



## **SCYLLA UNIFIED PLUGIN FOR MILESTONE**

# TABLE OF CONTENTS

<b>INSTALLATION RESOURCE</b>	4
<b>INTRODUCTION</b>	5
<b>CONFIGURATION</b>	7
<b>SETUP</b>	8
<b>CONFIGURATION- HARDWARE</b>	9
<b>CONFIGURATION- ONVIF BRIDGE</b>	22
<b>CONFIGURATION- PLUGIN</b>	28
<b>TROUBLESHOOTING</b>	38
<b>CONCLUSION</b>	39

## VERSION HISTORY

Document Version	Date
1.2.0	29.06.2021

Plugin Version	Date
1.0.0	20.04.2021

# INSTALLATION RESOURCES

4

Download the software from the Internet (<https://www.milestonesys.com/downloads/>) and run the **Milestone XProtect VMS Products 2020 R3 System Installer.exe** file.

## Download software

Welcome to the Download section, where you can download Milestone software and device packs in the version and language you need.

Product

XProtect Corporate

Version

XProtect Corporate 2020 R2 (20.2a)

Free Search

Type

Software

Language

English

Filter



# INTRODUCTION

Scylla unified plugin for Milestone adds additional functionality to Milestone VMS (Video Management System) to support Scylla Intrusion Detection System (IDS) and Occupancy Counting System (OCS) solutions.

The unified plugin was developed for AI-based Scylla video analytics system that is dedicated to support existing intrusion detection and occupancy counting solutions are based on 24-7 video streaming. This plugin is dedicated for the two-way connection of Milestone XProtect Smart Client system with Scylla Intrusion Detection and Occupancy Counting Systems.

It connects to the Milestone ONVIF Bridge, retrieves the RTSP streams and provides to Scylla AI video analytics tools installed on a dedicated server. The latter analyse video streams and once an event or an object of interest is detected, it sends the corresponding alert back through the plugin to Milestone Dashboard. In addition, similar alerts are optionally reflected in Scylla Web-based dashboard and Scylla Mobile alerting app (iOS/Android).

The unified plugin allows for each camera to configure an active area where the detection will be valid as well as the time schedule of the activation.

## INTRODUCTION - Milestone Alarm Management System

XProtect alarm management system allows one to see different events configured in Management Client as alarms in Smart Client alarm management tab, get notifications and see recorded previews and additional data from associated cameras.

Custom alarms need to be configured in Management Client, then processed through Milestone Event Server to become available in the alarm management tab. More details are available from Milestone official documentation.

For Scylla unified plugin for Milestone no manual alarm configuration is needed - all configurations are set automatically when the plugin is activated.



## CONFIGURATION- MILESTONE PLUGIN

Scylla unified plugin for Milestone setup file can be downloaded from Scylla web page or Milestone Marketplace.

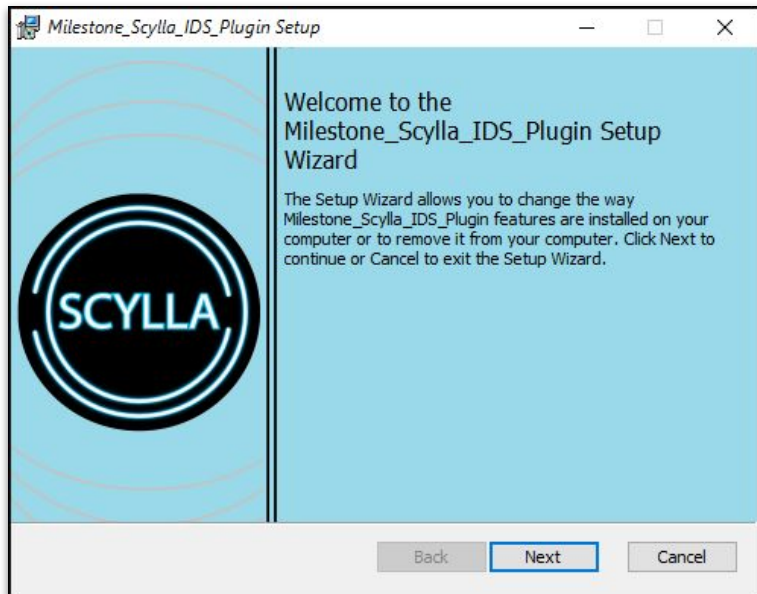
Plugin connects to Scylla web server to perform image processing.

Plugin creates a local MSSQL database to store nuccessary data needed for plugin correct functionality.

# SETUP

For correct setup please follow steps below:

Double click on Milestone\_Scylla\_IDS\_Plugin\_Setup.msi file.  
You will see a welcome screen, click on **Next** to continue.

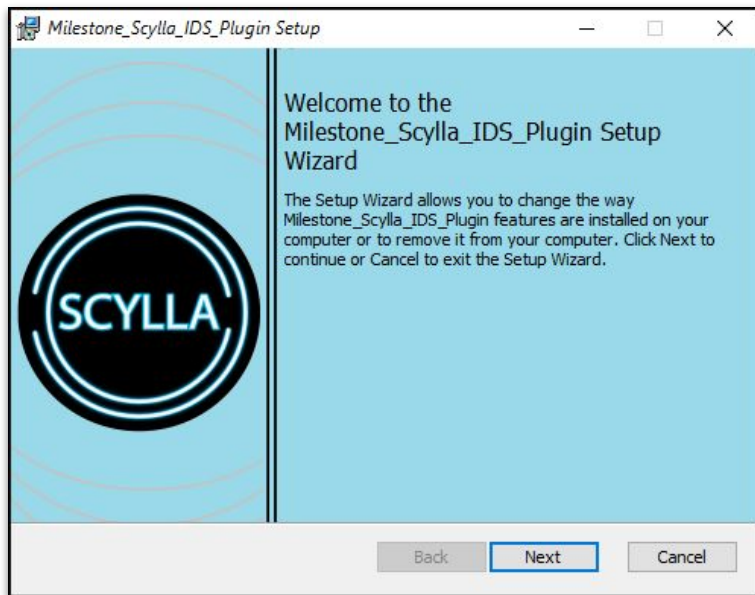




# SETUP

Set the plugin installation folder path at the next step. All plugins developed for Milestone VMS need to be installed in “MIPPlugins” folder (for example default Milestone path for 64 bit operating system is C:\ProgramFiles\Milestone, so plugin installation folder in this case is C:\Program Files\Milestone\MIPPlugins\Scylla-IDS).

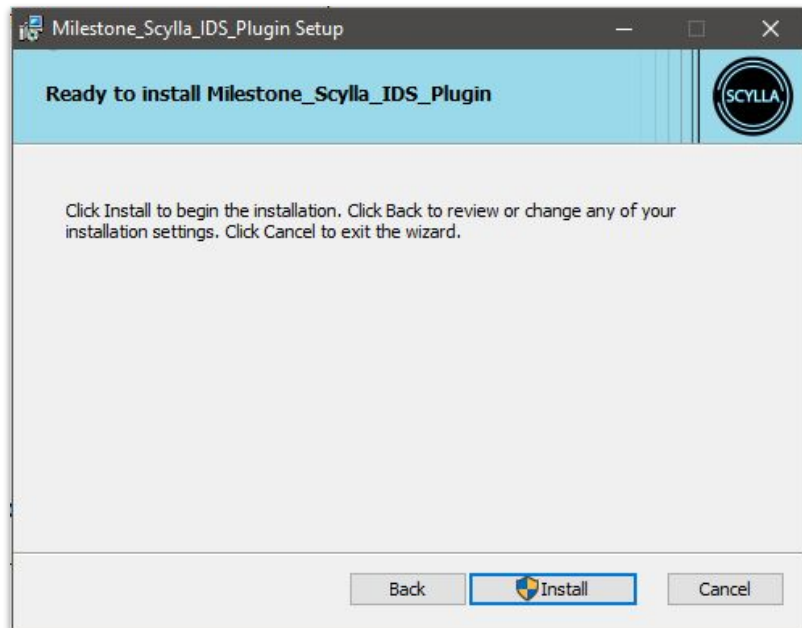
Click **Next** onafter setting the correct path .



# SETUP

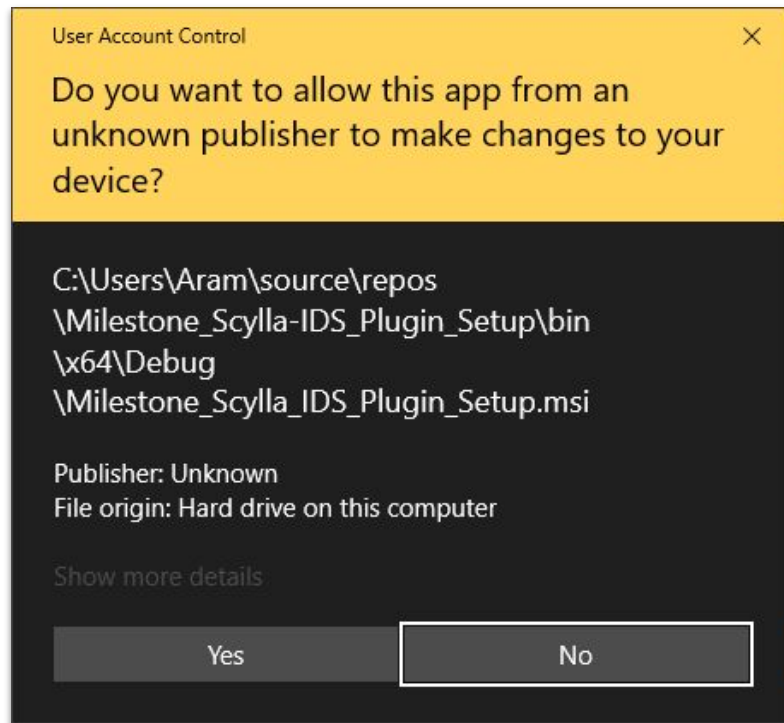
10

Click **Install**.



# SETUP

Setup needs administrator permissions to install files. Click **Yes**.



# SETUP

Then click **Finish** to complete the installation.



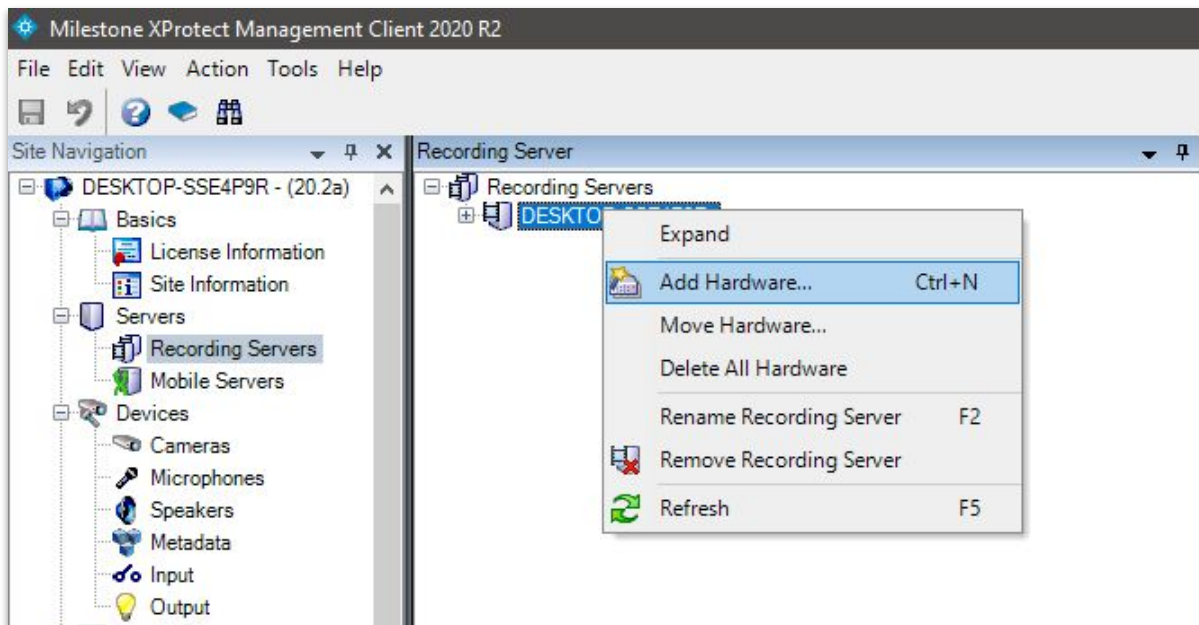
## CONFIGURATION- HARDWARE

After installation is complete you have to configure hardware devices (cameras, VMS) in XProtect Management Client.

Open **Recording Servers** on navigation tab.

Right click on the server installed on your machine (seen on right panel)

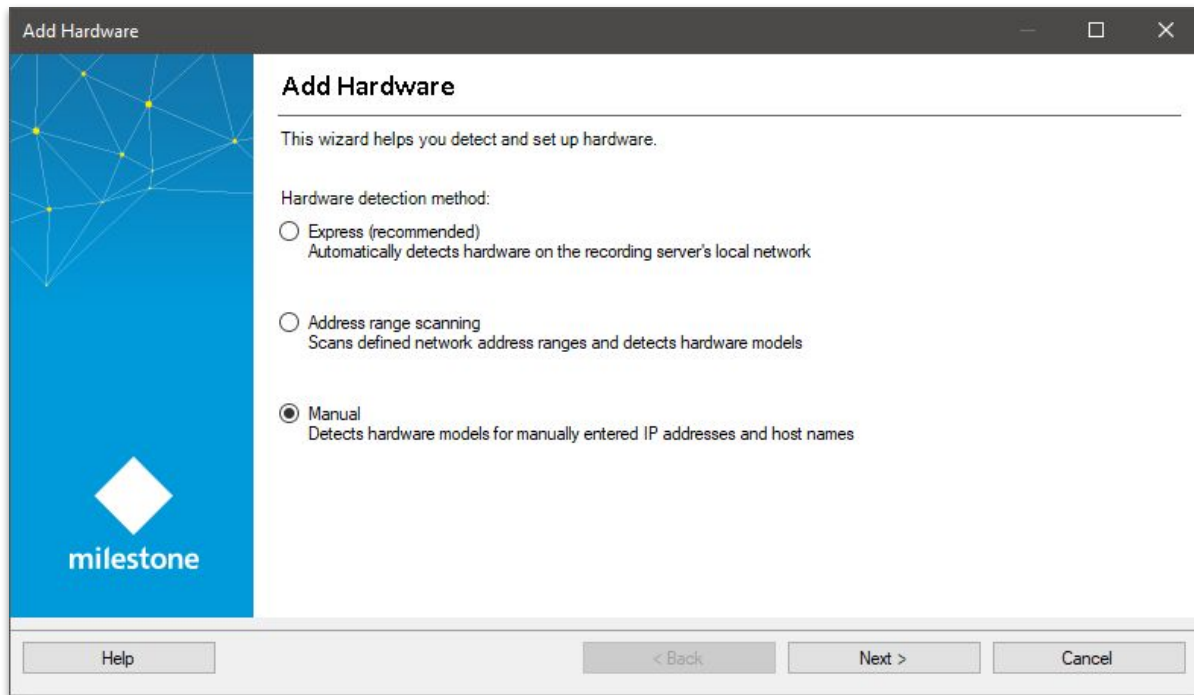
Click on **Add Hardware...**



# CONFIGURATION- HARDWARE

14

Select **Manual** and click **Next**



# CONFIGURATION- HARDWARE

15

Add camera **Username** and **Password** and click **Next**

Add Hardware

Optionally, specify additional user credentials to connect with if the hardware is not using the factory defaults.

milestone

Include	User name	Password
<input type="checkbox"/>	(Factory default)	.....
<input checked="" type="checkbox"/>	admin	.....

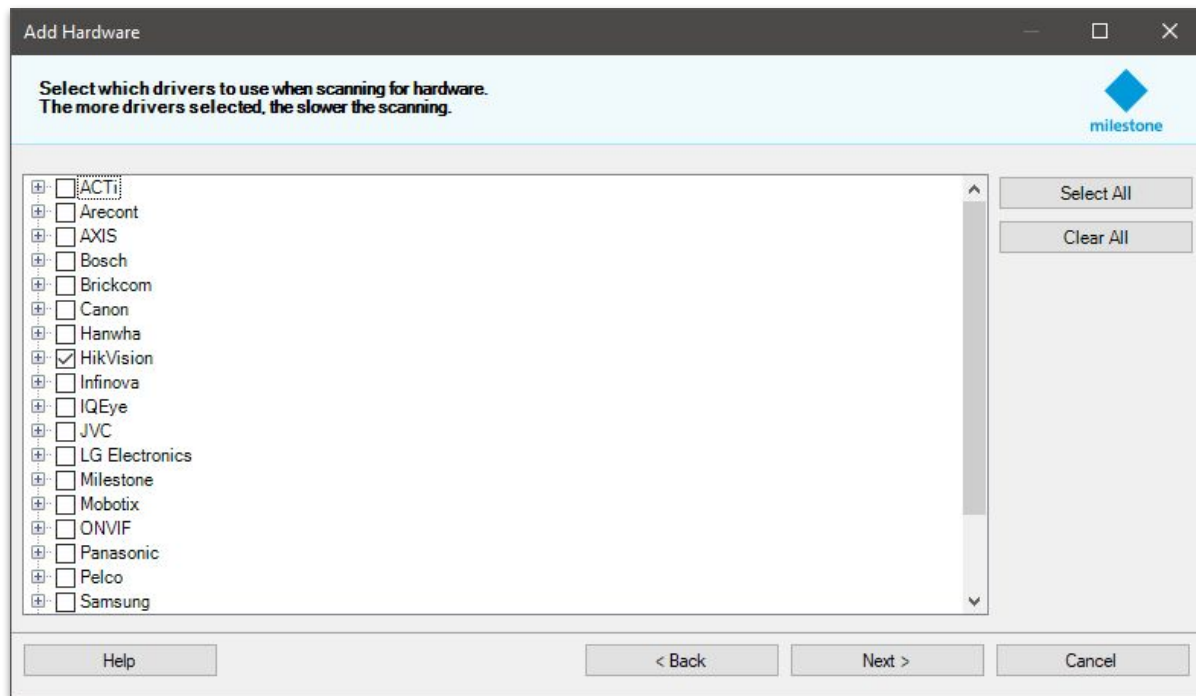
Add

Remove

Help < Back Next > Cancel

# CONFIGURATION- HARDWARE

Choose your camera type and click **Next**






# CONFIGURATION- HARDWARE



17

Wait until successful detection and click **Next** and then **Next**

Add Hardware

Enter the network address and port of the hardware you want to add.  
Optionally, select the hardware model to speed up detection.

  
milestone

	Address	Port	Use HTTPS	HTTPS port	Hardware model	
	192.168.11.40	80	<input type="checkbox"/>	443	(Auto-detect)	

Add

Remove

Help

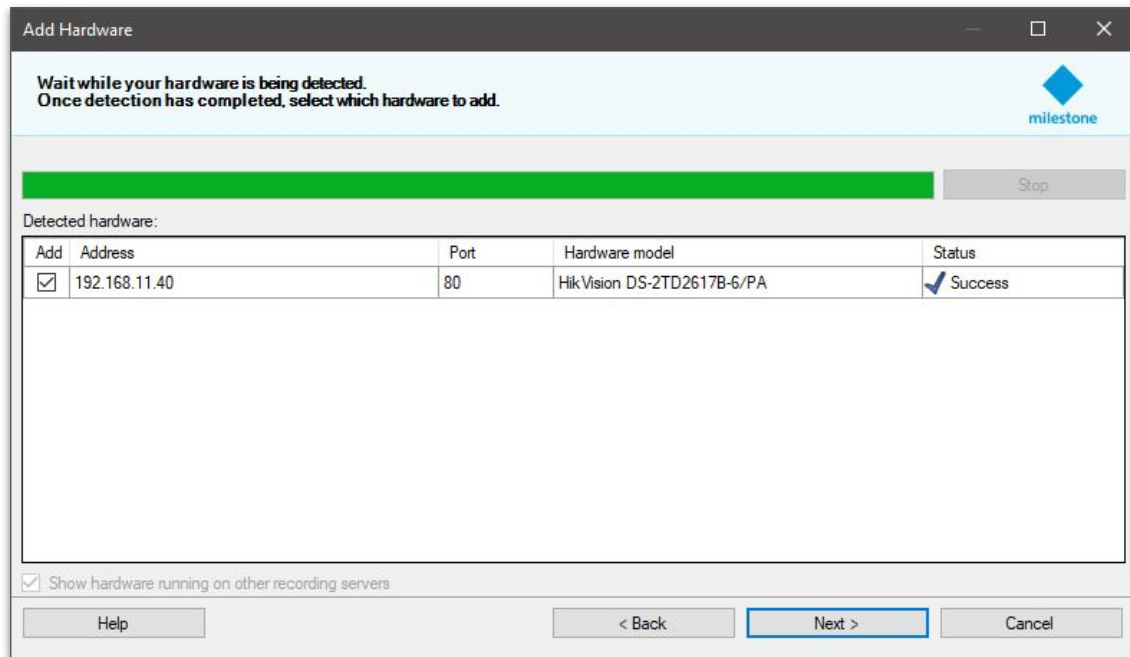
< Back

Next >

Cancel

# CONFIGURATION- HARDWARE

Enter **IP Address** and click **Next**



Add Hardware

Wait while your hardware is being detected.  
Once detection has completed, select which hardware to add.

milestone

Stop

Detected hardware:

Add	Address	Port	Hardware model	Status
<input checked="" type="checkbox"/>	192.168.11.40	80	HikVision DS-2TD2617B-6/PA	✓ Success

☒ Show hardware running on other recording servers

Help < Back Next > Cancel


**Note:** If detection failed please check your camera http port. The default http ports for ONVIF cameras are usually 8080 or 8000.

# CONFIGURATION- HARDWARE

Enable the cameras you want to use in the next step:

Add Hardware

Hardware and cameras are enabled per default. Manually enable additional devices to be used.  
The hardware and its devices will be assigned auto-generated names. Alternatively, enter names manually.



Hardware name template:  
Default

Device name template:  
Default

☒ Hardware

☒ Camera








☐ Microphone

☐ Speaker

☐ Metadata

☐ Input

☐ Output

Hardware to Add	Enabled	Name
Hik Vision DS-2TD2617B-6/PA - 192.168.11.40	<input type="checkbox"/>	
 Hardware:	<input checked="" type="checkbox"/>	Hik Vision DS-2TD2617B-6/PA (192.168.11.40)
 Camera port 1:	<input checked="" type="checkbox"/>	Hik Vision DS-2TD2617B-6/PA (192.168.11.40) - Camera 1
 Camera port 2:	<input checked="" type="checkbox"/>	Hik Vision DS-2TD2617B-6/PA (192.168.11.40) - Camera 2
 Microphone port 1:	<input type="checkbox"/>	Hik Vision DS-2TD2617B-6/PA (192.168.11.40) - Microphone 1
 Speaker port 1:	<input type="checkbox"/>	Hik Vision DS-2TD2617B-6/PA (192.168.11.40) - Speaker 1
 Metadata port 1:	<input type="checkbox"/>	Hik Vision DS-2TD2617B-6/PA (192.168.11.40) - Metadata 1
 Input port 1:	<input type="checkbox"/>	Hik Vision DS-2TD2617B-6/PA (192.168.11.40) - Input 1

Help

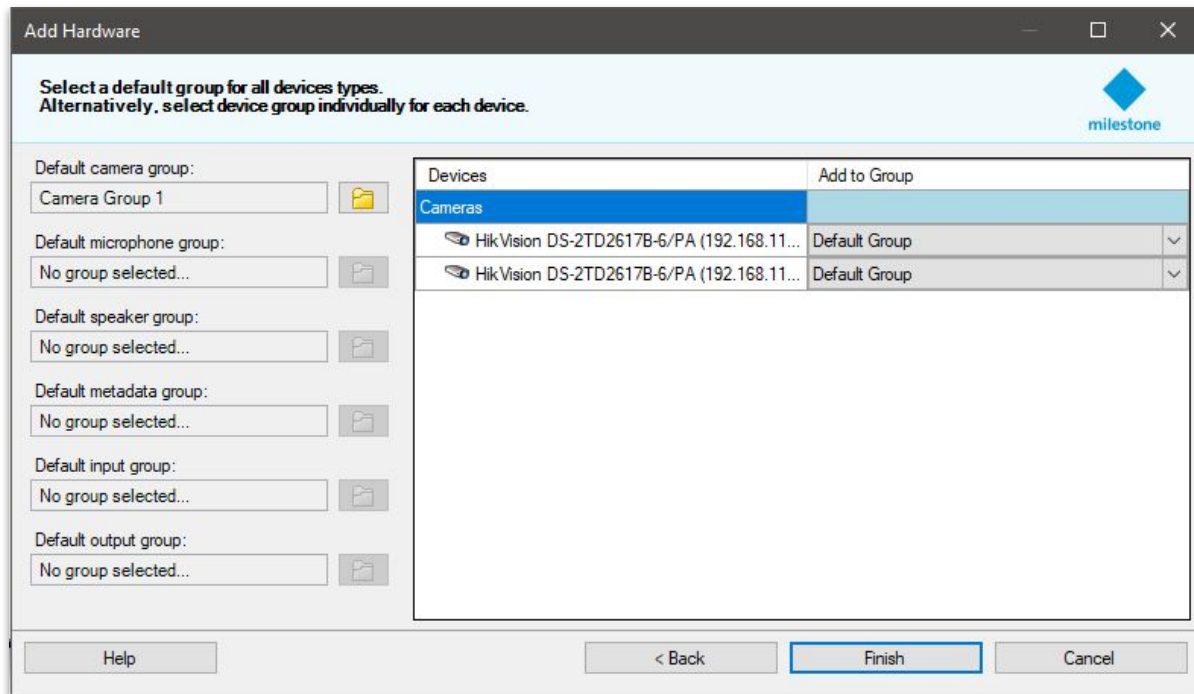
< Back

Next >

Cancel

# CONFIGURATION- HARDWARE

Ensure that camera ports are checked and click **Next**



**Add Hardware**

Select a default group for all devices types.  
Alternatively, select device group individually for each device.

Default camera group:  
Camera Group 1

Default microphone group:  
No group selected...

Default speaker group:  
No group selected...

Default metadata group:  
No group selected...

Default input group:  
No group selected...

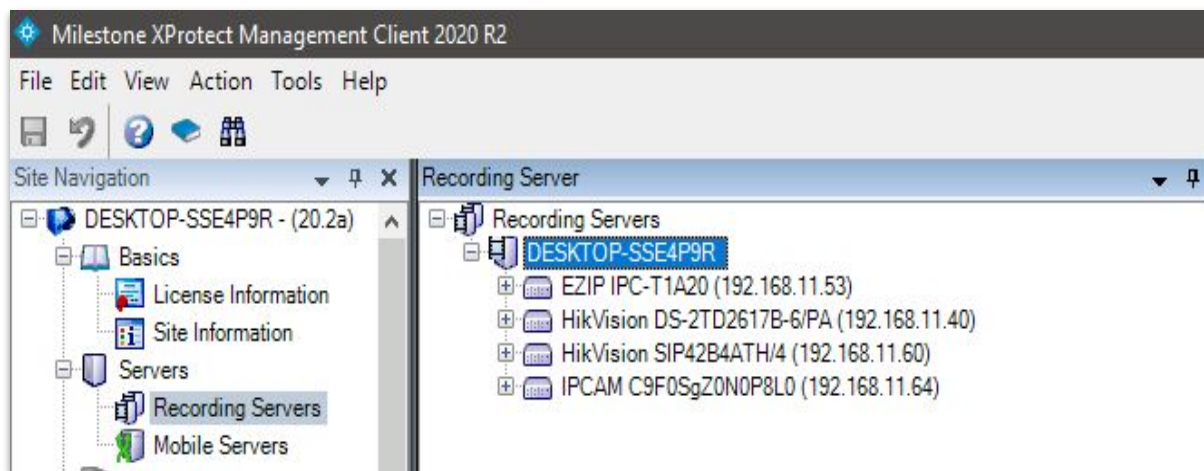
Default output group:  
No group selected...

Devices	Add to Group
<b>Cameras</b>	
HikVision DS-2TD2617B-6/PA (192.168.11...	Default Group
HikVision DS-2TD2617B-6/PA (192.168.11...	Default Group

Help < Back **Finish** Cancel

## CONFIGURATION- HARDWARE

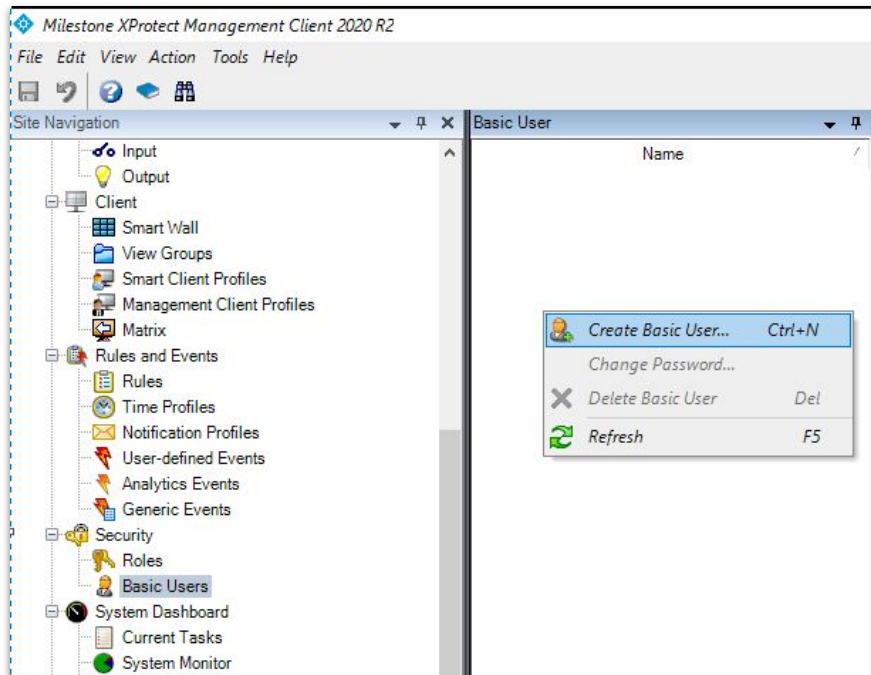
Click **Finish** to complete hardware configuration. New camera will appear in the list.



# CONFIGURATION- Onvif Bridge

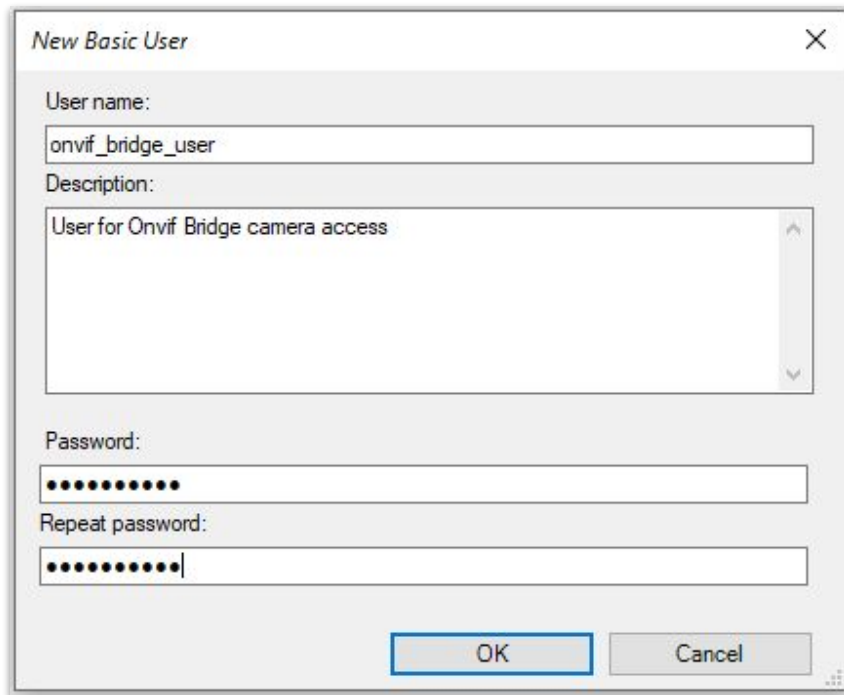
After Onvif Bridge installation a **Basic User** needs to be created:

- Click on Site Navigation -> Security -> Basic Users
- On the right side panel **right click** on empty space and chose **Create Basic User** in the context window or use **Ctrl+N** shortcut.



## CONFIGURATION- Onvif Bridge

- In the opened window enter the user name and password, and click **OK**.



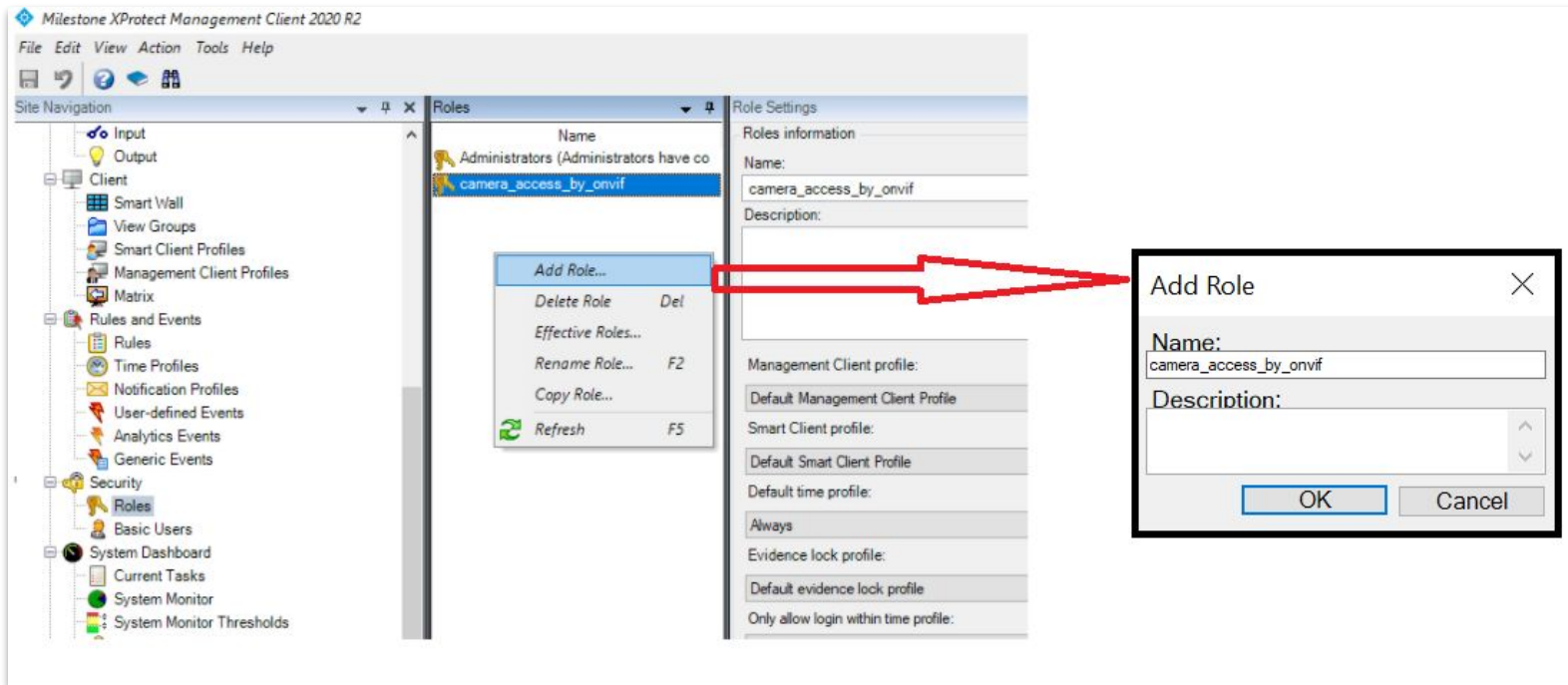
The image shows a 'New Basic User' dialog box with the following fields and controls:

- User name:** A text box containing 'onvif\_bridge\_user'.
- Description:** A text box containing 'User for Onvif Bridge camera access'.
- Password:** A text box with masked characters (dots).
- Repeat password:** A text box with masked characters (dots) and a cursor at the end.
- Buttons:** 'OK' and 'Cancel' buttons at the bottom right.

# CONFIGURATION- Onvif Bridge

Add a new role in Site Navigation -> Security -> Roles (the role gives access to specific cameras by Onvif Bridge).

- Right-click on the empty space and click **Add Role**. Then set the **Name** and press OK.

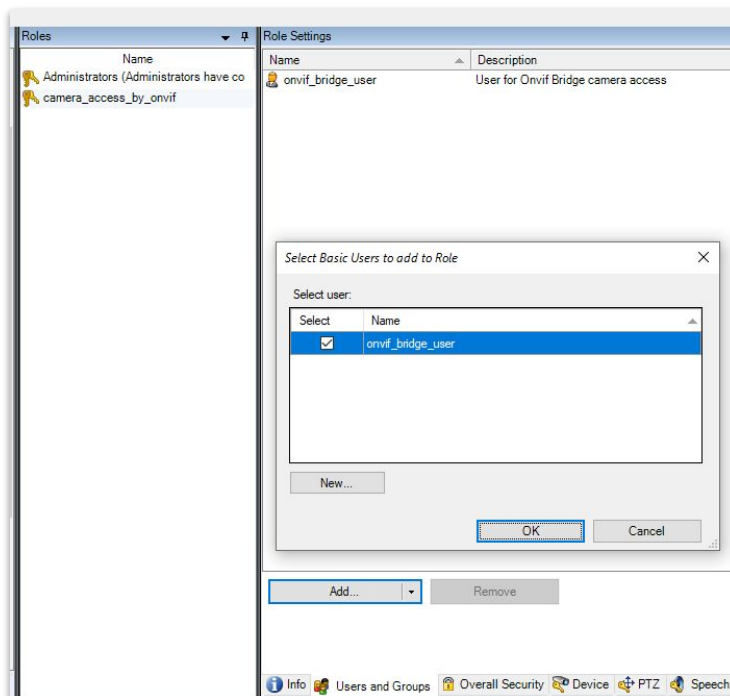




# CONFIGURATION- Onvif Bridge

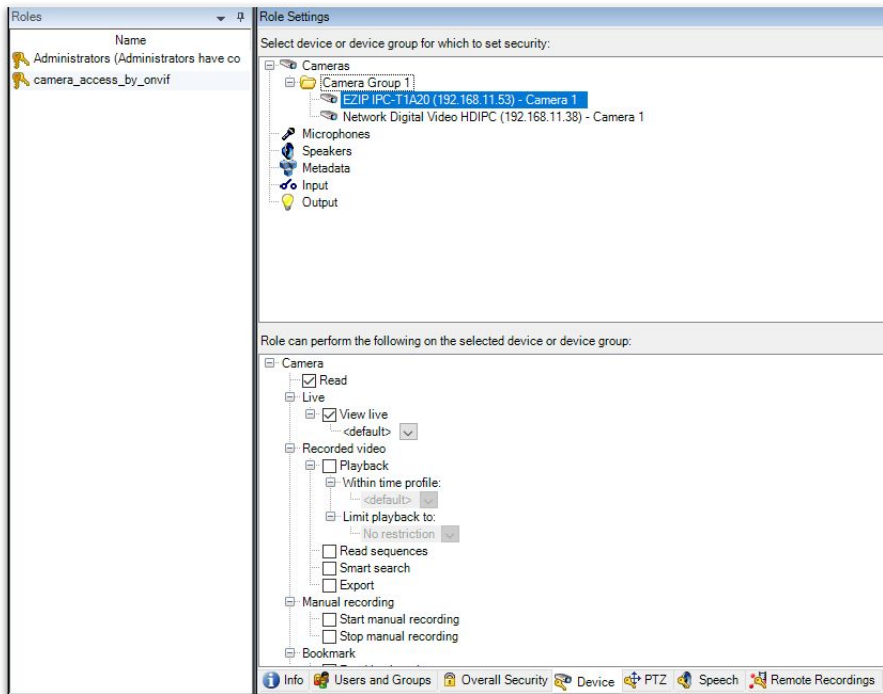
25

- In **Role Settings** -> **Users and Groups** tab **Add** -> **Basic User**, select the newly created user and press **OK**.



# CONFIGURATION- Onvif Bridge

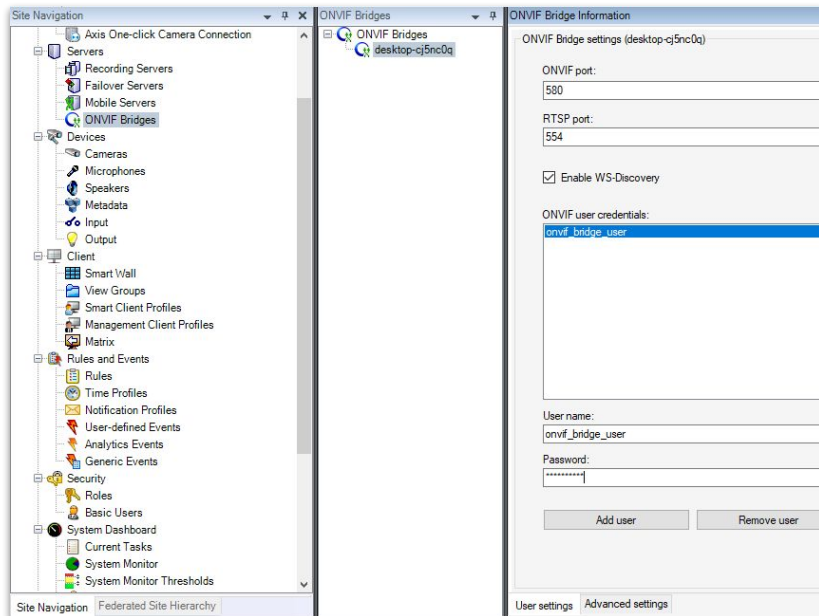
- In the **Role Settings** -> **Device** tab select the camera you want to get access through Onvif Bridge, select **Read** and **View live**.



# CONFIGURATION- Onvif Bridge

- Then navigate to the **Site Navigation -> Servers -> ONVIF Bridges**, select your desktop server and in **User settings** tab insert the created **User name** and **Password**, then press on **Add user**.

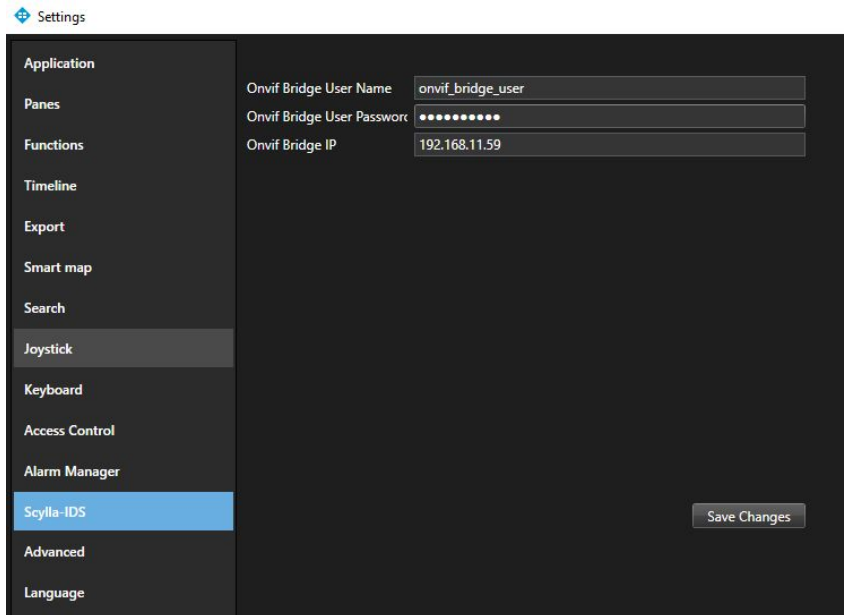
Now Onvif Bridge is configured and you can check if RTSP stream is available right in the Smart Client by opening the plugins tab or by using Onvif Device Manager.



## CONFIGURATION- PLUGIN - Scylla IDS settings

Before starting to use the plugin you have to go to XProtect Smart Client Settings, then click on Scylla IDS and type the Onvif Bridge configurations

- Onvif Bridge User Name - the name of XProtect basic user
- Onvif Bridge User Password - the password of XProtect basic user
- Onvif Bridge IP - IP address of the host for XProtect Server



The screenshot shows the 'Settings' window of the XProtect Smart Client. On the left is a sidebar menu with various settings categories. The 'Scylla-IDS' category is highlighted in blue. The main area on the right is titled 'Application' and contains three configuration fields for the Onvif Bridge:

Field	Value
Onvif Bridge User Name	onvif_bridge_user
Onvif Bridge User Password	••••••••
Onvif Bridge IP	192.168.11.59

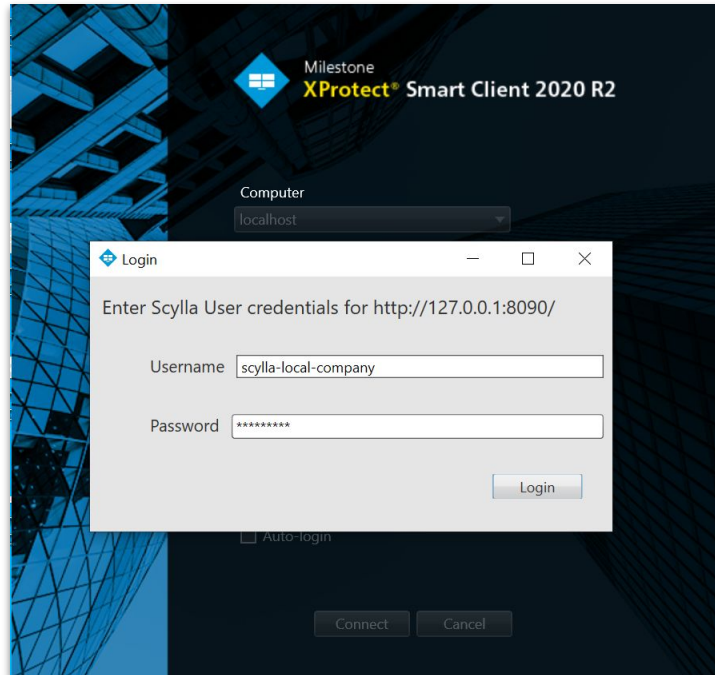
At the bottom right of the main area is a 'Save Changes' button.

## CONFIGURATION- PLUGIN - Scylla Web Service User Credentials

Currently for plugin function it needs to be signed in as Scylla User and Scylla Admin in Scylla Web Service.

At the start of Xprotect Smart Client user will be asked to provide user credentials (for each service (OCS, IDS) if they are located at different hosts).

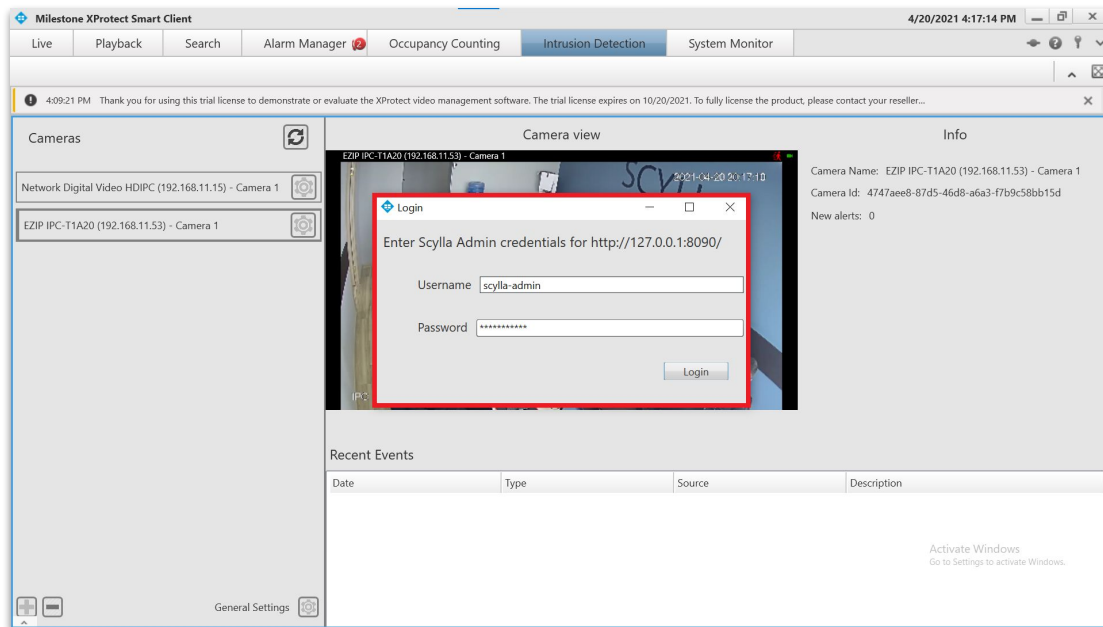
The **Username** and **Password** will be provided by Scylla support department after successful installation of Scylla Web Service



## CONFIGURATION- PLUGIN - Scylla Web Service Administrator Credentials

The installed plugin will create new tabs in XProtect Smart Client - **Occupancy Counting** and/or **Intrusion Detection**. These tabs are created to prepare and set configurations for Scylla Web Service, as well as to see and manage notifications.

After Xprotect Smart Client initialization, any time user selects Occupancy Counting or Intrusion Detection tab the plugin asks for Scylla Web Service Administrator username and password. Please fill the **Username** and **Password** with correct admin credentials provided by Scylla support department.



## CONFIGURATION- PLUGIN - Occupancy Counting Tab

All available cameras will be listed at the left side of Occupancy Counting tab to enable possibility to configure each camera separately.

Red box around the camera indicates that the RTSP stream is not available (for details see Troubleshooting part of this manual).

By clicking on the upper **refresh** button user can force to re-check if RTSP streams are available for all the listed cameras.

**Cameras**

- Network Digital Video HDIPC (192.168.11.38) - Camera 1
- EZIP IPC-T1A20 (192.168.11.53) - Camera 1

**Camera view**

2021-03-29 16:42:21

**Info**

Camera Name: EZIP IPC-T1A20 (192.168.11.53) - Camera 1  
 Camera Id: f036c519-f6b7-45ab-95d3-1cb039d0df96  
 Alarming threshold: 8  
 New alerts: 0

☐ HeatMap

**Recent Events**

Date	Type	Source	Description
3/26/2021 3:02:05 PM	Soylla OCS event	EZIP IPC-T1A20 (192.168.11.53) - Camera 1	Warning threshold reached, count: 10
3/26/2021 3:01:55 PM	Soylla OCS event	EZIP IPC-T1A20 (192.168.11.53) - Camera 1	Warning threshold reached, count: 9
3/26/2021 3:01:45 PM	Soylla OCS event	EZIP IPC-T1A20 (192.168.11.53) - Camera 1	Warning threshold reached, count: 8
3/26/2021 3:01:35 PM	Soylla OCS event	EZIP IPC-T1A20 (192.168.11.53) - Camera 1	Warning threshold reached, count: 7
3/26/2021 3:01:25 PM	Soylla OCS event	EZIP IPC-T1A20 (192.168.11.53) - Camera 1	Warning threshold reached, count: 6
3/26/2021 3:01:15 PM	Soylla OCS event	EZIP IPC-T1A20 (192.168.11.53) - Camera 1	Warning threshold reached, count: 5
3/26/2021 3:01:05 PM	Soylla OCS event	EZIP IPC-T1A20 (192.168.11.53) - Camera 1	Warning threshold reached, count: 4

General Settings

## CONFIGURATION- PLUGIN - Occupancy Counting Tab

To configure the camera for occupancy counting:

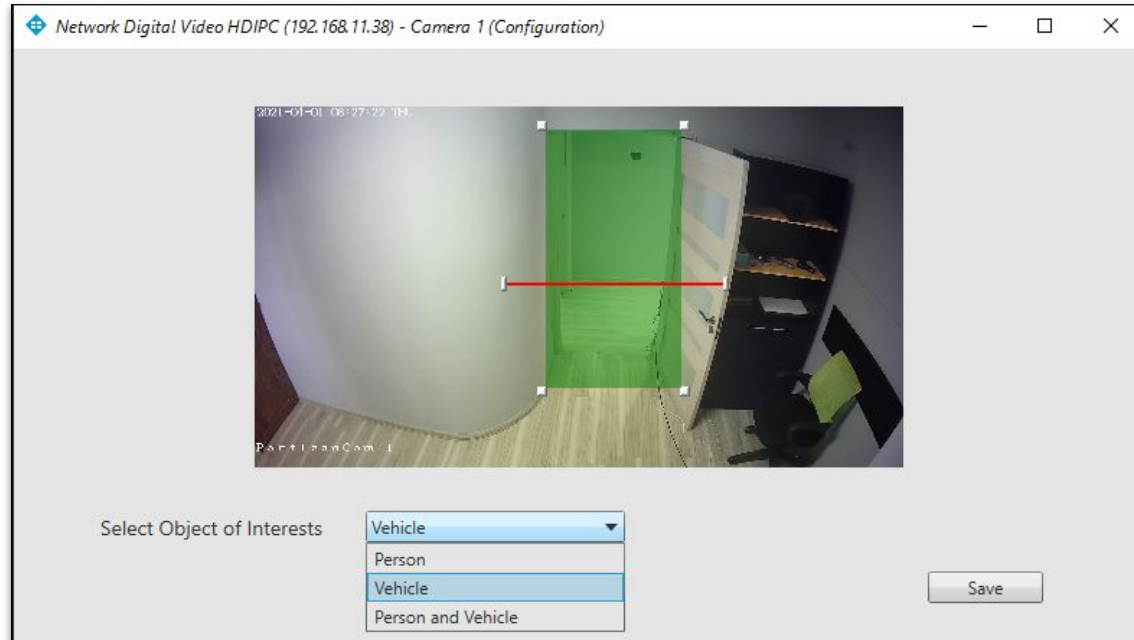
Select the region where people will be passing (green area)

Select the line passing which +1 or -1 will be counted.

Select the objects that will be counted as human, vehicle or both.

Press Save to store the configuration.

*Note that increment or decrement is registered only when the object (person/vehicle) left the view of camera for more than 3 seconds.*



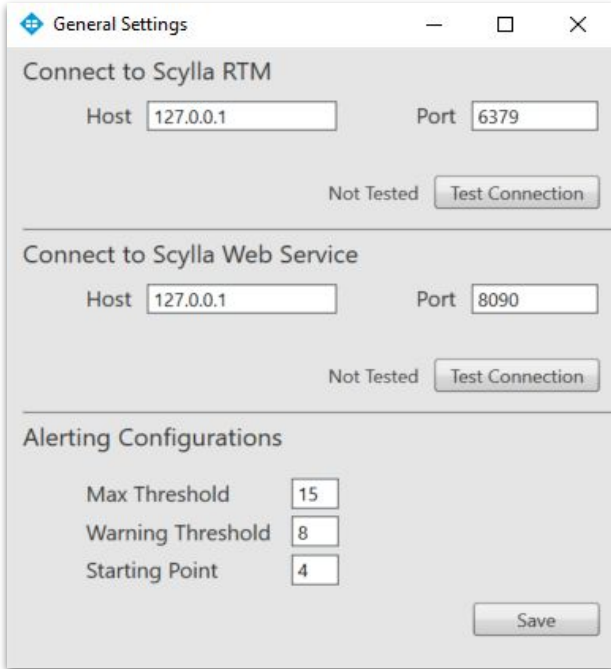


## CONFIGURATION- PLUGIN

In general settings the IPs to **Scylla RTM** (Redis server host) and **Scylla Web Service** (Backend socket) with their corresponding port numbers need to be set. Both will be provided by Scylla Support department.

Set here also:

- **Maximum threshold** value - to get a “red” alert indicating that the maximum allowed number of person/car is reached.
- **Warning threshold** value to get warning notifications when it is reached.
- Set **Starting point** - the number of objects already located inside the monitoring area at the time of initialization.



The screenshot shows a 'General Settings' window with three main sections. The first section, 'Connect to Scylla RTM', has 'Host' set to '127.0.0.1' and 'Port' set to '6379'. Below these fields are the labels 'Not Tested' and a 'Test Connection' button. The second section, 'Connect to Scylla Web Service', has 'Host' set to '127.0.0.1' and 'Port' set to '8090', also with 'Not Tested' and a 'Test Connection' button. The third section, 'Alerting Configurations', contains three input fields: 'Max Threshold' with the value '15', 'Warning Threshold' with the value '8', and 'Starting Point' with the value '4'. A 'Save' button is located at the bottom right of the window.

Section	Field	Value
Connect to Scylla RTM	Host	127.0.0.1
	Port	6379
Connect to Scylla Web Service	Host	127.0.0.1
	Port	8090
Alerting Configurations	Max Threshold	15
	Warning Threshold	8
	Starting Point	4

# CONFIGURATION- PLUGIN - Intrusion Detection Tab

34

In the Intrusion Detection tab the list of alerts is shown. Double click on any one to open the alarm info window with the frame and the alarm info.

**Milestone XProtect Smart Client**

Live | Playback | Search | Alarm Manager | **Intrusion Detection** | System Monitor

1:44:21 PM Thank you for using this trial license to demonstrate or evaluate the XProtect video management software. The trial license expires on 10/20/2021. To fully license the product, please contact your reseller or find one on [www.milestonesys.com](http://www.milestonesys.com).

**Cameras**

- Network Digital Video HDIPC (192.168.11.15) - Camera 1
- EZIP IPC-T1A20 (192.168.11.53) - Camera 1

**Camera view**

Network Digital Video HDIPC (192.168.11.15) - Camera 1

2021-04-24 05:25:58 S/L

**Info**

Camera Name: Network Digital Video HDIPC (192.168.11.15) - Camera 1  
Camera Id: 155888f6-8d04-4384-881a-28d59a84a297  
New alerts: 11

**person detected**

**Frame**

2021-04-24 05:25:58 S/L

**Alarm Info**

Date: 4/21/2021 1:49:09 PM  
Type: Scylla IDS event  
Source: Network Digital Video HDIPC (192.168.11.15) - Camera 1  
Description: person detected

**Recent Events**

Date	Type	Source	Description
4/21/2021 1:49:11 PM	Scylla IDS event	Network Digital Video HDIPC (192.1	person detected
4/21/2021 1:49:09 PM	Scylla IDS event	Network Digital Video HDIPC (192.1	person detected
4/21/2021 1:49:09 PM	Scylla IDS event	Network Digital Video HDIPC (192.1	person detected
4/21/2021 1:49:07 PM	Scylla IDS event	Network Digital Video HDIPC (192.1	person detected
4/21/2021 1:48:50 PM	Scylla IDS event	Network Digital Video HDIPC (192.1	person detected
4/21/2021 1:48:07 PM	Scylla IDS event	Network Digital Video HDIPC (192.1	person detected
4/21/2021 1:47:17 PM	Scylla IDS event	Network Digital Video HDIPC (192.1	person detected
4/21/2021 1:47:15 PM	Scylla IDS event	Network Digital Video HDIPC (192.1	person detected
4/21/2021 1:46:48 PM	Scylla IDS event	Network Digital Video HDIPC (192.1	person detected
4/21/2021 1:46:47 PM	Scylla IDS event	Network Digital Video HDIPC (192.1	person detected
4/21/2021 1:46:44 PM	Scylla IDS event	Network Digital Video HDIPC (192.1	person detected
4/15/2021 1:52:53 PM	Scylla IDS event	Network Digital Video HDIPC (192.1	person detected

General Settings

# CONFIGURATION- PLUGIN - Alarm Manager Tab

More detailed information about the alarms can be found in the Alarm Manager tab. If the recording is enabled, each alert is accompanied by a short video of the detection.

The screenshot displays the Milestone XProtect Smart Client interface, specifically the Alarm Manager tab. The top navigation bar includes options like Live, Playback, Search, Alarm Manager (selected), Occupancy Counting, Intrusion Detection, and System Monitor. The main area is divided into two sections: a left pane showing a map (currently empty) and a right pane displaying video recordings. The video recordings show a room with people, with red bounding boxes and labels identifying detected objects (e.g., person 49%, person 54%, person 54%, person 54%).

Below the video recordings, a table lists the detected alarms. The table has columns for Time, Priority Level, State Level, State Name, Message, Source, Owner, and ID. The table shows a series of alarms detected by EZIP IPC-T1A20 (192.168.11.53) - Camera 1, all with a priority level of 1 and a state level of 1. The messages indicate detected object type person with varying probabilities.

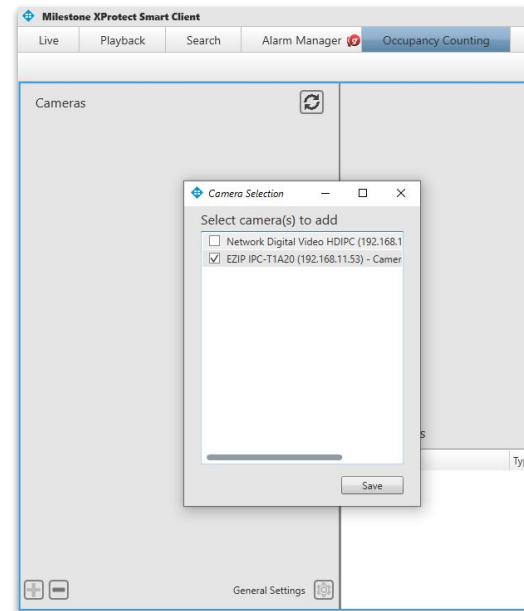
Time	Priority Level	State Level	State Name	Message	Source	Owner	ID
1:45:19 PM 4/21/2021	1	1	New	Detected object type person, probability 0.306335	EZIP IPC-T1A20 (192.168.11.53) - Camera 1		1959
1:45:20 PM 4/21/2021	1	1	New	Detected object type person, probability 0.826219	EZIP IPC-T1A20 (192.168.11.53) - Camera 1		1960
1:45:20 PM 4/21/2021	1	1	New	Detected object type person, probability 0.448888	EZIP IPC-T1A20 (192.168.11.53) - Camera 1		1961
1:45:20 PM 4/21/2021	1	1	New	Detected object type person, probability 0.302347	EZIP IPC-T1A20 (192.168.11.53) - Camera 1		1962
1:45:20 PM 4/21/2021	1	1	New	Detected object type person, probability 0.553908	EZIP IPC-T1A20 (192.168.11.53) - Camera 1		1963
1:45:20 PM 4/21/2021	1	1	New	Detected object type person, probability 0.399111	EZIP IPC-T1A20 (192.168.11.53) - Camera 1		1964
1:45:21 PM 4/21/2021	1	1	New	Detected object type person, probability 0.351489	EZIP IPC-T1A20 (192.168.11.53) - Camera 1		1965
1:45:21 PM 4/21/2021	1	1	New	Detected object type person, probability 0.401744	EZIP IPC-T1A20 (192.168.11.53) - Camera 1		1966
1:45:21 PM 4/21/2021	1	1	New	Detected object type person, probability 0.340612	EZIP IPC-T1A20 (192.168.11.53) - Camera 1		1967
1:45:21 PM 4/21/2021	1	1	New	Detected object type person, probability 0.331348	EZIP IPC-T1A20 (192.168.11.53) - Camera 1		1968
1:45:21 PM 4/21/2021	1	1	New	Detected object type person, probability 0.529121	EZIP IPC-T1A20 (192.168.11.53) - Camera 1		1969
1:45:22 PM 4/21/2021	1	1	New	Detected object type person, probability 0.843236	EZIP IPC-T1A20 (192.168.11.53) - Camera 1		1970
1:45:22 PM 4/21/2021	1	1	New	Detected object type person, probability 0.495083	EZIP IPC-T1A20 (192.168.11.53) - Camera 1		1971
1:45:22 PM 4/21/2021	1	1	New	Detected object type person, probability 0.541248	EZIP IPC-T1A20 (192.168.11.53) - Camera 1		1972
1:45:22 PM 4/21/2021	1	1	New	Detected object type person, probability 0.319144	EZIP IPC-T1A20 (192.168.11.53) - Camera 1		1973
1:45:22 PM 4/21/2021	1	1	New	Detected object type person, probability 0.515289	EZIP IPC-T1A20 (192.168.11.53) - Camera 1		1974
1:45:23 PM 4/21/2021	1	1	New	Detected object type person, probability 0.84594	EZIP IPC-T1A20 (192.168.11.53) - Camera 1		1975
1:45:23 PM 4/21/2021	1	1	New	Detected object type person, probability 0.482216	EZIP IPC-T1A20 (192.168.11.53) - Camera 1		1976
1:45:23 PM 4/21/2021	1	1	New	Detected object type person, probability 0.463143	EZIP IPC-T1A20 (192.168.11.53) - Camera 1		1977

# CONFIGURATION- PLUGIN

“+” and “-” buttons in the bottom left corner of the screen provide functionality to activate and deactivate available cameras.

Similar functionality is available in the **Intrusion Detection** tab. The only difference is in **camera settings** section where for Intrusion detection only the region of interest can be selected but not the line of crossing.

As soon as you have saved general settings parameters, the plugin will connect to the remote server and start video processing on the Scylla backend engine. The plugin will convert notifications coming from backend to the alarm format appropriate for Milestone XProtect and show it to the end user on the Occupancy Counting tab or Intrusion Detection tab as well in XProtect Alarm Management tab.



1. If camera preview is not available after configuration, check hardware authentication settings:
  - Right click on hardware
  - Click on Edit Hardware
  - Verify/set **Username** and **Password**
2. If XProtect Smart Client is already running during configuration you should restart it for the changes to take effect, otherwise motion detection will not be operational.
3. If RTSP stream is not available, check if access permissions are correct (**XProtect Management Client** -> **Site Navigation** -> **Security** -> **Role** -> **Roles** -> **Onvif Bridge Role** -> **Role Settings** -> **Device** -> **Cameras** (for details see page 26).



## CONCLUSION

If you find an issue or have questions you want to ask,  
please contact us on the following email [support@scylla.ai](mailto:support@scylla.ai),  
Or call us on +1 747 231 1868. Our team is ready to help you.