

# Milestone XProtect VMS Integration Guide



Milestone XProtect VMS Integration Guide	3
Preparing XProtect VMS	3
1) Milestone Open Network Bridge must be installed within the Milestone XProtect VMS.	3
2) Create a user for Icetana AI connection. The user type must be a 'Basic' user.	4
3) Create a new Role and assign required permissions.	5
4) Add Icetana AI Basic user to the Milestone Open Network Bridge.	7
5) (Optional but highly recommended) Configure a second stream for Icetana AI.	9
6) Propagating Icetana AI events as Alarms into Milestone Alarm Manager	10
Icetana AI Configuration	12
1) Configure Icetana VMS Bridge if previously not configured.	12
2) Create VMS object for Milestone XProtect VMS	15
Populating Cameras into Icetana AI	17

# Milestone XProtect VMS

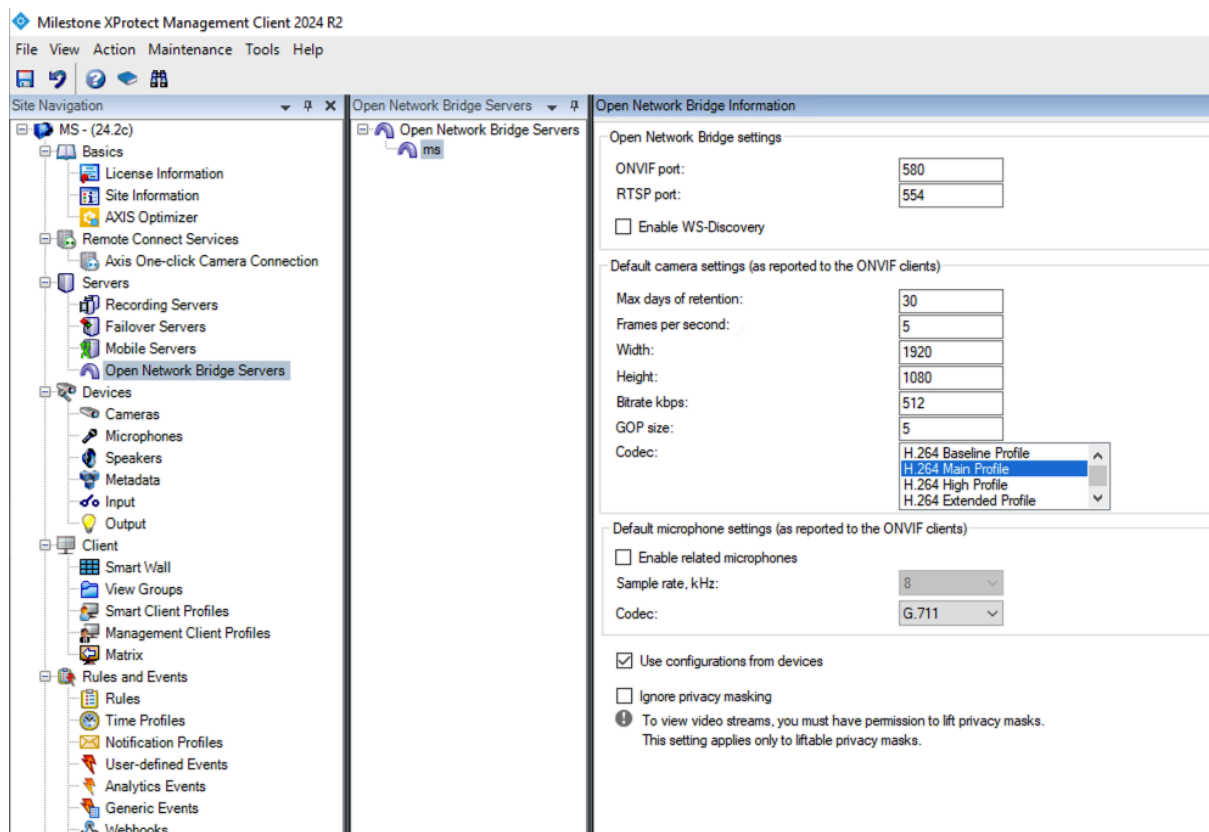
## Integration Guide

This document aims to show and guide the steps for integrating Icetana AI with Milestone XProtect VMS.

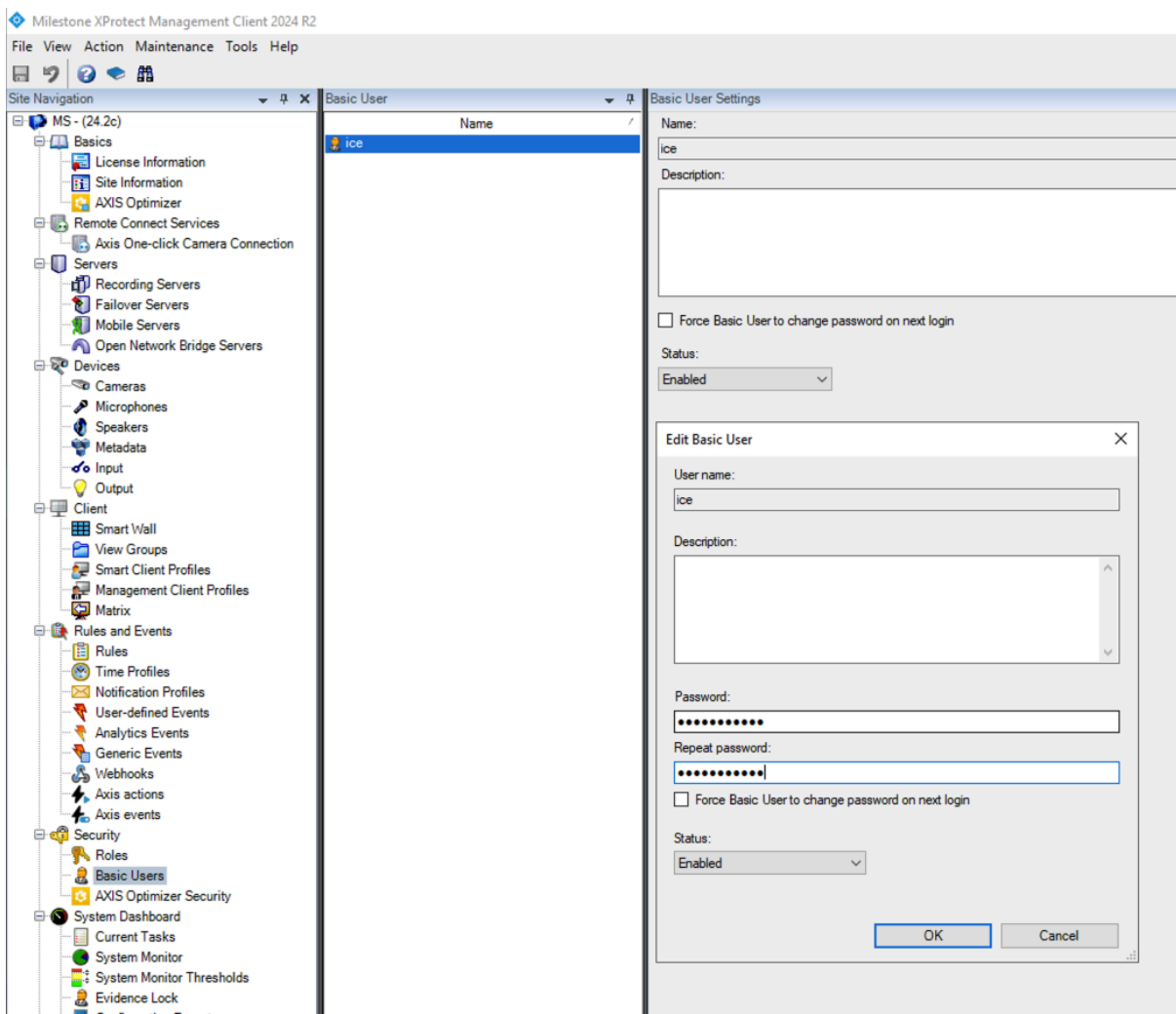
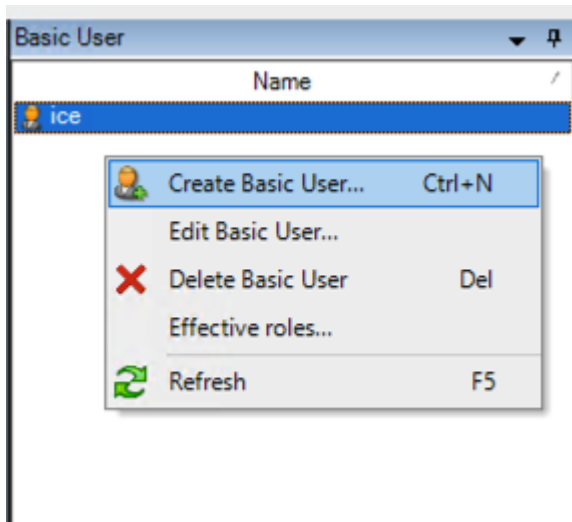
### Preparing XProtect VMS

Certain steps should be performed on XProtect VMS in preparation for Icetana AI connection. Below you will find required steps.

- 1) Milestone Open Network Bridge must be installed within the Milestone XProtect VMS.



- 2) Create a user for Icetana AI connection. The user type must be a 'Basic' user.



### 3) Create a new Role and assign required permissions.

*Note: If the Icetana AI user is assigned to the Administrators group, there is no need to create a new group. This is applicable only if the Icetana AI system has one server.*

- If multiple Icetana AI servers are part of the same instance, each server must have its own dedicated Basic user and Role created. For each Role permissions must be set to access certain cameras to distribute the load. Please refer to the project HW BoM calculation.

Milestone XProtect Management Client 2024 R2

File View Action Maintenance Tools Help

Site Navigation

- MS - (24.2c)
  - Basics
    - License Information
    - Site Information
    - AXIS Optimizer
  - Remote Connect Services
    - Axis One-click Camera Connection
  - Servers
    - Recording Servers
    - Failover Servers
    - Mobile Servers
    - Open Network Bridge Servers
  - Devices
    - Cameras
    - Microphones
    - Speakers
    - Metadata
    - Input
    - Output
  - Client
    - Smart Wall
    - View Groups
    - Smart Client Profiles
    - Management Client Profiles
    - Matrix
  - Rules and Events
    - Rules
    - Time Profiles
    - Notification Profiles
    - User-defined Events
    - Analytics Events
    - Generic Events
    - Webhooks
    - Axis actions
    - Axis events
  - Security
    - Roles
    - Basic Users
    - AXIS Optimizer Security
  - System Dashboard
    - Current Tasks
    - System Monitor
    - System Monitor Thresholds
    - Evidence Lock

Roles

Name
Administrators (Administrators have co
AxisOptimizer (Basic permission neede

Add Role...

Delete Role Del

Effective Roles...

Rename Role... F2

Copy Role...

Refresh F5

Role Settings

Roles information

Name:

Administrators

Description:

Administrators have complete and unrestricted access to the

Smart Client profile:

Default Smart Client Profile

Evidence lock profile:

Default evidence lock profile

☒ Allow Smart Client login

☒ Allow Mobile Client login

☒ Allow Web Client login

☐ Make users anonymous during PTZ sessions

File View Action Maintenance Tools Help

Site Navigation Roles Role Settings

MS - (24.2c)

- Basics
  - License Information
  - Site Information
  - AXIS Optimizer
- Remote Connect Services
  - Axis One-click Camera Connection
- Servers
  - Recording Servers
  - Failover Servers
  - Mobile Servers
  - Open Network Bridge Servers
- Devices
  - Cameras
  - Microphones
  - Speakers
  - Metadata
  - Input
  - Output
- Client
  - Smart Wall
  - View Groups
  - Smart Client Profiles
  - Management Client Profiles
  - Matrix
- Rules and Events
  - Rules
  - Time Profiles
  - Notification Profiles
  - User-defined Events
  - Analytics Events
  - Generic Events
  - Webhooks
  - Axis actions
  - Axis events
- Security
  - Roles
  - Basic Users
  - AXIS Optimizer Security
- System Dashboard
  - Current Tasks
  - System Monitor
  - System Monitor Thresholds
  - Evidence Lock
  - Configuration Reports
- Server Logs
- Metadata Use
- Metadata Search
- Access Control
- Incidents
  - Incident properties
- AXIS Optimizer

Roles

Name
Administrators (Administrators have co
AxisOptimizer (Basic permission neede
Icetana01

Role Settings

Name	Description
------	-------------

Select Basic Users to add to Role

Select user:

Select	Name
<input checked="" type="checkbox"/>	ice

New...

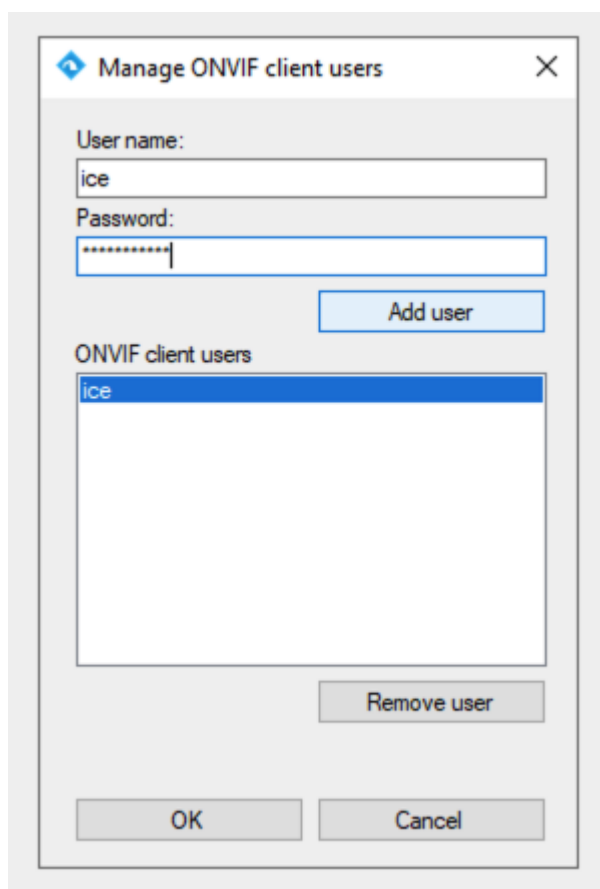
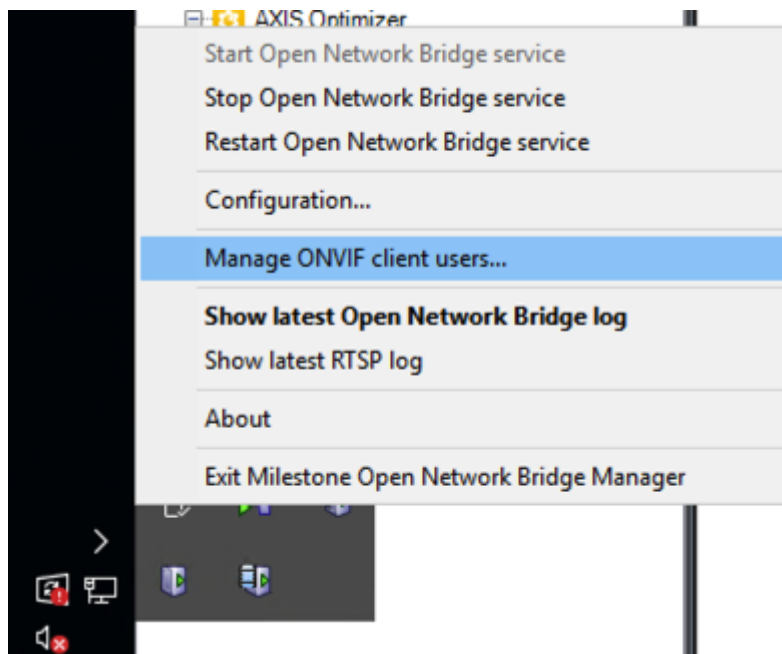
OK Cancel

Add... Remove

Info Users and Groups External IDP Overall Security Device PTZ Speech

#### 4) Add Icetana AI Basic user to the Milestone Open Network Bridge.

Access to the server hosting Milestone Open Network Bridge, right click to the Network Bridge icon in the Windows Tray, select the option 'Manage ONVIF client users', enter the exact same username and password for the Icetana AI Basic user created in the *Step 2*, follow with Add user and OK buttons.



Milestone XProtect Management Client 2024 R2

File View Action Maintenance Tools Help

Site Navigation Roles Role Settings

MS - (24.2c)

Basics

- License Information
- Site Information
- AXIS Optimizer

Remote Connect Services

- Axis One-click Camera Connection

Servers

- Recording Servers
- Fallover Servers
- Mobile Servers
- Open Network Bridge Servers

Devices

- Cameras
- Microphones
- Speakers
- Metadata
- Input
- Output

Client

- Smart Wall
- View Groups
- Smart Client Profiles
- Management Client Profiles
- Matrix

Rules and Events

- Rules
- Time Profiles
- Notification Profiles
- User-defined Events
- Analytics Events
- Generic Events
- Webhooks
- Axis actions
- Axis events

Security

- Roles
- Basic Users
- AXIS Optimizer Security

System Dashboard

- Current Tasks
- System Monitor
- System Monitor Thresholds
- Evidence Lock
- Configuration Reports
- Server Logs
- Metadata Use
- Metadata Search
- Access Control
- Incidents
- Incident properties
- AXIS Optimizer

Roles

Name
Administrators (Administrators have co
AxisOptimizer (Basic permission neede
Icetana01

Role Settings

Select device or device group for which to set security:

- Cameras
  - Camera Group 1
    - AXIS Q1798-LE Network Camera (192.168.70.137) - Camera 1
- Microphones
  - Microphone Group 1
- Speakers
- Metadata
- Input
- Output

Role can perform the following on the selected device or device group:

- Camera
  - ☒ Read
  - Live
    - ☒ View live
    - ☐ View restricted live
  - Recorded video
    - Playback
      - Within time profile: ☐ ☐ ☐
      - Limit playback to: ☐ ☐ ☐
    - Playback restricted recordings
    - Read sequences
    - Smart search
    - Export
  - Manual recording
    - Start manual recording
    - Stop manual recording
  - Bookmark
    - ☐ Read bookmarks
    - ☐ Edit bookmarks
    - ☒ Create bookmarks
    - ☐ Delete bookmarks
  - AUX commands
  - Evidence Lock
    - Create and extend evidence locks
    - Delete and reduce evidence locks
    - Read evidence locks
  - Playback restrictions
    - Create and extend live and playback restrictions

Site Navigation Federated Site Hierarchy

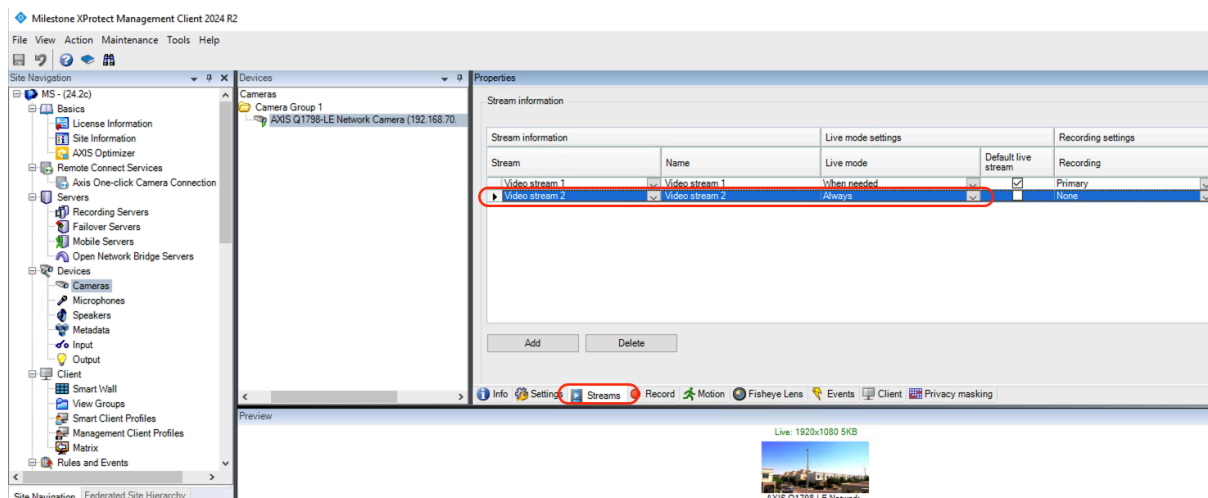
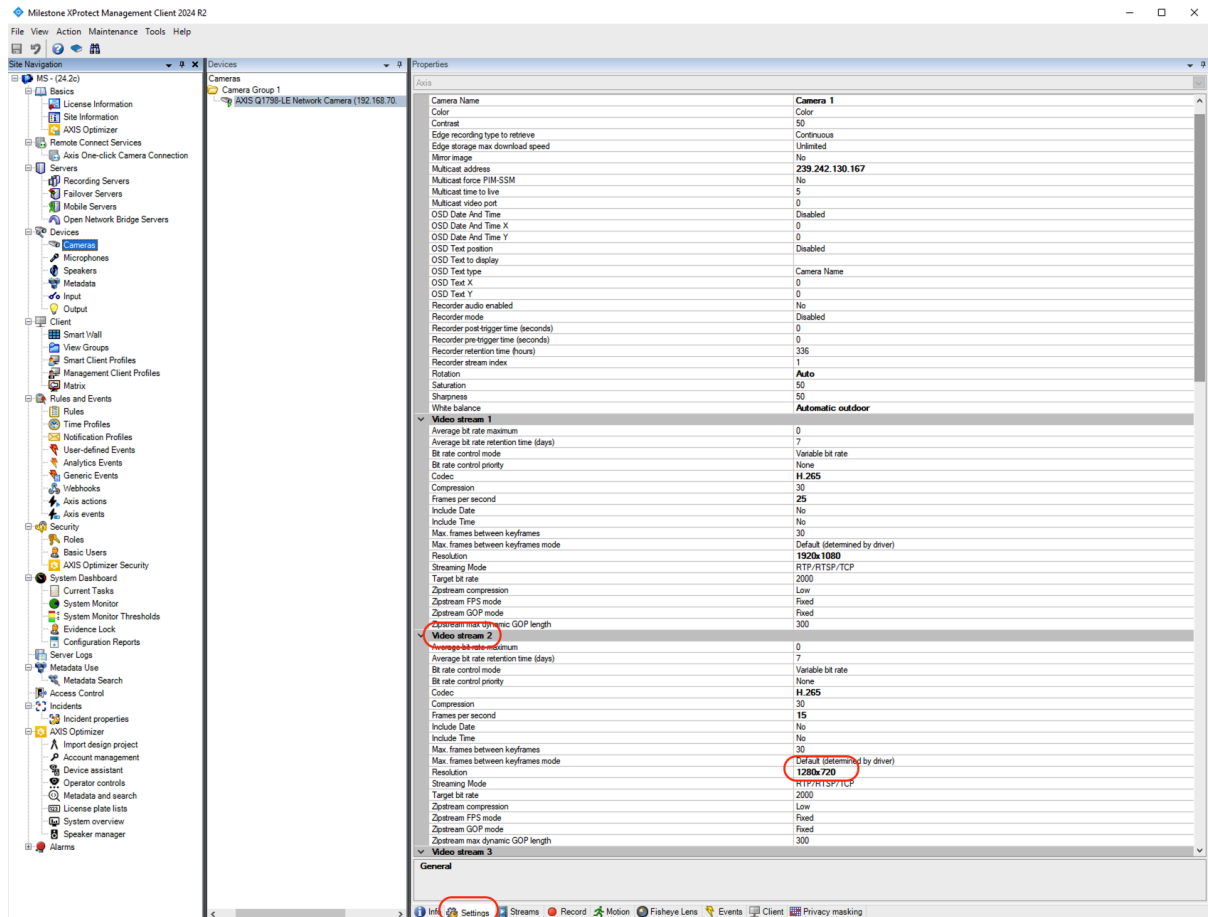
Info Users and Groups External IDP Overall Security Device PTZ Speech Remote



## 5) (Optional but highly recommended) Configure a second stream for Icetana AI.

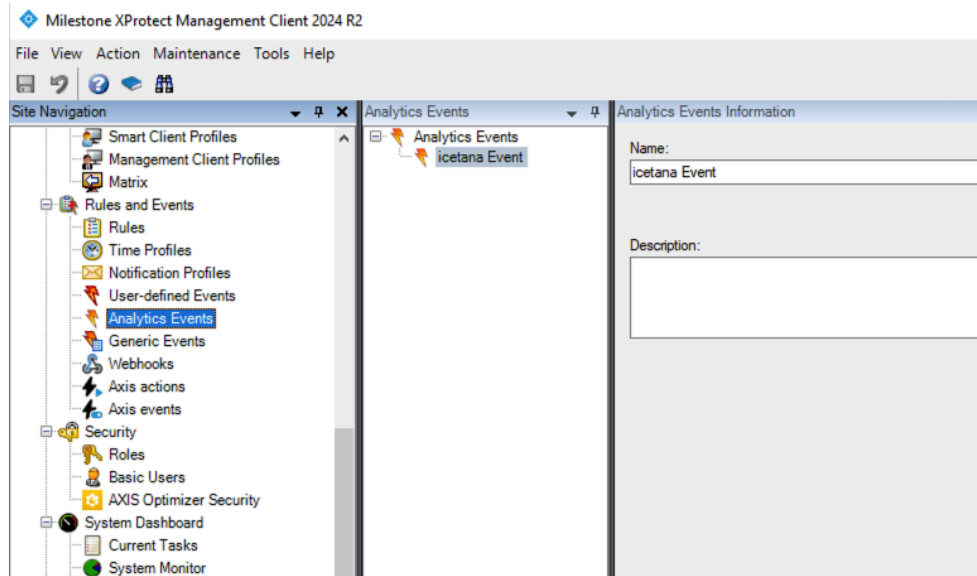
Icetana AI server(s) resources are utilised most efficiently when camera resolutions are set based on the intended application:

- Safety and Security product: 720P
- Facial Recognition product: 4MP
- Licence Plate Recognition product: 1080P

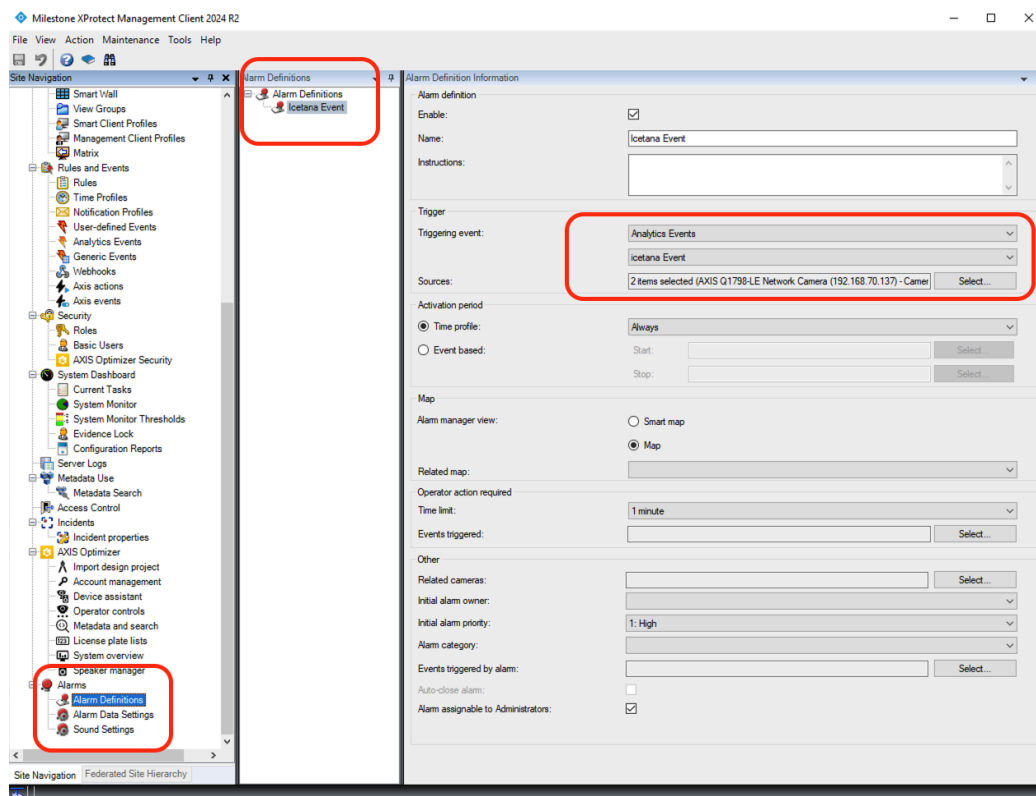


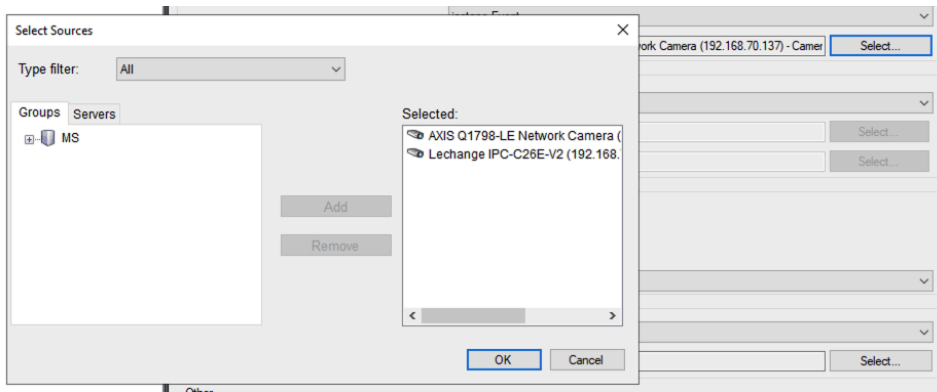
## 6) Propagating Icetana AI events as Alarms into Milestone Alarm Manager

- Create an Analytic Event from Milestone Management client. Name of the Analytic event must be in the following format: *icetana Event*

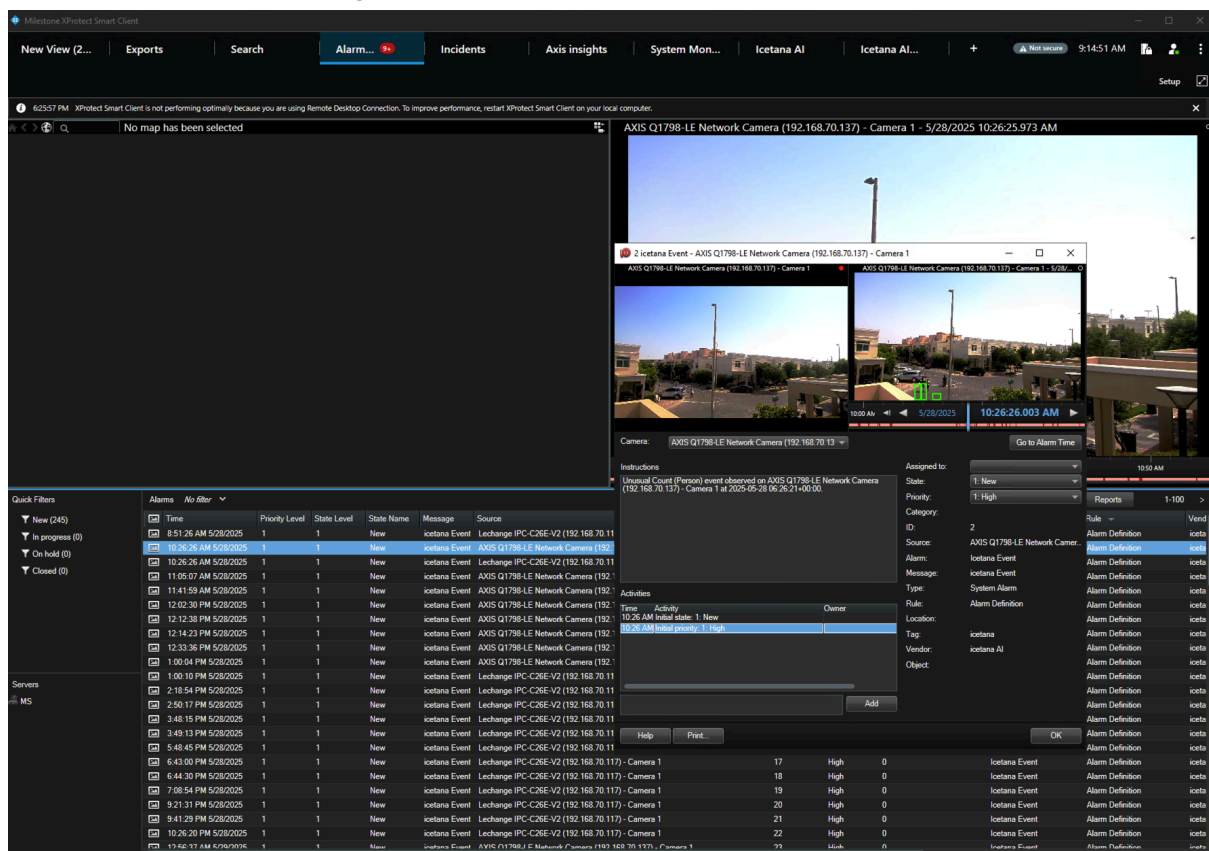


- Create an Alarm Definition linking Analytic Event to the Cameras





- Alarms will be triggered and displayed in the Milestone XProtect Smart Client, under Alarm Manager tab



# Icetana AI Configuration

## 1) Configure Icetana VMS Bridge if previously not configured.

- Navigate to <https://<icetanaServer>/admin> and log in using Icetana AI credentials
- Scroll down to the VMS section, select VMS Bridge Settings and go inside the VMS Bridge Object

CLIENTS

Clients + Add

Sites + Add

FEATURE

Feature Object Aggregations + Add

Feature Objects + Add

INCIDENT\_REPORTING

Categories + Add

Incident status + Add

Incidents + Add

MODEL

Models + Add

Training Jobs + Add

Venue Event Categories + Add

Venue Events + Add

SYSTEM\_SETTINGS

Settings + Add

VMS

VMS Bridge Settings

VMS Configurations + Add

Select VMS Bridge Settings to change

VMS BRIDGE SETTINGS

VMSBridgeSettings object (1)

1 VMS Bridge Settings

- Select the checkbox for Enable VMS Bridge Service
- Enter the Icetana Credentials in the Backend - Username and Password fields.
- Select the checkbox for 'Feature - Enable Milestone Event Trigger' to enable Icetana AI to create Bookmarks and Analytic Events in Milestone XProtect VMS

Home > Vms > VMS Bridge Settings > VMSBridgeSettings object (1)

CLIENTS

Clients [+ Add](#)

Sites [+ Add](#)

FEATURE

Feature Object Aggregations [+ Add](#)

Feature Objects [+ Add](#)

INCIDENT\_REPORTING

Categories [+ Add](#)

Incident status [+ Add](#)

Incidents [+ Add](#)

MODEL

Models [+ Add](#)

Training Jobs [+ Add](#)

Venue Event Categories [+ Add](#)

Venue Events [+ Add](#)

SYSTEM\_SETTINGS

Settings [+ Add](#)

VMS

VMS Bridge Settings

VMS Configurations [+ Add](#)

### Change VMS Bridge Settings

**VMSBridgeSettings object (1)**

☒ **Enable VMS Bridge Service**  
Enables the VMS bridge service, allowing events & cameras to be synchronised between icetana and VMS servers.

**Backend - Origin HTTP URI:**   
The URI (HTTP/HTTPS) to the icetana backend's REST API.

**Backend - Username:**   
The username or email-address to authenticate to the icetana backend's REST API.

**Backend - Password:**   
The password to authenticate to the icetana backend's REST API.

☒ **Feature - Enable Milestone Event Trigger**  
Enables the feature to trigger events on Milestone VMS installations.

**Genetec - Certificate Application ID:**   
The ApplicationId field from the certificate file used for icetana's integration with Genetec.

**Kafka - Server Hostname/IP-Address & Port:**   
The Kafka broker server hostname/ip-address and port.

**Kafka - Topics - Live Events:**   
The name of the Kafka topic for live event updates.

**Logging - General - Logging Level:**   
The logging level for all other loggers for the VMS Bridge service.

**Logging - Scheduler - Logging Level:**   
The logging level for the scheduler.

- Select the site where cameras will be populated from the Scheduler - Camera Synchronisation - Site: field.
- Select Save from the bottom

CLIENTS

Clients

+ Add

Sites

+ Add

FEATURE

Feature Object Aggregations

+ Add

Feature Objects

+ Add

INCIDENT\_REPORTING

Categories

+ Add

Incident status

+ Add

Incidents

+ Add

MODEL

Models

+ Add

Training Jobs

+ Add

Venue Event Categories

+ Add

Venue Events

+ Add

SYSTEM\_SETTINGS

Settings

+ Add

VMS

VMS Bridge Settings

VMS Configurations

+ Add

The logging level for the task scheduler used by the VMS Bridge service.

Logging - VMS Bridge - Logging Level:

INFO

The logging level for all logs emitted by the VMS Bridge service itself.

RSA - Credentials Private Key Path:

/opt/icetana/certs/crypt

The path to the RSA private key used to decrypt encrypted credentials.

RSA - Credentials Private Key Passphrase:

The passphrase to decrypt the RSA private key for encrypted credentials.

RSA - JWT Private Key Path:

/opt/icetana/certs/back

The path to the RSA private key for extracting the public key used to verify encoded JWT signatures.

RSA - JWT Private Key Passphrase:

The passphrase to decrypt the RSA private key used for encoded JWT signatures.

Scheduler - Camera Synchronisation - Interval:

300

The interval (in seconds) between camera synchronisation attempts.

Scheduler - Camera Synchronisation - Site:

FM

The default site to add all VMS cameras to.

Scheduler - Update Live Events Consumer - Interval:

120

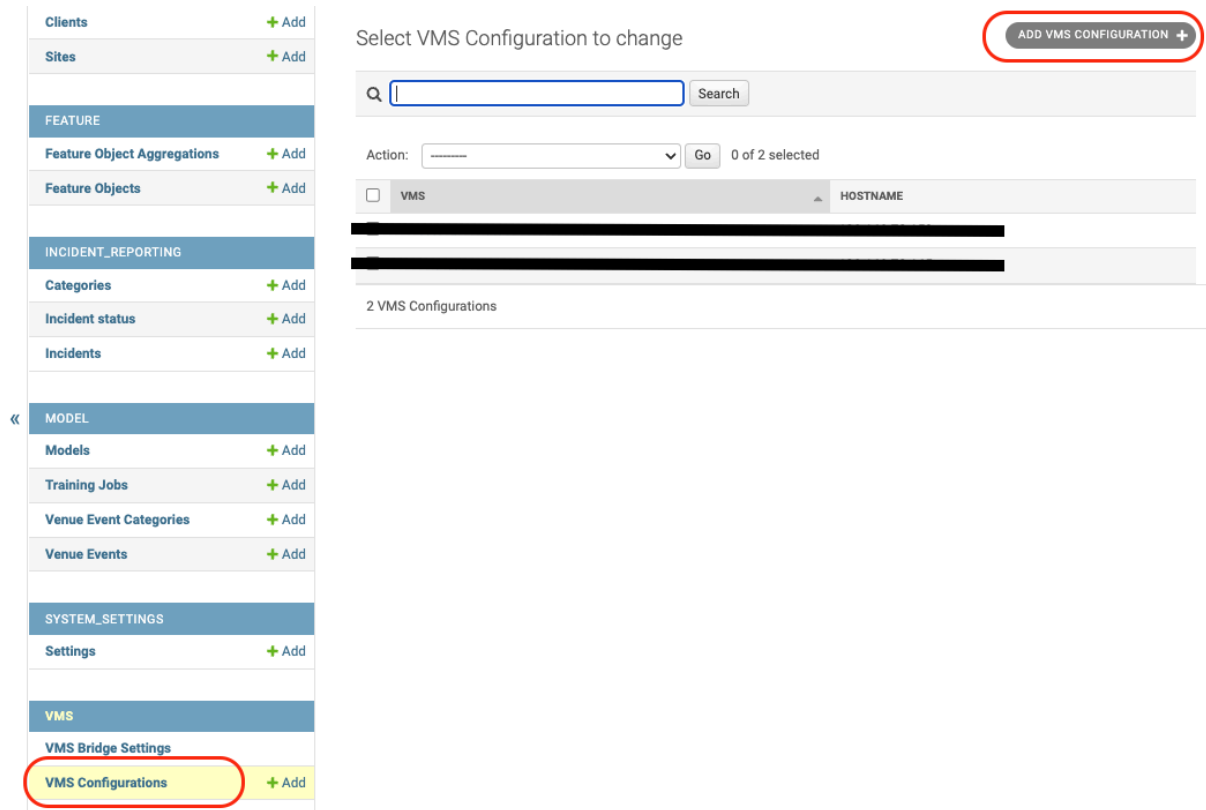
The interval (in seconds) between live events consumer update attempts.

Save and continue editing

SAVE

## 2) Create VMS object for Milestone XProtect VMS

- Navigate to <https://<icetanaServer>/admin> and log in using icetana credentials
- Scroll down to the VMS section, select VMS Configurations and add a new object



The screenshot displays the Icetana AI admin interface. On the left is a sidebar menu with various categories: Clients, Sites, FEATURE, INCIDENT\_REPORTING, MODEL, SYSTEM\_SETTINGS, and VMS. The VMS category is expanded, showing 'VMS Bridge Settings' and 'VMS Configurations'. The 'VMS Configurations' item is highlighted with a red circle. The main content area is titled 'Select VMS Configuration to change' and features a search bar, an 'ADD VMS CONFIGURATION +' button (circled in red), and a table with columns for 'VMS' and 'HOSTNAME'. Below the table, it indicates '2 VMS Configurations'.

- Vms dropdown select Milestone XProtect
- Hostname: Hostname/IP of Milestone XProtect Management Server
- Port: Milestone XProtect Management Server port, default is 443
- Enter Username/Password created in the Milestone for Icetana: *Refer to the section: 'Preparing XProtect VMS'*
- RTSP Hostname: Milestone Open Network Bridge IP/Hostname
- RTSP Port: Milestone Open Network Bridge RTSP port, default 554
- RTSP Default Stream field: can have the following stream options 0/, 1/, 2/ etc. 0/ is the default profile and 1/ is the second stream profile. *Refer to the section: Configure a second stream for Icetana AI.*
- Select Save from the bottom

Home › Vms › VMS Configurations › MILESTONE configuration - 192.168.70.159

Clients + Add

Sites + Add

FEATURE

Feature Object Aggregations + Add

Feature Objects + Add

INCIDENT\_REPORTING

Categories + Add

Incident status + Add

Incidents + Add

MODEL

Models + Add

Training Jobs + Add

Venue Event Categories + Add

Venue Events + Add

SYSTEM\_SETTINGS

Settings + Add

VMS

Change VMS Configuration

MILESTONE configuration - 192.168.70.159 HISTORY

Vms: Milestone XProtect

Hostname: 192.168.70.159

Port: 443

Username: \*\*\*

Password: \*\*\*\*\*

RTSP Hostname: 192.168.70.159

Rtsp port: 554

RTSP Default Stream: 1/

☒ Milestone - Enable RTSP TCP-interlaced input  
Enables the ability to consume Milestone ONB (Open Network Bridge) streams over RTSP with TCP-interlaced (RTP-over-RTSP) stream content.

Delete

Save and add another

Save and continue editing

SAVE

Note: When configuring the RTSP Default Stream, the trailing “/” at the end of the stream number is required for Milestone XProtect integration. If it is missing, the Stream will connect to the main stream without a warning.



# Populating Cameras into Icetana AI

Once a new Icetana AI VMS Bridge is created and configured or an existing VMS configuration is changed following commands must be executed.

- SSH to the Icetana AI server and navigate to the scripts folder. 'cd /opt/icetana/scripts/'
- Run the following command 'sudo docker restart icetana-vms-bridge'
- Cameras should start populating in the Cameras section on the Icetana AI main GUI

