1.0.0:

Copyright © IntelXVision 2019. All rights reserved.

Some trademark information

This document is intended for general Information purposes only and due care has been taken in its preparation. Any risk arising from the use of this information rests with the recipient, and nothing herein should be construed as constituting any kind of warranty.

SmartProtect reserves the right to make adjustments without prior notification.

All names of people and organisations used in this document's examples are fictitious. Any resemblance to any actual organisation or person, living or dead, is purely coincidental and unintended.

This product may make use of third party software for which specific terms and conditions may apply.

CONTENTS

PREREQUISITES.....	2
COMPATABILITY.....	3
SECTION 1: SYSTEM OVERVIEW AND ARCHITECTURE.....	4
SECTION 2: INSTALLING THE SYSTEM.....	8
SECTION 3: CONFIGURING THE SYSTEM.....	15
SECTION 4: GENERAL CONFIGURATION.....	23
SETTINGS.....	24
SERVERS.....	26
DEVICES.....	30
CAMERA CONFIGURATION (ADVANCED CAMERA CONFIGURATION).....	39
CAMERAS.....	48
PROFILES.....	49
ALERTS.....	50
NOTIFICATION.....	51
CONFIGURE TELEGRAM MESSAGING.....	54
REGISTERING RECIPIENTS.....	55
CONFIGURING EMAIL MESSAGES.....	55
SYSTEM STATUS.....	55
SYSTEM LOGS.....	56
TROUBLESHOOTING.....	57

PREREQUISITES

.NET Framework 4.6.1

Installed and functional Milestone VMS system with H.264 encoded camera feeds

Minimum Hardware Requirement

iSentry Analytics (8 X 720p Camera system)

iSentry Processing Server

Intel i5 8400

16 GB Ram

256GB SSD

iSentry Object Classification and Facial Extraction (Deep Learning) Server

Intel i5 8400

4GB Ram

nVidia RTX 2060

COMPATIBILITY

Supported Microsoft Operating Systems

Windows 10 Professional

Windows Server 2016

Supported Milestone Versions

Milestone 2019

XProtect Express+

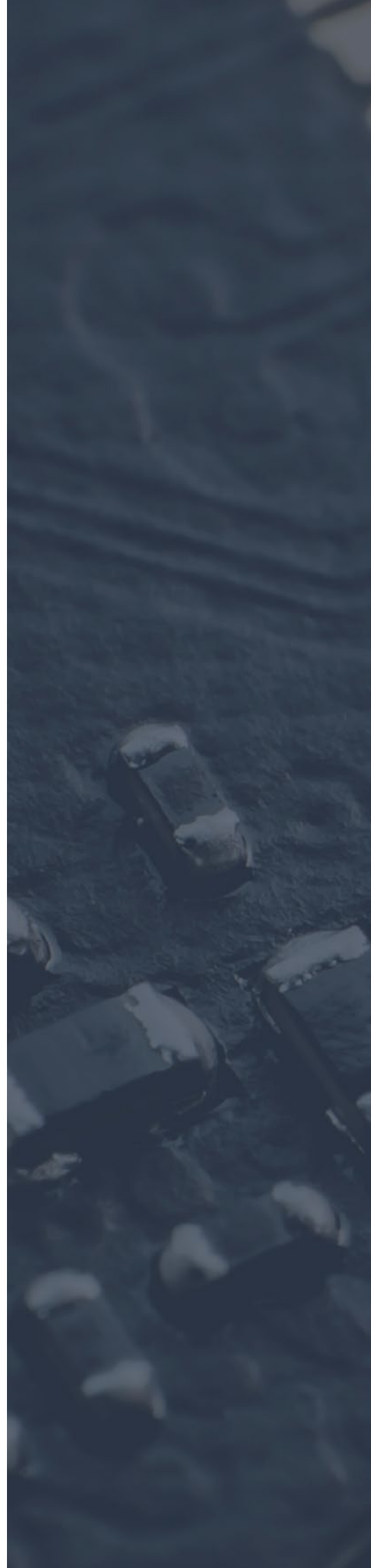
XProtect Professional+

XProtect Expert

XProtect Corporate

Section 1

SYSTEM OVERVIEW AND ARCHITECTURE





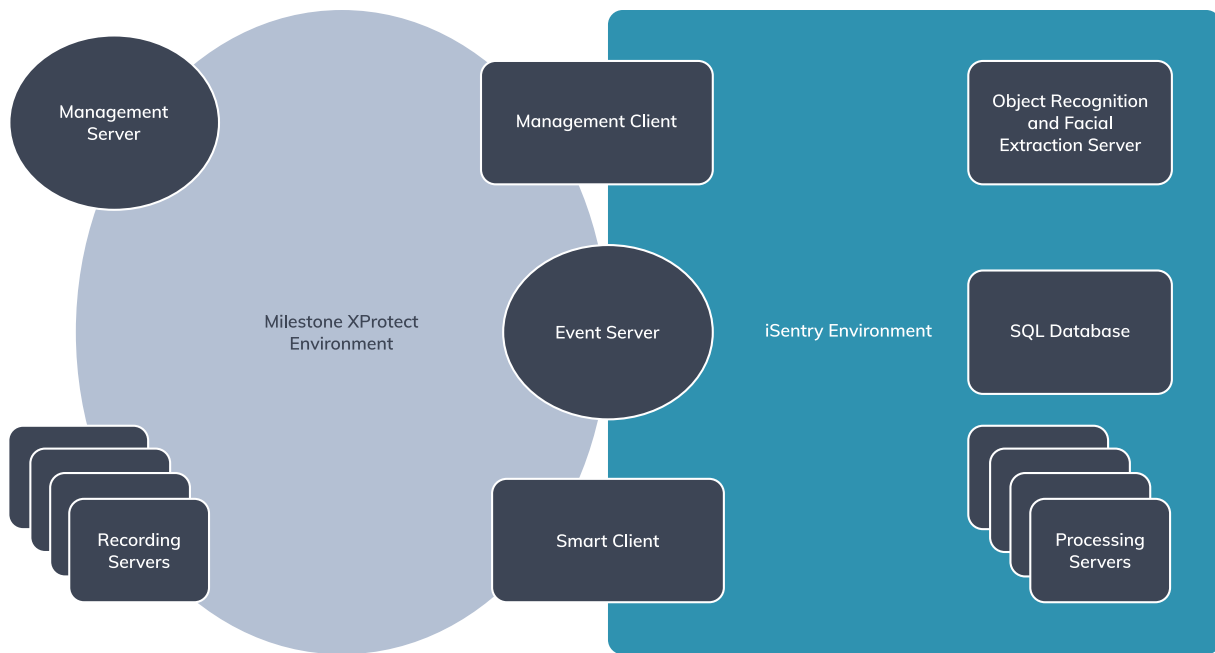


Fig. 1 - Component overview

The above system component overview shows the various Milestone XProtect components as well as the iSentry system components. The overlap as seen for the Management and Smart Clients as well as the Event server, implies that plugins exist for these.

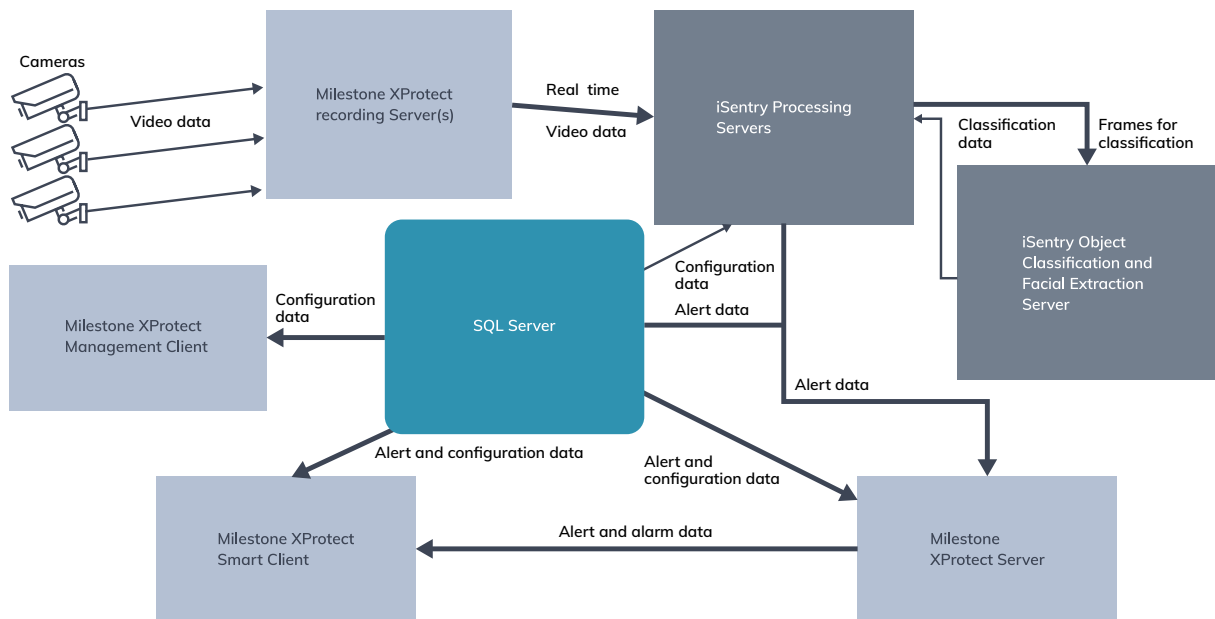
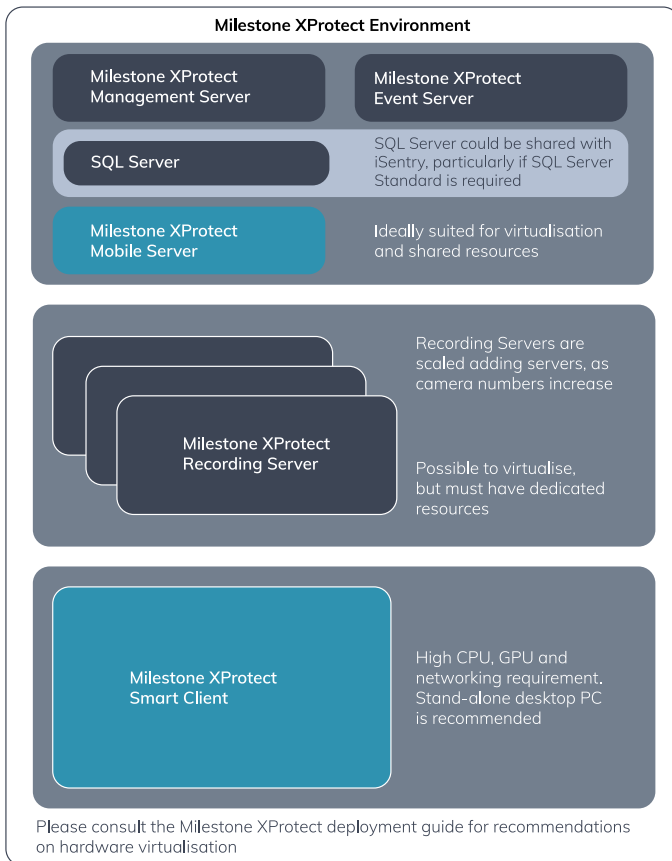


Fig. 2 - Data flow architecture



All data for the system originates at the camera. Video data is captured by one or more recording servers, from where data is directed towards the iSentry Processing Server(s).

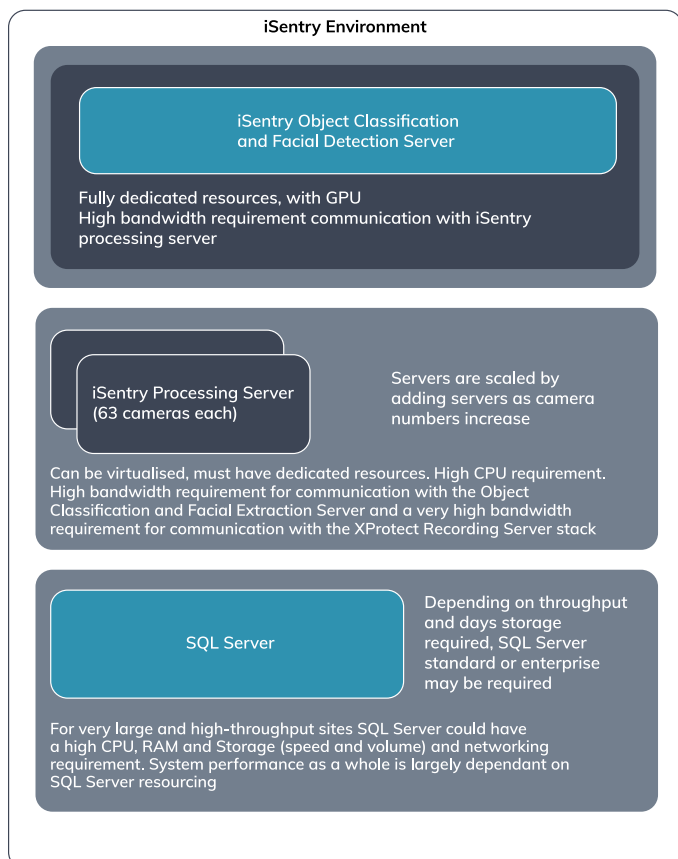
The Processing Server produces alerts which are further enriched by the iSentry Object Classification and Facial Extraction (Deep Learning) Server.

Alerts are stored in a SQL Server Database, and simultaneously communicated to the Milestone XProtect Event server from where alerts are distributed to all connected Milestone XProtect Smart Clients.

Smart Clients are also able to query past alerts directly from the SQL Database.

The XProtect Management Client is primarily responsible for Configuration management which is also stored in the SQL Database.

Fig. 3 - System hardware architecture



From a hardware perspective the iSentry system can be split into three areas

iSentry Object Classification and Facial Extraction (Deep Learning) Server

It is recommended to use physical hardware for this server, with an nVidia GPU. For high volume sites, bandwidth from the Processing Servers will be high.

iSentry Processing Servers

Dedicated resources are important for these servers, particularly from a CPU perspective. Video data for all processed cameras will be transferred from Milestone Recording servers to iSentry Processing Servers, resulting in a very high bandwidth requirement.

SQL Server

SQL Server 2016 Express is part of the default installation of the system. This is a free version and is limited in terms of performance and size. The physical data file is limited to 10GB in size, RAM is limited to 1410 MB and CPU is limited to one physical CPU or four cores.

For a higher storage and performance requirement, SQL Server Standard or Enterprise should be used.



Section 2

INSTALLING THE SYSTEM

The order in which the installers are run does not matter, but it is recommended to start with the database installer.

The Milestone MIP installer should be installed once on any PC where the following is installed. Milestone Administration Client, Milestone Event Server and any PC where the Milestone Smart Client is installed. The Milestone MIP installer only needs to be installed once on a PC if multiple Milestone products is installed. For instance, if a PC has Milestone Admin Client and Milestone Event Server installed, then the Milestone MIP installer only needs to be installed once on this PC.

Installing the Database

The database can be installed on any SQL Server 2016 or higher instance. The default SQL Server instance is called “SPSQLSERVER”. If the installer does not find this instance, the user has the option to install it.

Using the installer to install the default instance is recommended. When a custom SQL Server instance is used, please ensure that the “file stream for Tansact-SQL access” feature is enabled.

If the installer detects that the database is already installed, the database will be overwritten.

Step 1: Run the Installer

Open the “iSentry Xprotect System - SQL Installer V-xx.xx.xx.msi” installer package. The “welcome” screen will be displayed.

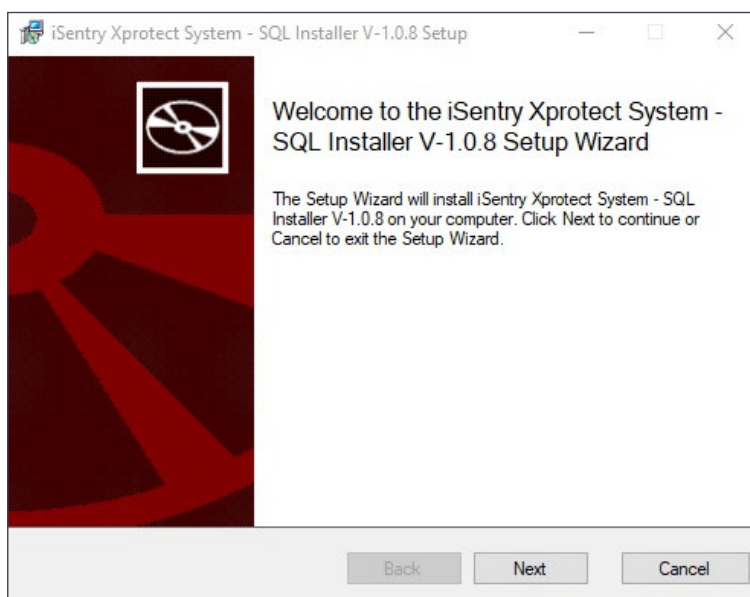


Fig. 1 - The “Welcome” screen displaying the version of the application being installed. This screen is common to all installers.

Step 2: Accept the License Agreement

Open the “iSentry Xprotect System - SQL Installer V-xx.xx.xx.msi” installer package. The “welcome” screen will be displayed.

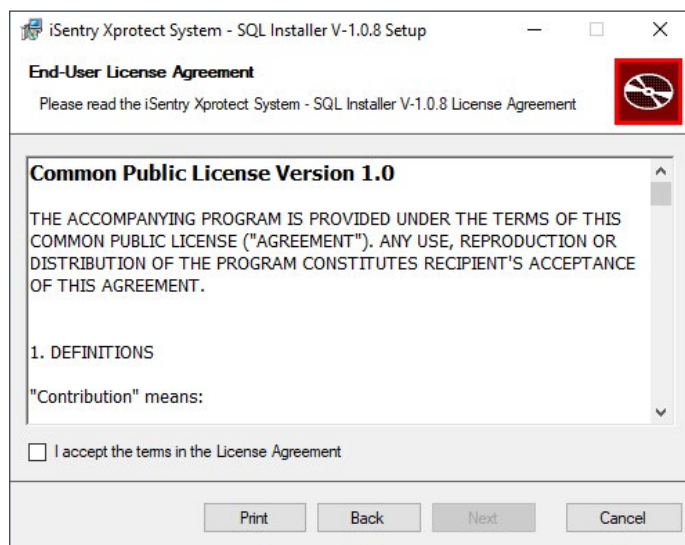


Fig. 2 - The “License” screen. This screen is common to all installers.

Step 3: Setup the SQL Instance

If the installer does not detect a “SPSQLSERVER” instance, the “Install a new SPSQLSERVER instance” option will be automatically selected. The user can choose to install this instance (recommended). The user also have the option to install the database on an existing SQL instance. In this case, choose the “Connect to an existing SQL server instance” option. The user credentials used to connect to SQL must be a user with rights to create a database.

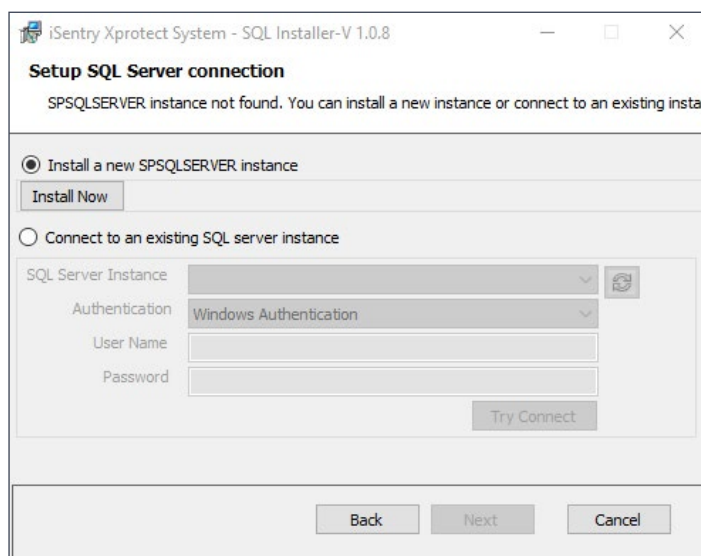


Fig. 3 - SQL Server connection info.

Step 4: Installing SQL Server

If the user chose to install the “SPSQLSERVER” instance, the installer will launch the SQL Server install package.

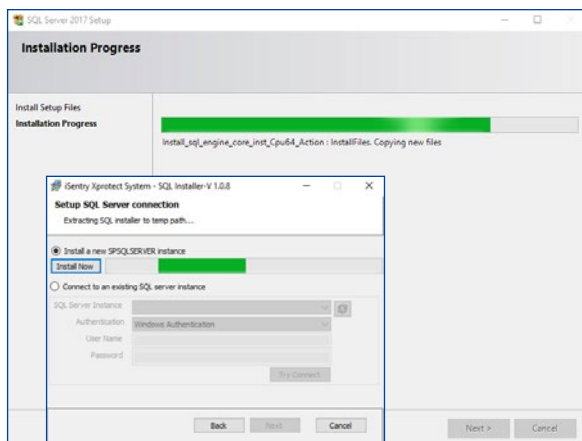


Fig. 4 - Installing SQL Server progress.

Step 5: Choose the SQL Server Instance

If the user chose to install the “SPSQLSERVER” instance in the previous step, the user credentials will automatically be filled in. In this case the user can click “Next” to continue the process.

If a user chose to install the database on an existing SQL Server instance, click on the “Refresh” icon to get a list of existing SQL Server instances. If a SQL Server instance is not listed, then type in the Instance name manually. Fill in the user credentials to connect to the SQL Server instance where the database should be installed. The SQL user credentials should have rights to drop and create a database on the chosen SQL Server instance. Click on “Try Connect” to confirm that the chosen SQL Server instance is accessible. If successful the “Next” button will be enabled.

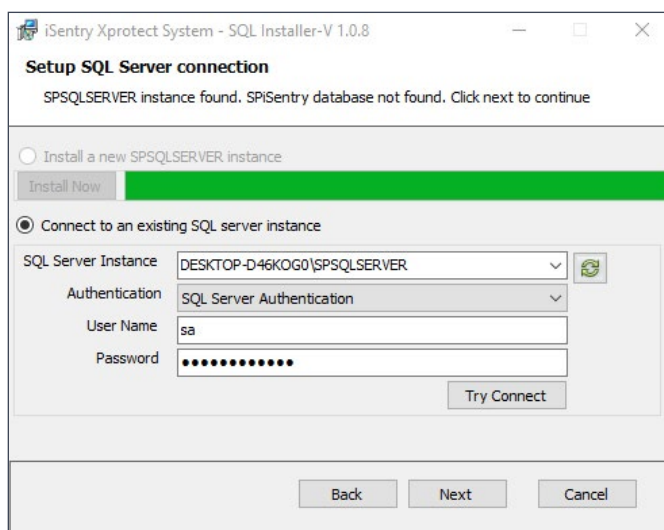


Fig. 5 - Choose the SQL Server instance where the database should be installed.

Step 6: Choose the Database Location

Users can choose where to install the different components of the database. It is recommended that the different components is split between physical drives. This will split disc Read/Write operations across drives.

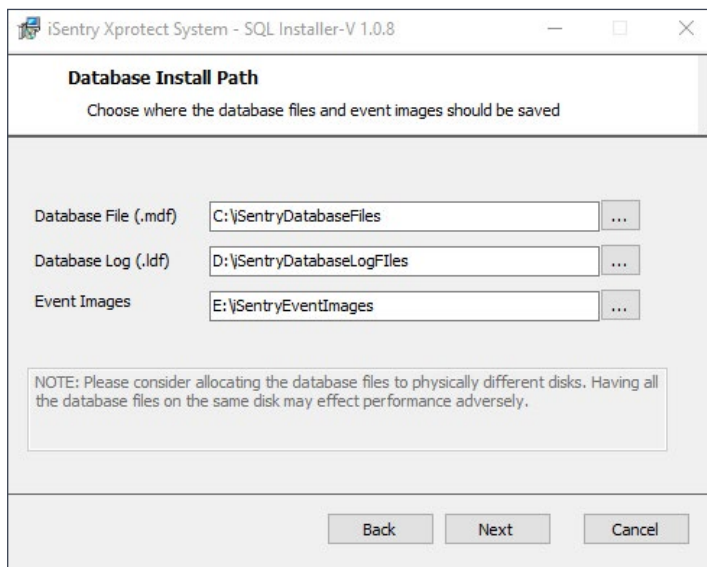


Fig. 6 - Installing SQL Server progress.

Step 7: Install Progress

The installer is busy installing the files on the target system. Progress is shown.

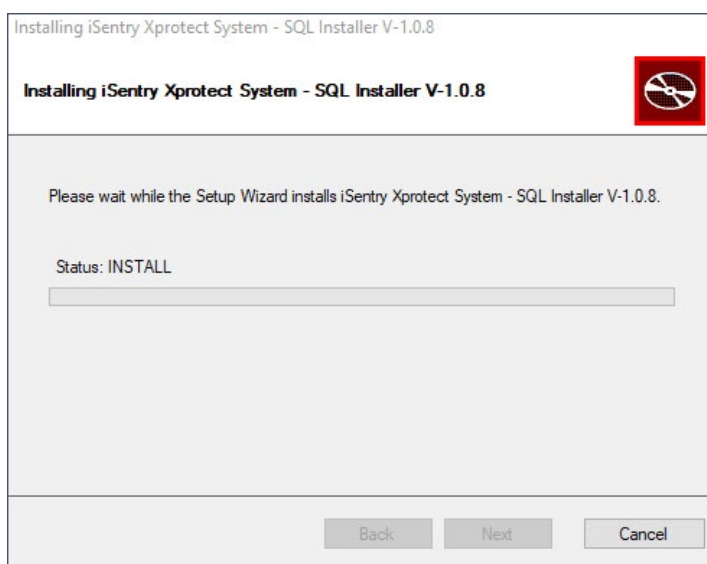


Fig. 7 - The “Progress” screen. This screen is common to all installers.

Step 8: Finish

Once the installer is finished the “Exit” screen will display. This screen shows if the install was successful.

Click on “View Log”, to view the installer log.

Click “Finish” to exit the installer.

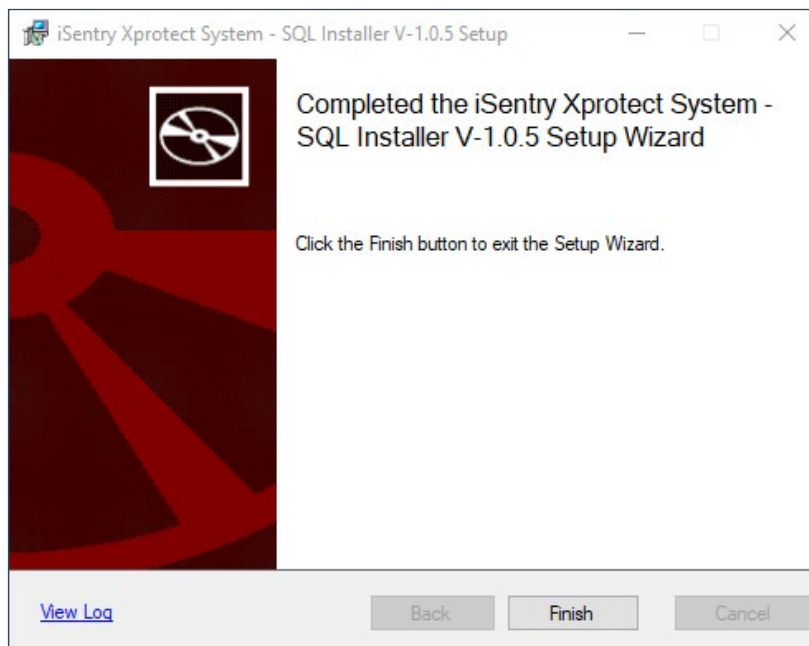


Fig. 8 - The “Exit” screen. This screen is common to all installers.



Section 3

CONFIGURING THE SYSTEM

After Successful Installation the Following Components Will be Present:

SQL Server Database: "SPiSentry"

iSentry Object Classification and Facial Extraction (Deep Learning) Server

iSentry Processing Server

iSentry Plugin for the Following Milestone Components

- Milestone XProtect Event Server;
- Milestone XProtect Management Client;
- Milestone XProtect Smart Client.

First Start (Basic Configuration)

In order to get the System Running, the following Steps should be followed.

Step 1: Find Your SQL Server Address

The preferred method for connecting to a SQL server Instance is by using a Port number and IP Address. Hostname and Instance Name resolution is also supported depending on SQL server Configuration.

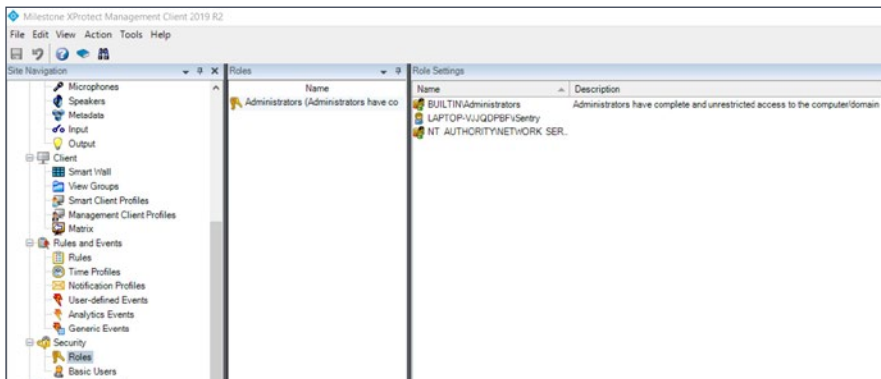
If the Default SQL Server installation was used the TCP/IP network protocol will be enabled for the Server. The Instance can then be identified by "IP_Address,Port_Number" e.g "192.168.1.100,50011". The Default Port Number will be 50011, unless this port is already in use, in which case the port number will be increased to 50012..13..14 etc. The Default Username and Password for the iSentry Database is: Username = "isentry" and Password = "isentry".

If an Existing SQL Server was used for the installation, the database administrator must ensure that a user with full access to this database is created, and that the Database is accessible to the system.

NOTE: The XProtect Smart Client must be able to access this database, so Firewalls and Routing must be considered.

Step 2: Create a Milestone User for the "Administrator" Role

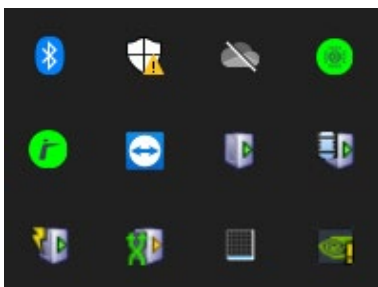
Log into the Milestone Management Client with an Administrator user with full access to the Milestone System. Open up the "Roles" window under the "Security" Node in the Tree view. Select the "Administrators" role and select the "Users and Groups" Tab at the bottom of the window.



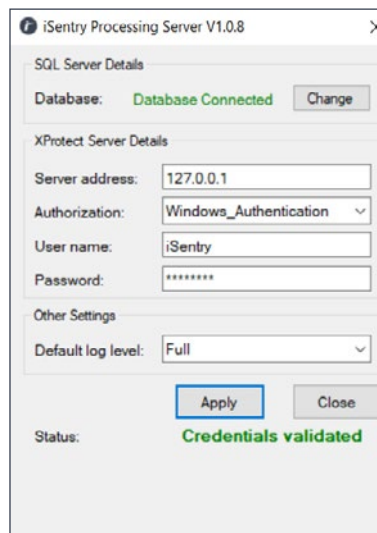
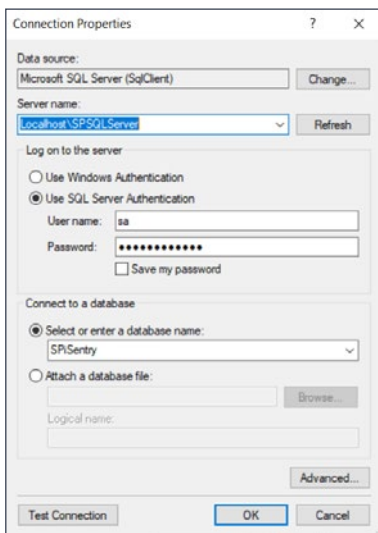
Add a user to this role for the iSentry processing server login, and click “Save”, in the left top corner of the Milestone Management Client window.

Step 3: Connect and Start the iSentry Processing Server

In the System Tray of the server you should find the iSentry Processing Server icon



If this icon does not appear in the tray, please start it by double-clicking on the icon on the desktop



Right Click on the iSentry Processing Server Tray icon and select Settings, to show the settings window.

In the setting window, click the “Change” button in the SQL Server Details Group box:

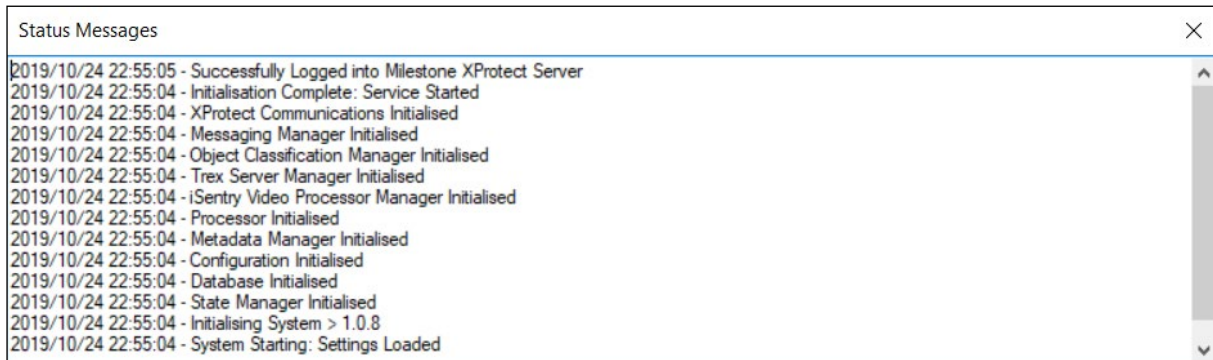
Make sure that “Microsoft SQL Server (SQL Client)” is selected as the Data source. Enter (or search for) your SQL server instance details as established in Step 1 above, and enter the SQL Server Database username and password. Dropdown the Database list and select: “SPiSentry”.

Click “Test” to verify the connection and “OK” to save.

Enter your Milestone Management Server Hostname or IP address in the Server address box, and enter the user details as configured in Step 2 above.

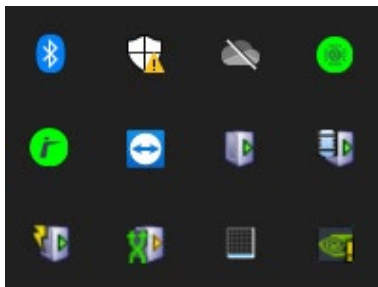
Click “Apply” to save the settings and start the Processing Server.

The Tray icon should turn green and the Status messages should confirm successful login to the Milestone Management Server.



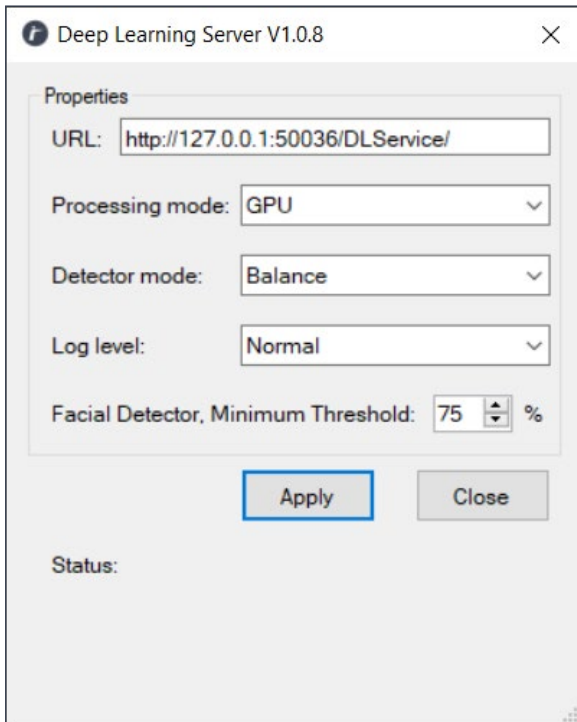
Step 4: Configure and Start your iSentry Object Classification and Facial Extraction (Deep Learning) Server

In the system Tray of the server you should find the iSentry Object Classification and Facial Extraction (Deep Learning) Server Icon



If this Icon does not appear in the tray, please start it by double-clicking on the icon on the desktop

Right click on the tray icon and select settings

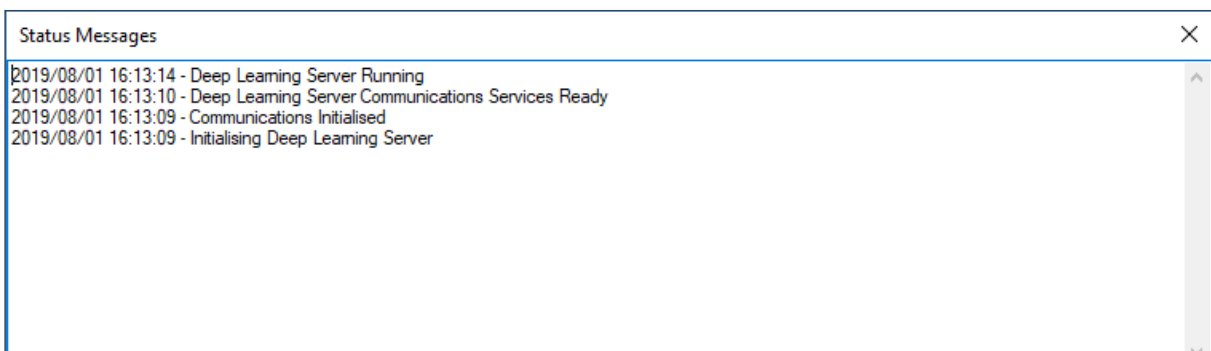


Please Update the URL in the properties window with an appropriate Ip Address and port number.

Select the Processing Mode, Detector Mode, Log Level and Facial Detector, Minimum Threshold, and Click Apply to save the settings and Start the server.

NOTE: CPU mode should never be used on a physical machine installed with any other software besides the OS, since 100% of the CPU will be utilised by this Server. It is therefore Highly recommended to use the GPU mode in conjunction with a suitable nVidia GPU.

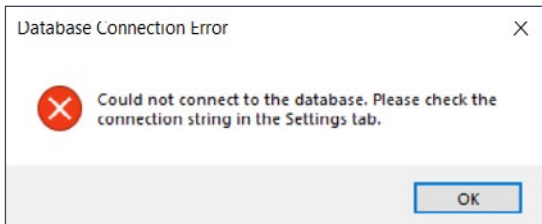
The Tray Icon should Turn Green, and the Status Messages should confirm successful start-up:



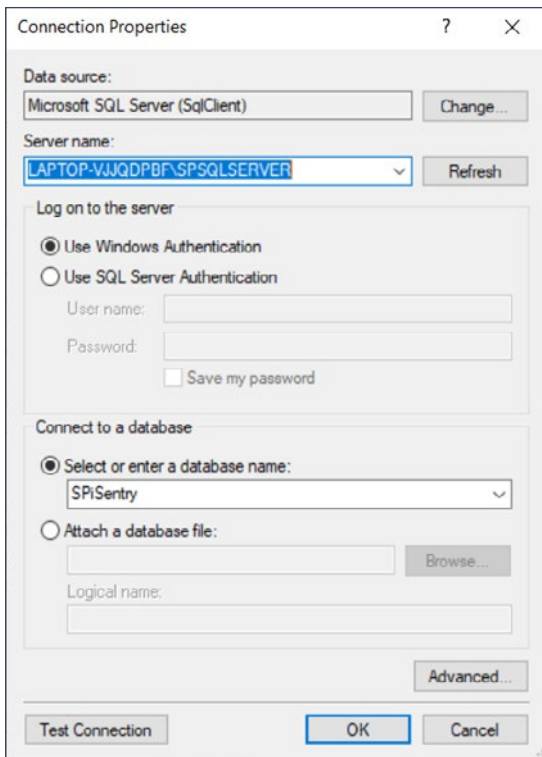
Step 5: Connect and Configure your Milestone Management Client

Log into the Milestone Management Client with an Administrator user with full rights to the system. Navigate to the “iSentry Alert Plugin” node and expand it. Click on the second node and wait for the Settings to load.

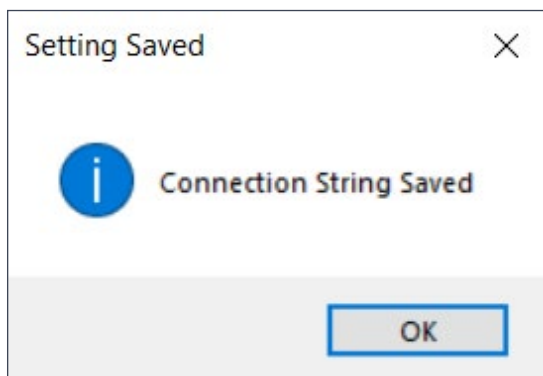
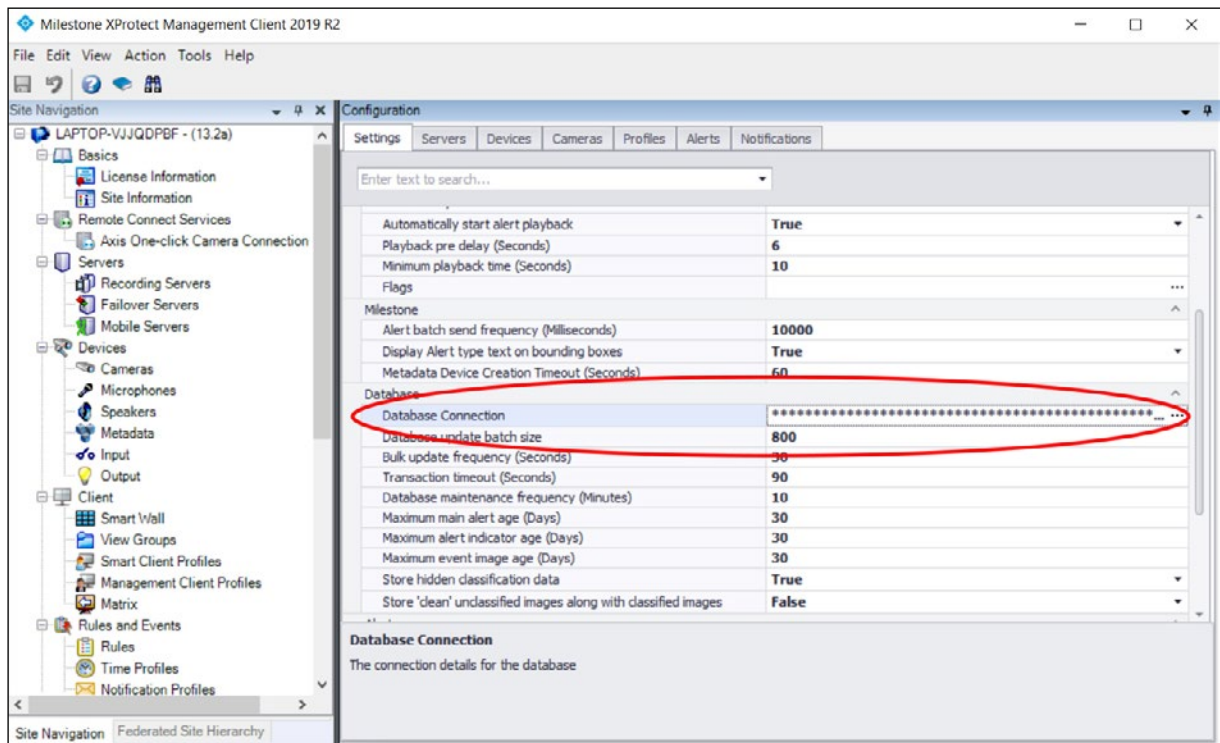
If the Database connection has not been configured yet, or if the Milestone XProtect Event Server is not running, the following Message will be displayed



Please Complete the Database Connection properties as was done in Step 3 above:



If the Database connection window does not appear automatically, please select it from the settings Tab



After successful update of the connection the following message appears

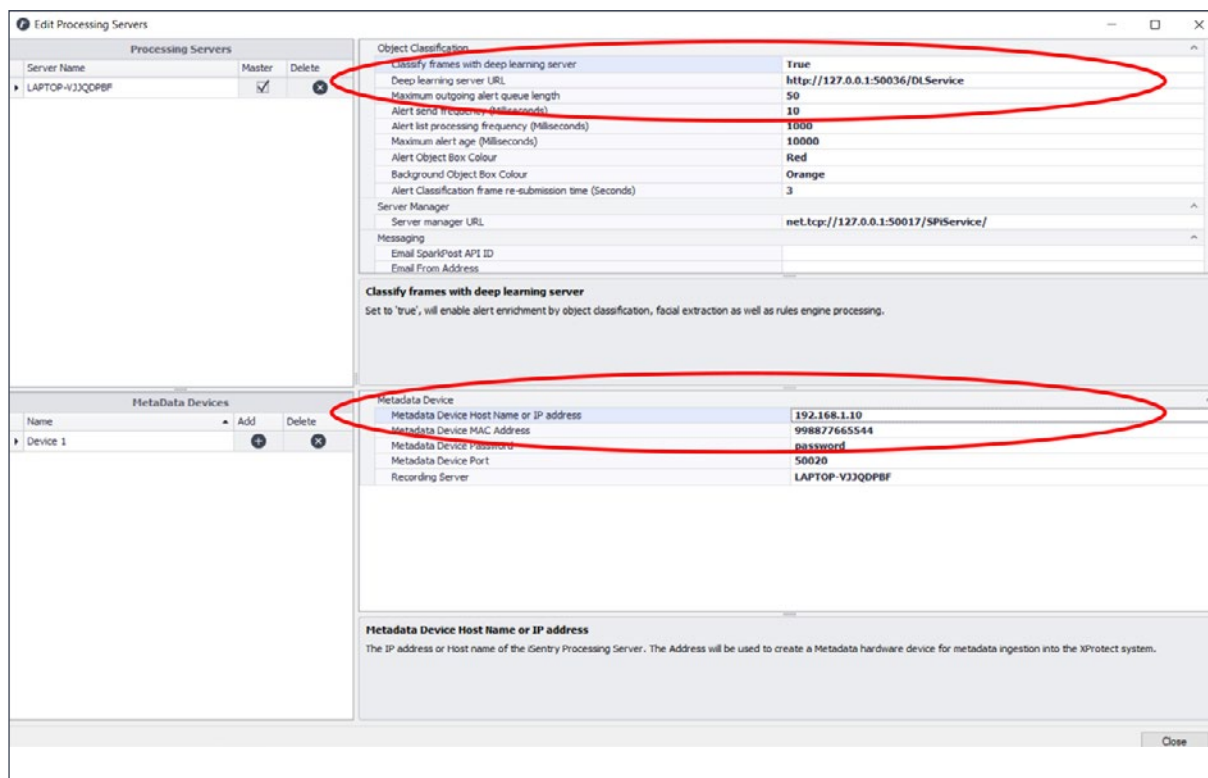
Press "F5" to reload the page and click "OK" if Settings confirmation is required. If a Confirmation message does not appear, the connection will not have been saved. Please ensure that the XProtect Event Server is running and retry updating the connection.

Step 6: Deep Learning and Metadata Connections

In the XProtect Management Client, iSentry Alert Plugin, Select the “Servers” Tab.

If the Previous Steps were successful, then you should find the Processing Server Configured in Step3 above, listed in the “Processing Servers” list.

Click on the Gear Icon above the List and select the (Click) Processing Server in the list.



For the Default Metadata device (Device 1), in the “Metadata Device IP address” field, fill in the IP Address of the Server that the Processing Server resides on, and make sure that the “Deep Learning Server URL” resolves to the address used in Step 4 above.

Close the window.



Section 4

GENERAL CONFIGURATION

Configuration of the system is done in the XProtect Management Client. The iSentry Alert Plugin is divided into Tab pages, each configuring a different functional area of the system.

SETTINGS

General System Settings are configured in the “Settings” Tab in the XProtect Management Client iSentry Alert Plugin.

As a general rule the settings should be left at their default values.

Items marked in yellow, are standard settings and may be adjusted by the system administrator.

The Settings page is split into the following sections:

Miscellaneous:

Log Level: Level of detail that is logged.

- **Normal:** Only errors, and general statuses.
- **Intermediate:** Error Detail and general statuses.
- **Full:** Error Detail and Detailed status logs.
- **Trace:** Error Detail, detailed status logs and full transactional communication logs.

Smart Client:

Maximum number of live alert images: Maximum number of classified and alert frames sent with live alerts for display in the Smart Client.

NOTE: in the case of a high camera count site or a site generating a high volume of alerts, this setting may be set to zero (0), to accommodate faster network transfer.

Maximum Alert Image Width (pixels) [Before resize]: Maximum alert image width before a size limit is applied (pixels).

Play Sound When Alert is Received: Set to true, the Smart Client will play a sound when a new alert is received.

Show Classified Alert Image: Set to true, will display the Alert image when an alert is selected, in the Live Alerts tab in the Smart Client.

Immediately Show Live Video: Set to true, will display live video for the alert camera when the alert is opened.

Automatically Start Alert Playback: Set to true, will start video playback for the selected alert camera when the alert is opened.

Playback Pre-Delay (Seconds): The number of seconds a playback should start before the actual event time.

Minimum Playback Time (Seconds): The minimum number of seconds an event must be displayed before an operator can Dismiss / Escalate the event.

Flags: Create or edit past alert Flag categories.

Milestone:

Alert Batch Send Frequency (Milliseconds): Time, in Milliseconds, between sending batches of alerts to the Milestone environment.

Metadata Device Creation Timeout (Seconds): The Maximum time allowed, to create or update, a Metadata device, in seconds.

Display Alert Type Text on Bounding Boxes: Display the type name of each alert with bounding boxes.

Database:

Database Connection: The connection details for the database.

Database Update Batch Size: The size of the alert list being updated in a batch.

Bulk Update Frequency (Seconds): The number of seconds between batch updates to the database.

Transaction Timeout (Seconds): The number of seconds before a Timeout error is generated for database alert updates.

Database Maintenance Frequency (Minutes): Database maintenance cycle frequency in minutes.

Maximum Main Alert Age (Days): Number of days, which an Alert is stored in the database.

Maximum Alert Indicator Age (Days): Number of days, which the Alert indicators and Classification data, are stored in the database.

Maximum Event Image Age (Days): Number of days, which the Alert images are stored in the database.

Store Hidden Classification Data: Set to 'true', the system will store all classified object data. 'false', hidden object types data will be discarded.

Alerts:

Minimum TREX Alert Length (Frames): Minimum age, in Frames (assume 100Ms / Frame), before a TREX alert is recognized.

Maximum TREX Alert Length (Seconds): Maximum number of seconds a TREX alert is allowed to exist before it is replaced.

Maximum Active Alert Age (Minutes): Maximum number of minutes an alert is regarded as 'Active', in case of a server restart.

Default Auto-Promotion Time (Seconds): Time, in seconds, after which an inactive alert is promoted to an Alarm or Dismissed.

Automatically Promote Inactive Alerts to Alarms: Set to true, will cause alerts to be automatically promoted to Alarms (false will result in automatic Dismissal).

Enable Manual Video Recording for Alerts: Set to true, manual video recording instruction will be sent to Milestone for alerts.

Manual Video Recording Duration (Seconds): Number of seconds that video is recorded for a manual recording event.

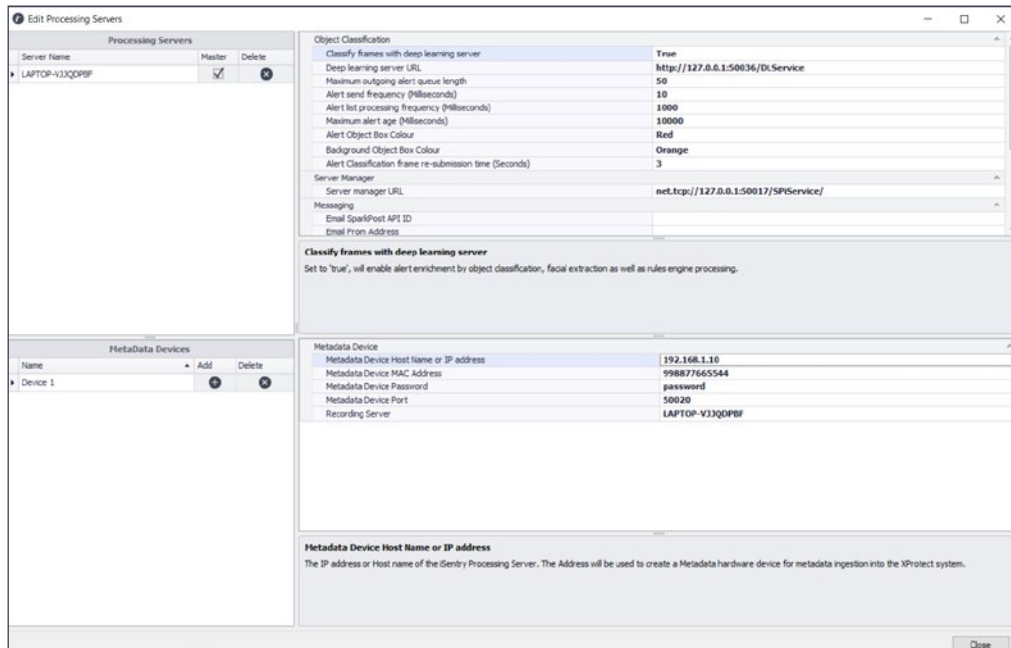
Maximum Colour Image Buffer Size: Maximum size in bytes, of the colour frame buffer used by the internal system.

NOTE: *in the case of Very high resolution cameras, the default buffer size may be too small. To calculate the buffer size required, the following formula may be used as an example.*

Take a camera with the resolution of 1920X1080. We assume 3 colour channels, and one byte per pixel. So the buffer size becomes $1920 \times 1080 \times 3 = 6220800$ bytes. Find the highest resolution camera in the system and adjust the buffer higher than that requirement.

SERVERS

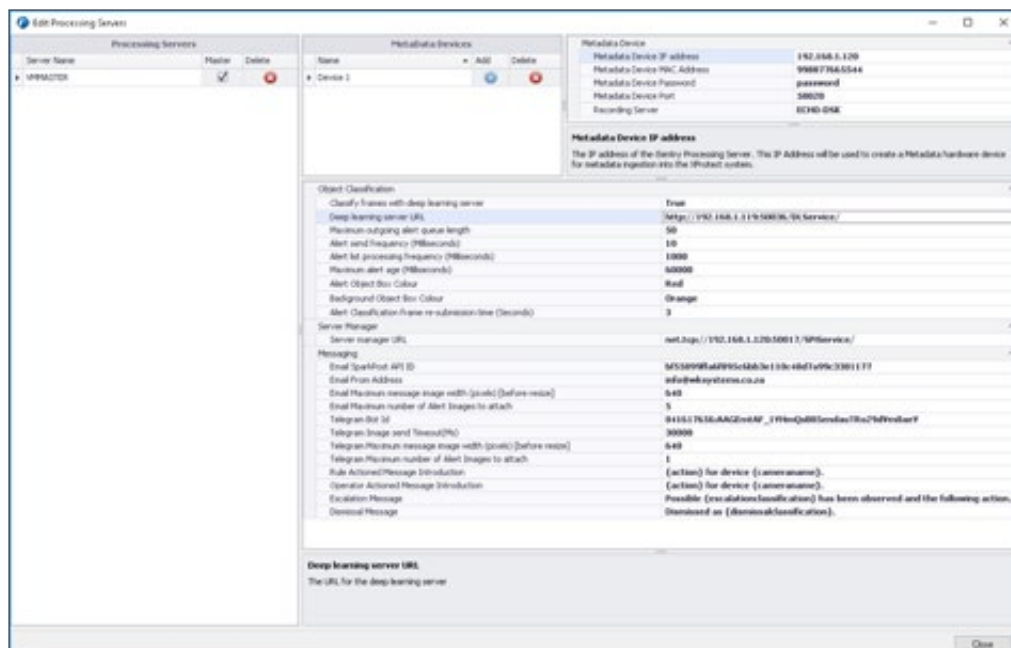
Whenever a Processing Server is started and successfully connected to the database and the XProtect system, it will be added to the List of Processing Servers in the “Servers” Tab in the iSentry Alert Plugin.



Processing Servers:

The basic minimum configuration of a Processing server is described in Step 6 above.

In order to access the settings for a Processing server, click on the Gear Icon above the List and select (Click on) the desired Processing Server in the list.



Metadata Device:

Metadata Device IP Address: The IP address of the iSentry Processing Server. This IP Address will be used to create a Metadata hardware device for metadata ingestion into the XProtect system. This must be unique for each Device.

Metadata Device Port: The Port number used for the Metadata connection.

Metadata Device Password: Password used to access this Metadata device.

Metadata Device MAC Address: Mac address assigned to the Metadata device. This must be unique for each Device.

Object Classification:

Classify Frames with Deep Learning Server: Set to 'true', will enable alert enrichment by object classification, facial extraction as well as rules engine processing.

Deep Learning Server URL: The URL for the deep learning server.

Maximum Outgoing Alert Queue Length: Maximum number of alerts buffered if the connection to the deep learning server is temporarily lost.

Alert Send Frequency (Milliseconds): The frequency, in Milliseconds, which alerts are sent to the Deep Learning server.

Alert List Processing Frequency (Milliseconds): Frequency, in Milliseconds, that the alert list is processed.

Maximum Alert Age (Milliseconds): Maximum duration, in Milliseconds, that an alert is buffered to wait for classification information. This buffer depends on the speed at which frames are classified by the Deep Learning server.

Alert Object Box Colour: The colour of the bounding boxes for objects directly related to the alert.

Background Object Box Colour: The colour of the bounding boxes for background objects.

Alert Classification Frame Re-Submission Time (Seconds): For long running alerts, the amount of time in seconds, before additional alert frames are submitted for classification.

Server Manager:

Server Manager URL: The communication URL for the Server tray icon.

Messaging:

Telegram Bot ID: The ID of the Telegram Bot used for alert messaging.

Telegram Image Send Timeout(Ms): The maximum amount of time, in Milliseconds, that the system will wait for an image to upload before the process is cancelled.

Telegram Maximum Message Image Width (pixels) [Before Resize]: Maximum message image width before size limit is applied (pixels).

Telegram Maximum number of Alert Images to Attach: Maximum number of alert images that will be attached to each Telegram message.

Rule Actioned Message Introduction: Introductory Message for rule processed Alerts. Items in curly brackets will be replaced by actual values.

Operator Actioned Message Introduction: Introductory Message for operator processed Alerts. Items in curly brackets will be replaced by actual values.

Escalation Message: The message used in case of an escalation. Items in curly brackets will be replaced by actual values.

Dismissal Message: The message used in case of a dismissal. Items in curly brackets will be replaced by actual values.

Email SparkPost API ID: The ID of the SparksPost API used for alert email messaging.

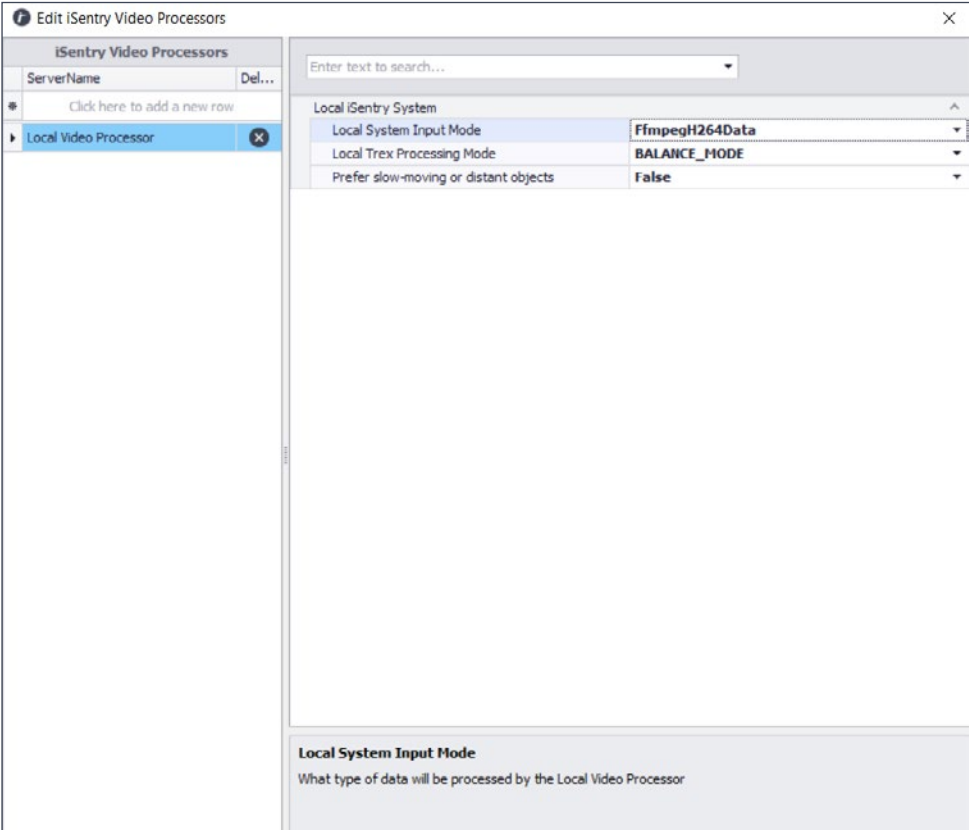
Email From Address: The From Email Address for the registered domain.

Email Maximum Message Image Width (pixels) [Before Resize]: Maximum message image width before size limit is applied (pixels).

Email Maximum Number of Alert Images to Attach: Maximum number of alert images that will be attached to each email.

iSentry Video Processing Servers:

In order to access the settings for an iSentry Video processing server, click on the Gear Icon above the List and select (Click on) the desired Video processing Server in the list.



Local System Input Mode: What type of data will be processed by the Local Video Processor.

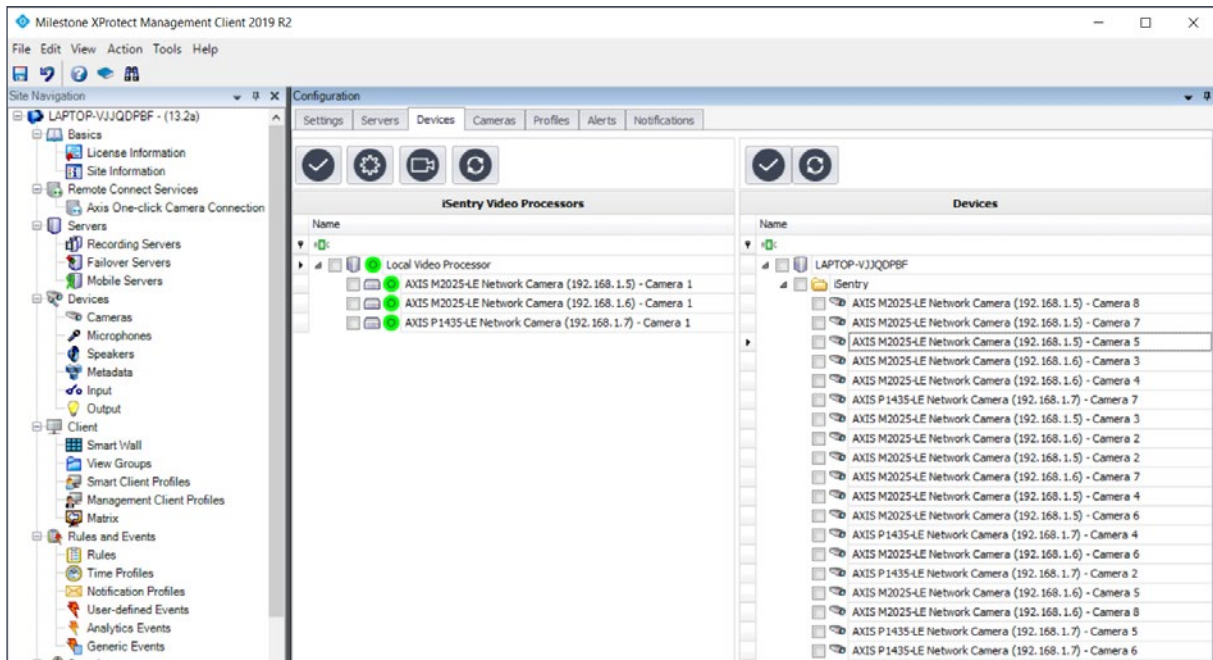
Local Trex Processing Mode: Adjust Trex (Target Ranking and Extraction) system processing for Accuracy vs Speed.

Prefer Slow-Moving or Distant Objects: Set to 'true', the Trex system will prioritize slow-moving objects and/or objects that are far away.

DEVICES

The Devices Tab is responsible for Camera Configuration and Mapping, as well as advanced configuration of the system.

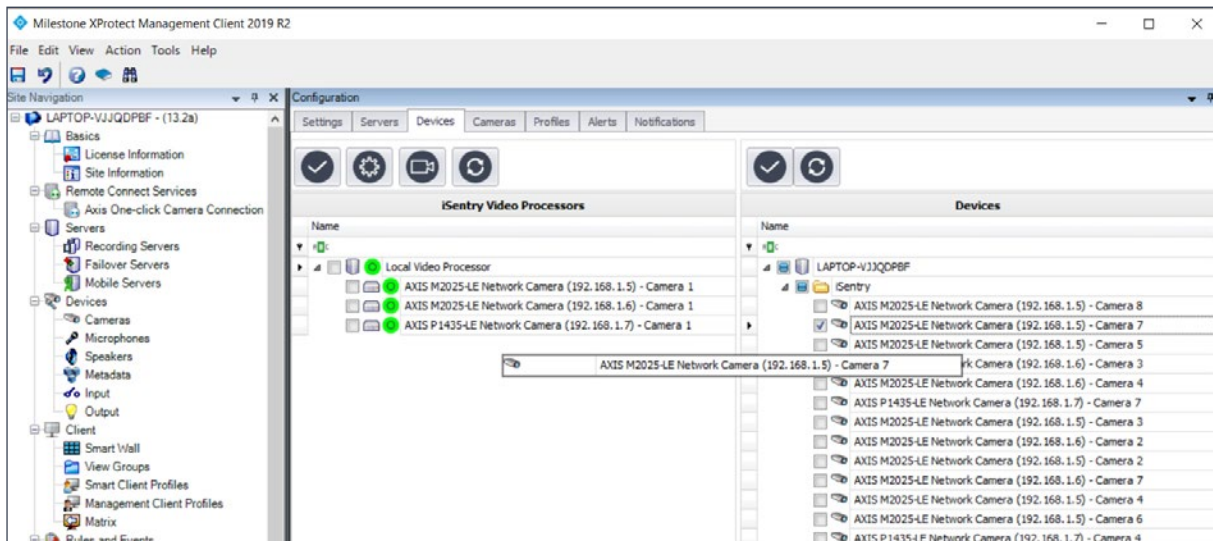
Click on the refresh button at the top of each section, to update the view and display the latest iSentry Processing Servers as well as cameras added to the system.



All the available iSentry processing servers are listed in the left-hand pane of the Devices Tab, and all the available cameras are listed in the right-hand pane.

Here follows a breakdown of the main configuration areas available in the Devices Tab:

Adding Cameras (Devices):




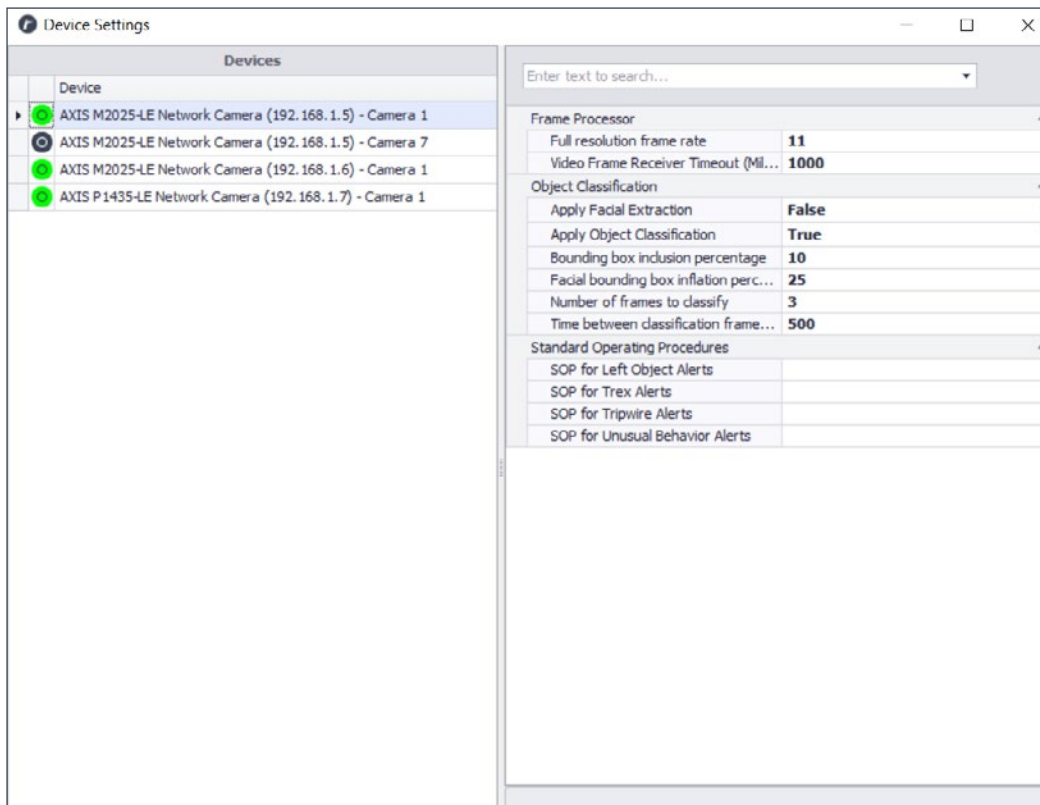
In order for an iSentry server to process camera feeds, cameras must be associated to the desired server.

To add cameras to an iSentry processing server, check the checkboxes of one or more cameras in the right-hand pane of the Tab, and with your mouse drag-and-drop the camera(s) on to the desired iSentry processing server in the left-hand pane.

Device Settings:

The Devices Tab is responsible for Camera Configuration and Mapping, as well as advanced configuration of the system.

Device settings for each camera can be accessed by clicking on the  gear icon at the top of the window.



Frame Processor:

Video Frame Receiver Timeout (Milliseconds): Amount of time, in Milliseconds, that the Frame receiver will wait to receive a frame, before the connection is deemed to be broken. A broken connection will trigger a reconnection attempt.

Full Resolution Frame Rate: Frame rate (Frames per second) of full resolution images.

Object Classification:

Apply Object Classification: Set to 'true', the system will attempt to identify objects for alerts from this camera.

Apply Facial Extraction: Set to 'true', the system will attempt to extract human faces for alerts from this camera.

Facial Bounding Box Inflation Percentage: The amount, as a percentage of the original facial image size, to increase the resulting facial image size in order to include relevant detail to the final image.

Bounding Box Inclusion Percentage: The size, as a percentage, of the area of relevance surrounding the alert indicator.

Number of Frames to Classify: The number of frames, for which the system will attempt to identify objects for alerts from this camera. More frames will increase the likelihood of accurate object classifications, but will also create latency and processing overhead.

Time Between Classification Frames (Milliseconds): In the Case of Multiple Frames. The time, in Milliseconds, between frames to be sent to the Object Classifier.(100 - 1000)

Standard Operating Procedures:

SOP for Unusual Behaviour Alerts: Description of the Procedure that an Operator should follow in case of an Unusual Behaviour Alert.

SOP for Tripwire Alerts: Description of the Procedure that an Operator should follow in case of a Tripwire Alert.

SOP for Left Object Alerts: Description of the Procedure that an Operator should follow in case of a Left Object Alert.

SOP for Trex Alerts: Description of the Procedure that an Operator should follow in case of a Trex Alert.

Metadata Devices:


Metadata devices can be created or updated by right-clicking on any iSentry processing server and selecting “Update Milestone Metadata Device”. If the system detects that no changes have been made to camera mappings, a dialog will appear giving the user the opportunity to continue or cancel the operation.

As soon as the process is started, the progress bar is displayed at the top of the window.

If the process succeeds, as dialog is displayed, confirming that a Metadata device has been added.

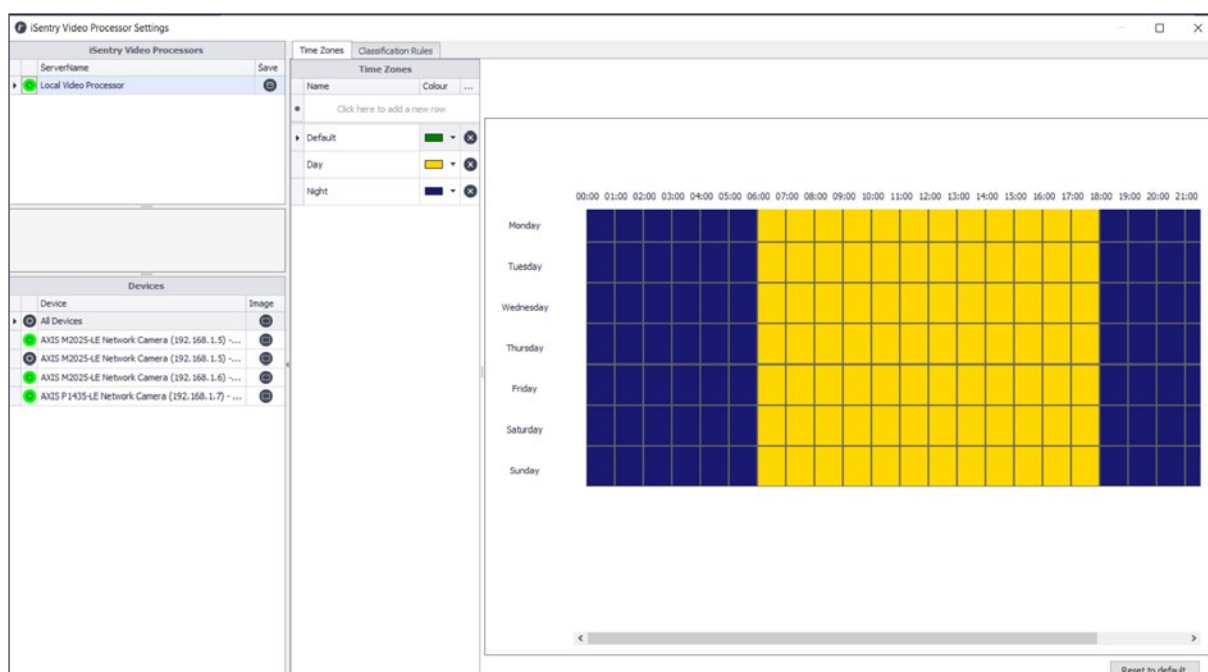
If the process fails, please see the troubleshooting section of this manual on Metadata devices. Often multiple attempts are required.

Video Processor Settings:

Video processor settings are accessed by clicking on the  gear icon at the top of the window.

Select a Video Processor, to access settings for it.

Time Zones: Select “All Devices” and the “Time Zones” Tab, to View or edit current Time zones.



Adding a Time Zone: Click in the top row of the “Time Zones” list and type a name for the new Time Zone, select a colour, and press the enter key or click on an existing row.

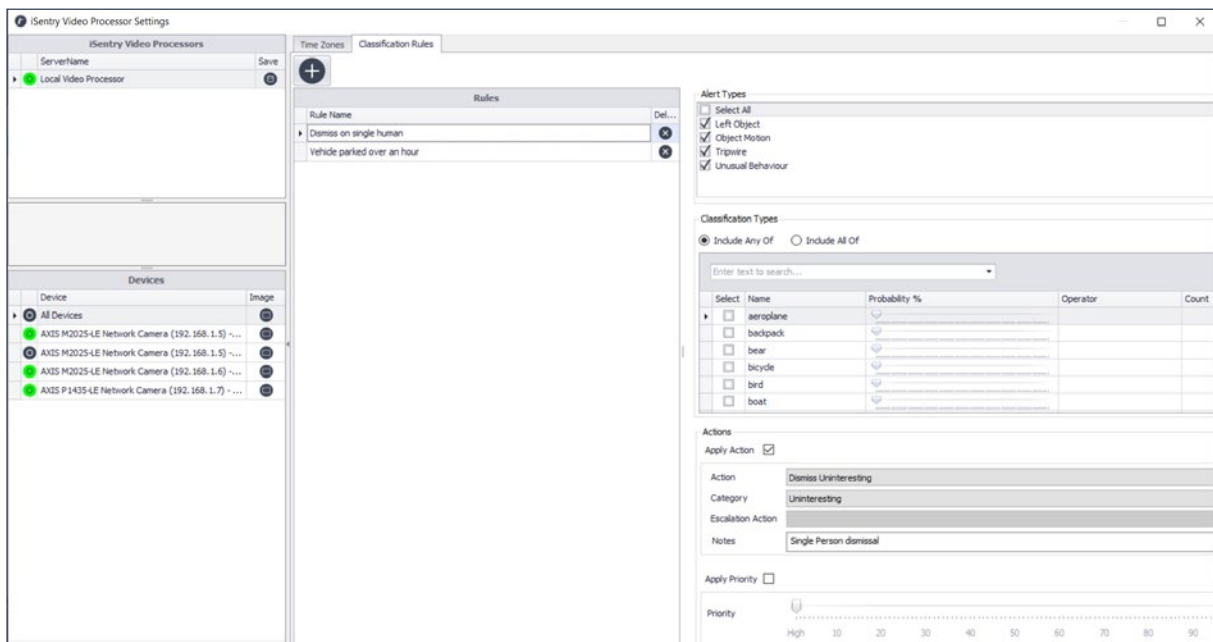
Deleting a Time Zone: Click on the Delete Icon , next to the Time zone to be deleted.

Configuring Time Zones: The grid in the right-hand pane of the window represents one hour slices of each day of the week. Any “time Slice” may be allocated to a Time zone, by selecting the desired time zone and clicking on the “time slice” to be allocated. The selected “time Slice” will change colour to match the colour of the selected time zone.

In this way the grid can be “painted” to represent when time zones are applied to settings, for each camera.

Rules:

Select “All Devices” and the “Classification Rules” Tab, to View or edit current rules.

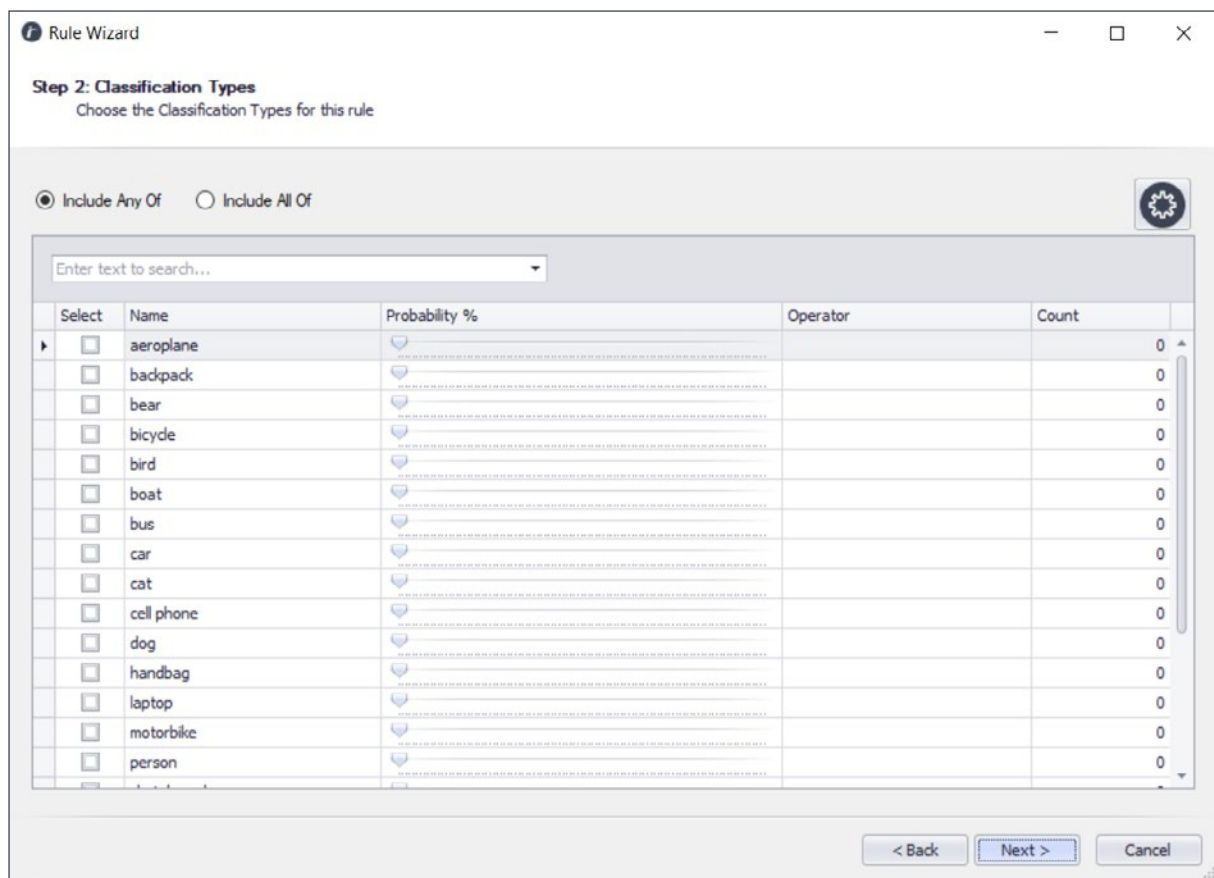


Creating a Rule:

To create a new rule, click on the **+** button at the top of the Rules list. A rule creating wizard will appear guiding the user through the steps of the process.

Type a name for your new rule and click “Next”. Please note that it is recommended to add the alert type as well as detail describing the rule to the name, to ease the implementation of the rule.

1. Select the Alert Type(s) that apply to this rule, and click “Next”.
2. Setup the rule logic:



Setup rule conditions:

- a. Select the object type(s) that must be evaluated for this rule, by checking the box next to it.
- b. Next set the minimum probability of each object type, which must be satisfied in the evaluation of this rule.
- c. Select the operator for the number of objects, of each type.
- d. Set the number threshold, to be evaluated.

Example: In order to create a rule where we want to create an alarm for a group of people gathering (in this example, let’s assume a group is 5 or more people), we would make the following selections:

- i. Object type: “person” ~ we are only interested in people for this rule.
- ii. Probability: “30%” ~ chosen probability will depend on various factors, like camera type, scene type, angle, importance of accuracy, etc. This will be a subjective choice depending on the administrator.
- iii. Operator: “>= ” ~ greater than or equal to.
- iv. Number: “5” ~ Five.

The condition logic now reads as follows:

5 or more person objects with a probability of more than 30%
If this condition is satisfied the rule will be triggered.


NOTE: As a General Rule, a higher probability should be applied to Dismissals and a lower probability for escalations.

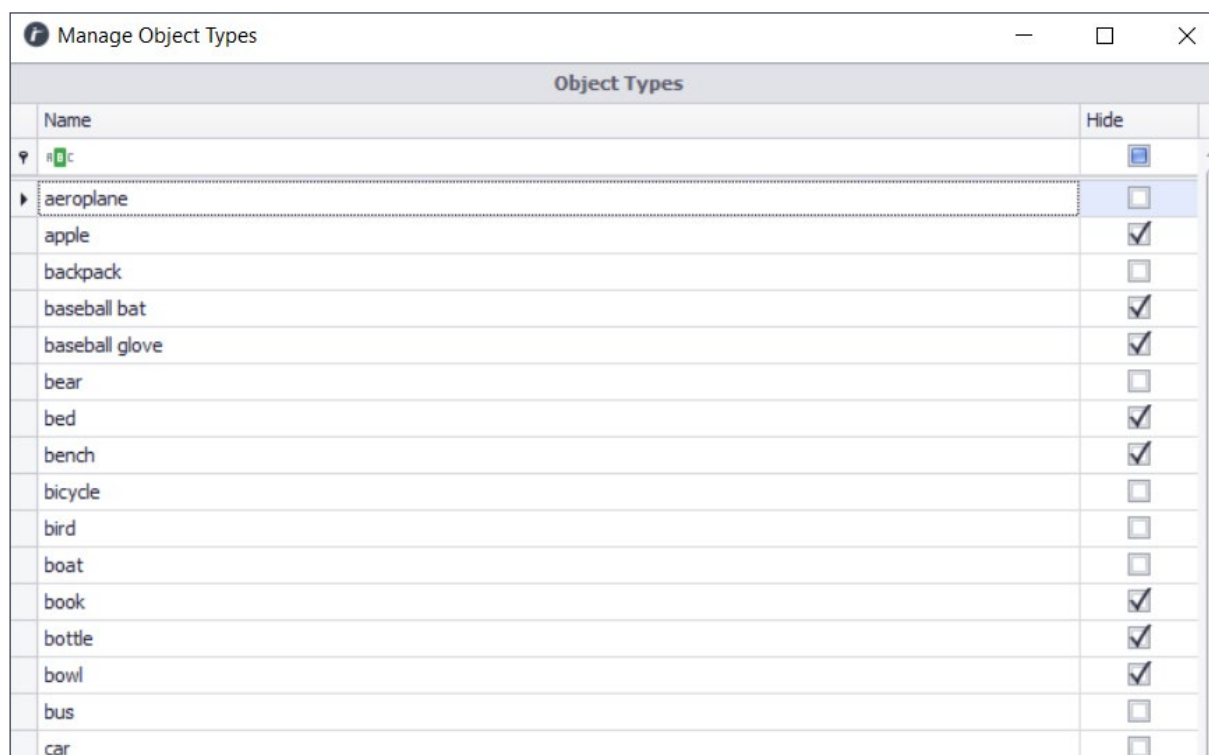
Multiple object type rules:



In the case where multiple conditions are applied in one rule, one of two scenarios exist:

1. All of the conditions must be satisfied for the rule as a whole to be satisfied:
In this case the “Include All Of” option must be checked.
2. Any one of the conditions must be satisfied for the rule as a whole to be satisfied. In this case the “Include Any Of” option must be checked.

Manage Classification Object Types:

In order to hide or show certain classification types, Click the  icon top right of the “Classification Types” box. A list of all available object types are displayed. Checking the “Hide” checkbox to the right of the object, will cause that object type to be ignored in future.



Object Types	
Name	Hide
 	<input type="checkbox"/>
▶ aeroplane	<input type="checkbox"/>
apple	<input checked="" type="checkbox"/>
backpack	<input type="checkbox"/>
baseball bat	<input checked="" type="checkbox"/>
baseball glove	<input checked="" type="checkbox"/>
bear	<input type="checkbox"/>
bed	<input checked="" type="checkbox"/>
bench	<input checked="" type="checkbox"/>
bicycle	<input type="checkbox"/>
bird	<input type="checkbox"/>
boat	<input type="checkbox"/>
book	<input checked="" type="checkbox"/>
bottle	<input checked="" type="checkbox"/>
bowl	<input checked="" type="checkbox"/>
bus	<input type="checkbox"/>
car	<input type="checkbox"/>

3. Choose the Action to be applied when the rule has been satisfied:

The screenshot shows the 'Rule Wizard' window at 'Step 3: Actions'. The title bar reads 'Rule Wizard' with standard window controls. Below the title, it says 'Step 3: Actions' and 'Choose the Action to execute when this rule is applied'. There are two main sections: 'Apply Action' and 'Set Priority'. The 'Apply Action' section has a checked checkbox and three dropdown menus: 'Action' (Escalate to Alarm), 'Category' (Hijacking), and 'Escalation Action' (Keep Watch). Below these is a large empty text box for 'Notes'. The 'Set Priority' section has a checked checkbox and a horizontal slider. The slider is labeled 'Priority' and ranges from 'High' (0) to 'Low' (100), with numerical markers at 10, 20, 30, 40, 50, 60, 70, 80, and 90. The slider handle is positioned at approximately 45. At the bottom right, there are three buttons: '< Back', 'Next >', and 'Cancel'.

Apply Action:

Check the “Apply action” Check box, to set the values for an action:

- a. **Action:** Select an Escalation or Dismissal type.
- b. **Category:** Select an Escalation or Dismissal sub-category.
- c. **Operator Action (Escalations only):** For Escalations, select the Proposed operator action.
- d. **Notes:** Type a Note describing the rule logic that triggered the action. This is not required but eases future investigation.

Set Priority:

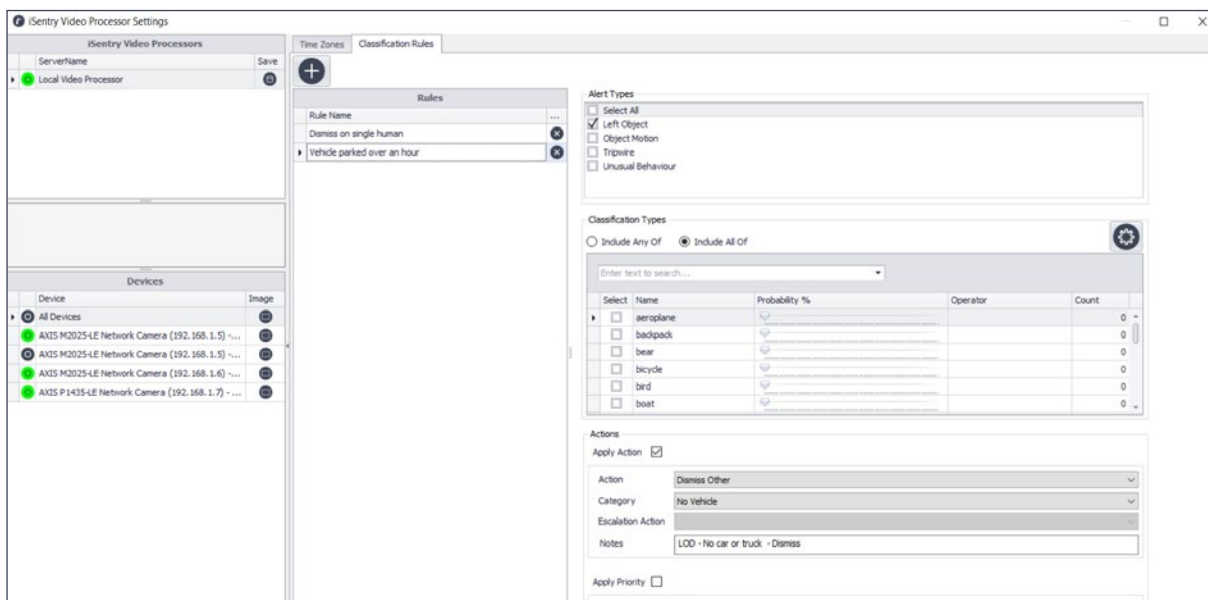
Check the “Set Priority” Check box, in order to change the priority of the alert. Use the Slider to change the priority. Higher priority alerts will be displayed at the top of the alert list in the Smart Client live alert view.

Click “Next” and “Finish” to save the Rule.

If any validation errors occur, a message will appear informing the user, equally, a success message is displayed upon successful rule creation.

Editing a Rule:

Rules may be edited by selecting a rule in the “rules” list and changing values in the right-hand pane of the window.



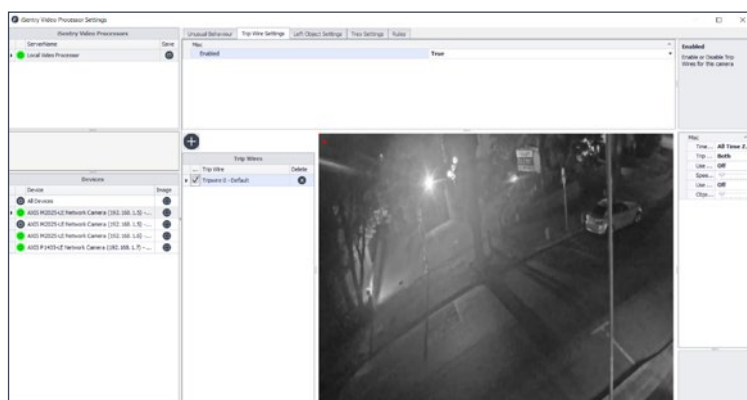
After changes have been made, clicking on another rule, will save the changes made.

CAMERA CONFIGURATION: (ADVANCED CONFIGURATION)

Camera configuration requires a thorough understanding of the iSentry and Trex analytic systems, and should not be attempted by novice users.

To access the configuration for a camera, select the camera, and the Tab corresponding to the analytic that needs to be configured.

Unusual Behaviour: To enable unusual behaviour monitoring for the selected camera, set “Enabled” to true.



Sensitivities:

Select a time zone in the “Time Zones” list, the sensitivities that are configured for that Time zone is displayed as 64 values for the image split into blocks. These values can be edited by selecting one or more blocks and changing the slider at the bottom of the image. A setting of Zero (0) means no alerts will be triggered. The iSentry analysis will be switched off for that region. A setting of 1 - 9 will cause an increasing number of alerts to be raised. The default setting is 5, which should filter out over 95% of the normal behaviour in a busy pedestrian area. If the sensitivity is too low, there is a risk that important events can be missed. If the sensitivity is too high, there will be too many alerts, most of which will be uninteresting.

Advanced:

Advanced settings can be viewed by expanding the “Advanced Settings” row in the settings grid.

Lock Memory: You can also lock the memory. Once the system has fully learned the behaviour from a camera and is performing well, you can choose to lock that memory. The system will then stop learning more from that camera. This would normally only be used in cases where the expected behaviour was very regular and well understood. For example, when monitoring traffic, once the system had learned about normal traffic flow, it might be appropriate to lock the memory. This would avoid the situation where the traffic flow deteriorated over a period of time to the extent that gridlock became accepted as the normal behaviour.

Erase Memory: The Erase memory function allows you to erase all learned knowledge. You MUST erase all knowledge if you relocate a camera because behaviour learnt from one view is location specific and is invalid from different viewpoints. iSentry cannot analyse video from manually controlled PTZ cameras for this reason: even a change in camera view direction will require erasing and relearning.

Decay Memory: The memory decay function allows the system to slowly forget the past. The half life indicated the speed at which past events should be forgotten. With a high half-life, a longer time frame of past events is used to determine normal behaviour. With a low half-life, the past is forgotten more quickly. By default the half-life is set at 100 hours, so the system should more strongly remember things that happened over the last few days. With this setting, something that occurred more than 100 hours ago will have its expected probability reduced by 50%. After 200 hours, its expected probability is reduced by a further 50% to one quarter of its original probability. After 300 hours, this is reduced again.

The system would completely forget something that occurred more than 6 half-lives ago. Please note that the half life must be more than twice the time it takes to learn the initial knowledge (see Learning Period below). If you want a camera to quickly relearn new behaviour but don't want to erase the camera's memory (because of the relearning blackout period), temporarily set the half-life to a lower value.

Learn Only With Motion: In low motion environments, long periods of zero motion can make the system learn that no motion is normal. Therefore, any motion will be considered abnormal. This will cause alerts on any motion. If Learn Only with Motion is set to true, this will cause the system to stop learning when there is no motion. An example for when this would be useful is when a shopping centre is closed over night.

Human Only Detection: Enables "Humans Only" mode. This is a simple filter designed primarily for outdoor use when there are people walking upright amongst trees that move in the breeze. Do not enable it for indoor scenes or scenes with low motion.

Use Dynamic Sensitivities: If "true" the system will dynamically adjust the sensitivity to try and maintain a consistent number of alerts. This could potentially lead to discarding alerts during periods of high activity and sending false alerts during periods of low activity.

Maximum Object Age: The minimum amount of time an object must be visible before raising an alert.

Minimum Object Size: The minimum size required to alert on an object, measured in pixels.

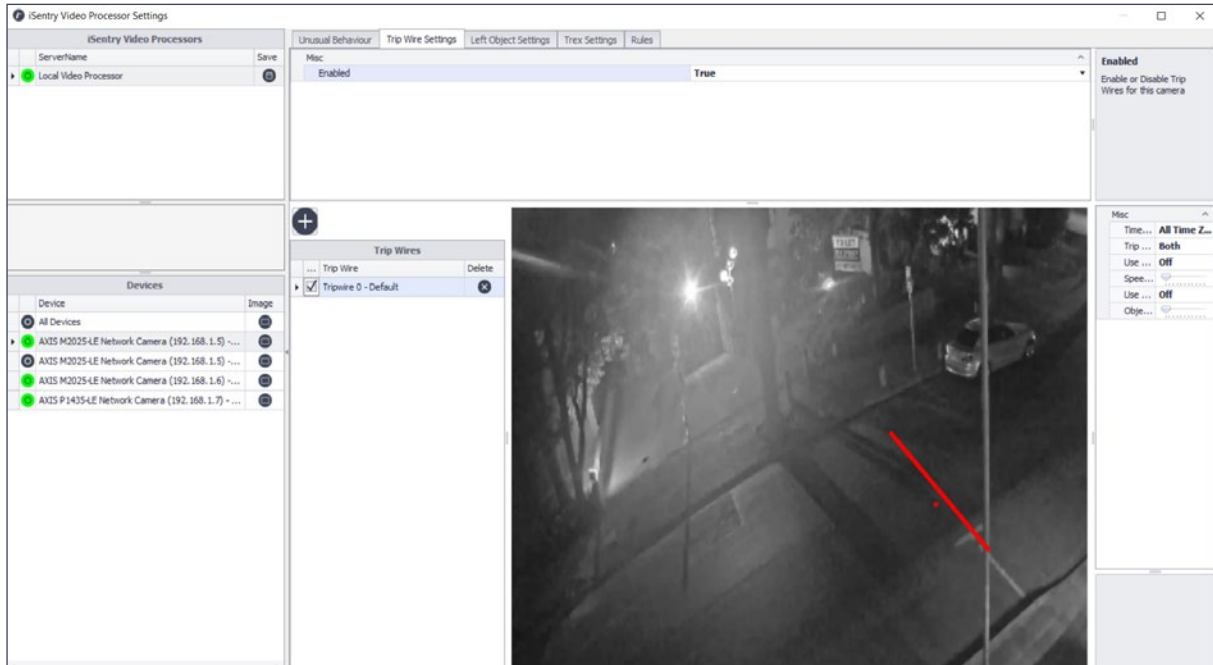
Memory Half Life: The half-life of the memory (in hours). With a high half-life, a longer time frame of past events is used to determine normal behavior. With a low half-life, the past is forgotten more quickly. At 100 hours (default), something that occurred more than 100 hours ago will have its expected probability reduced by 50%. After 200 hours, its expected probability is reduced by a further 50% to one quarter of its original probability. Please note that the half-life must be more than TWICE the time it takes to learn the initial knowledge.

Learn Speed: The number of minutes over which the system should be able to determine "normal" behaviour.

Initialisation Period: Specifies the percentage of the Learn Speed time that the analytic will be in "Blackout", i.e. learning but not raising alerts.

Trip Wires:

To enable trip wire monitoring for the selected camera, set “Enabled” to true.



Create a Trip Wire:

In order to create a new trip wire, click the **+** button, and the new trip wire will be added to the “Trip Wires” list.

Configuring a Trip Wire:

A Trip wire is selected by clicking on the checkbox in the trip wire list. The line on the image, representing the trip wire, will be displayed, and can be altered by clicking and holding the left mouse button while dragging the mouse cursor. The forward direction of the trip wire is represented by the direction of the dot added to the image. Forward is considered as the direction from the line to the dot.

Delete a Trip Wire:

In order to delete a tripwire, click on the **×** button next to the trip wire to be deleted.

Trip wire properties:

Time Zone: Choose the time zone when this trip wire is applied.

Trip Direction: A uni-directional trip wire will raise an alert only if an object crosses it in the specified direction. A bi-directional trip wire will raise an alert if an object crosses it in either direction.

Use Speed: When active, decide on the speed threshold required to trigger an alert and whether the trip wire should react to objects with speeds either above or below the threshold.

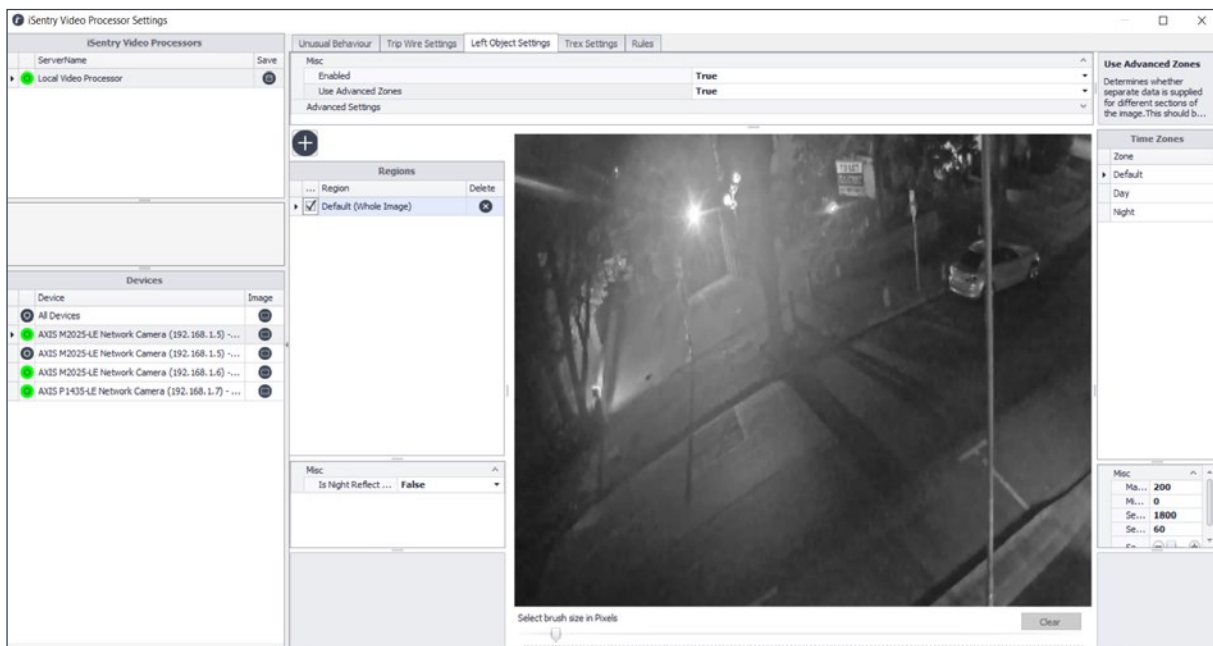
Speed Level: When active, decide on the speed threshold required to trigger an alert and whether the trip wire should react to objects with speeds either above or below the threshold.

Use Object Size: When active, decide on the object size threshold required to trigger an alert and whether the trip wire should react to objects with sizes either greater or lesser below the threshold.

Object Size Level: When active, decide on the object size threshold required to trigger an alert and whether the trip wire should react to objects with sizes either greater or lesser below the threshold.

Left Objects

To enable left object monitoring for the selected camera, set “Enabled” to true.



Having “Use Advanced Zones” set to false, Left objects will be detected over the entire view of the camera. The following properties are available in this mode:

Seconds Before Trigger: The length of time in seconds an object must be stationary in the scene before an alert is generated.


Seconds Before Merge: The length of time in seconds before a detected object is assumed to be part of the background. Once merged, a secondary alert may be generated when that object departs.

Minimum Size: The minimum size for a left object to be detected, measured in total square pixel count.

Sensitivity: The sensitivity between 0-8, where 0 is off, and 8 is the most sensitive.

Having “Use Advanced Zones” set to true, regions may be created in the image for the detection of left objects.

The Default region will be for the whole image, and an area may not be painted when this region is selected.

Create a new Region: Click on the  button to add a new region to the “Regions” list.

Configure a region: A Region is selected when it’s corresponding check box is checked.

A region can be painted by selecting a brush size (surface area in pixels), and then applying the brush to the required area. The brush is applied by clicking and holding the left mouse button and dragging the cursor over the image.

The following property is available for a Left object region:

Is Night Reflect Region: On wet nights, streetlights may be reflected in puddles and cause nuisance alerts when the puddle is disturbed. When this value is set to true, alerts in these regions are suppressed at night.”

Properties can be configured for each region per time zone. Select a Region and the Time zone to be configured:


Sensitivity: The sensitivity between 0-8, where 0 is off, and 8 is the most sensitive.

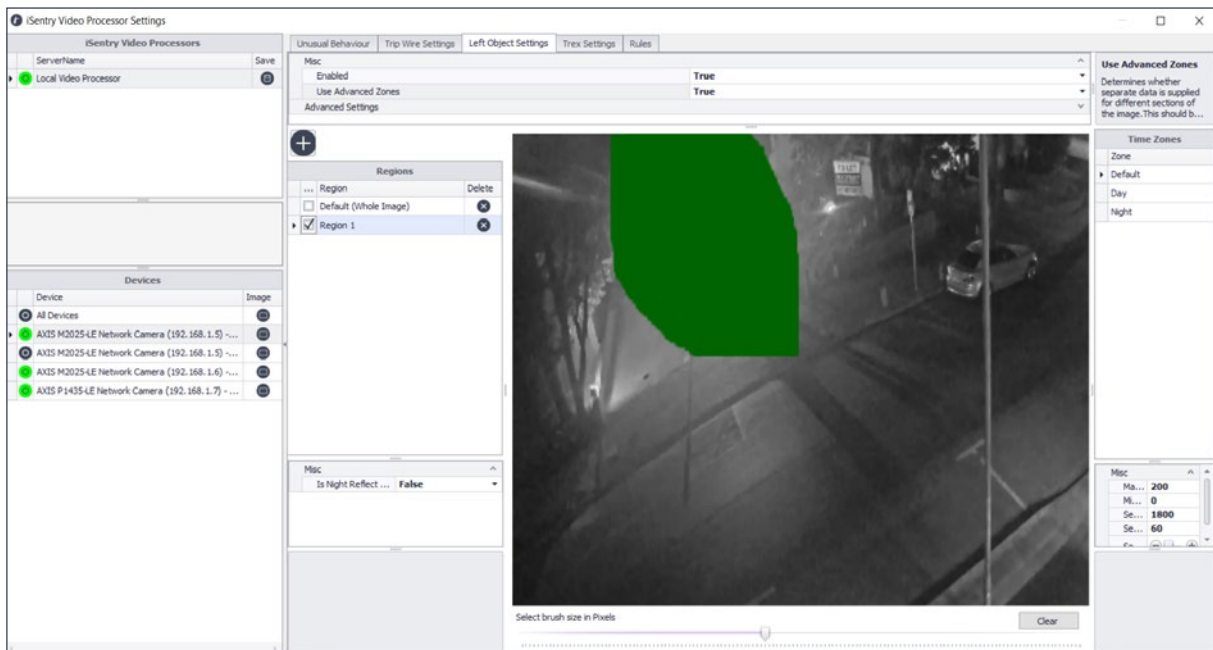
Seconds Before Trigger: The length of time an object must be stationary in the scene before an alert is generated.

Seconds Before Merge: The length of time before a detected object is assumed to be part of the background.

Minimum Object Size: The minimum size for a left object to be detected, measured in total pixel count.

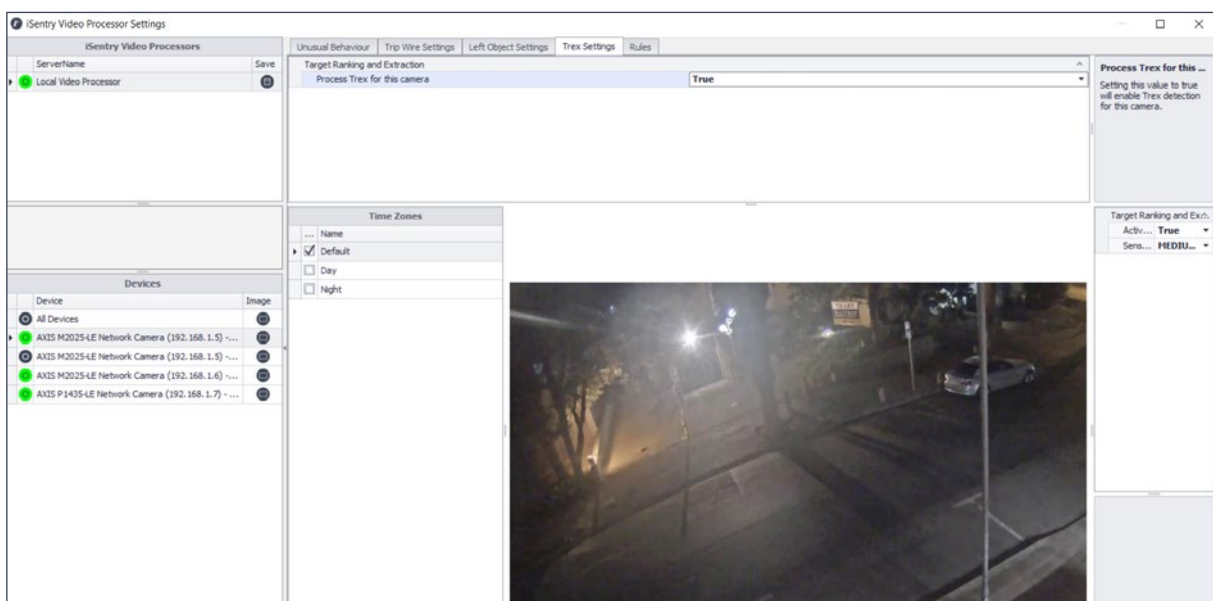
Maximum Object Size: The maximum size for a left object to be detected, measured in total pixel count.

Delete a Region: In order to delete a region, click on the  button next to the region to be deleted.



Trex (Target Ranking and Extraction):

To enable Trex monitoring for the selected camera, set “Enabled” to true.



To configure the Trex in each time zone, select the desired time zone by checking the checkbox next to it. The following properties are available:

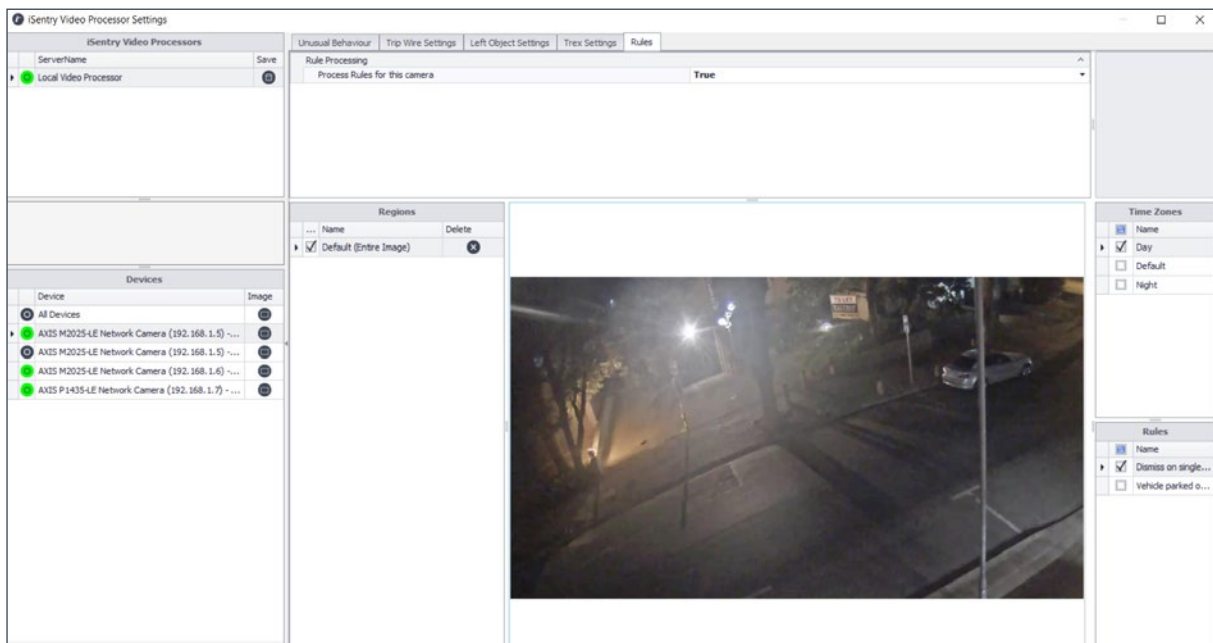
Active in This Time Zone: Set to 'true', Target Ranking and Extraction will be active in this time zone.

Sensitivity: Target Ranking and Extraction processing sensitivity.

Masking: Each time zone can have separate masks. The thickness of the masking brush can be changed by changing the value in the track bar below the image. The area that is masked out, by the brush, will be IGNORED by the Trex system, and no objects will be tracked.

Rules by Region:

To enable rule processing for the selected camera, set “Process Rules for the camera” to true.



To facilitate alert accuracy and the reduction in nuisance alerts, different rules can be applied to particular regions and for particular time zones, where rule relevance is maximised. For example you may want to apply an environmental dismissal rule to the upper part of the image to immediately eliminate factors like wind and birds that may cause false alerts.

Regions:

Regions are areas within the view of the camera, for which rules are applied. The default region, will apply rules to the whole image.


Add a Region:

A region can be added by left clicking on the image and dragging the mouse cursor to create a rectangle. A new Region will appear in the “Regions” list.

Configure a Region:

A region can be selected by checking the checkbox in the region row. To the right of the image, available time zones as well as rules are listed and, in order to set up rules for your selected region, simply select the relevant time zones as well as the required rules, by checking the checkboxes for each item.

Deleting a Region:

A Region may be deleted by clicking the  button next to the region name.

Saving Configuration changes:

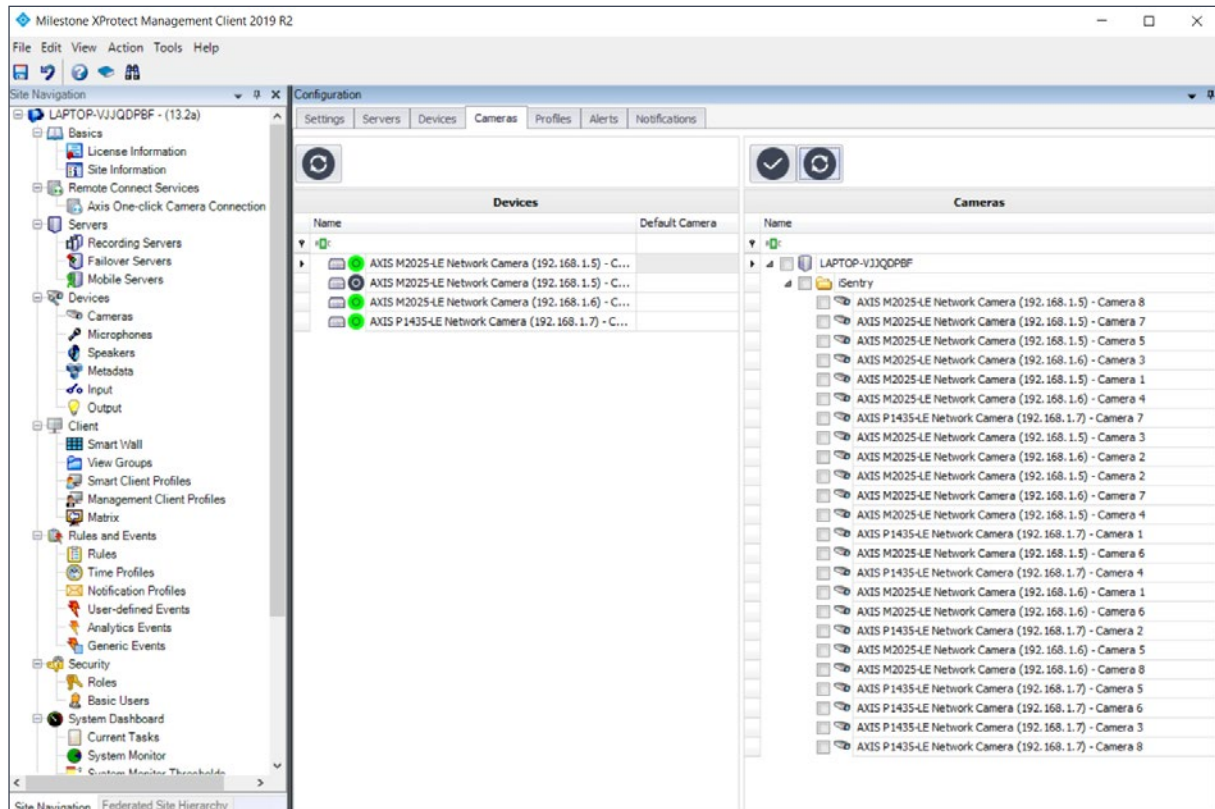
After any changes to the configuration has been made, the iSentry Video Processor must be updated.

Click the save button  next to the iSentry Video Processor that has been edited.

Confirmation or error messages will be displayed in the feedback box below the server list.

CAMERAS

The “Cameras” tab is used to associate default cameras to the “Devices”(cameras) that are processed by the iSentry Video processor and produces alerts. These Default cameras will be linked to the alert and displayed when needed, in order to provide the operator additional situational awareness.



In order to associate one or more cameras to a “device”, select one or more cameras in the right-hand pane by checking their corresponding checkboxes, and then by left mouse click, drag-and-drop these camera(s) on the required device in the “Devices” list on the left

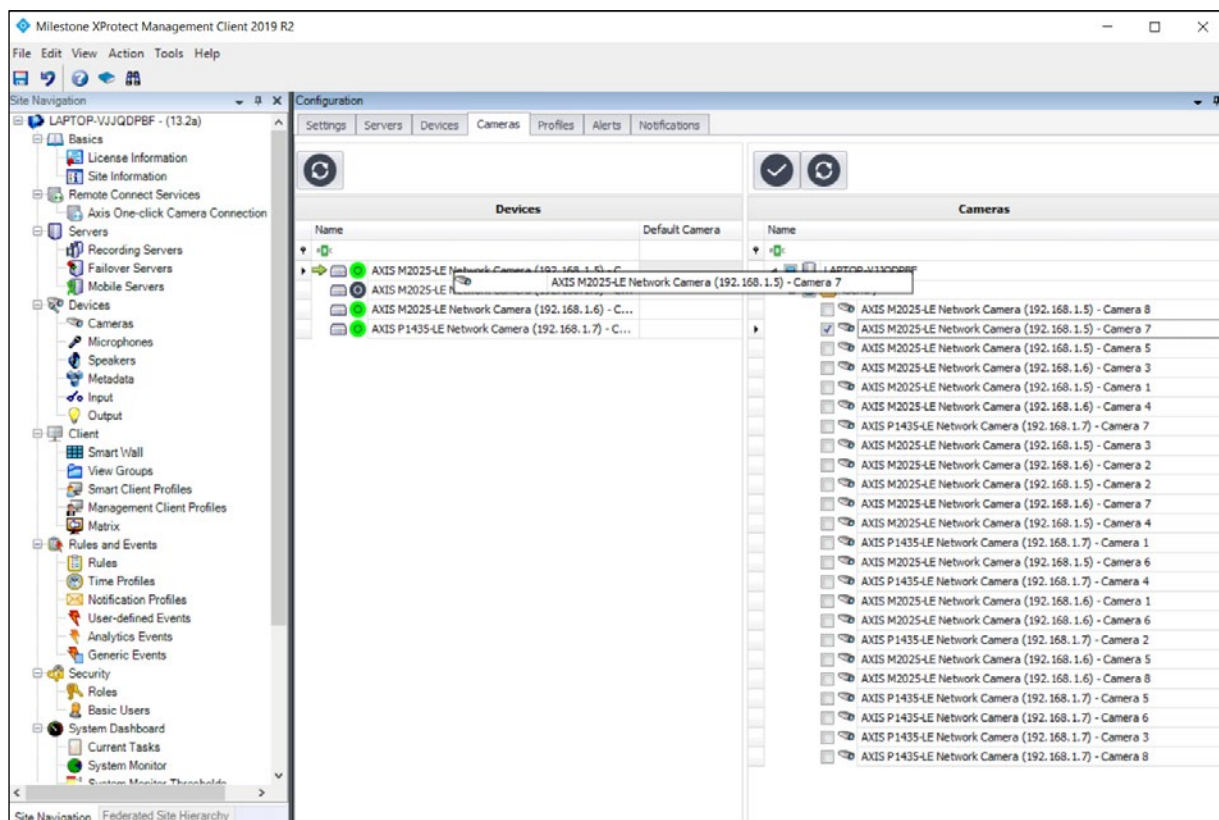
If multiple cameras are associated to a device, a default camera should be selected. This default camera will be the first to be displayed when an alert is received.

PROFILES

The “Profiles” Tab is used to configure device and alert access for milestone profiles and their associated users.

The creation and management of profiles and their associated users are done in the “Security” node in the Milestone XProtect Management Client. For more information on this process please consult the Milestone XProtect user manual.

When a user is logged into the XProtect Smart Client, only the cameras configured in this Tab (for the user role) will be visible to that user. To associate devices to roles, select one or more devices(cameras) in the right-hand pane by checking their corresponding checkboxes, and then by left mouse click, drag-and-drop these camera(s) on the required role in the “Roles” list on the left.



ALERTS

The “Cameras” tab is used to associate default cameras to the “Devices”(cameras) that are processed by the iSentry Video processor and produces alerts. These Default cameras will be linked to the alert and displayed when needed, in order to provide the operator additional situational awareness.

Alert Types

In the “Alert Types” section of this window, the Default Standard Operating Procedures (SOPs) for each alert type can be configured. A Standard Operating Procedure, is the instruction given to an operator for a particular alert type, when an alert is generated.

An SOP may be altered by clicking on the SOP box and typing some new text. The SOP is saved when the mouse is clicked on another row.


Alert Categories

When an alert is generated, it is expected that either the operator, or the rules engine should process the alert and make a decision on its outcome. The outcome of an alert, is called the Action taken, and this action will always either be an escalation to an alarm, or a dismissal. For each of these two cases, there are additional information captured by the operator (or rules engine) to explain the action taken.


In the “Alert Categories” section of this window, the available escalation and dismissal options are configured.

The current Alert Categories are listed in the list in the “Alert Categories” section of the window. The “Is Escalation” checkbox, marks the event category as an escalation, and where it is not checked, as a dismissal. The “Auto Escalate” checkbox, is the Category used for auto escalation or dismissal, when the “Auto Promotion time” for a new alert runs out.

Create a New Alert Category:

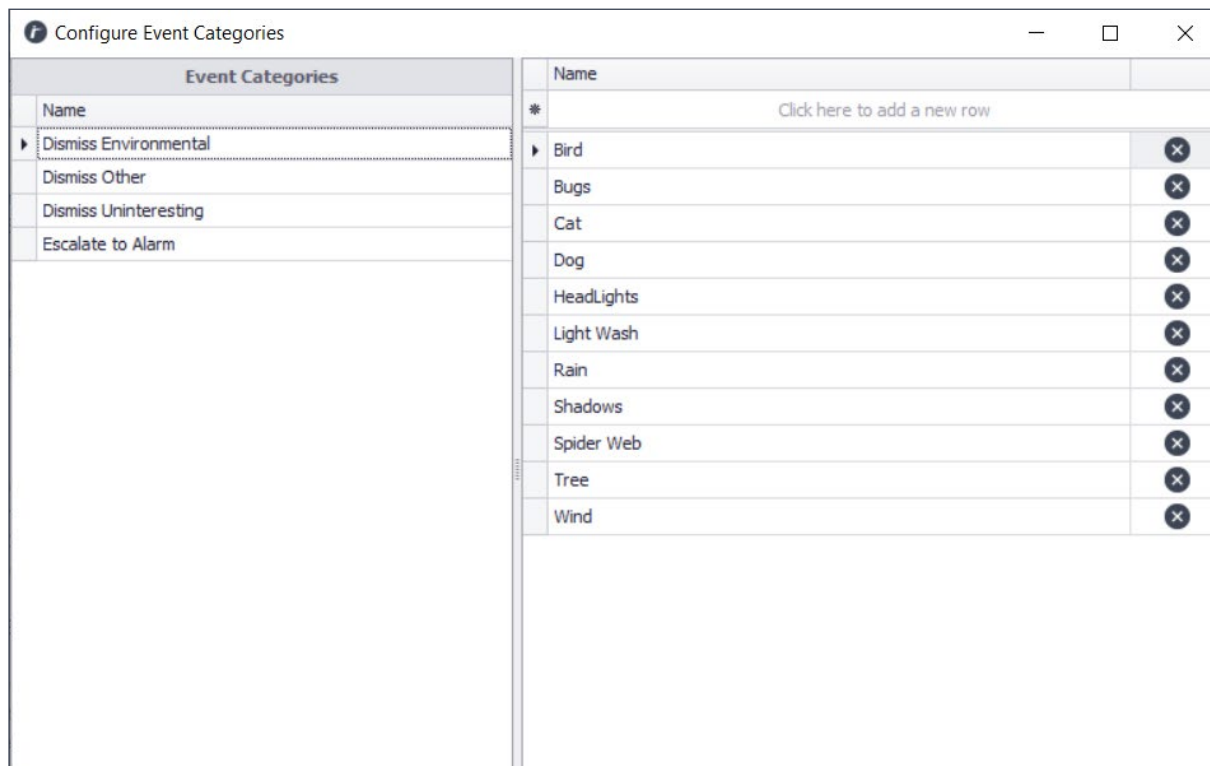
Click on the  button at the top of the list, to pop up an “Add Alert Category” window. Please complete the details in this window and click “Save” to create the new Category.

Delete an Alert Category:

Click on the  button next to the category to be deleted. Please note that Alert categories cannot be deleted, once an alert has been associated with it.

Configure an Alert Category:

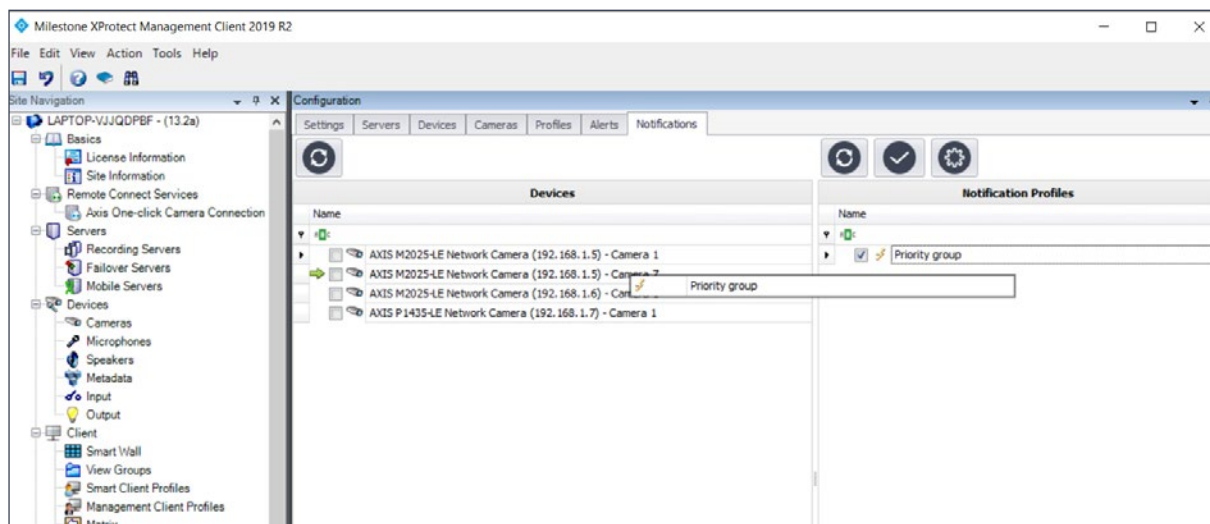
Click on the  icon to display the “Configure Event Categories” window.



Click on an Event Category in the list to display and edit its Sub-Categories. In the Case of Dismissals, a single categorisation list is available, where with Escalations, a further “Operator Action” list is available.

NOTIFICATIONS

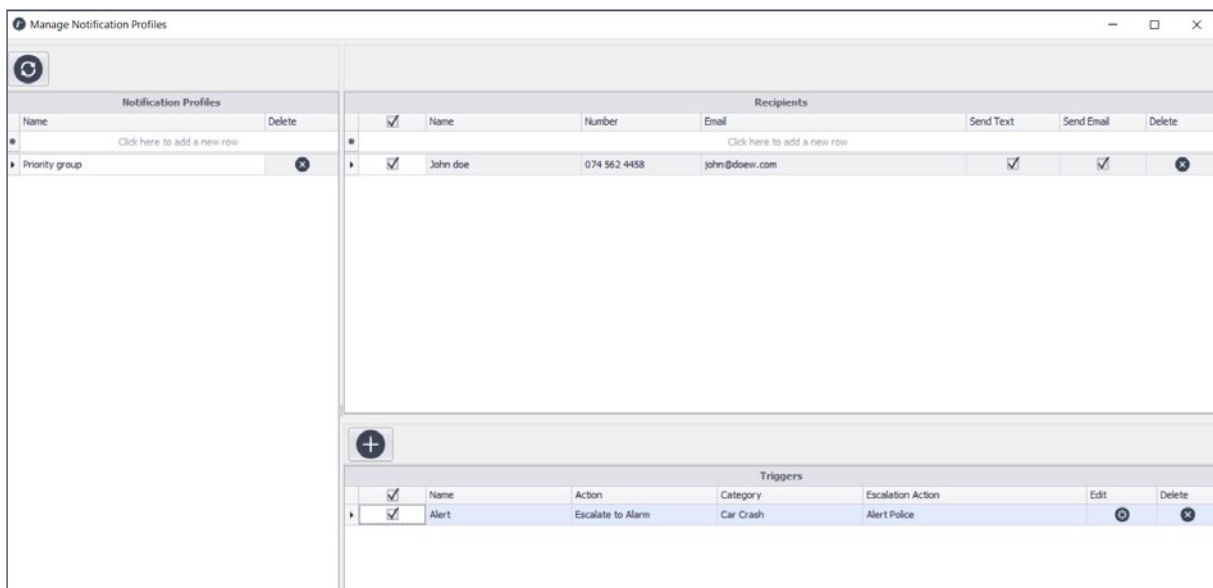
In the “Notifications” tab, Notification profiles are mapped to devices.



When an alert occurs, and is handled either by the Rules engine or an operator, the action taken will be tested against notification profiles, for devices that has been mapped in this tab. Notifications in the form of Telegram messages and/or Email messages will be sent to all recipients linked to a notification profile, when trigger criteria is matched.

Notification Profiles

Notification Profiles can be managed by clicking the  button at the top of the Notification Profiles list.




Create a new Notification Profile:

A new profile is created when a name for the profile is typed in the top row of the “Notification Profiles” list. Move to a new row or press enter twice to save.

Configure a Notification Profile:

Configuring a profile, entails linking the Users, to the Triggers, by checking the check boxes for the items that must be included in the profile.

Delete a Notification Profile:

A Profile is deleted when the  delete button, next to the chosen profile, is pressed. Confirm deletion by clicking ‘Yes’ in the pop-up window.

Recipients

Recipients, are the individuals, who will receive a Telegram and/or email message for a configured Notification Profile, when an action is taken satisfying the trigger criteria.

Add a Recipient:

Message recipients can be added by typing details into the top row of the “Recipients” list.

The following information is required:

Name: This is the Name (and Last name) of the recipient.


Number: this is the mobile number of the recipient, as registered on the Telegram application. Numbers must be typed in the international format i.e. country code first followed by the rest of the number. The “+” plus sign in front of the country code is not required, and brackets as well as other special characters including spaces, should be avoided.

Email: The email address of the recipient.

Send Text: if this is ticked, Telegram messages will be sent to this recipient.

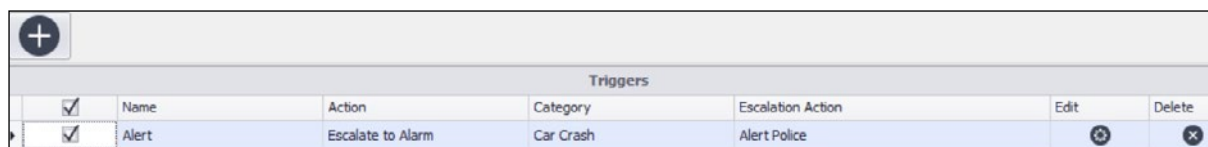
Send Email: if this is ticked, then email messages will be sent to this recipient.

Delete a Recipient:



A recipient can be deleted by clicking the  button next to the chosen recipient. Click ‘Yes’ to confirm deletion in the pop-up window.

Triggers

A trigger is the starting point of the messaging process. Each trigger is a set of actions and categorisations that define the action taken by an operator or the rules engine, in processing an alert



The screenshot shows a table with a header row and one data row. The header row is titled 'Triggers' and has columns for Name, Action, Category, Escalation Action, Edit, and Delete. The data row has a checked checkbox in the first column, 'Alert' in the Name column, 'Escalate to Alarm' in the Action column, 'Car Crash' in the Category column, 'Alert Police' in the Escalation Action column, a plus icon in the Edit column, and a minus icon in the Delete column.

Triggers						
<input checked="" type="checkbox"/>	Name	Action	Category	Escalation Action	Edit	Delete
<input checked="" type="checkbox"/>	Alert	Escalate to Alarm	Car Crash	Alert Police		

For example if an operator escalates an alert to an alarm, and defines the Action as “Escalate to Alarm”, Category as “Suspicious Person” and the Escalation Action as “Alert Armed Reaction” then this will be tested against the configured notification profile triggers and if it is a match, a message will be sent to the relevant recipients.

Add a Trigger:

Click on the add button to pop-up the notification triggers window. The following information must be added:

Trigger Name: Descriptive name to ease identification of this trigger for re-use.

Action: Make a selection for dismissals or escalations.

Category: Select a sub-category for the trigger.

Escalation Action: (this only applies to escalations) Select an escalation action for the trigger.


Click “Add” to save the new trigger.

Edit a Trigger:

Click on the  button in the row of the Trigger to be edited. A notification triggers window will appear.

Edit any of the fields in the window and click “Update” to save the changes.

Delete a Trigger:

Click on the  button in the row of the trigger to be deleted. Click “Yes” in the confirmation dialog to delete the trigger.

CONFIGURE TELEGRAM MESSAGING

The “Cameras” tab is used to associate default cameras to the “Devices”(cameras) that are processed by the iSentry Video processor and produces alerts. These Default cameras will be linked to the alert and displayed when needed, in order to provide the operator additional situational awareness.

The Telegram Bot

To configure a BOT the following steps may be followed:

1. Download the Telegram application on a phone; and open.
2. Search for “BotFather”.
3. Send the “BotFather” a text message “/newbot”
4. Follow the instructions displayed on screen. Make a note regarding the name of the Bot, recipients will need the name to register themselves.
5. After successful completion of the Bot Creation process, a HTTP API Token will be received.

Enter this token value into the “Telegram Bot Id” field in the Processing Server Settings.

Restart the processing server to apply the settings.

The bot will now be ready to send messages.

REGISTERING RECIPIENTS

In order to receive Telegram messages a recipient must be registered for this service.

Firstly, a Recipient must be added in the “Notifications” tab, when managing “Notification Profiles”. Please note that the telephone number must be entered starting with the country code, and without any special characters. eg
2.7123455678

When a Recipient has been added, that recipient must install the Telegram Application on their phone with the correct number, and then follow the following steps:

1. Open the Telegram Application;
2. Search for the Bot, by typing the name of the bot;
3. Send a Text Message to the bot “/join”
4. If the Bot is Online, a message will be received asking the user to share his or her phone number. Click the “Share my Phone Number” button, to allow access.
5. A message will be received confirming registration, or failure to do so.

CONFIGURE EMAIL MESSAGING

In order to use email messaging, a SparkPost API id is required.

To get this API ID, visit to www.sparkpost.com and register an account. The process will require an active Domain and the ability to add DNS entries. Please consult the website for instructions on this process.

When an API ID has been obtained please enter this id into the “SparksPost API ID” field in the Processing Server Settings. Also enter a valid “From” email address for the registered domain, in the “From Email Address” field.

SYSTEM STATUS

In the XProtect Management Client as well as the XProtect Smart Client, iSentry Alert Plugin, the Status of Cameras and various other components are visible in the form of various status icons.

Status icons can take the following forms:

Unknown: Status for this item is not available or has not been reported. Usually this status will be replaced by another status within a few seconds. If this Status Persists, please ensure that the Processing Server is Started and Connected.

Good: This means that this item is running within normal parameters.

Warning: This means that the item is running, but that there is a trouble condition.

Error: This means that this item is not functioning, or has experienced an error.

Hovering your mouse pointer over any of these icons will reveal detail describing the current condition of the item in question.

This information will also include limited diagnostic info for fault finding and performance of the system.

SYSTEM LOGS

The system will create a wide variety of logs, to report on warnings, errors as well as performance of the system.

In iSentry Processing Server Settings, as well as the iSentry Plugin, Settings Tab in the XProtect Management Client, the “Log Level” of the system may be adjusted to increase or decrease the amount of information written to the log files. A log Level of “Normal” will only log errors and basic status information, a log level of “Full” will log debug information, will result in large log files as some additional processing overhead. Setting the Log to “Trace” is not generally recommended, as this will maximise logging and create a substantial processing overhead. “Trace” can be used for short periods of time to allow for detailed investigation.

The default location of all the system logs is:

C:\ProgramData\SmartProtect\iSentry\Logs

Milestone iSentry Alert Plugin Logs

XProtect Event Server Logs: “Service_YYYYMMDD.log”

XProtect Management Client Logs: “Administration_YYYYMMDD.log”

XProtect Smart Client Logs: “SmartClient_YYYYMMDD.log”

Processing Server Logs

Processing Server Master Log: “SPiSentryServer_YYYYMMDD.log”

Processing Server Manager Log: “SPiSentryServerManager_YYYYMMDD.log”

Deep Learning Server Communications Log: “DLServerYYYYMMDD.log”

Rules Processor Log: “RulesProcessorYYYYMMDD.log”

Deep Learning Server Logs

Deep Learning Server Master Log: “SPiSentryDLServerYYYYMMDD.log”

Deep Learning Server Manager Log: “SPiSentryDLServerManagerLogYYYYMMDD.log”

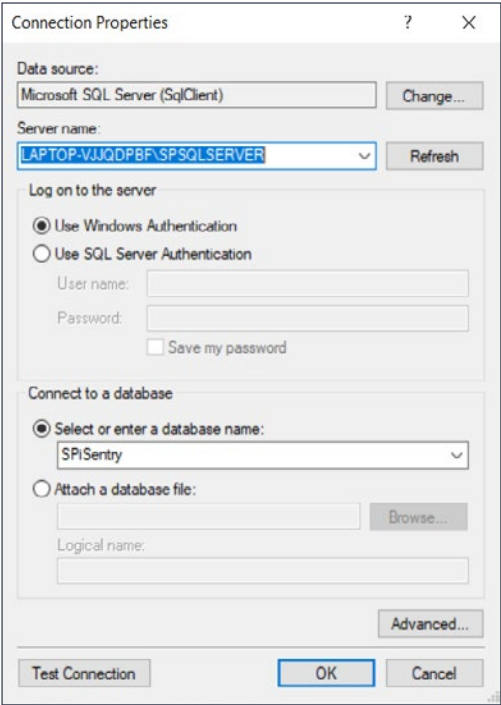
TROUBLESHOOTING

When troubleshooting, the investigation of logs are one of the most valuable tools at your disposal, and it is recommended that logs are investigated as part of any trouble shooting procedure. Setting the “Log Level” to “Full” is recommended when trying to solve issues.

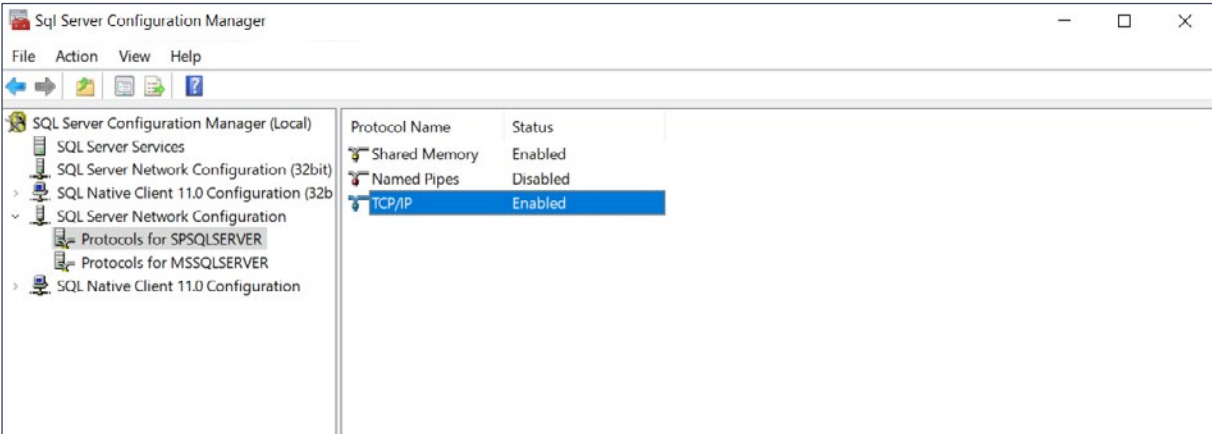
Database Connection Issues

General

If the database resides on a different machine in the Network, routing and firewall settings must be checked. Consult your Network administrator for assistance in this task.



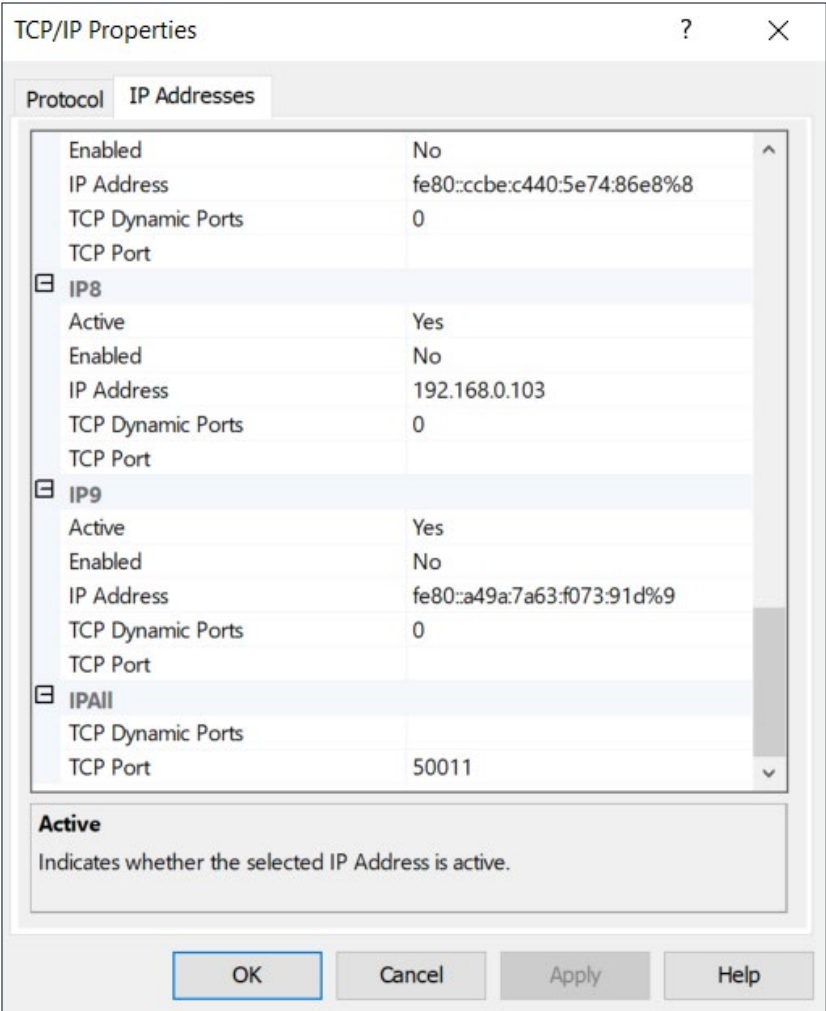
When refresh is clicked, the system will attempt to find all available SQL Server Instances, both locally and on the local network. This process depends on SQL Browser running on each instance, as well as the correct ports being open to these servers. It is common for the refresh function not to show the desired SQL Server instance. For the default installed SQL Server Instance TCP communication will be enabled and the port number can be used.



To find the port number of the SQL instance, open the “SQL Server Configuration Manager”. Select the “SQL Server Network Configuration”, and Click the “Protocols for SPSQLSERVER” (“SPSQLSERVER” to be replaced by the custom instance name for a custom installation).

Select on the “TCP/IP” protocol, if this protocol is not enabled, port number Instance connections will not be available. Enabling this protocol will require a SQL Server Service restart.

Right Click on the “TCP/IP” protocol row and select “Properties”. Select the “IP Addresses” tab and select the required IP configuration node, or scroll to “IPALL” ports applied to all.



The “TCP Port” value can be used, for the SQL Instance connection. If the “TCP Port” value is unassigned, then the “TCP Dynamic Ports” value can be used.

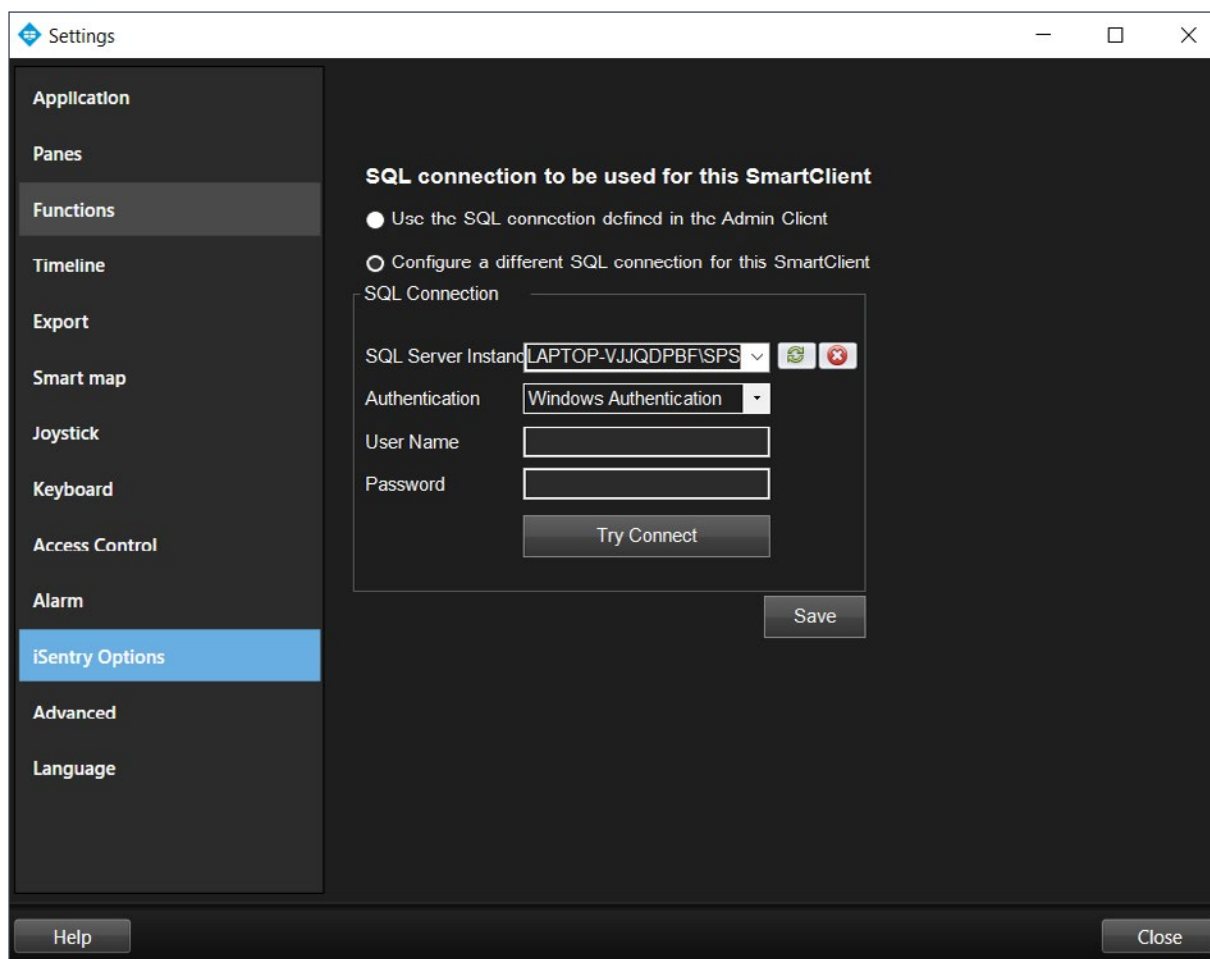
Please follow the instructions described in Step1 and Step3 of the basic configuration guide, to configure the connection.

XProtect Management and Smart Clients

If this server is not running, or if it is inaccessible, a message will be displayed stating that the database connection could not be loaded. Please ensure that the XProtect event server is indeed running and perhaps re-start this service if the error persists.

Smart Client (Special Case)

In the case where the Smart Client cannot access the SQL server with the same connection properties as the Management Client, a Smart Client specific setting exists to configure the SQL server connection for only that one client. This setting can be accessed by selecting the “Settings” menu at the top right-hand corner of the Smart Client.

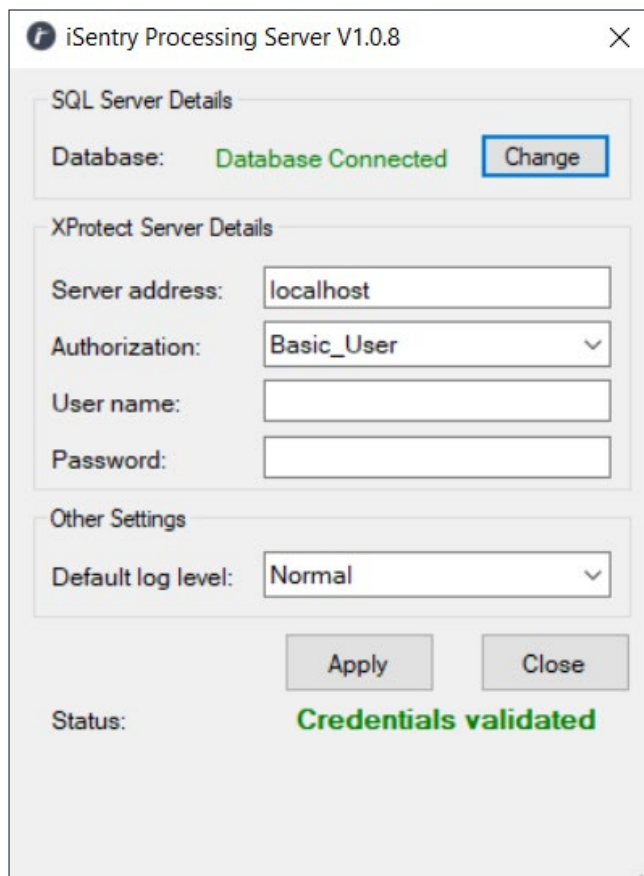


Here the Smart Client specific database connection may be configured and Saved.

Processing Server will not connect to the Milestone XProtect Management Server

The first thing to consider will be the Server Address, this address must resolve to the correct XProtect Management Server. Secondly, the Details of the user must match the credentials as configured in the Milestone Management Client under the Roles tab. It is important that the user used for this login is part of the Administrators role, in order to have unrestricted access.

Please consult the Milestone XProtect Manuals for the correct port numbers to be opened, if firewalls exist between the iSentry Processing server and the XProtect Management Server.

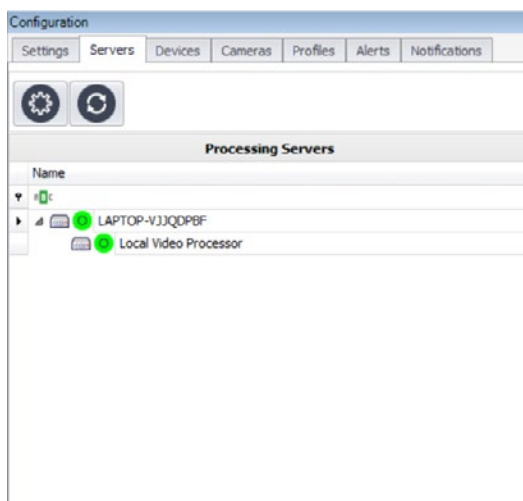
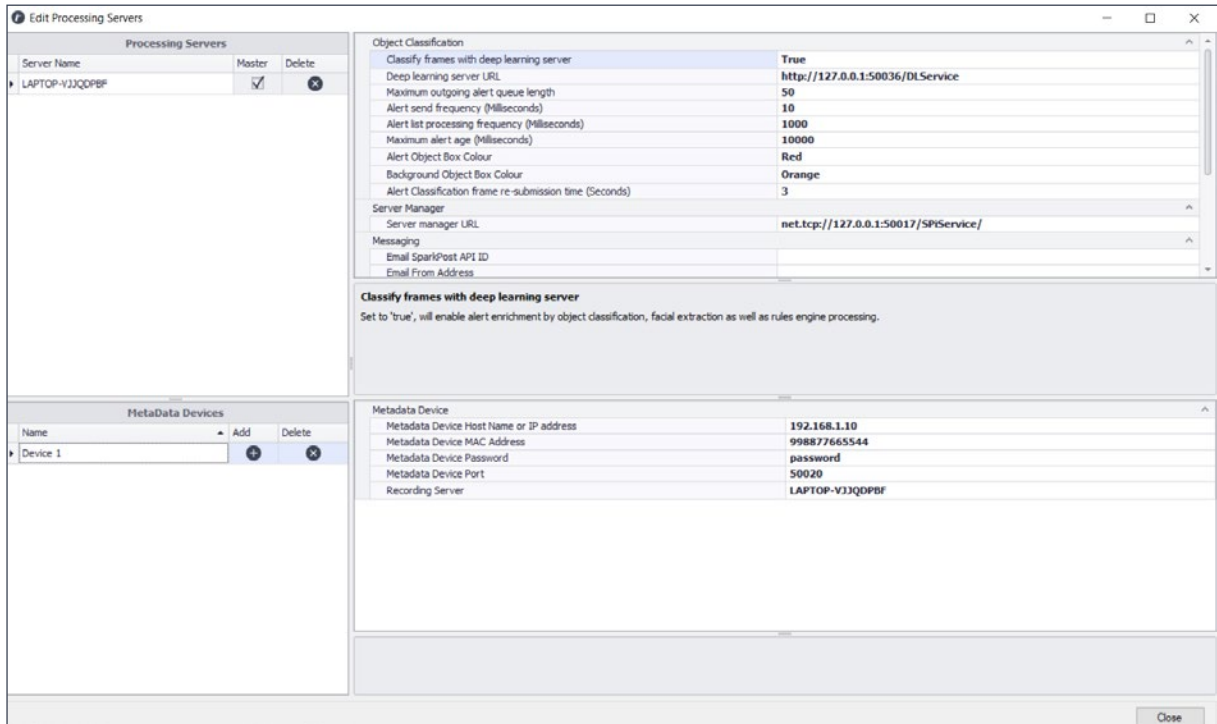


iSentry Object Classification and Facial Extraction (Deep Learning) Server crashes as soon as an alert is received

When the Object Classification and Facial Extraction (Deep Learning) Server is running in GPU mode, it relies on the nVidia drivers for the installed GPU. Please ensure that the drivers have been updated to the latest versions available. Also make sure that the GPU meets or exceeds the minimum hardware requirement. CPU mode is not recommended, but in both CPU and GPU mode, the Server logs will assist in identifying underlying problems.

iSentry Object Classification and Facial Extraction (Deep Learning) Server connection problems:

In the case where facial extraction and Object classification is not applied to the alert images, this may be due to incorrect configuration or networking issues. As a starting point, make sure that the “Classify frames with deep learning server”, setting is enabled in the Management Client



In the XProtect Management Client, iSentry plugin, “Servers” tab, the status of the Processing server will be red, if the connection to the Object Classification and Facial Extraction (Deep Learning) Server fails.

Furthermore, please ensure that the “Deep learning server URL” in the Server settings matched the URL specified in the Object Classification and Facial Extraction (Deep Learning) Server tray exactly.

Object Classification	
Classify frames with deep learning server	True
Deep learning server URL	http://127.0.0.1:50036/DLService
Maximum outgoing alert queue length	50
Alert send frequency (Milliseconds)	10
Alert list processing frequency (Milliseconds)	1000
Maximum alert age (Milliseconds)	10000
Alert Object Box Colour	Red
Background Object Box Colour	Orange

If these settings have all been configured properly, and the connection still fails, the likely culprit will be a networking problem. Please ensure that the URL of the Object Classification and Facial Extraction (Deep Learning) Server resolves from the Processing server, and that any firewalls are configured to allow the specified port. Please consult your network administrator for additional support.

Metadata Device issues

Creating Metadata Devices Fails

Firstly the related Processing server must be connected and running, to be able to create a Metadata device.

If metadata device creation fails, firstly ensure that the “Metadata device IP Address” is specified correctly in the server settings. Also make sure that the “Metadata device Port number” is unused and that the “Metadata device MAC Address” is unique. It is common for a Firewall on the Processing server to block the Metadata traffic, so also ensure that the metadata port is allowed through the firewall.

Restart the Processing Server, wait for 60 seconds and retry creating the metadata device.

If the Metadata device creation fails due to a “Timeout” error, and processing server connectivity is confirmed, then the “Timeout” setting in the “General settings”, under the “Milestone” section may be adjusted to a higher value. This could be helpful

particularly with a large number of cameras connected to the system or a busy network adaptor.

If a pre-existing metadata device, for the related Processing server, is present in the “Recording servers” Node in the XProtect Management Client, this Metadata device should be deleted, by right-clicking on the device and choosing “Delete Hardware”. Re-try creating the Metadata device.

IMPORTANT: When a metadata device is deleted or re-created, all pre-existing metadata will be deleted and permanently lost!

Creating Metadata Devices Fails

IMPORTANT: When a metadata device is deleted or re-created, all pre-existing metadata will be deleted and permanently lost!

Firstly, Smart clients may just not be displaying the Metadata, which is being recorded.

Logging off and back in may correct Metadata display issues.

Permissions may also effect the display of metadata, and as a test, log into the Smart Client with an administrator user, and confirm that the Metadata is not displayed. If this corrects the issue, there is likely a user rights configuration issue. Please consult the Milestone XProtect manual for Permissions configuration.

When Smart Client issues, as well as rights have been eliminated, the following procedure may be followed:

Navigate to the “Recording Servers” node, in the XProtect Management Client, find the metadata device in question, in the “Recording server” window, and expand the Metadata Device node. Please confirm that the Metadata device has a channel configured for each camera linked to it in the iSentry Plugin.

If the number of channels are different to what is expected, press “F5” to refresh and re-check, if this is confirmed, please delete the device by right-clicking on the device and choosing “Delete Hardware”. After successful delete, please press “F5” again to refresh and then re-create the Metadata device in question, in the iSentry Plugin, as described in the “Devices” section of the configuration manual.

If the Metadata Device is configured correctly, then right click on the Metadata Device and un-check the “Enabled” option, in order to disable the device. After several seconds, re-enable the device by repeating the process and checking the “Enabled” option for the metadata device. Allow some alerts to be generated and check if Metadata is recorded.

If the problem is still not resolved, the Recording server to which the Metadata device is connected, may be restarted. Please NOTE that this is not recommended for live systems as Camera recordings for this server will be suspended for the duration of the restart.



info@intellexvision.com | www.intellexvision.com