



# RMF - Role Based View Creation Steps

Vega Systems Inc.

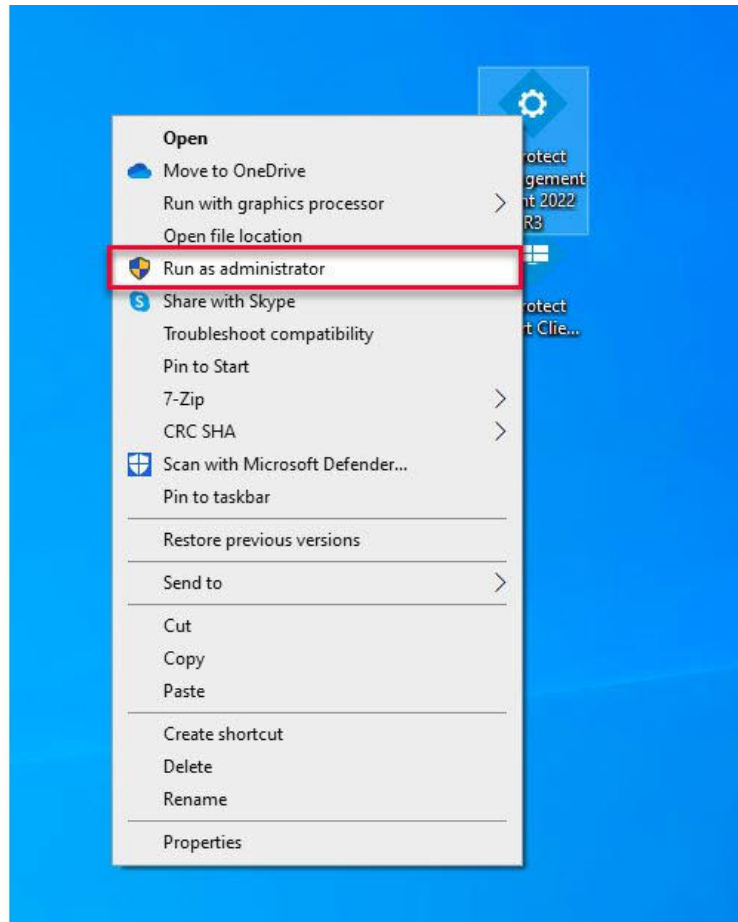
03/08/2022

<https://www.vega25.com/rmf>



# Part 1: Configuring Roles

## Parent (**Primary**) Management Server



**Step 1:** Open the **Management Client**.

**Note:** Run as administrator

Milestone  
XProtect® Management Client 2022 R3

Computer:  
primaryrec1.vegadomn.com

Authentication:  
Windows authentication

Domain: vegadomn.com

User name:  
vegadomn.com\milestone

Password:  
●●●●●●●

Remember password

Sign in Close

Management Server

**Step 2:** Login into the **Parent Management Server** as a domain user with admin privileges. (Federated Deployments)  
**Login into Management Server** as a user with admin privileges (Non-Federated Deployments)

The screenshot displays the Milestone XProtect Management Client 2022 R3 interface. The window title is "Milestone XProtect Management Client 2022 R3". The menu bar includes "File", "View", "Action", "Maintenance", "Tools", and "Help".

The interface is divided into three main sections:

- Site Navigation:** A tree view on the left showing the system hierarchy. The "Security" folder is expanded, and the "Roles" sub-item is highlighted with a red rectangle.
- Roles:** A list of roles in the center pane. The "Administrators (Administrators have co" role is selected, showing a "UserLimited" icon.
- Role Settings:** The right pane shows configuration options for the selected role:
  - Roles information:** Name: Administrators; Description: Administrators have complete and unrestricted access to the system.
  - Smart Client profile:** Default Smart Client Profile.
  - Evidence lock profile:** Default evidence lock profile.
  - Permissions:**  Allow Smart Client login;  Allow Mobile Client login;  Allow Web Client login;  Make users anonymous during PTZ sessions.

The bottom status bar contains various system icons and navigation controls.

**Step 3:** Select Roles under Site Navigation → Security



Milestone XProtect Management Client 2022 R3

File View Action Maintenance Tools Help

Site Navigation

- PRIMARYREC1 - (22.3c)
  - Basics
    - License Information
    - Site Information
    - Remote Connect Services
    - Axis One-click Camera Connection
  - Servers
    - Recording Servers
    - Fallover Servers
    - Mobile 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
  - Security
    - Roles
    - Add Role...**
    - Delete Role... Del
    - Effective Roles...
    - Rename Role... F2
    - Copy Role...
    - Refresh F5
  - Metadata Use
    - Metadata Search
  - Access Control
  - Incidents
    - Incident properties
    - Transact
      - Transaction sources
      - Transaction definitions
    - Alarms
    - MIP Plugins

Roles

Name

- Administrators (Administrators have co
- UserLimited

Role Settings

Roles information

Name:

Administrators

Description:

Administrators have complete and unrestricted access to the system

Smart Client profile:

Default Smart Client Profile

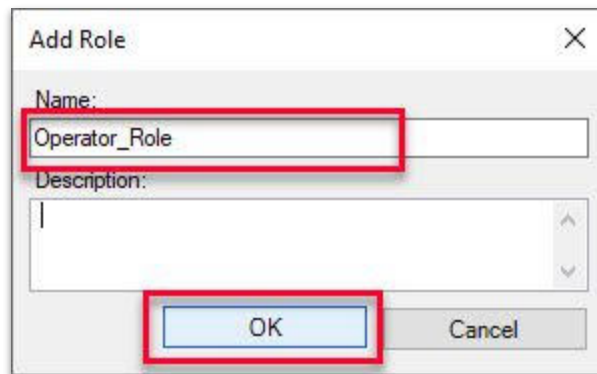
Evidence lock profile:

Default evidence lock profile

- Allow Smart Client login
- Allow Mobile Client login
- Allow Web Client login
- Make users anonymous during PTZ sessions

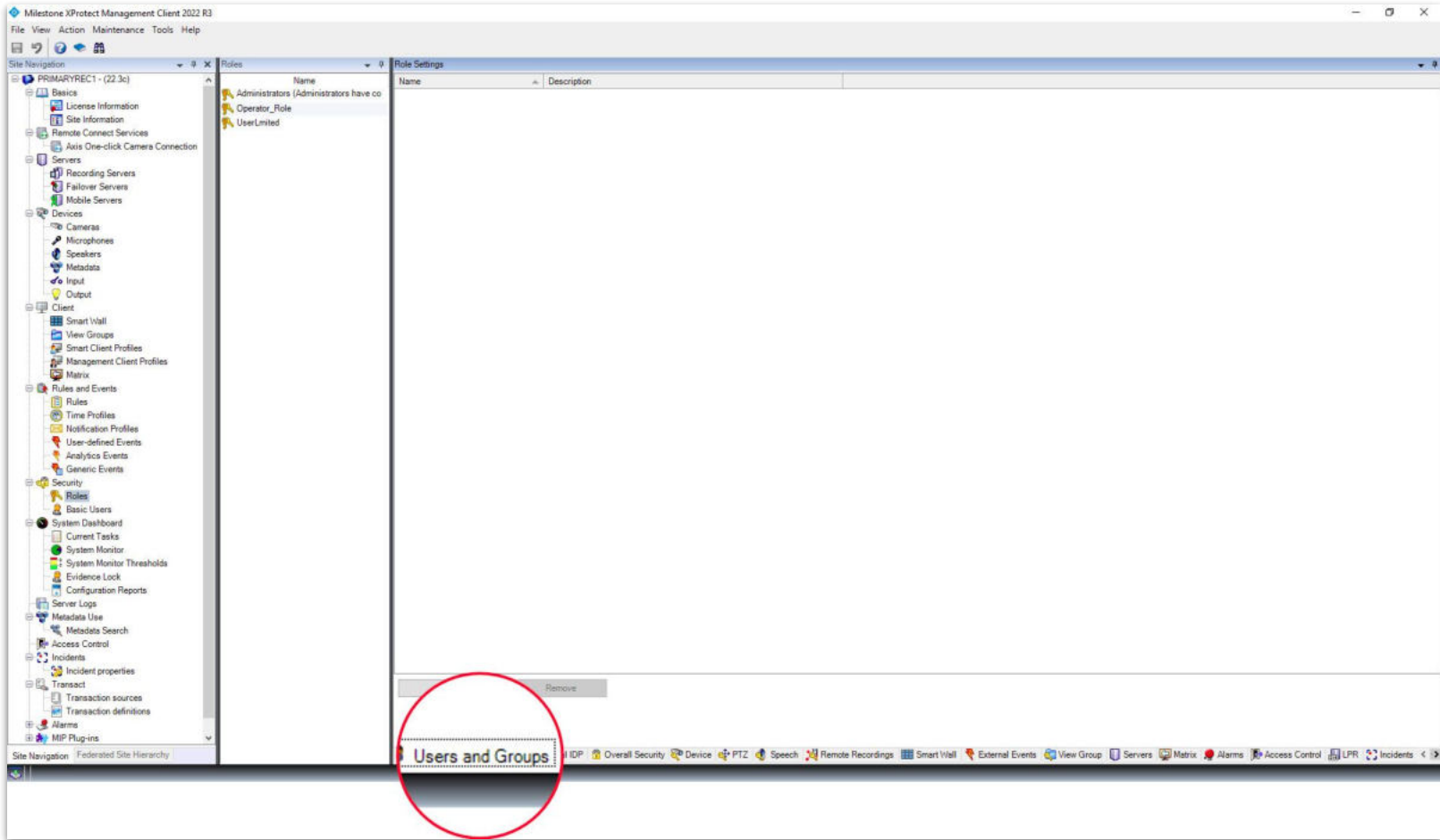
Info Users and Groups External IDP Overall Security Device PTZ Speech Remote Recordings Smart Wall External Events View Group Servers Matrix Alarms Access Control LPR Incidents

**Step 4:** Right-Click Roles and select **Add Role**



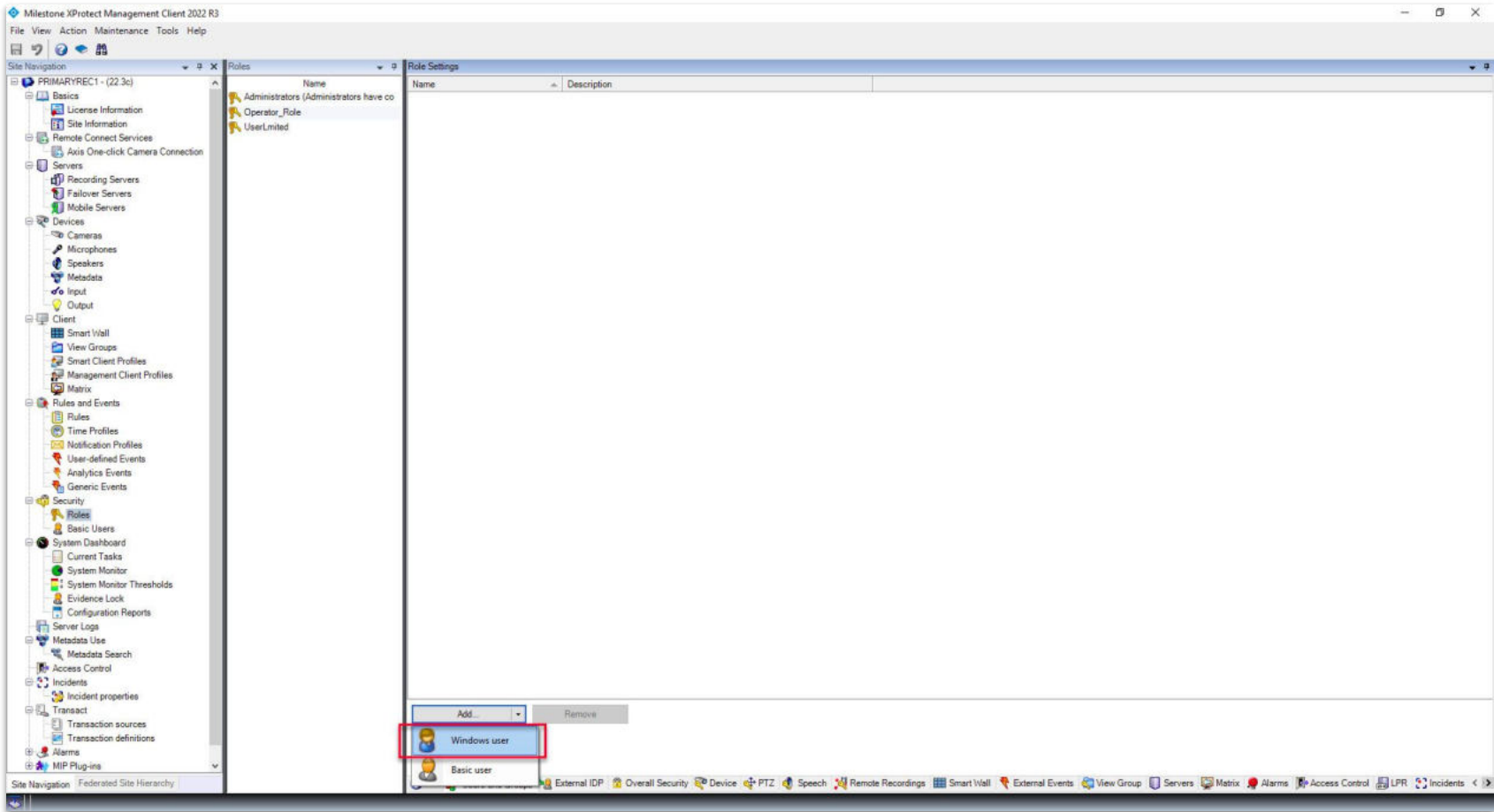
The image shows a dialog box titled "Add Role" with a close button (X) in the top right corner. It contains two input fields: "Name:" and "Description:". The "Name:" field is filled with the text "Operator\_Role" and is highlighted with a red rectangular box. The "Description:" field is empty and has a vertical scrollbar on its right side. At the bottom of the dialog, there are two buttons: "OK" and "Cancel". The "OK" button is highlighted with a red rectangular box.

**Step 5:** Provide a **Role name** and click **OK**.

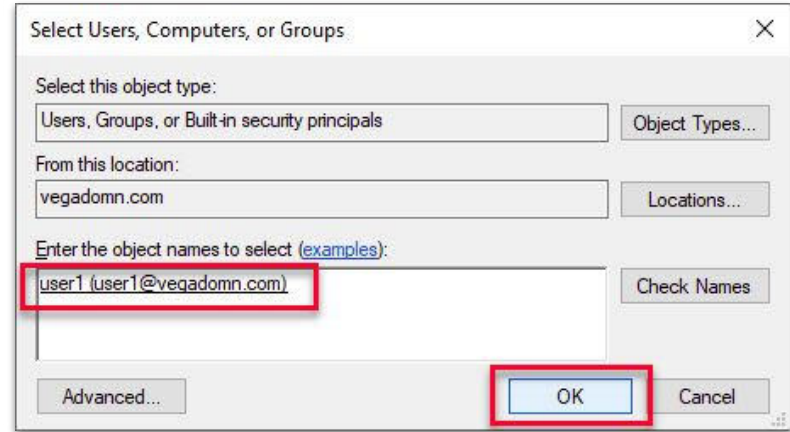
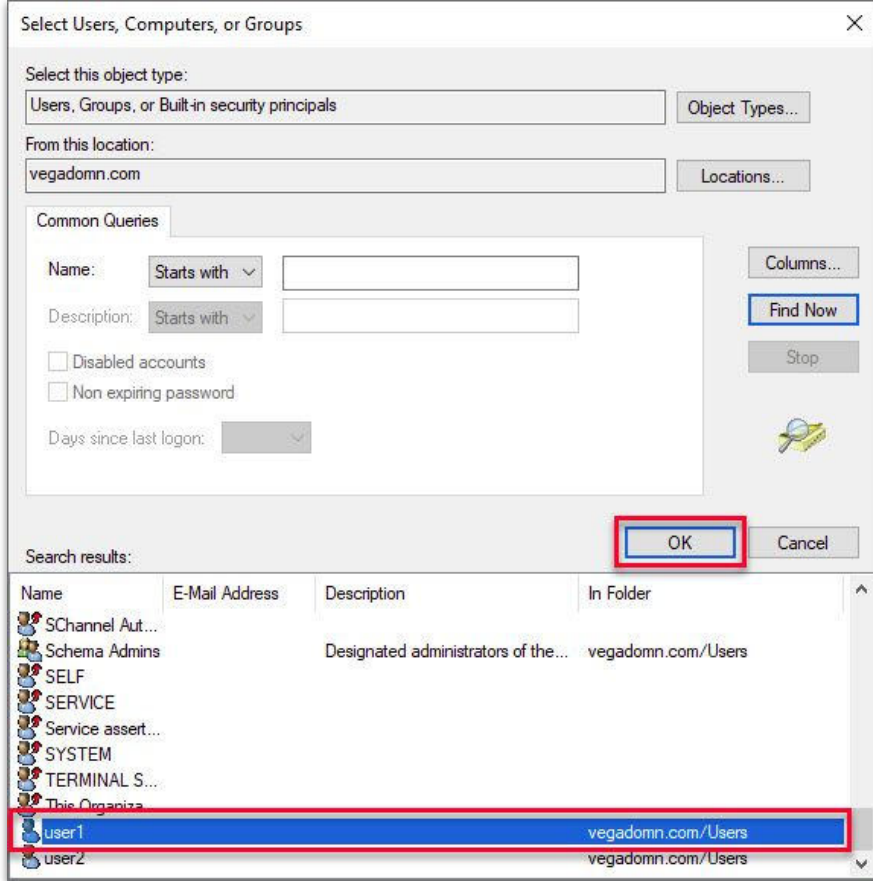


**Step 6:** Select **Users and Groups** from the bottom toolbar for the created role.

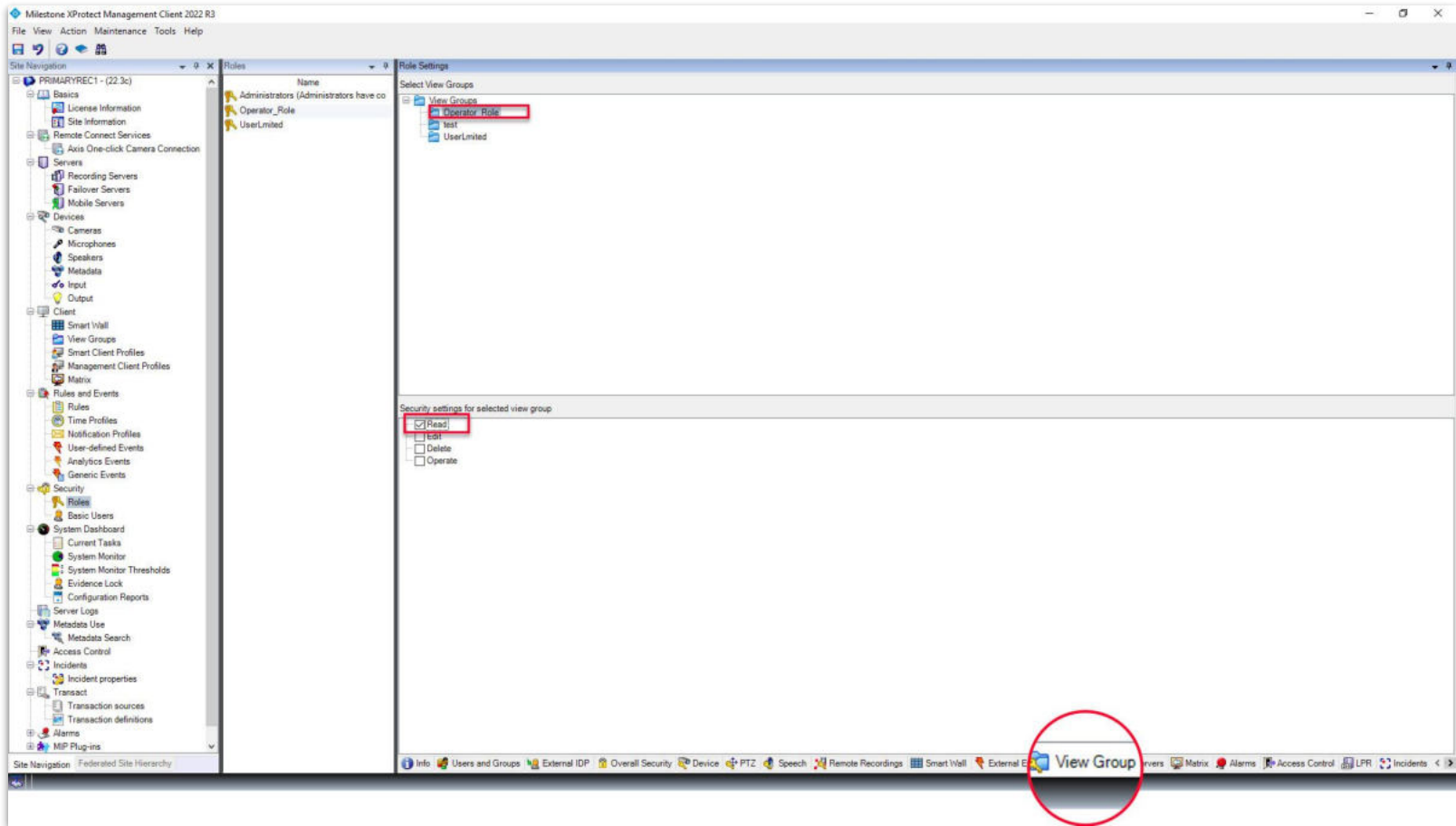




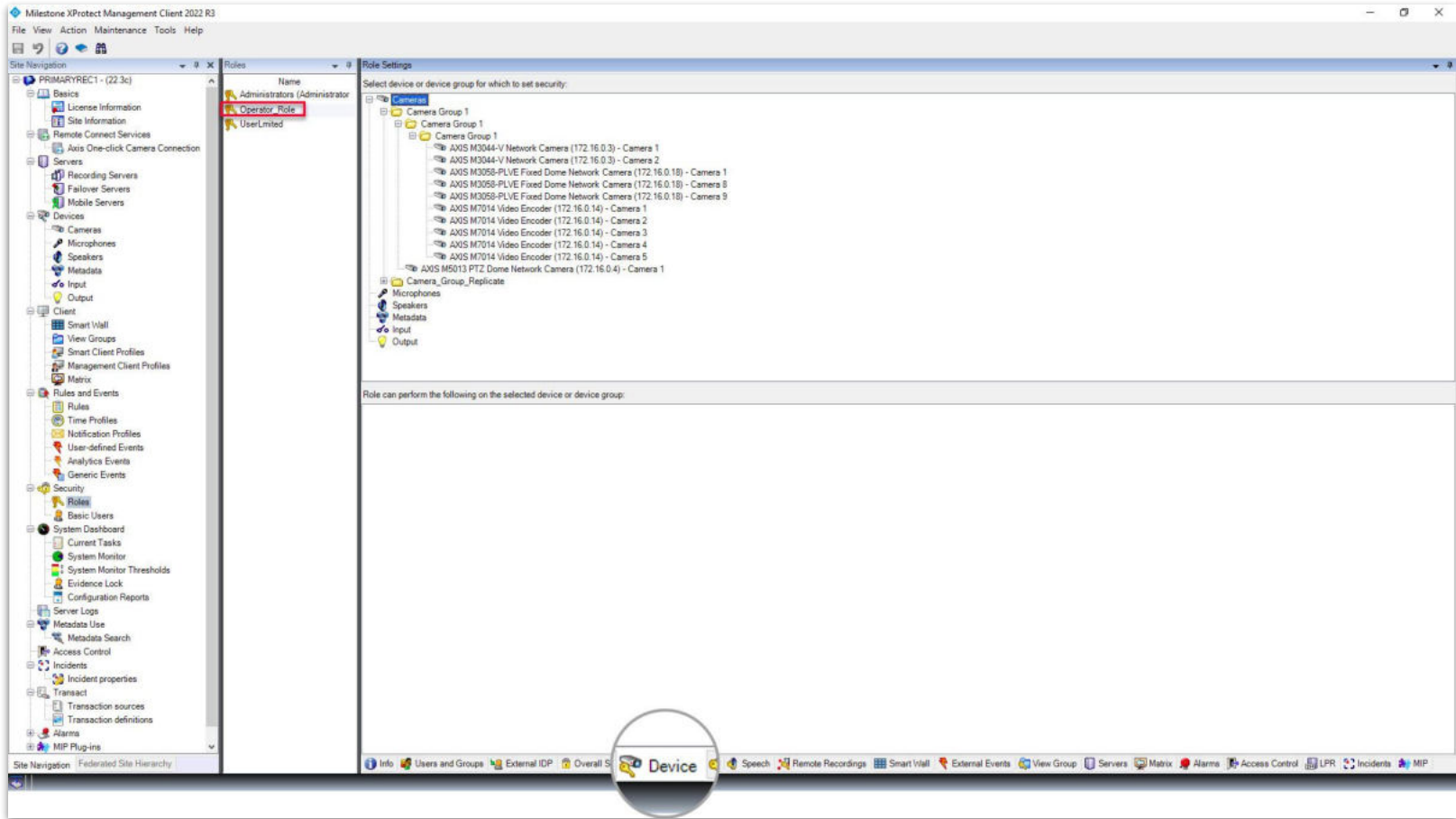
**Step 7:** Click **Add** and Select **Windows user** (Federated Deployments)  
Click **Add** and Select **Basic or Windows User** (Non-Federated Deployments)



**Step 8:** Select **domain user(s)** from the list and click **OK**. (Federated Deployments)  
Select **basic or windows user(s)** from the list and click **OK**. (Non-Federated Deployments)  
In the following step, **verify the selected user** and click **OK**.



**Step 9:** Select **View Group** from the bottom toolbar. Select the created **Role**.  
Select the permissions for the Role - **Read**, **Edit**, **Delete**, and **Operate**.



**Step 10:** Select **Device** from the bottom toolbar.  
Select a **camera or camera group** from the list to be permitted for the user.

Milestone XProtect Management Client 2022 R3

File View Action Maintenance Tools Help

Site Navigation

PRIMARYRECT - (22.3c)

Basics

- License Information
- Site Information
- Remote Connect Services
- Axis One-click Camera Connection

Servers

- Recording Servers
- Failover Servers
- Mobile 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

Security

- Roles
- Basic Users
- System Dashboard
- Current Tasks
- System Monitor
- System Monitor Thresholds
- Evidence Lock
- Configuration Reports
- Server Logs

Metadata Use

- Metadata Search

Access Control

- Incidents
- Incident properties
- Transact
- Transaction sources
- Transaction definitions

Alarms

- MIP Plug-ins

Federated Site Hierarchy

Roles

- Administrators (Administrator)
- Operator\_Role
- UserLimited

Role Settings

Select device or device group for which to set security:

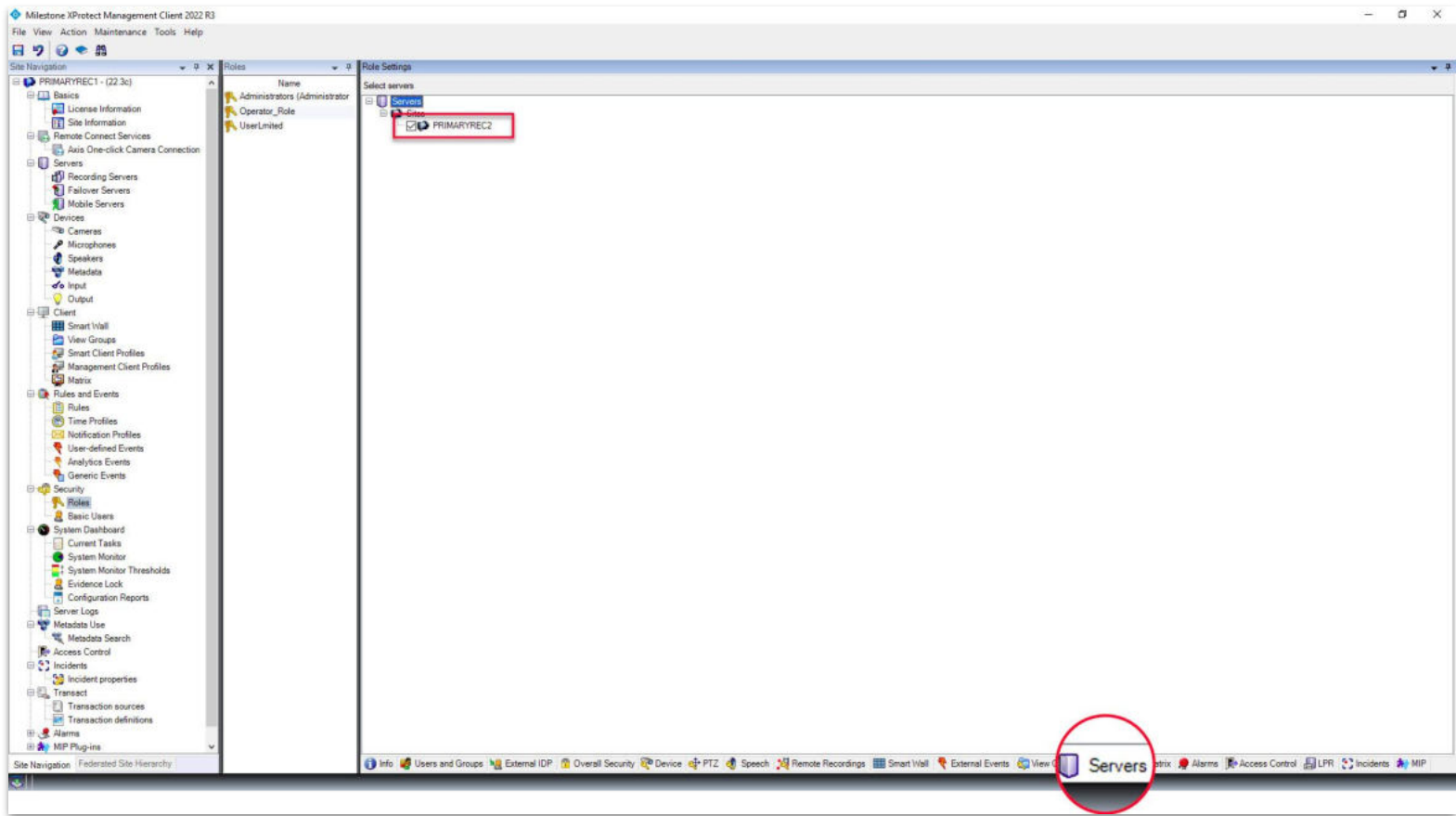
- Cameras
  - Camera Group 1
    - Camera Group 1
      - AXIS M3044-V Network Camera (172.16.0.3) - Camera 1**
      - AXIS M3058-PLVE Fixed Dome Network Camera (172.16.0.3) - Camera 2
      - AXIS M3058-PLVE Fixed Dome Network Camera (172.16.0.18) - Camera 1
      - AXIS M3058-PLVE Fixed Dome Network Camera (172.16.0.18) - Camera 8
      - AXIS M3058-PLVE Fixed Dome Network Camera (172.16.0.18) - Camera 9
      - AXIS M7014 Video Encoder (172.16.0.14) - Camera 1
      - AXIS M7014 Video Encoder (172.16.0.14) - Camera 2
      - AXIS M7014 Video Encoder (172.16.0.14) - Camera 3
      - AXIS M7014 Video Encoder (172.16.0.14) - Camera 4
      - AXIS M7014 Video Encoder (172.16.0.14) - Camera 5
    - AXIS M5013 PTZ Dome Network Camera (172.16.0.4) - Camera 1
  - Camera\_Group\_Replicate
- Microphones
- Speakers
- Metadata
- Input
- Output

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

- Camera
  - Read
  - Live
    - default
  - Recorded video
    - Playback
      - Within time profile:
        - default
      - Limit playback to:
        - No restriction
    - 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

Info Users and Groups External IDP Overall Security Device PTZ Speech Remote Recordings Smart Wall External Events View Group Servers Matrix Alarms Access Control LPR Incidents MIP

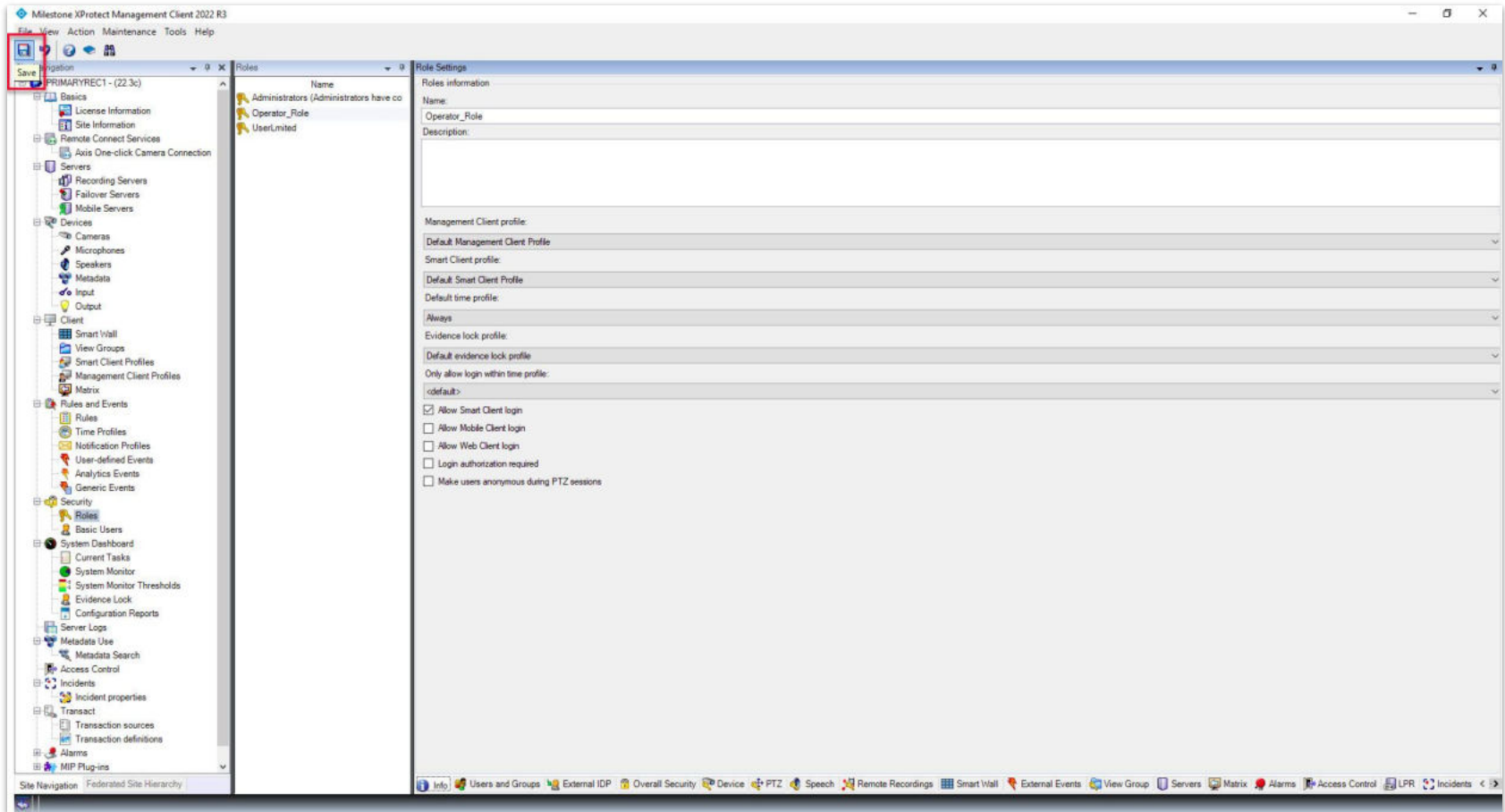
**Step 11:** Select the needed camera actions (Read, Live, Playback and Read Sequence) for the selected camera or camera group.



**Step 12:** Select **Servers** from the bottom toolbar. Tick the **child management server** listed.

**Note:** By giving access to the child server, RMF switching will be possible when the parent site is offline.

**Note:** Skip this step, if non-federated deployment



**Step 13:** Save all the changes.



## Part 2: Role Replication



Milestone XProtect Management Client 2022 R3

File View Action Maintenance Tools Help

Site Navigation

- PRIMARYREC1 - (22.3c)
  - Basics
    - License Information
    - Site Information
    - Remote Connect Services
    - Axis One-click Camera Connection
  - Servers
    - Recording Servers
    - Failover Servers
    - Mobile Servers
  - Devices
    - Cameras
    - Microphones
    - Speakers
    - Metadata
    - Input
    - Output
  - Client
    - Smart Wall
    - View Groups
    - Smart Client Profiles
    - Management Client Profiles
    - Matrix
  - Rules and Events
  - Security
    - Roles
    - Basic Users
  - System Dashboard
    - Current Tasks
    - System Monitor
    - System Monitor Thresholds
    - Evidence Lock
    - Configuration Reports
    - Server Logs
  - Metadata Use
    - Metadata Search
  - Access Control
  - Incidents
    - Incident properties
  - Transact
    - Transaction sources
    - Transaction definitions
  - Alarms
    - MIP Plug-ins
      - RMF
      - MIP SDK Samples
      - SureStream

Site Navigation Federated Site Hierarchy

**milestone | XProtect®**

## RMF

### Redundancy Management Framework

The *Redundancy Management Framework (RMF)* seamlessly integrates with Milestone XProtect VMS to assist facilities in maintaining high-security standards while minimizing the impact of potential failures. Some of its key features include:

- Cause Agnostic Failure detection:** RMF integrates failure detectors into each Smart Client view window to identify and address issues quickly.
- Rapid mitigation:** With near instantaneous live video recovery and automatic playback sourcing, RMF ensures constant access to critical video data.
- Flexible, asymmetric redundancy:** RMF offers greater flexibility in redundancy configurations, allowing cameras to be distributed across multiple secondary servers or aggregated into fewer secondary recorders.
- Support for XProtect Federation:** RMF provides redundant recording and sourcing capabilities in an XProtect federated architecture, ensuring uninterrupted situational awareness for end users during total site failures.

RMF is a valuable tool for seamlessly and efficiently managing redundant video in various settings, including airports, seaports, data centers, campuses, transportation networks, or cities.

We hope you enjoy our product.

Website - [www.vega25.com](http://www.vega25.com)  
Email - [support@vega25.com](mailto:support@vega25.com).

**License Information:**

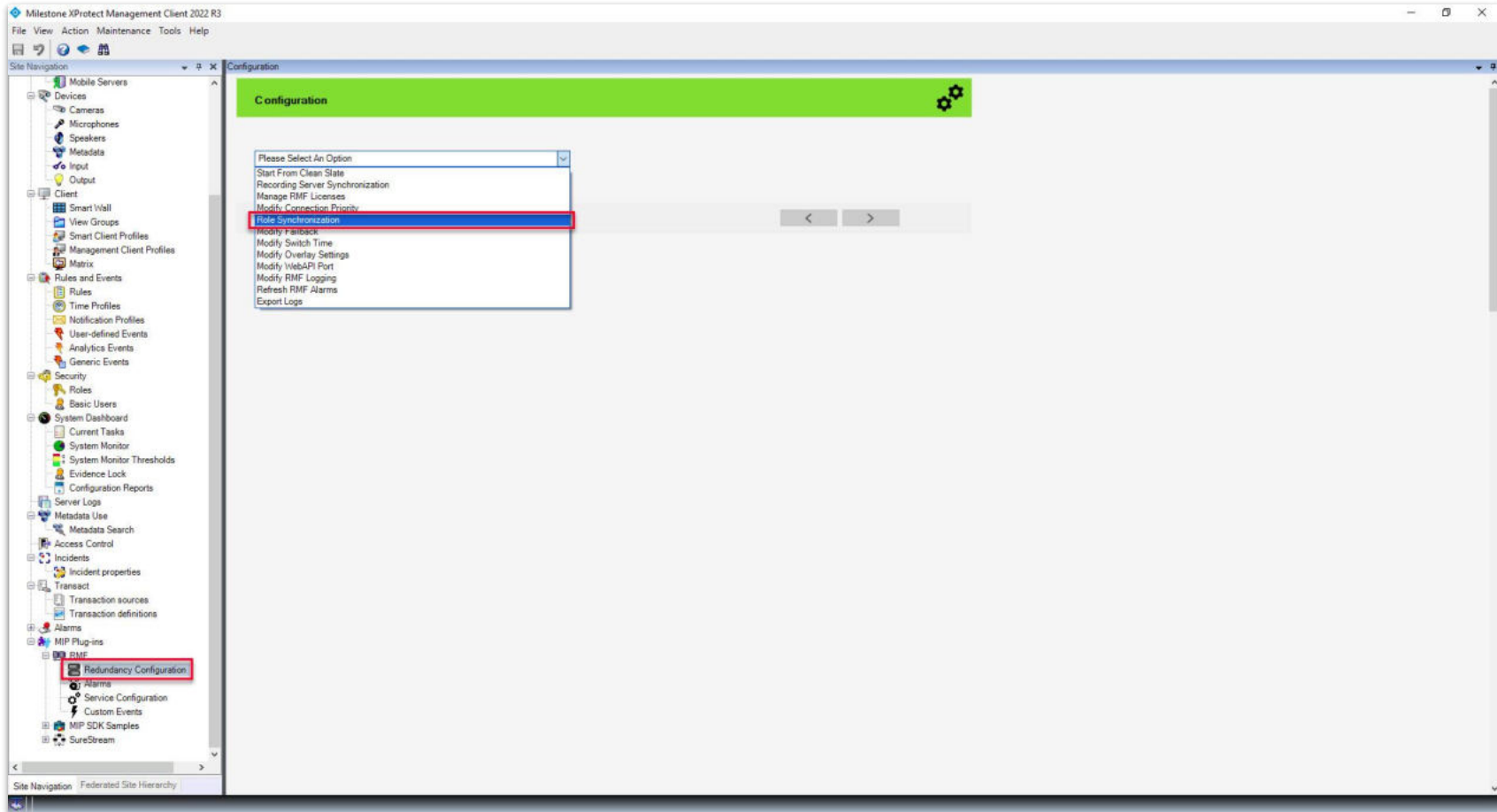
Demo for 15 channels - Expires on 3/31/2023  
Used here - 5, Other sites - 8

Version - 5.2.0

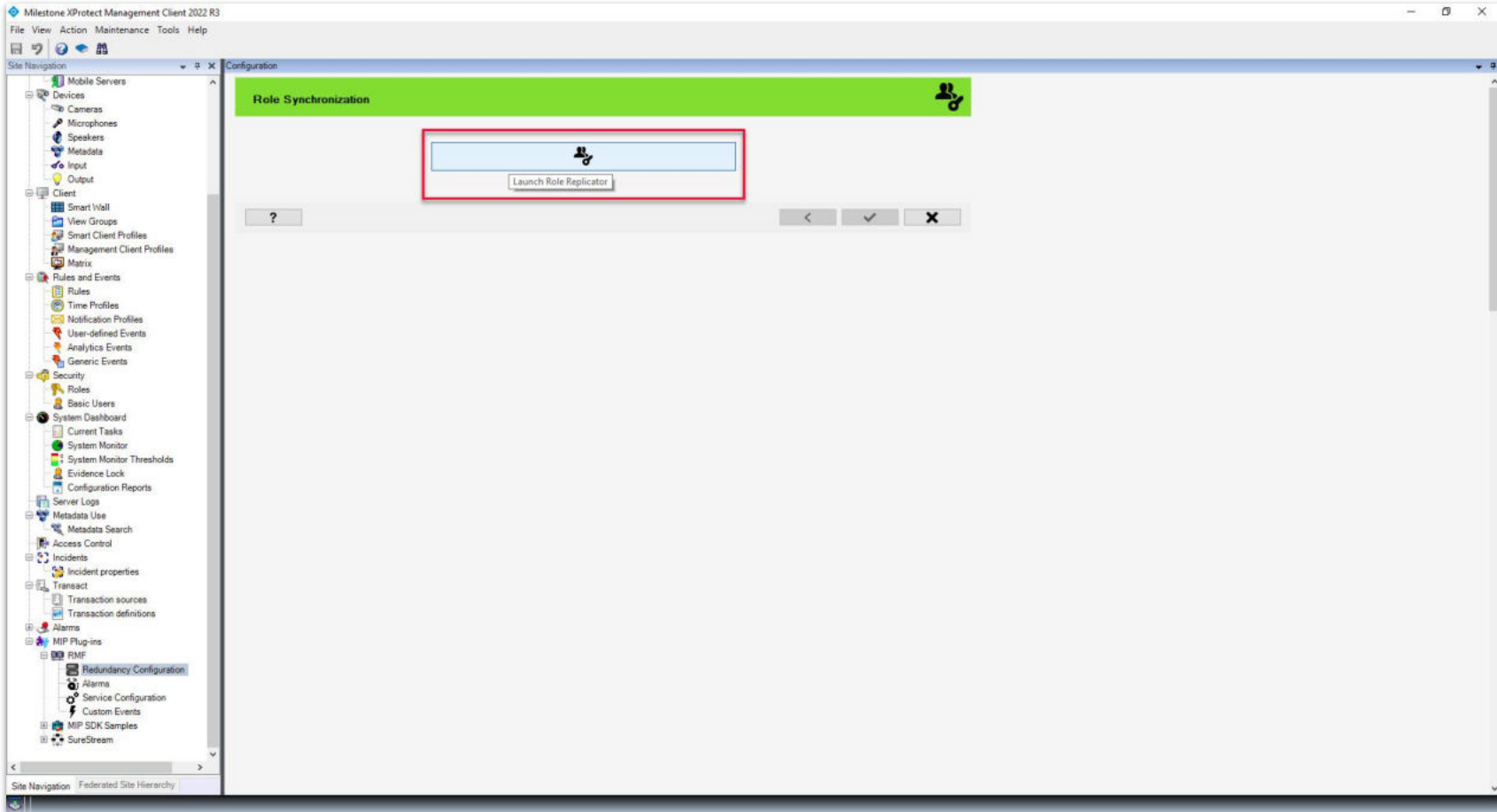
MIP Plug-ins

- RMF
- MIP SDK Samples
- SureStream

**Step 1:** Select the RMF plugin from Site Navigation → MIP Plugins



**Step 2:** Expand RMF and select **Redundancy Configuration**.  
Choose **Role Synchronization** from the list.



**Step 3: Click Launch Role Replicator.**

Roles

### Connect to Site

Management Server address and credentials

Server:

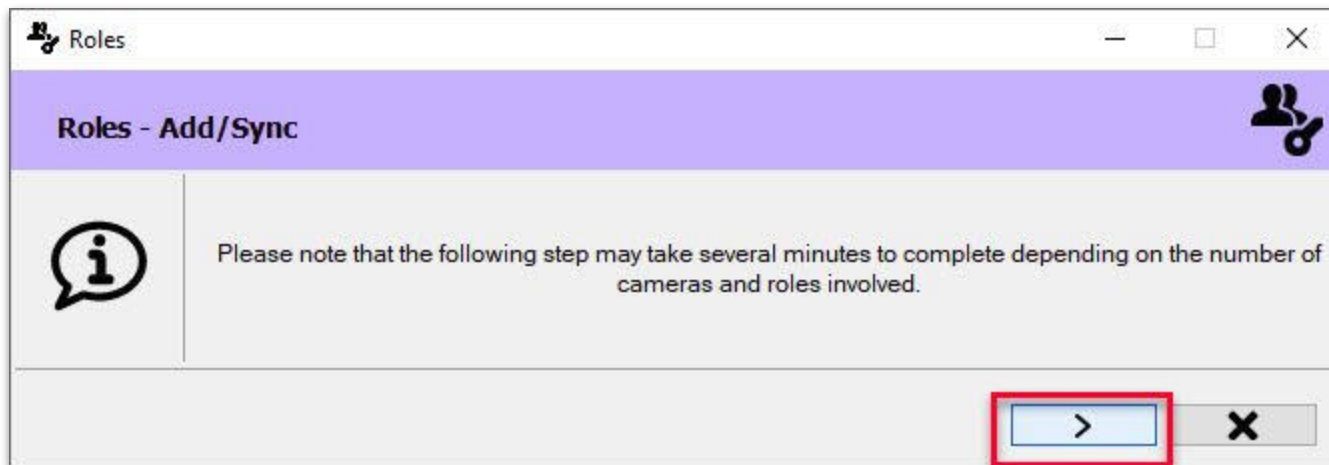
Authentication:

Username:

Password:

**Note:** If you're in an XProtect Federated Setup, please log in to the parent management server.

**Step 4:** Login into the **Parent Management Server** as a domain user with admin privileges. (Federated Deployments)  
Login into the **Management Server** as a user with admin privileges. (Non-Federated Deployments)





**Step 5:** Click **Next** to continue with the role replication process.

**Note:** RMF Role Replicator replicates only the roles that are associated with the cameras that are being managed by RMF.

Roles - Add/Sync

RMF Cameras	Status	Result
AXIS M3044-V Network Camera (172.16.0.3) - Camera 1	Skip(admin only)	
AXIS M3044-V Network Camera (172.16.0.3) - Camera 2	Skip(admin only)	
AXIS M3058-PLVE Fixed Dome Network Camera (172.16.0.18) - Camera 1	Skip(admin only)	
AXIS M3058-PLVE Fixed Dome Network Camera (172.16.0.18) - Camera 2	Skip(admin only)	
AXIS M3058-PLVE Fixed Dome Network Camera (172.16.0.18) - Camera 11	Skip(admin only)	
AXIS M3058-PLVE Fixed Dome Network Camera (172.16.0.18) - Camera 12	Skip(admin only)	
AXIS M3058-PLVE Fixed Dome Network Camera (172.16.0.18) - Camera 2	Skip(admin only)	
AXIS M3058-PLVE Fixed Dome Network Camera (172.16.0.18) - Camera 3	Skip(admin only)	
AXIS M3058-PLVE Fixed Dome Network Camera (172.16.0.18) - Camera 4	Skip(admin only)	
AXIS M3058-PLVE Fixed Dome Network Camera (172.16.0.18) - Camera 5	Skip(admin only)	
AXIS M3058-PLVE Fixed Dome Network Camera (172.16.0.18) - Camera 6	Skip(admin only)	
AXIS M3058-PLVE Fixed Dome Network Camera (172.16.0.18) - Camera 7	Skip(admin only)	
AXIS M3058-PLVE Fixed Dome Network Camera (172.16.0.18) - Camera 8	Skip(admin only)	
AXIS M3058-PLVE Fixed Dome Network Camera (172.16.0.18) - Camera 9	Skip(admin only)	
AXIS M5013 PTZ Dome Network Camera (172.16.0.4) - Camera 1	Re-check	
AXIS M7014 Video Encoder (172.16.0.14) - Camera 1	Skip(admin only)	
AXIS M7014 Video Encoder (172.16.0.14) - Camera 2	Skip(admin only)	
AXIS M7014 Video Encoder (172.16.0.14) - Camera 3	Skip(admin only)	
AXIS M7014 Video Encoder (172.16.0.14) - Camera 4	Skip(admin only)	
AXIS M7014 Video Encoder (172.16.0.14) - Camera 5	Skip(admin only)	

**Step 6:** All the roles from the parent (primary) site are listed.  
Click **Sync** to copy the roles to the child (secondary) site.

Roles - Add/Sync

RMF Cameras	Progress	Status	Result
AXIS M3044-V Network Camera (172.16.0.3) - Camera 1	<div style="width: 100%;"></div>	Skip(admin only)	
AXIS M3044-V Network Camera (172.16.0.3) - Camera 2	<div style="width: 100%;"></div>	Skip(admin only)	
AXIS M3058-PLVE Fixed Dome Network Camera (172.16.0.18) - Camera 1	<div style="width: 100%;"></div>	Skip(admin only)	
AXIS M3058-PLVE Fixed Dome Network Camera (172.16.0.18) - Camera 10	<div style="width: 100%;"></div>	Skip(admin only)	
AXIS M3058-PLVE Fixed Dome Network Camera (172.16.0.18) - Camera 11	<div style="width: 100%;"></div>	Skip(admin only)	
AXIS M3058-PLVE Fixed Dome Network Camera (172.16.0.18) - Camera 12	<div style="width: 100%;"></div>	Skip(admin only)	
AXIS M3058-PLVE Fixed Dome Network Camera (172.16.0.18) - Camera 3	<div style="width: 100%;"></div>	Skip(admin only)	
AXIS M3058-PLVE Fixed Dome Network Camera (172.16.0.18) - Camera 4	<div style="width: 100%;"></div>	Skip(admin only)	
AXIS M3058-PLVE Fixed Dome Network Camera (172.16.0.18) - Camera 5	<div style="width: 100%;"></div>	Skip(admin only)	
AXIS M3058-PLVE Fixed Dome Network Camera (172.16.0.18) - Camera 6	<div style="width: 100%;"></div>	Skip(admin only)	
AXIS M3058-PLVE Fixed Dome Network Camera (172.16.0.18) - Camera 7	<div style="width: 100%;"></div>	Skip(admin only)	
AXIS M3058-PLVE Fixed Dome Network Camera (172.16.0.18) - Camera 8	<div style="width: 100%;"></div>	Skip(admin only)	
AXIS M3058-PLVE Fixed Dome Network Camera (172.16.0.18) - Camera 9	<div style="width: 100%;"></div>	Skip(admin only)	
AXIS M5013 PTZ Dome Network Camera (172.16.0.4) - Camera 1	<div style="width: 100%;"></div>	Re-check	
AXIS M7014 Video Encoder (172.16.0.14) - Camera 1	<div style="width: 100%;"></div>	Skip(admin only)	
AXIS M7014 Video Encoder (172.16.0.14) - Camera 2	<div style="width: 100%;"></div>	Skip(admin only)	
AXIS M7014 Video Encoder (172.16.0.14) - Camera 3	<div style="width: 100%;"></div>	Skip(admin only)	
AXIS M7014 Video Encoder (172.16.0.14) - Camera 4	<div style="width: 100%;"></div>	Skip(admin only)	

Synchronizing camera role settings across recording servers. Please wait.

**Step 7:** Roles being synchronized from the parent (primary) site to the child (secondary) site.

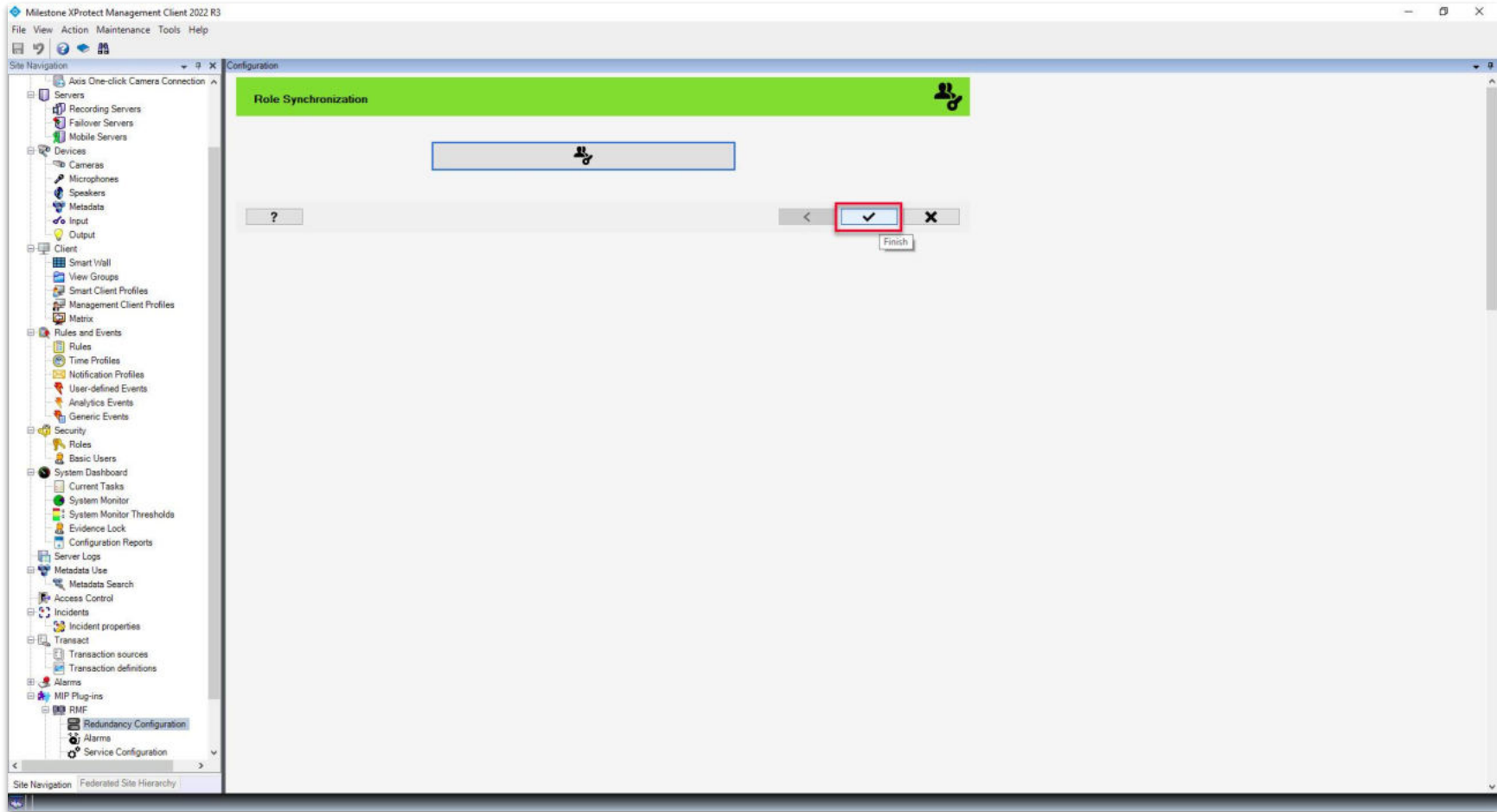
Roles - Add/Sync

Device	Status	Result
RMF Cameras		
AXIS M3058-PLVE Fixed Dome Network Camera (172.16.0.18) - Camera 1	Skip(admin only)	✓
AXIS M3058-PLVE Fixed Dome Network Camera (172.16.0.18) - Camera 10	Skip(admin only)	✓
AXIS M3058-PLVE Fixed Dome Network Camera (172.16.0.18) - Camera 11	Skip(admin only)	✓
AXIS M3058-PLVE Fixed Dome Network Camera (172.16.0.18) - Camera 12	Skip(admin only)	✓
AXIS M3058-PLVE Fixed Dome Network Camera (172.16.0.18) - Camera 2	Skip(admin only)	✓
AXIS M3058-PLVE Fixed Dome Network Camera (172.16.0.18) - Camera 3	Skip(admin only)	✓
AXIS M3058-PLVE Fixed Dome Network Camera (172.16.0.18) - Camera 4	Skip(admin only)	✓
AXIS M3058-PLVE Fixed Dome Network Camera (172.16.0.18) - Camera 5	Skip(admin only)	✓
AXIS M3058-PLVE Fixed Dome Network Camera (172.16.0.18) - Camera 6	Skip(admin only)	✓
AXIS M3058-PLVE Fixed Dome Network Camera (172.16.0.18) - Camera 7	Skip(admin only)	✓
AXIS M3058-PLVE Fixed Dome Network Camera (172.16.0.18) - Camera 8	Skip(admin only)	✓
AXIS M3058-PLVE Fixed Dome Network Camera (172.16.0.18) - Camera 9	Skip(admin only)	✓
AXIS M5013 PTZ Dome Network Camera (172.16.0.4) - Camera 1	Re-checked successfully	✓
AXIS M7014 Video Encoder (172.16.0.14) - Camera 1	Skip(admin only)	✓
AXIS M7014 Video Encoder (172.16.0.14) - Camera 2	Skip(admin only)	✓
AXIS M7014 Video Encoder (172.16.0.14) - Camera 3	Skip(admin only)	✓
AXIS M7014 Video Encoder (172.16.0.14) - Camera 4	Skip(admin only)	✓
AXIS M7014 Video Encoder (172.16.0.14) - Camera 5	Skip(admin only)	✓
AXIS P3807-PVE Network Camera (172.16.0.26) - Camera 1	Skip(admin only)	✓

Finish

**Step 8:** Click **Finish** after role synchronization.

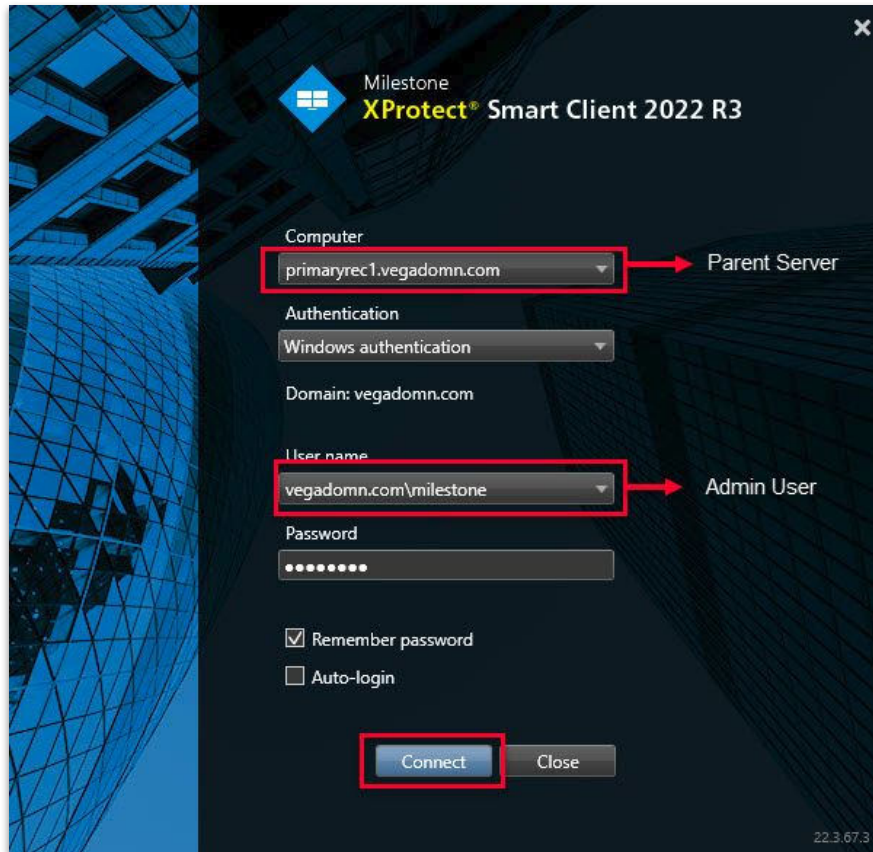




**Step 9: Click Finish.**

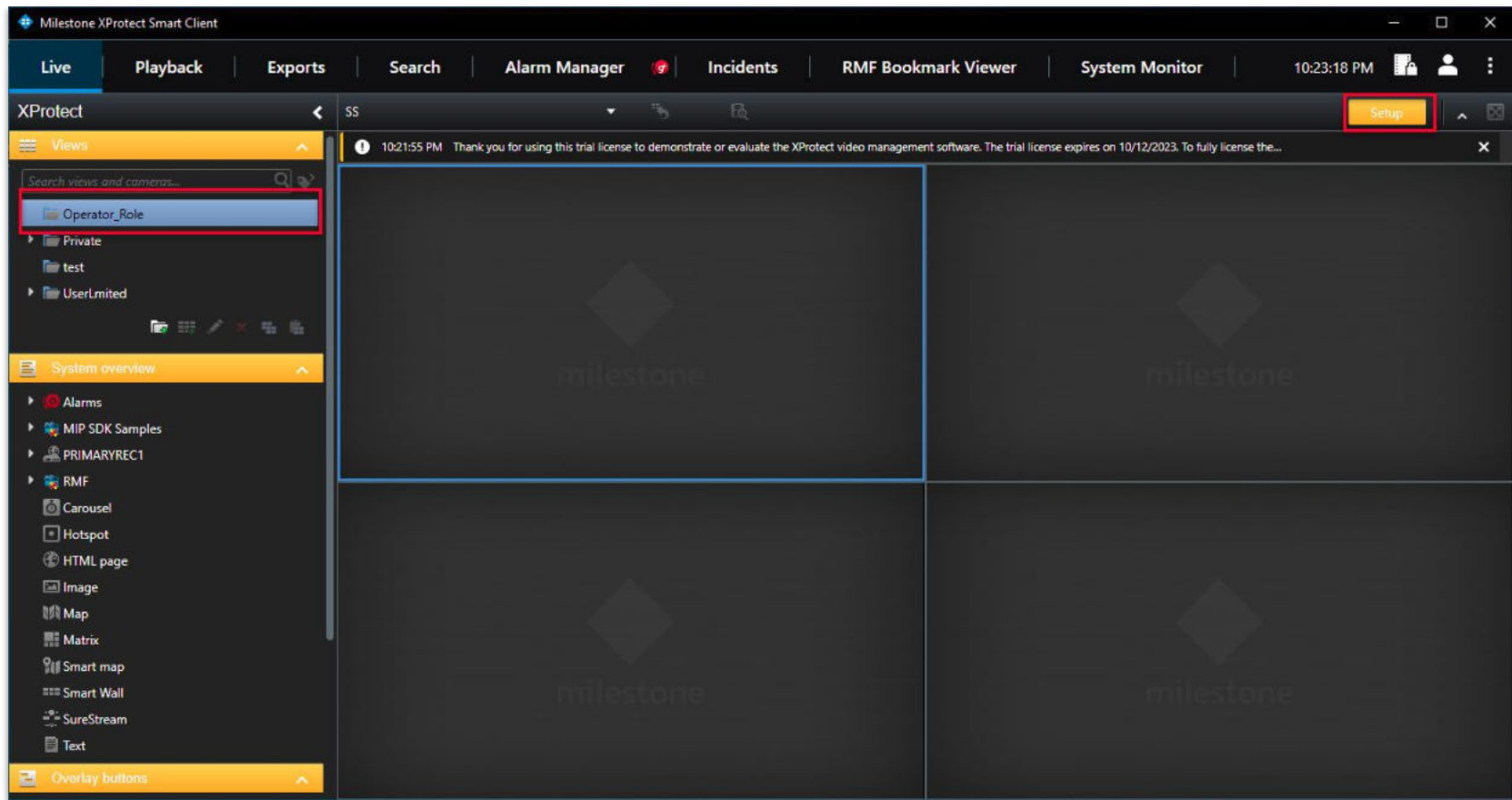


## Part 3: Configuring Views - Smart Client

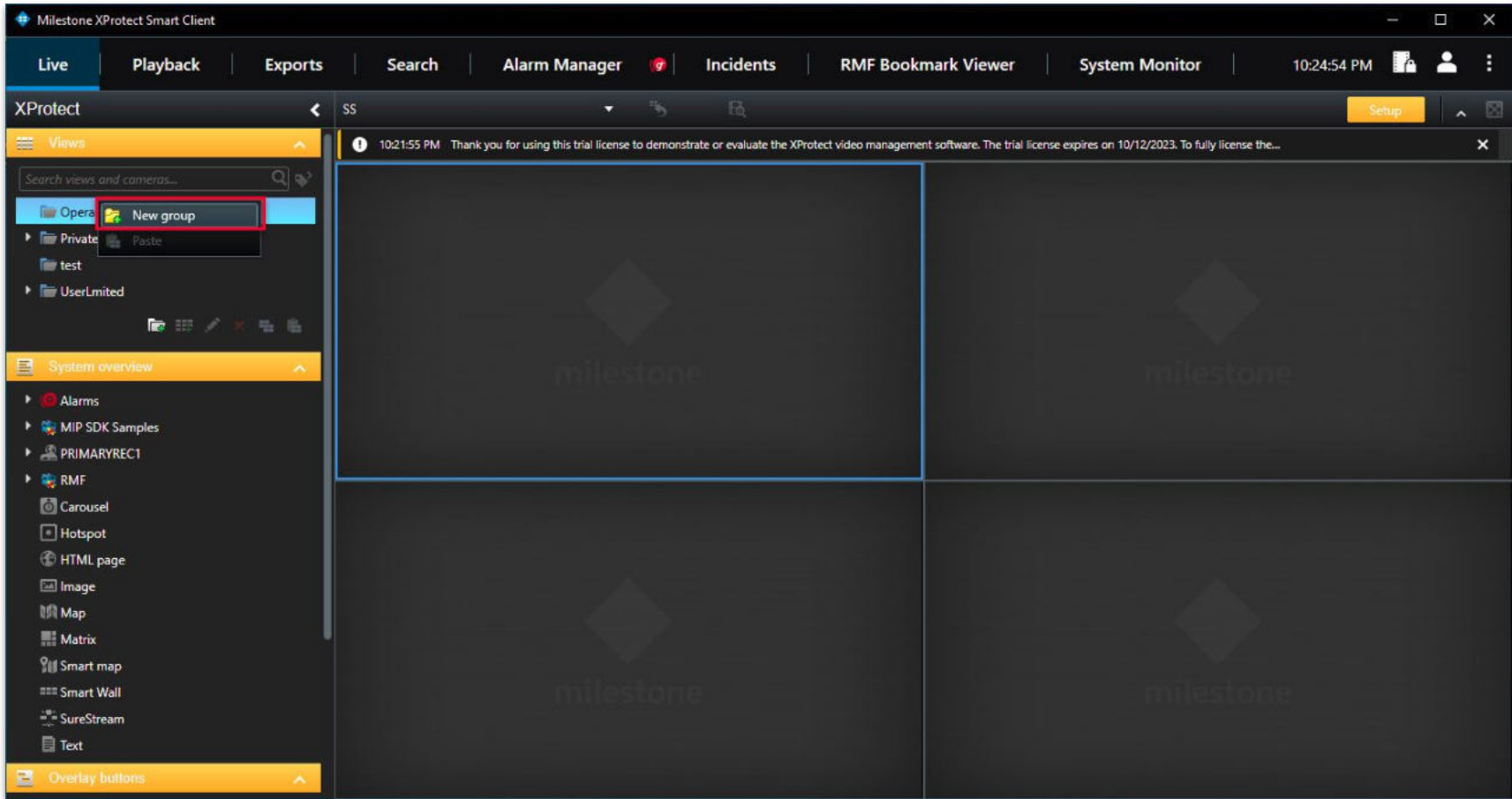


**Step 1: Open the Smart Client.**

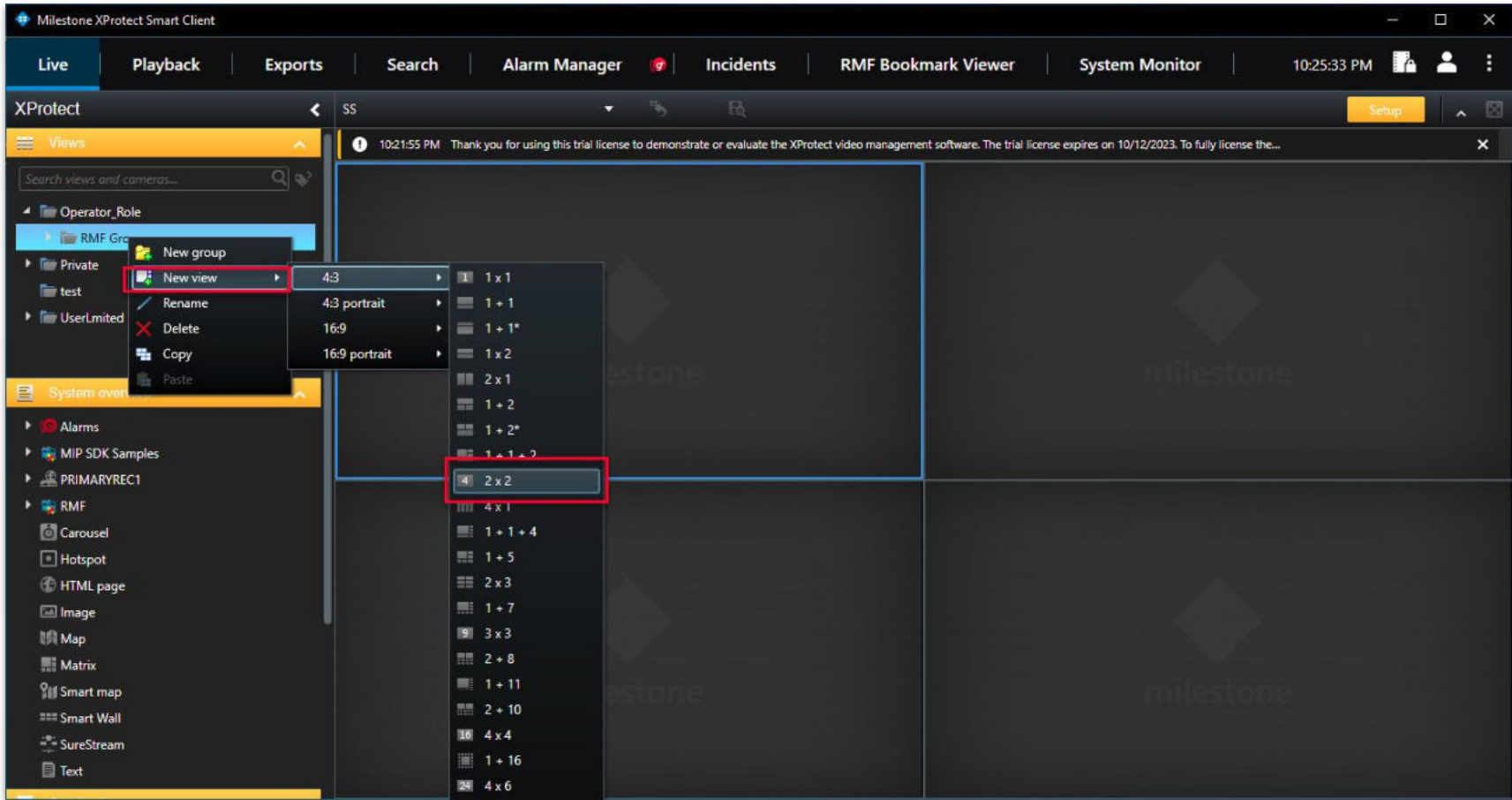
**Login** into the **Parent Management Server** using domain admin user credentials.(Federated Deployments)  
**Login** into **Management Server** using admin user credentials (Non-Federated Deployments)



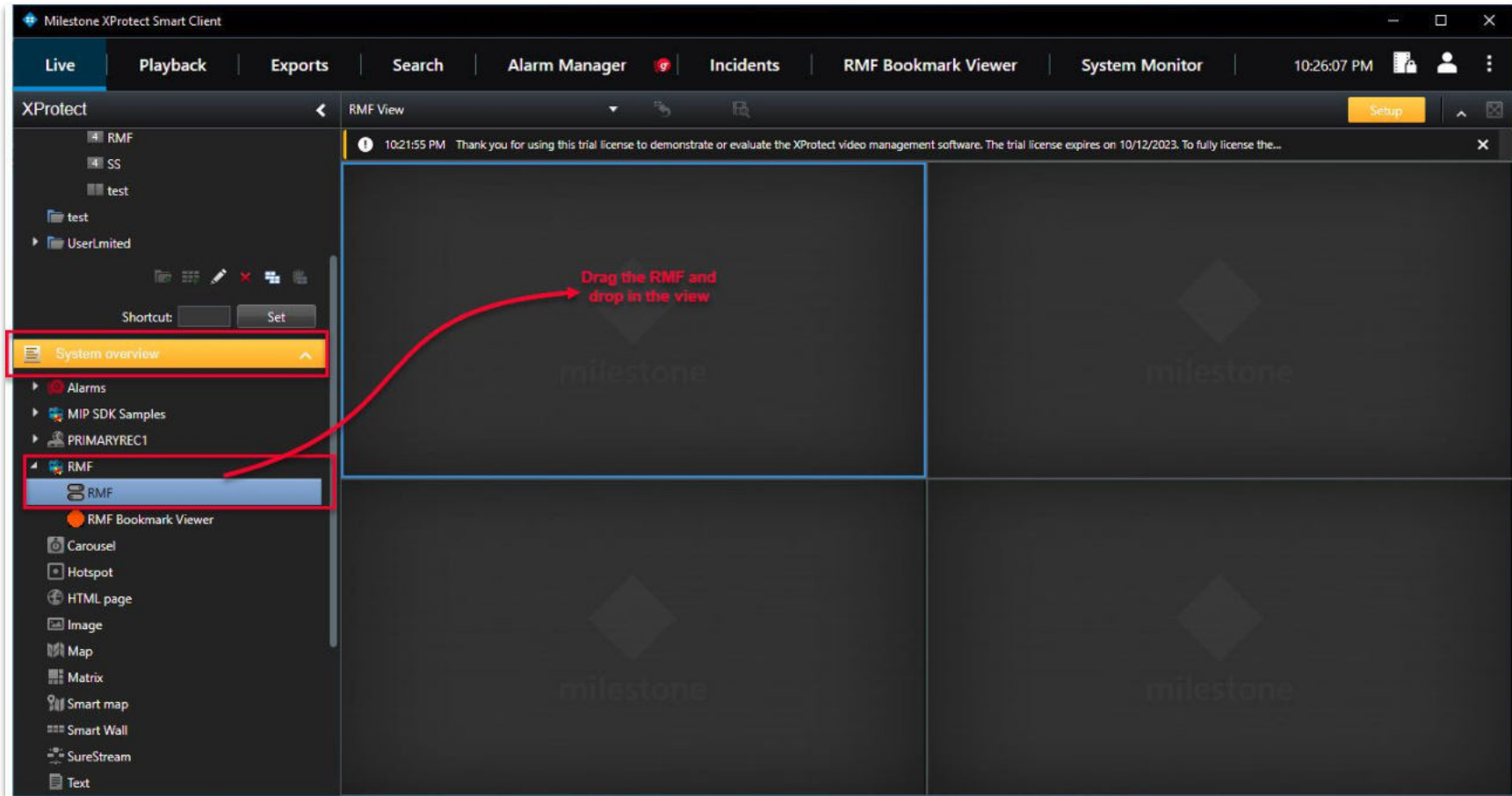
**Step 2:** Switch to **Setup** mode.  
Select the created **view set** corresponding to a **role** from the **Views** menu.  
(Milestone creates view sets for each role)



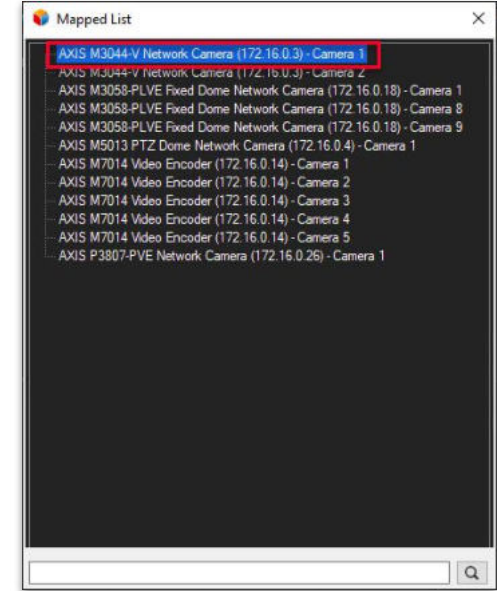
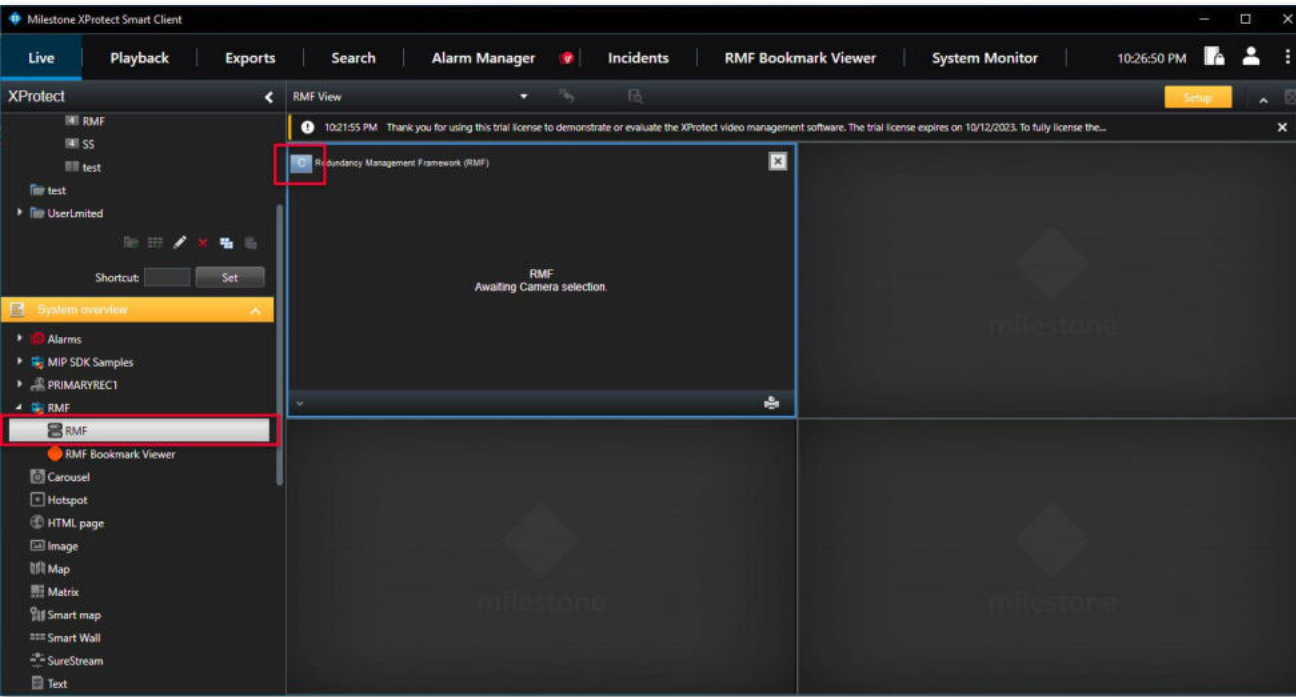
**Step 3:** Add a **New Group** by right-clicking the Role



**Step 4:** Right-click the group and add a **New View**. Select the needed view.

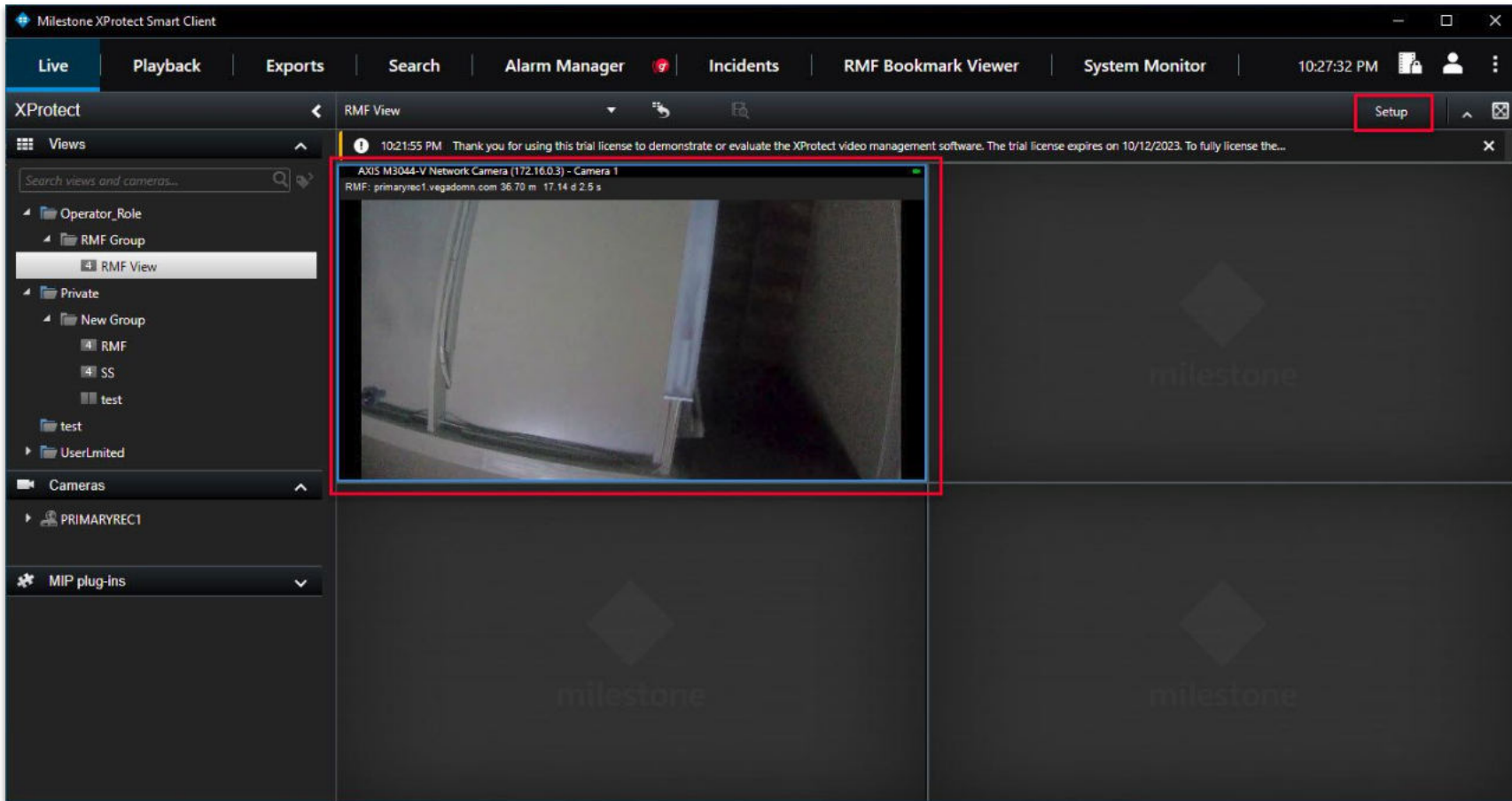


**Step 5:** Drag and drop the RMF plugin from the Systems Options to the view.



**Step 6:** Click the “C” button on the RMF view, as shown above. From the mapped (deduplicated) camera list, select a camera which was permitted to this role, when creating the role.

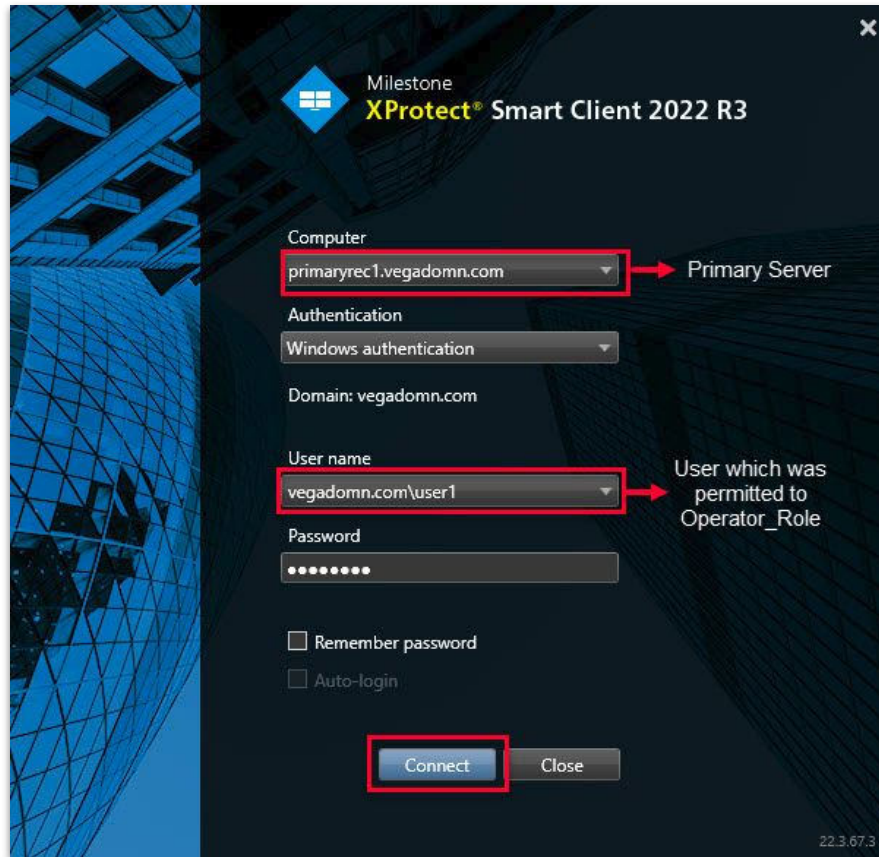




**Step 7:** Exit the Setup mode. Verify the **Live view** from the selected camera.



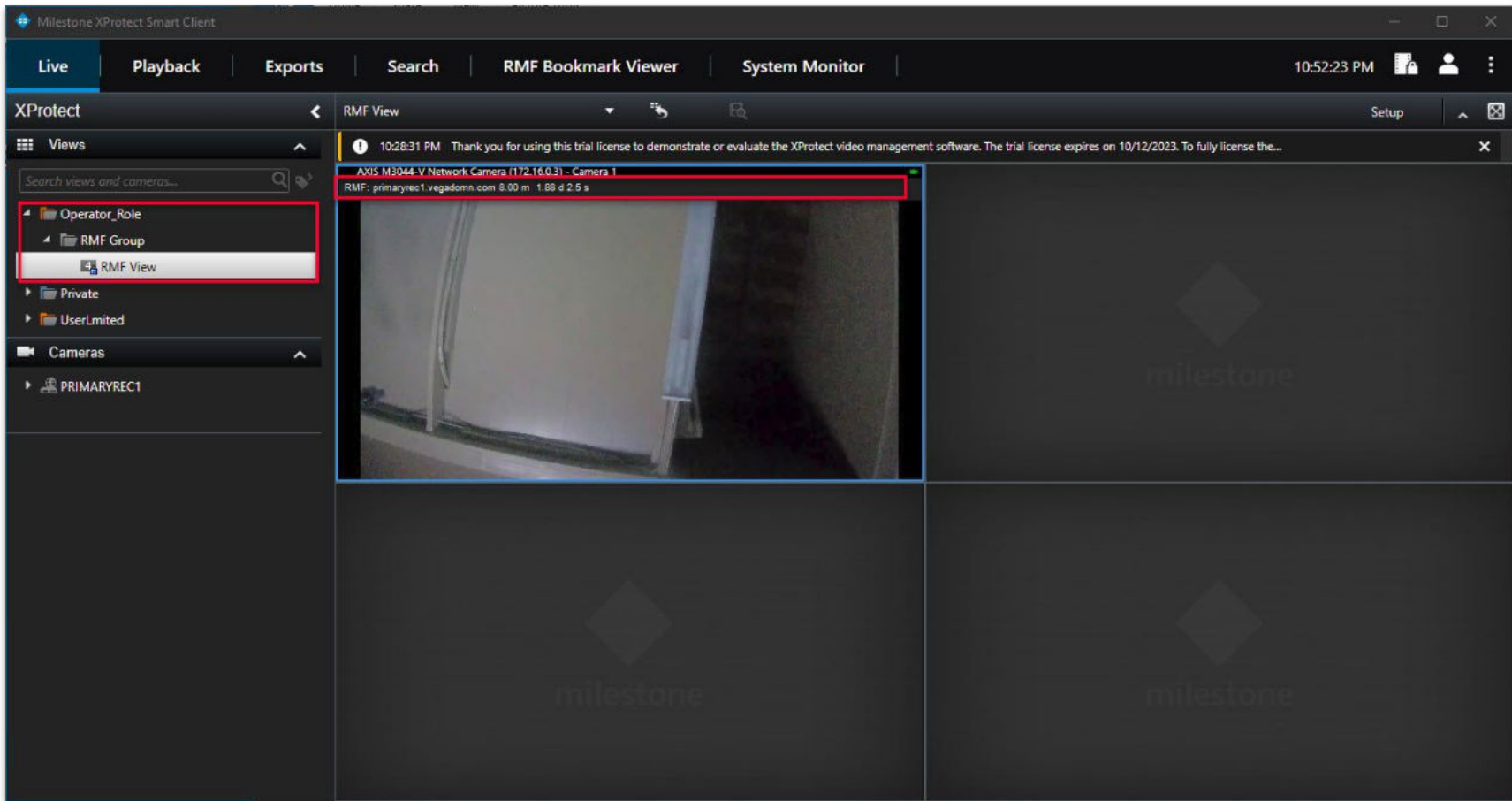
## **Part 4: Verifying live view switching for a permitted user**



**Step 1: Open the Smart Client.**

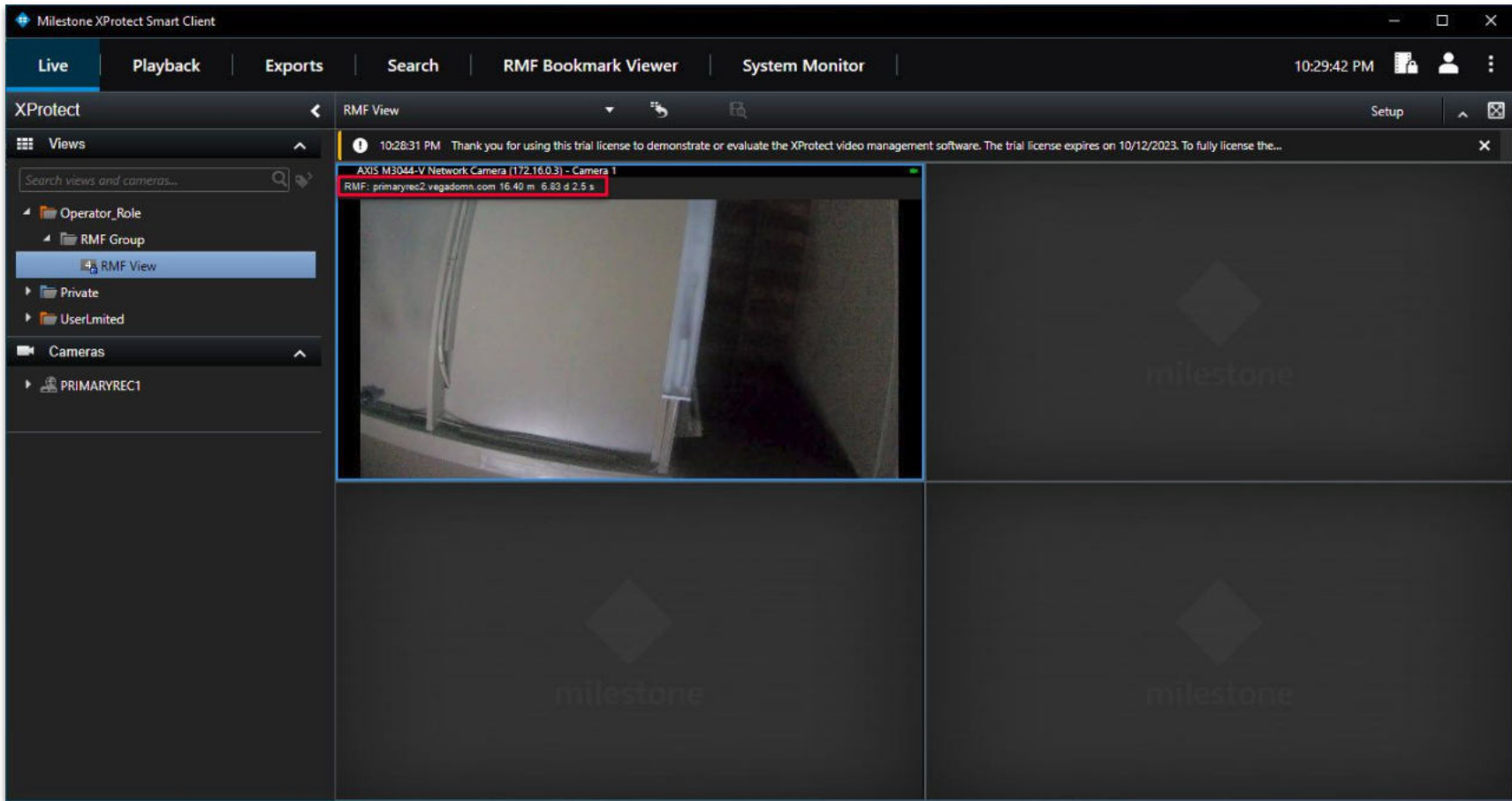
**Login** into the **Parent Management Server** using user credentials which was permitted in the role.(Federated Deployments)

**Login** into **Management Server** using user credentials which was permitted in the role (Non-Federated Deployments)



**Step 2:** Select the **newly created view** from the view group. Verify the live view.  
**Note:** The live view is from parent (**primary**) server.





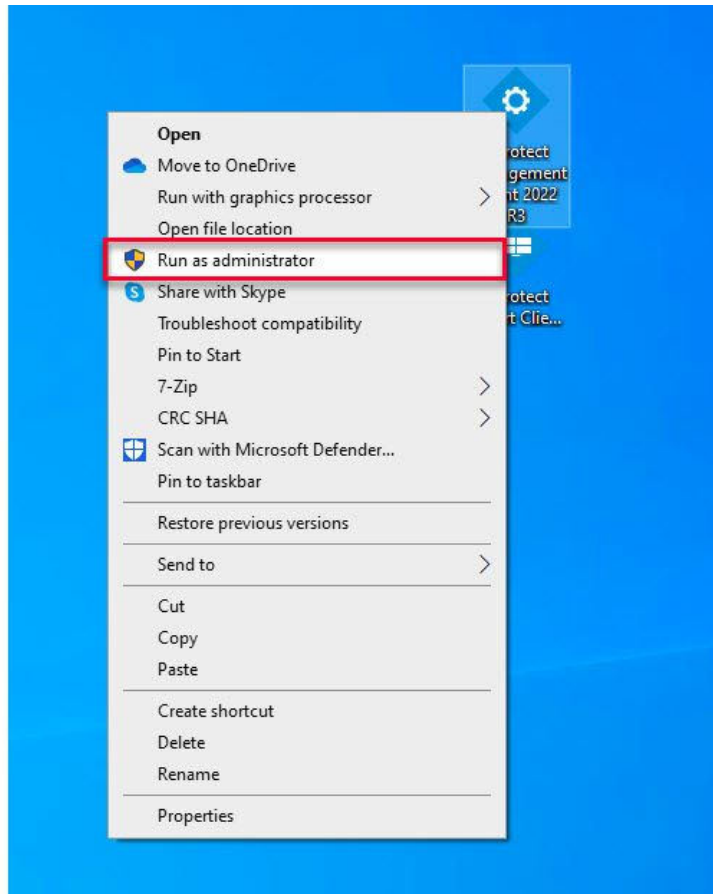
**Step 3:** Stop the parent (**primary**) recording server.  
The live view switches to the child (**secondary**) recording server.





## **Part 5: Setting “Do not skip gaps” from Management Client by admin user**

Note: Setting to “Do not skip gaps”, RMF will look for the missing video on another recording server and proceed to play it.



**Step 1: Open the Management Client.**  
**Note:** Run as administrator



Milestone  
XProtect® Management Client 2022 R3

Computer:  
primaryrec1.vegadomn.com

Authentication:  
Windows authentication

Domain: vegadomn.com

User name:  
vegadomn.com\milestone

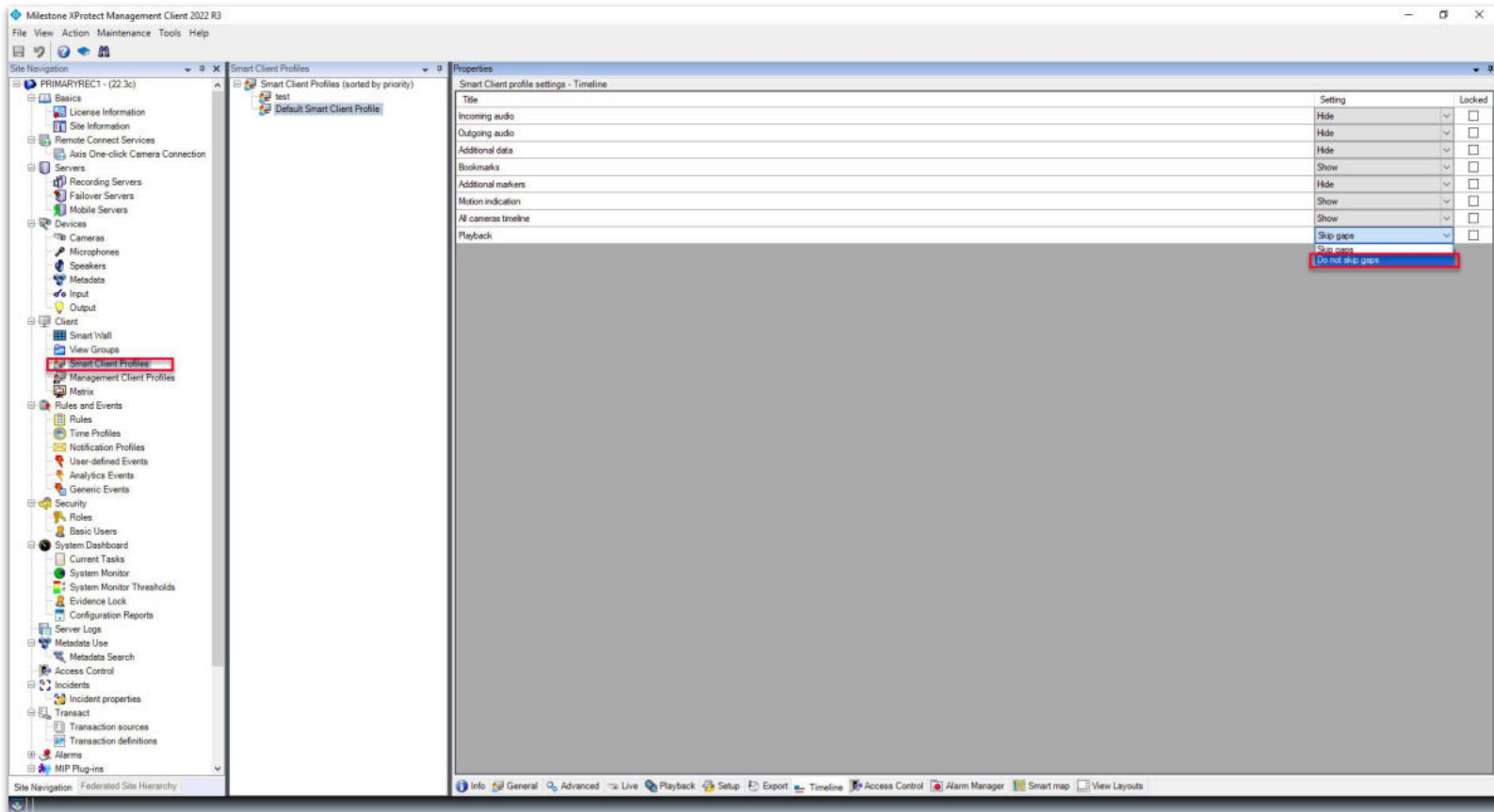
Password:  
•••••••

Remember password

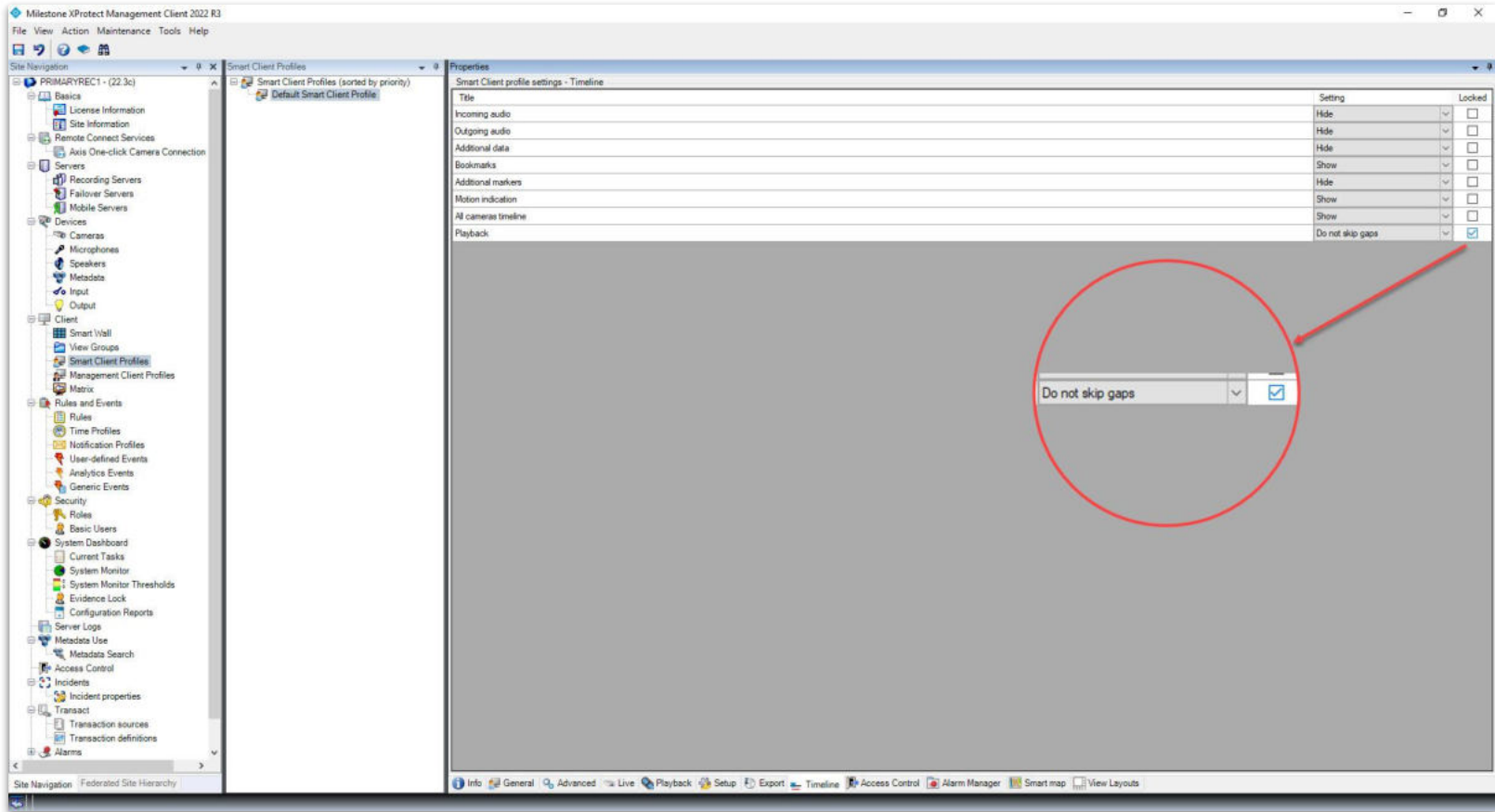
Sign in Close

Management Server

**Step 2:** Login into the **Parent Management Server** as a domain user with admin privileges. (Federated Deployments)  
**Login into Management Server** as a user with admin privileges (Non-Federated Deployments)



**Step 3:** Goto Site Navigation → Client → Smart Client Profiles.  
Select the **Smart Client Profile** associated with the Role. Select Timeline from the bottom toolbar.  
Set to **Do not skip gaps under Playback.**



**Step 4:** Tick the option **Locked** for Playback.

**Note:** Administrators can lock the settings for each role through Smart Client Profiles, users cannot change the setting that is locked.

Milestone XProtect Management Client 2022 R3

File View Action Maintenance Tools Help

Save

PRIMARY (CC1 - (22.3c))

Basics

License Information

Site Information

Remote Connect Services

Axis One-click Camera Connection

Servers

Recording Servers

Follower Servers

Mobile Servers

Devices

Cameras

Microphones

Speakers

Metadata

Input

Output

Client

Smart Vtall

View Groups

Smart Client Profiles

Management Client Profiles

Matrix

Rules and Events

Rules

Time Profiles

Notification Profiles

User-defined Events

Analytics Events

Generic Events

Security

Roles

Basic Users

System Dashboard

Current Tasks

System Monitor

System Monitor Thresholds

Evidence Lock

Configuration Reports

Server Logs

Metadata Use

Metadata Search

Access Control

Incidents

Incident properties

Transact

Transaction sources

Transaction definitions

Alarms

MIP Plug-ins

Site Navigation Federated Site Hierarchy

Smart Client Profiles (sorted by priority)

test

Default Smart Client Profile

File View

Save

Properties

Smart Client profile settings - Timeline

Title	Setting	Locked
Incoming audio	Hide	<input type="checkbox"/>
Outgoing audio	Hide	<input type="checkbox"/>
Additional data	Hide	<input type="checkbox"/>
Bookmarks	Show	<input type="checkbox"/>
Additional markers	Hide	<input type="checkbox"/>
Motion indication	Show	<input type="checkbox"/>
All cameras timeline	Show	<input type="checkbox"/>
Playback	Do not skip gaps	<input type="checkbox"/>

Info General Advanced Live Playback Setup Export Timeline Access Control Alarm Manager Smart map View Layouts

**Step 5:** Click **Save**.

**Note:** “Do not skip gaps” option has to be set for all the SmartClient profiles related to RMF.