MAKE THE
WORLD SEE

August 10 , 2023

White Paper

XProtect® Corporate – Advanced Security Management

Prepared by:

John Rasmussen, Platform Architect

milestone

Table of Content

Introduction

XProtect Corporate is Milestone's high-end video management software (VMS) is designed for large-scale high-security installations.

Large-scale installations often have more than one administrator managing the VMS, and in some cases external contractors handle specific management and maintenance functions such as replacing cameras, managing recording servers or managing a subset of the devices in the VMS.

To support scenarios where multiple administrators are responsible for different or overlapping functional areas of the installation, XProtect Corporate supports the creation of multiple administrator roles wherein the specific management areas and device permissions can be controlled in detail.

Furthermore, with Management Client profiles, XProtect Corporate supports customization of the XProtect Management Client's user interface. This enables optimization of the VMS' management interface for different responsibility areas. The customization is done by removing the parts of the XProtect Management Client interface that is not needed by the administrators in question, making the user interface simpler to navigate and use.

In addition to supporting customizable administrator roles and Management Client profiles, it is possible to further control access to the installation – even for administrators with management rights. This is done by enabling dual authorization for the roles in question. With dual authorization enabled for a role, the users with this role must first authenticate themselves in the XProtect Management Client, and after this they need a second "super" administrator with the '*Authorize users*' rights to log in and authorize their access to the VMS.

With customizable administrator roles, Management Client profiles and dual authorization, XProtect Corporate is the perfect fit for the variated and demanding ways that large-scale high-security installations are managed and maintained.

Purpose and target audience

The purpose of this white paper is to provide insights to the benefits and usage of the advanced roles and permissions functionality in XProtect Corporate. Readers can learn how the roles and permissions, in conjunction with Management Client profiles, can be used to control and tailor access and management permissions, as well as the user interface, to match the specific needs for various levels of VMS administrators.

This white paper should enable the reader to understand how to work with:

- Management Client profiles
- Advanced management permissions

- Inherited device permissions
- Dual authorization
- Time-based permissions

The primary audience for this white paper is individuals or organizations with needs for having their VMS managed by multiple administrators with different responsibilities and permissions. The target group might include (but is not limited to) the following audiences:

- VMS architects and designers
- VMS project consultants
- VMS and IT administrators

The white paper assumes the reader has a general understanding of Milestone's XProtect Corporate VMS and the roles concept in the XProtect Management Client.

Management Client profiles

XProtect Corporate supports customizing the XProtect Management Client to show only the user interface elements needed by a specific administrator role, thus making the XProtect Management Client easier to navigate and use.

The XProtect Management Client is customized in two steps:

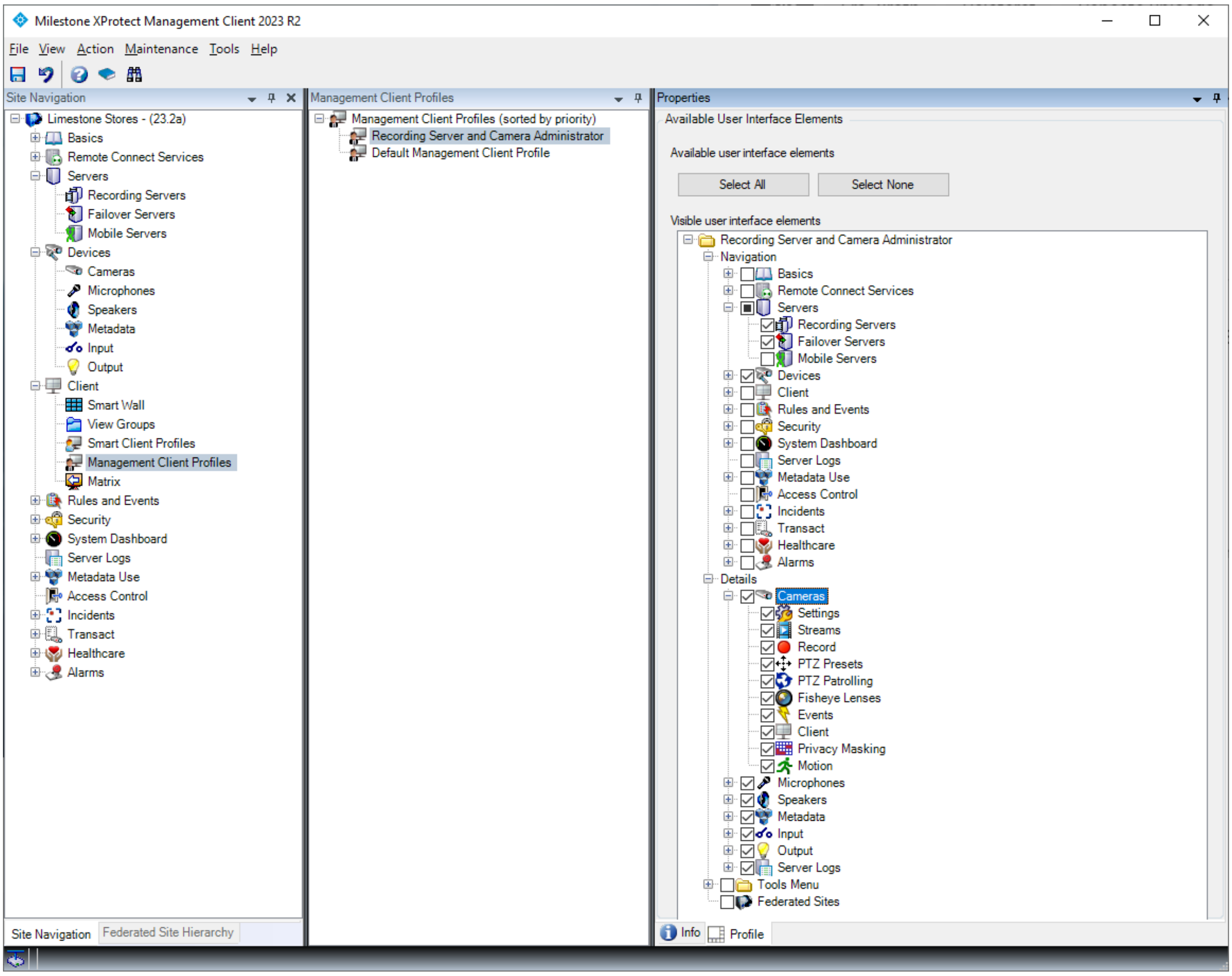
1. Create a Management Client profile, and select which user interface elements should be available
2. In the administrator's role, select the new Management Client profile

Having created a Management Client profile and selected it in the administrators' role, the administrators in that role will only see the user interface elements specifically enabled for them when logging in with the XProtect Management Client. All other elements that are not enabled in the Management Client profile are removed from the XProtect Management Client's user interface which makes it easier to navigate and use since only the needed user interface elements are shown.

Configuration Management Client profiles

Management Client profiles are located under the '*Client*' node in the XProtect Management Client.

When a Management Client profile is selected, the user interface elements that can be turned on or off are shown on the '*Profiles*' tab. Some nodes, like for instance the '*Camera*' node, can be expanded to show futher elements that can be controlled.



Recording Server and Camera Administrator
- Navigation
  - ☐ Basics
  - ☐ Remote Connect Services
  - ■ Servers
    - ☑ Recording Servers
    - ☑ Failover Servers
    - ☐ Mobile Servers
  - ☑ Devices
  - ☐ Client
  - ☐ Rules and Events
  - ☐ Security
  - ☐ System Dashboard
  - ☐ Server Logs
  - ☐ Metadata Use
  - ☐ Access Control
  - ☐ Incidents
  - ☐ Transact
  - ☐ Healthcare
  - ☐ Alarms
- Details
  - ☑ Cameras
    - ☑ Settings
    - ☑ Streams
    - ☑ Record
    - ☑ PTZ Presets
    - ☑ PTZ Patrolling
    - ☑ Fisheye Lenses
    - ☑ Events
    - ☑ Client
    - ☑ Privacy Masking
    - ☑ Motion
  - ☑ Microphones
  - ☑ Speakers
  - ☑ Metadata
  - ☑ Input
  - ☑ Output
  - ☑ Server Logs
- ☐ Tools Menu
- ☐ Federated Sites

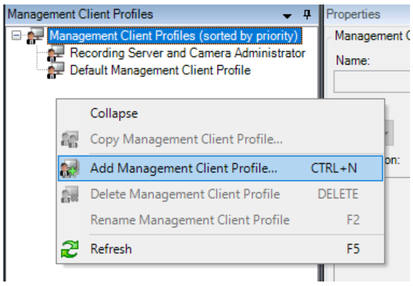
XProtect Management Client
Management Client Profiles node selected – Provides access to recording servers and devices

In above example, the created '*Recording Server and Camera Administrator*' profile provides access to the user interface elements needed to manage recording servers and devices.

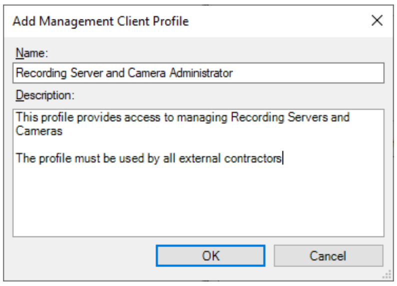
Create a Management Client Profile

To create a Management Client Profile:

1. Right-click the '*Mangement Client Profiles*' pane. and select' *Add Management Client Profile*'
2. Assign a name to it and, optionally, enter a description


Management Client Profiles
Management Client Profiles (sorted by priority)
Recording Server and Camera Administrator
Default Management Client Profile
Properties
Management C
Name:
Collapse
Copy Management Client Profile...
Add Management Client Profile... CTRL+N
Delete Management Client Profile DELETE
Rename Management Client Profile F2
Refresh F5

XProtect Management Client
Management Client Profiles, right-click menu



Name: Recording Server and Camera Administrator

Description: This profile provides access to managing Recording Servers and Cameras

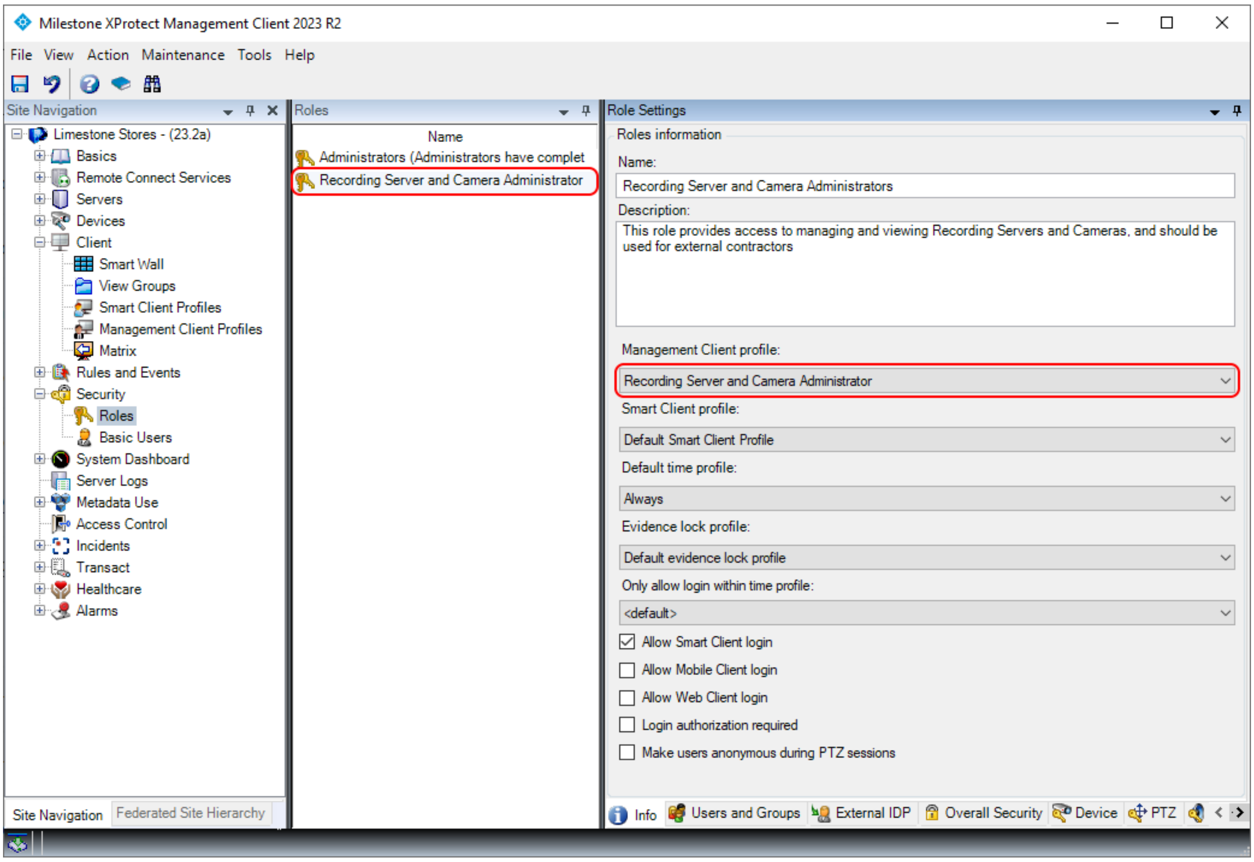
The profile must be used by all external contractors

XProtect Management Client
Management Client Profiles, Add Management Client Profile

By default, new profiles will provide access to all elements in the XProtect Management Client. To limit access to only some user interface elements, simply deselect the functions not needed.

Having created a Management Client profile, the next step is to use it in a role:

1. Create or select a role with management rights
2. In the '*Info*' tab's '*Management Client profile:*' dropdown, select the created profile



Name: Recording Server and Camera Administrators

Description: This role provides access to managing and viewing Recording Servers and Cameras, and should be used for external contractors

Management Client profile: Recording Server and Camera Administrator

Smart Client profile: Default Smart Client Profile

Default time profile: Always

Evidence lock profile: Default evidence lock profile

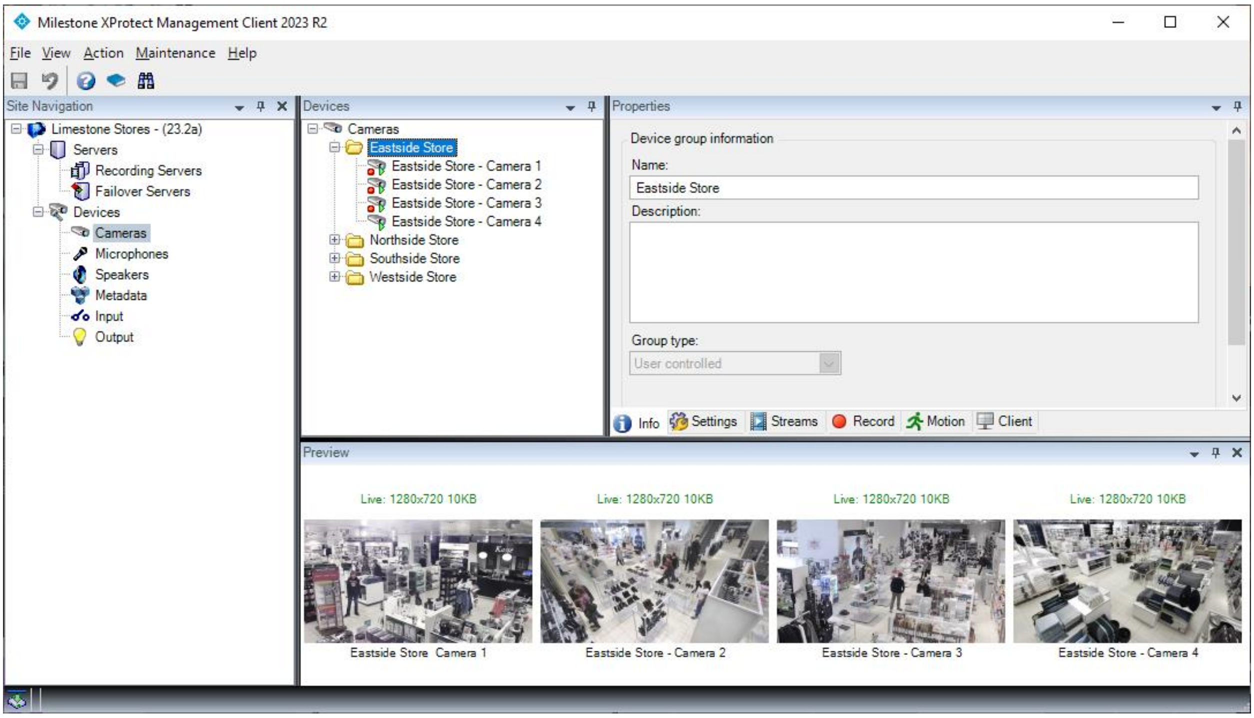
Only allow login within time profile: <default>

☑ Allow Smart Client login
☐ Allow Mobile Client login
☐ Allow Web Client login
☐ Login authorization required
☐ Make users anonymous during PTZ sessions

XProtect Management Client
Selecting a Management Client Profile for a role

When users in this role log in with the XProtect Management Client, it will only show the user interface elements that have been enabled in the Management Client profile. All other elements are removed.

The screenshot below shows how the XProtect Management Client looks with only recording servers and devices enabled in the Management Client profile.



Name: Eastside Store

Description:

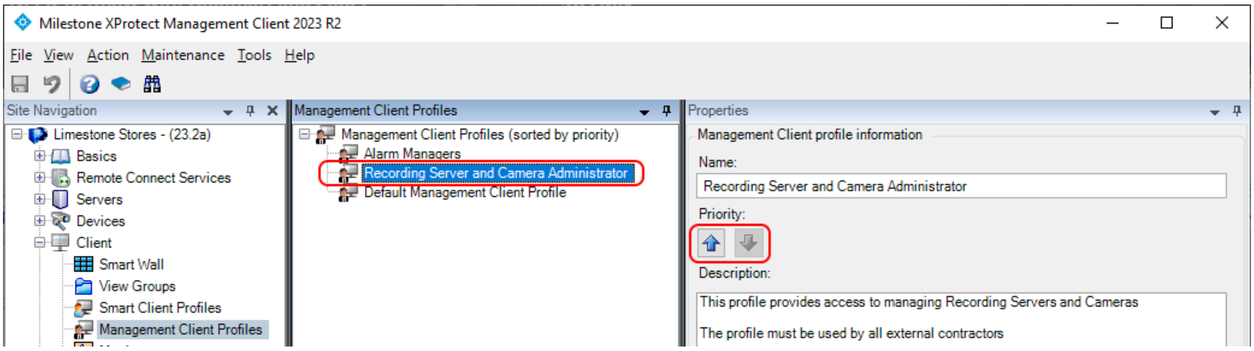
Group type: User controlled

XProtect Management Client
Management Client limited to only show the management interface for recording servers and cameras

Multiple Management Client profiles

If the administrator logging in with the XProtect Management Client is a member of multiple roles configured with different Management Client profiles, the profile with the highest priority will be assigned.

The profile priority is set by changing the order of the Management Client profiles in the '*Management Client Profiles*' pane. The profiles are listed with highest priority at the top, and lowest at the bottom. The priority can be changed by clicking the '*Priority:*' up/down buttons.


Milestone XProtect Management Client 2023 R2
File View Action Maintenance Tools Help
Site Navigation
Limestone Stores - (23.2a)
Basics
Remote Connect Services
Servers
Devices
Client
Smart Wall
View Groups
Smart Client Profiles
Management Client Profiles
Management Client Profiles
Management Client Profiles (sorted by priority)
Alarm Managers
Recording Server and Camera Administrator
Default Management Client Profile
Properties
Management Client profile information

Name: Recording Server and Camera Administrator

Priority:

Description:
This profile provides access to managing Recording Servers and Cameras
The profile must be used by all external contractors

XProtect Management Client
Setting the priority of the Management Client Profiles - highest priority at the top of the list.

Documentation – Management Client profiles

For details on usage of the Management Client profiles, please refer to the documentation which can be found by selecting the '*Management Client Profiles*' node in the XProtect Management Client and pressing '*F1*' on the keyboard. Alternatively, visit Milestone - Documentation; Management Client Profiles

Important Security notice!

Although the Management Client profiles are used to limit administrators access to user interface elements in the XProtect Management Client, it is important to understand that Management Client profiles is not a security permissions feature. It is only a feature for customizing the XProtect Management Client user interface.

This means that from a security perspective, it is not enough to just create a Management Client profile that limit the XProtect Management Client user interface for the administrators. A matching set of actual security permissions must also be set in the administrator's role to ensure that the administrators can manage only what they are supposed to.

The reason for this is that a Management Client profile only removes the user interface elements from the XProtect Management Client. It does not make the VMS servers control and enforce the actual permissions the administrators have. Therefore, if all permissions are allowed in a role where the selected Management Client profile removes user interface elements from the XProtect Management Client, an administrator could use another application than the XProtect Management Client to manage the VMS. For example, using a custom-made 3rd party "Management Tool" developed with the MIP SDK or the VMS API's the administrator can get access to manage areas of the VMS that would otherwise not be available in the XProtect Management Client, due to the set Management Client profile.

Therefore, as described in the next section, the proper thing to do to make sure administrators can only manage what they are supposed to, is to set permissions for the role so it matches the VMS areas and devices they are responcible for. When this is done and the right Management Client profile is selected for the role, the administrators can only manage the VMS areas and devices they have permissions to, no matter what client is used, and the XProtect Management Client user interface will only show the user interface elements needed for it.

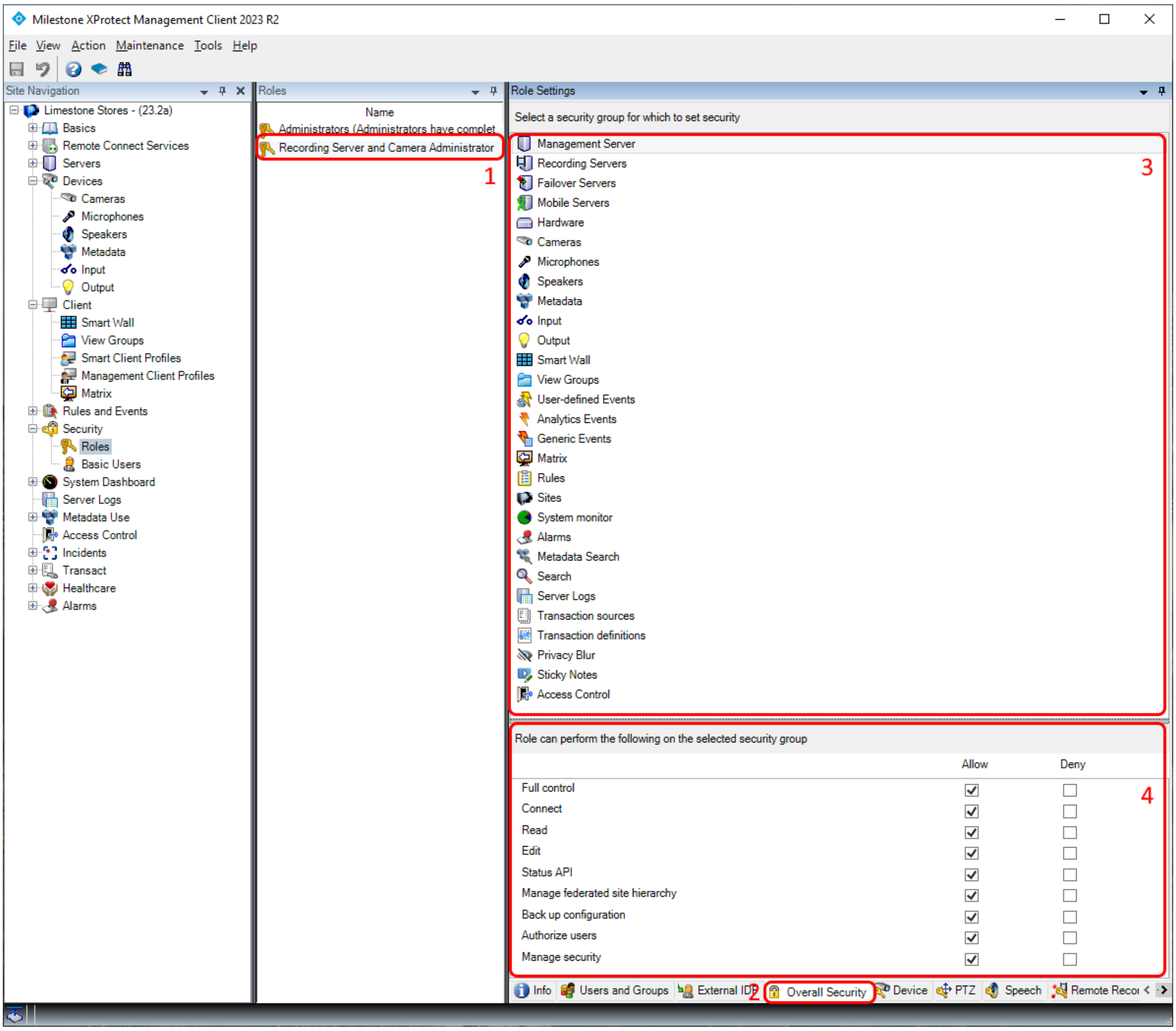
Management Permissions

In addition to the Management Client profiles, XProtect Corporate supports configuring permissions for accessing and managing the VMS, its functions, and the devices in it. In contrast to Management Client profiles which just customizes the user interface, the permissions rigorously control what the administrators actually can access and manage in the VMS. This works in the way that the VMS servers, for every request made, check if the user or the administrator have permissions to access and manage the function or resource in question.

This ensures that users and administrators can only access and manage the different devices and functions in the VMS that they have specifically been granted permissions to, no matter if they use the XProtect Management Client, the MIP SDK or the APIs directly.

Overall Security

The permissions to view and manage the various areas and functions of the VMS are configured by selecting a role (1), and then the '*Overall Security*' tab (2). This will show the security groups in the '*Role Settings*' pane (3). Selecting a security group in the list shows the permissions (4) that can be configured for the selected security group. The permissions available depend on the selected security group.



Milestone XProtect Management Client 2023 R2

Site Navigation

- Limestone Stores - (23.2a)
  - Basics
  - Remote Connect Services
  - 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
  - Server Logs
  - Metadata Use
  - Access Control
  - Incidents
  - Transact
  - Healthcare
  - Alarms

Roles

Name
Administrators (Administrators have complet
Recording Server and Camera Administrator

Role Settings

Select a security group for which to set security

- Management Server
- Recording Servers
- Failover Servers
- Mobile Servers
- Hardware
- Cameras
- Microphones
- Speakers
- Metadata
- Input
- Output
- Smart Wall
- View Groups
- User-defined Events
- Analytics Events
- Generic Events
- Matrix
- Rules
- Sites
- System monitor
- Alarms
- Metadata Search
- Search
- Server Logs
- Transaction sources
- Transaction definitions
- Privacy Blur
- Sticky Notes
- Access Control

Role can perform the following on the selected security group

	Allow	Deny
Full control	☑	□
Connect	☑	□
Read	☑	□
Edit	☑	□
Status API	☑	□
Manage federated site hierarchy	☑	□
Back up configuration	☑	□
Authorize users	☑	□
Manage security	☑	□

XProtect Management Client
Setting '*Overall Security*' for the selected role

Checking '*Allow*' for a function will grant access to the function and checking '*Deny*' will deny access. If the user or administrator is a member of two or more roles with conflicting permissions, deny will take precedence.

When configuring permissions to cameras, microphones, speakers, metadata, input and output, the settings apply to all current devices in the system as well as devices that are added later.

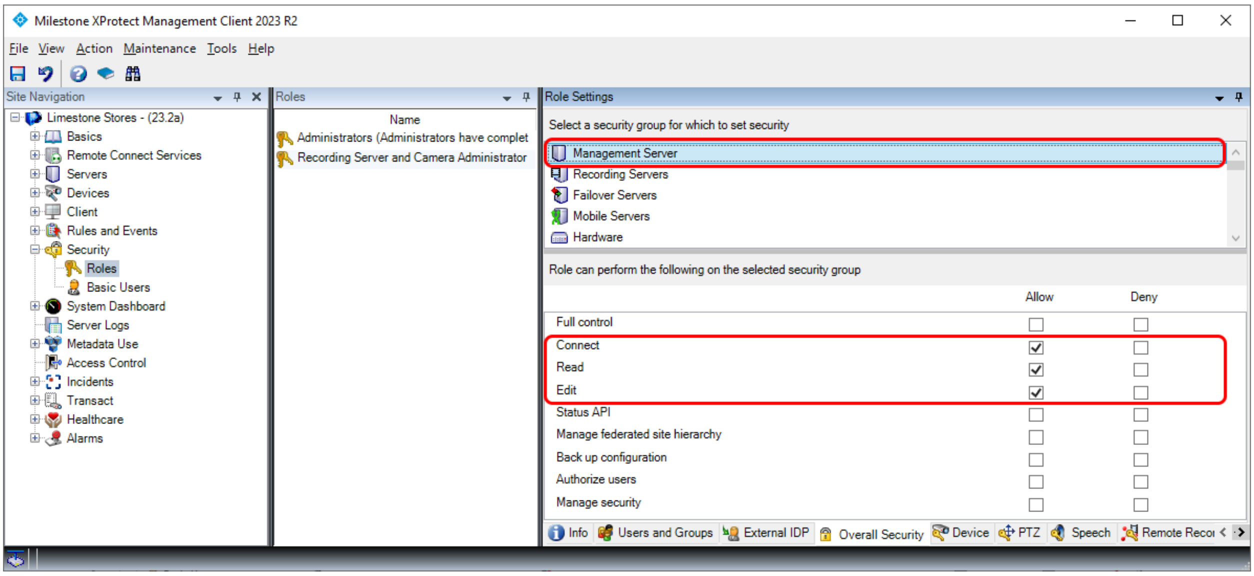
Configuration Example

In the example in the previous Management Client profiles section, an administrator role is configured with a profile that provides access to the Management Client elements for managing recording servers and devices (cameras, microphones, speakers, metadata, input and output) only. However, a matching set of permissions must also be configured for the role to ensure that the VMS servers can check the permissions and only allow access to the various resources and functions that the administrator has permissions to.

The permissions needed to enable administrators to just manage recording servers and devices, are configured on the '*Overall Security*' tab for a role as shown in the screenshots below.

For '*Management Server*', the following must be allowed as they are required to enable the administrator to log in with the Management Client and edit settings:

- '*Connect*'
- '*Read*'
- '*Edit*'



Milestone XProtect Management Client 2023 R2

File View Action Maintenance Tools Help

Site Navigation

- Limestone Stores - (23.2a)
  - Basics
  - Remote Connect Services
  - Servers
  - Devices
  - Client
  - Rules and Events
  - Security
    - Roles
    - Basic Users
  - System Dashboard
  - Server Logs
  - Metadata Use
  - Access Control
  - Incidents
  - Transact
  - Healthcare
  - Alarms

Roles

Name
- Administrators (Administrators have complet
- Recording Server and Camera Administrator

Role Settings

Select a security group for which to set security

- Management Server
- Recording Servers
- Failover Servers
- Mobile Servers
- Hardware

Role can perform the following on the selected security group

	Allow	Deny
Full control	□	□
Connect	☑	□
Read	☑	□
Edit	☑	□
Status API	□	□
Manage federated site hierarchy	□	□
Back up configuration	□	□
Authorize users	□	□
Manage security	□	□

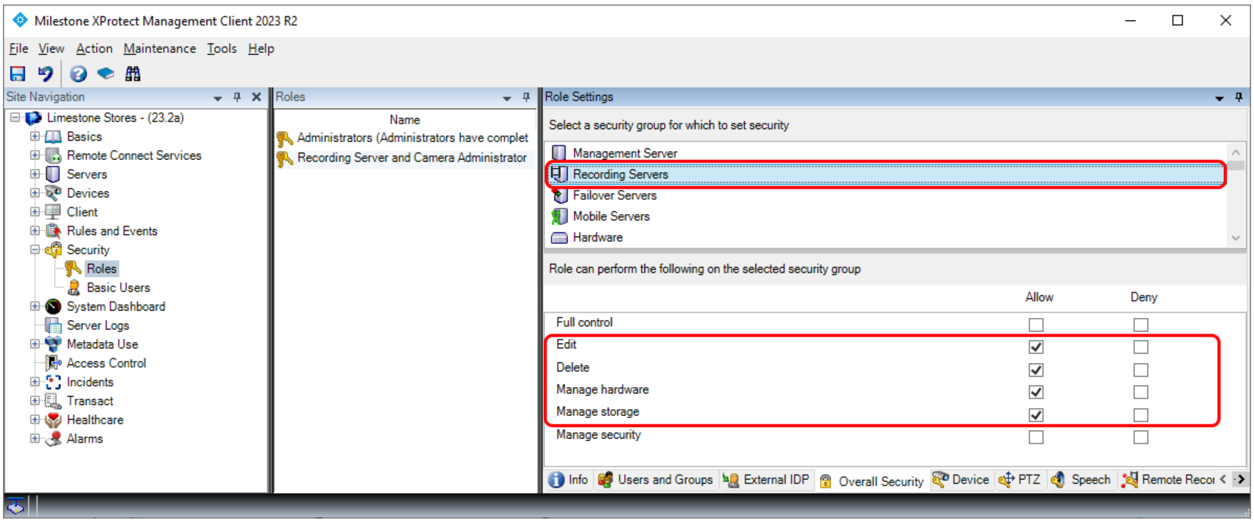
Info | Users and Groups | External IDP | Overall Security | Device | PTZ | Speech | Remote Recor

XProtect Management Client

Setting permissions to '*Management Server*' for the selected role

For '*Recording Server*', the following functions must be allowed:

- '*Edit*'
- '*Delete*'
- '*Manage Hardware*'
- '*Manage Storage*'



Select a security group for which to set security

- Management Server
- Recording Servers
- Failover Servers
- Mobile Servers
- Hardware

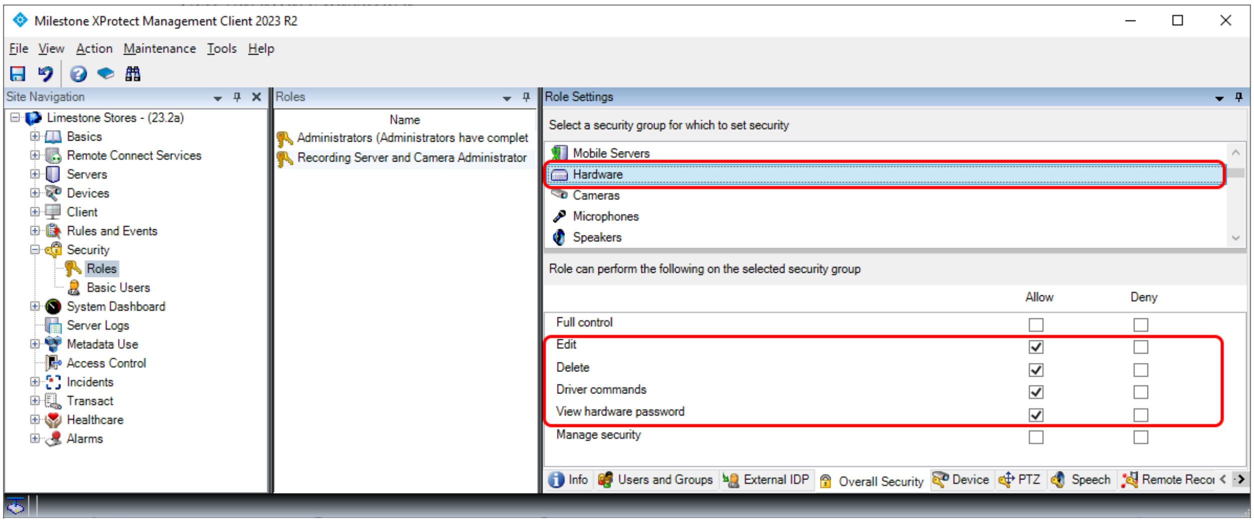
Role can perform the following on the selected security group

	Allow	Deny
Full control	□	□
Edit	☑	□
Delete	☑	□
Manage hardware	☑	□
Manage storage	☑	□
Manage security	□	□

XProtect Management Client
Setting permissions to '*Recording Server*' for the selected role

For '*Hardware*' (devices added to a recording server), the following must be allowed:

- '*Edit*'
- '*Delete*'
- '*Driver commands*'
- '*View hardware password*'



Select a security group for which to set security

- Mobile Servers
- Hardware
- Cameras
- Microphones
- Speakers

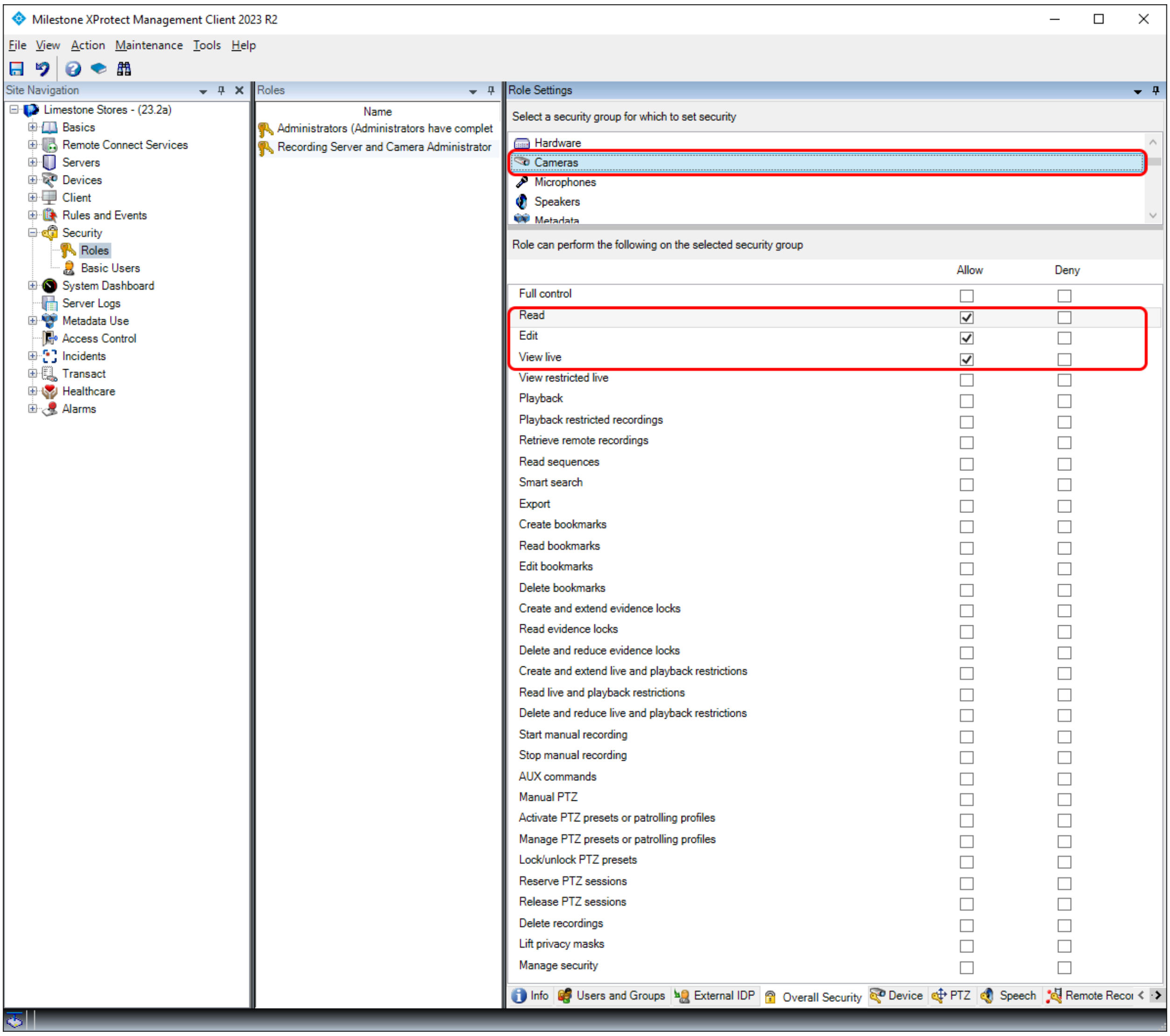
Role can perform the following on the selected security group

	Allow	Deny
Full control	□	□
Edit	☑	□
Delete	☑	□
Driver commands	☑	□
View hardware password	☑	□
Manage security	□	□

XProtect Management Client
Setting permissions to '*Hardware*' for the selected role

For ‘*Cameras*’ and the other device types (not shown with screenshots), the following must be allowed:

- ‘*Read*’
- ‘*Edit*’
- ‘*View live*’



Role can perform the following on the selected security group

	Allow	Deny
Full control	□	□
Read	☑	□
Edit	☑	□
View live	☑	□
View restricted live	□	□
Playback	□	□
Playback restricted recordings	□	□
Retrieve remote recordings	□	□
Read sequences	□	□
Smart search	□	□
Export	□	□
Create bookmarks	□	□
Read bookmarks	□	□
Edit bookmarks	□	□
Delete bookmarks	□	□
Create and extend evidence locks	□	□
Read evidence locks	□	□
Delete and reduce evidence locks	□	□
Create and extend live and playback restrictions	□	□
Read live and playback restrictions	□	□
Delete and reduce live and playback restrictions	□	□
Start manual recording	□	□
Stop manual recording	□	□
AUX commands	□	□
Manual PTZ	□	□
Activate PTZ presets or patrolling profiles	□	□
Manage PTZ presets or patrolling profiles	□	□
Lock/unlock PTZ presets	□	□
Reserve PTZ sessions	□	□
Release PTZ sessions	□	□
Delete recordings	□	□
Lift privacy masks	□	□
Manage security	□	□

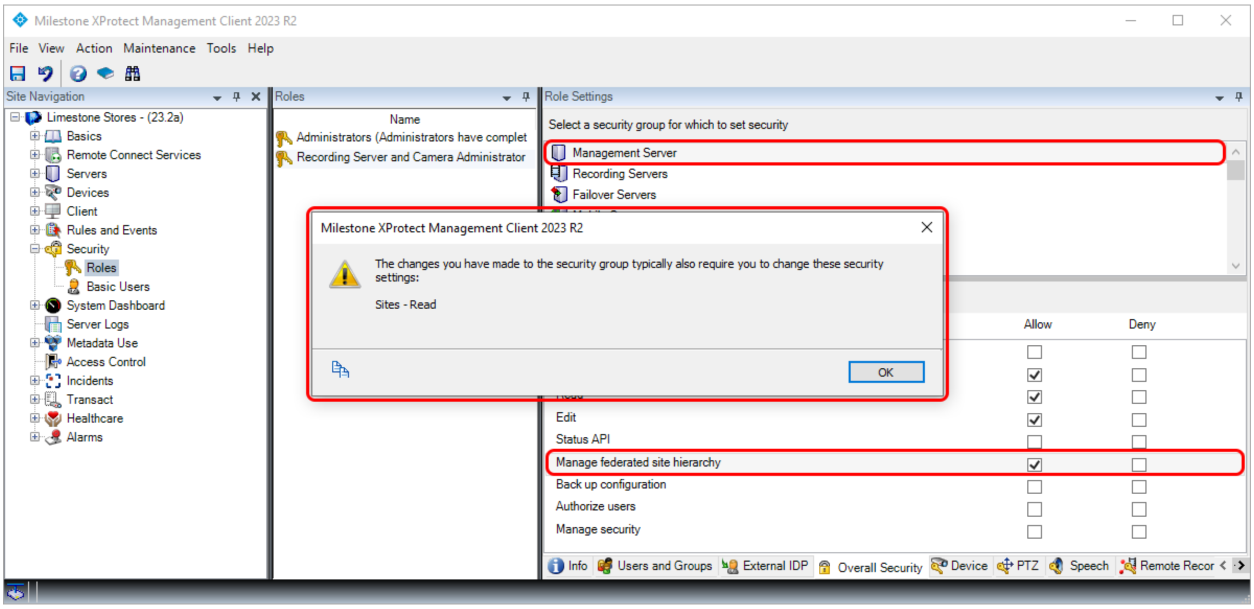
XProtect Management Client
Setting permissions to ‘*Cameras*’ for the selected role

With the above permissions settings set, access to managing the VMS functions and the devices will be checked and enforced by the VMS servers. This ensures that administrators in this role can only manage the specific areas of the VMS that they have been granted permissions to - even if using a custom-made 3rd party “Management Tool” that utilizes the MIP SDK or the VMS APIs.

Permission requirements advice

When certain overall permissions are allowed, the XProtect Management Client will notify the administrator that additional permissions are required to obtain access to the feature.

In the example below, the '*Manage federated site hierarchy*' for the '*Management Server*' has been allowed. However, to be able to manage the federated site hierarchy, the administrator must also have access to read federated sites. If permissions to read sites is not given, the administrator technically has permission to manage the federated site hierarchy, but in fact it will not be possible because the information for the federated sites cannot be read.



Select a security group for which to set security

- Management Server
- Recording Servers
- Failover Servers

Milestone XProtect Management Client 2023 R2

The changes you have made to the security group typically also require you to change these security settings:

Sites - Read

OK

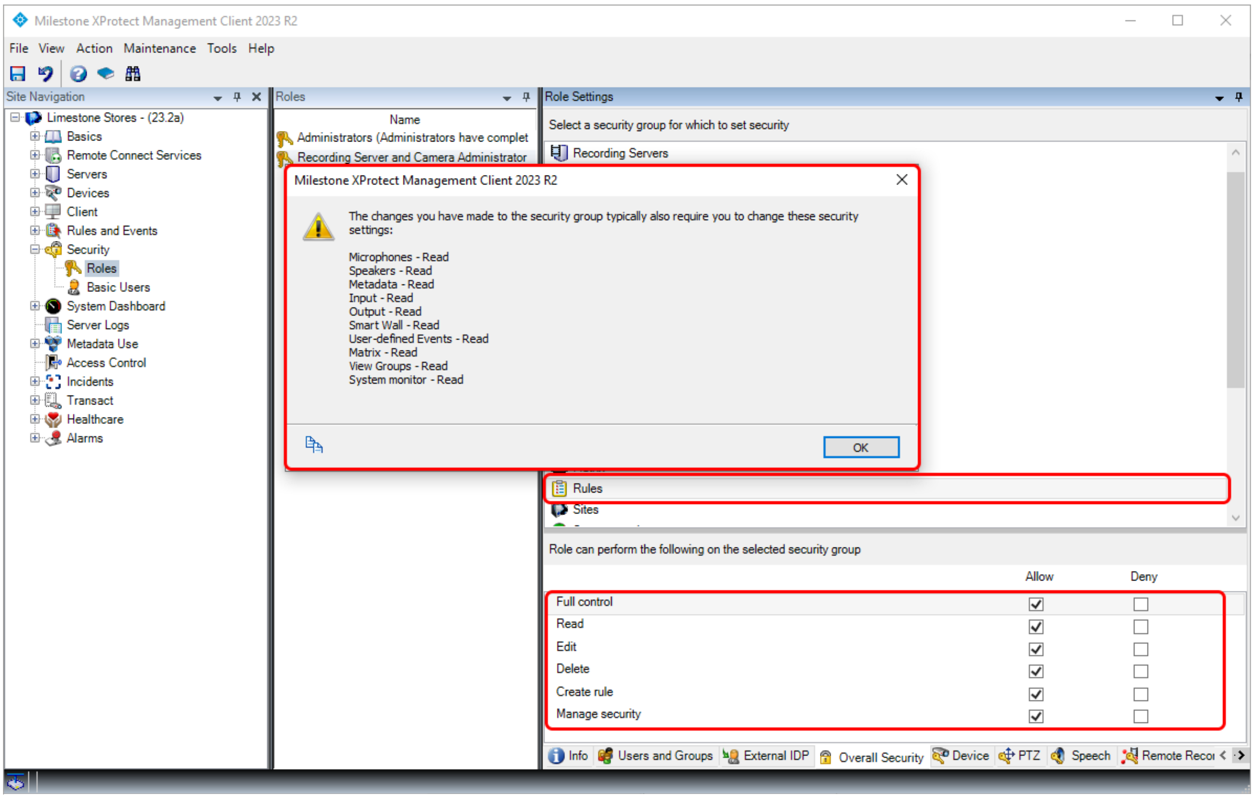
	Allow	Deny
Edit	☑	□
Status API	□	□
Manage federated site hierarchy	☑	□
Back up configuration	□	□
Authorize users	□	□
Manage security	□	□

XProtect Management Client
Notification of missing permissions

In the example above, the missing permissions are enabled by selecting the '*Sites*' node and allow '*Read*' (not shown in a screenshot).

Another case where the XProtect Management Client will notify the administrator that more permissions may be needed is when setting permissions to work with rules.

In this case, the administrator needs additional permissions to configure the rules. This is because rules can be trigged on events from several types of sources and can trigger various VMS actions. If the administrator lacks read permissions to event sources and to the VMS features that are triggered by the events, then it's technically possible for the administrator to manage rules but not to select triggering events and set actions to perform - making it impossible to properly manage rules.



Milestone XProtect Management Client 2023 R2

The changes you have made to the security group typically also require you to change these security settings:

Microphones - Read
Speakers - Read
Metadata - Read
Input - Read
Output - Read
Smart Wall - Read
User-defined Events - Read
Matrix - Read
View Groups - Read
System monitor - Read

OK

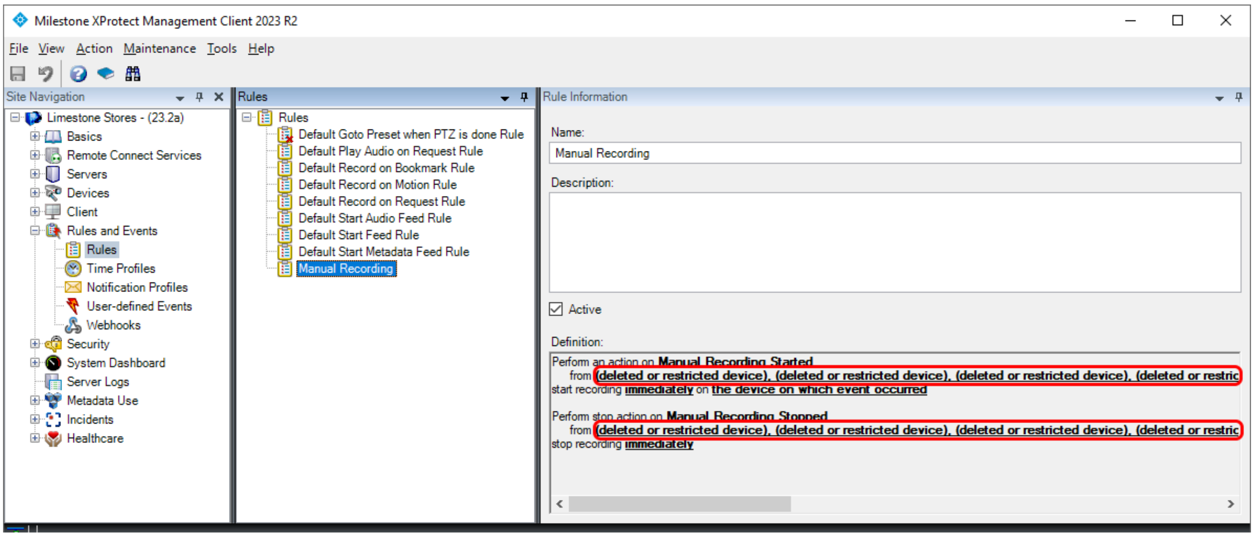
Role can perform the following on the selected security group

	Allow	Deny
Full control	☑	□
Read	☑	□
Edit	☑	□
Delete	☑	□
Create rule	☑	□
Manage security	☑	□

XProtect Management Client
Notification of missing permissions

That said, it may be desired to only grant the administrator permissions to a subset of sources and features as it is then possible to limit the sources and actions that the administrator can work with in the rule. For example, the administrator's permissions could be limited to rules for a specific group of cameras.

If an administrator attempts to work with a rule that includes cameras, that are not covered by the administrator's read permissions, the sources are listed as: '*(deleted or restricted device)*'.


Milestone XProtect Management Client 2023 R2
File View Action Maintenance Tools Help
Site Navigation
Limestone Stores - (23.2a)
Basics
Remote Connect Services
Servers
Devices
Client
Rules and Events
Rules
Time Profiles
Notification Profiles
User-defined Events
Webhooks
Security
System Dashboard
Server Logs
Metadata Use
Incidents
Healthcare
Rules
Rules
Default Goto Preset when PTZ is done Rule
Default Play Audio on Request Rule
Default Record on Bookmark Rule
Default Record on Motion Rule
Default Record on Request Rule
Default Start Audio Feed Rule
Default Start Feed Rule
Default Start Metadata Feed Rule
Manual Recording
Rule Information

Name:
Manual Recording

Description:

☑ Active

Definition:

Perform an action on **Manual Recording Started**
from **(deleted or restricted device), (deleted or restricted device), (deleted or restricted device), (deleted or restric**
start recording **immediately** on **the device on which event occurred**

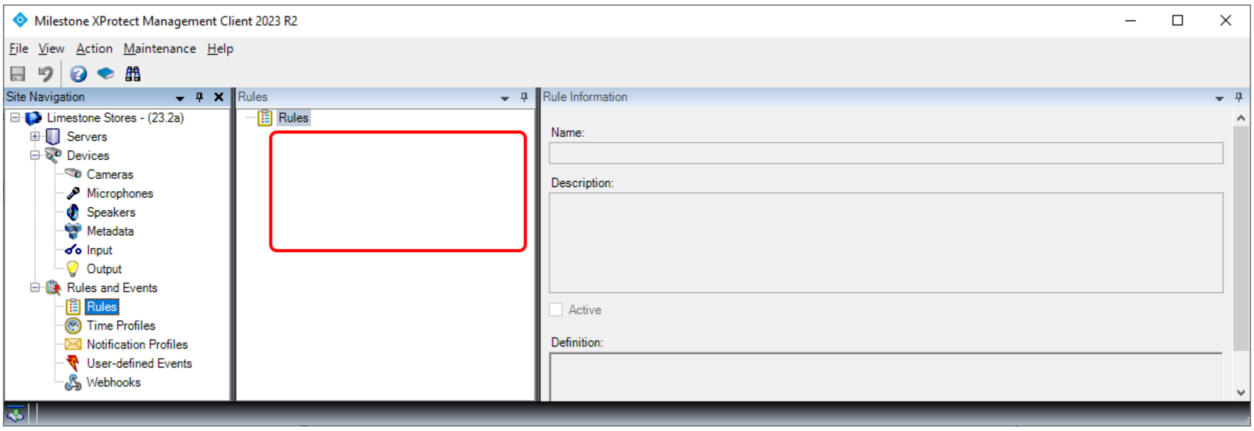
Perform stop action on **Manual Recording Stopped**
from **(deleted or restricted device), (deleted or restricted device), (deleted or restricted device), (deleted or restric**
stop recording **immediately**

XProtect Management Client
Rule details indicating missing permissions to read devices (or indicating deleted devices)

The reason why the rule shows the device name as '(*deleted or restricted device)*' and not as either "deleted" or "restricted" is that the Management Client's request to resolve the device ID to its name results in the same answer from the VMS – "device not found". Therefore, the XProtect Management Client does not know if this is because of missing device permissions or if the device has been deleted.

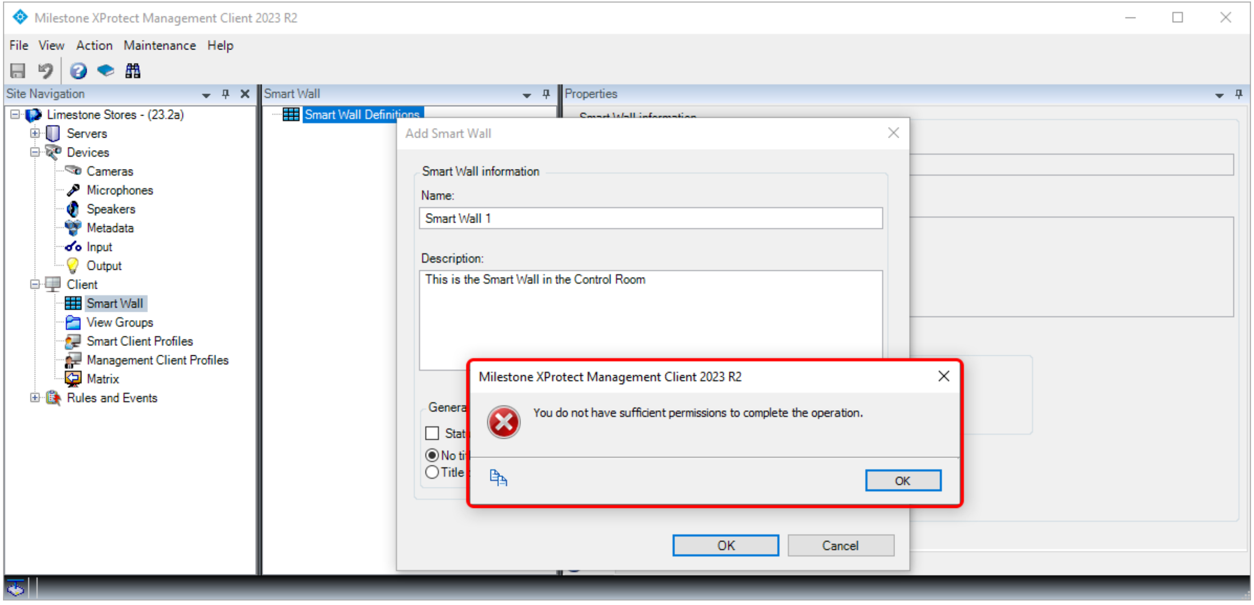
Missing permission handling

If there is a difference between the Management Client profile and the permissions in the role, the administrator may, in the XProtect Management Client, see empty dialogs, lists or settings as shown in the screenshot below. The administrator in the example has the ability to view rules enabled in the Management Client profile, but does not have security permission to read rules.



XProtect Management Client
Defined rules are not shown because the administrator lacks permissions to read rules

When trying to administrate settings, features or devices, that the administrator does not have permissions for, the XProtect Management Client will display an error message with information about the insufficient permissions for this management operation.



Name: Smart Wall 1

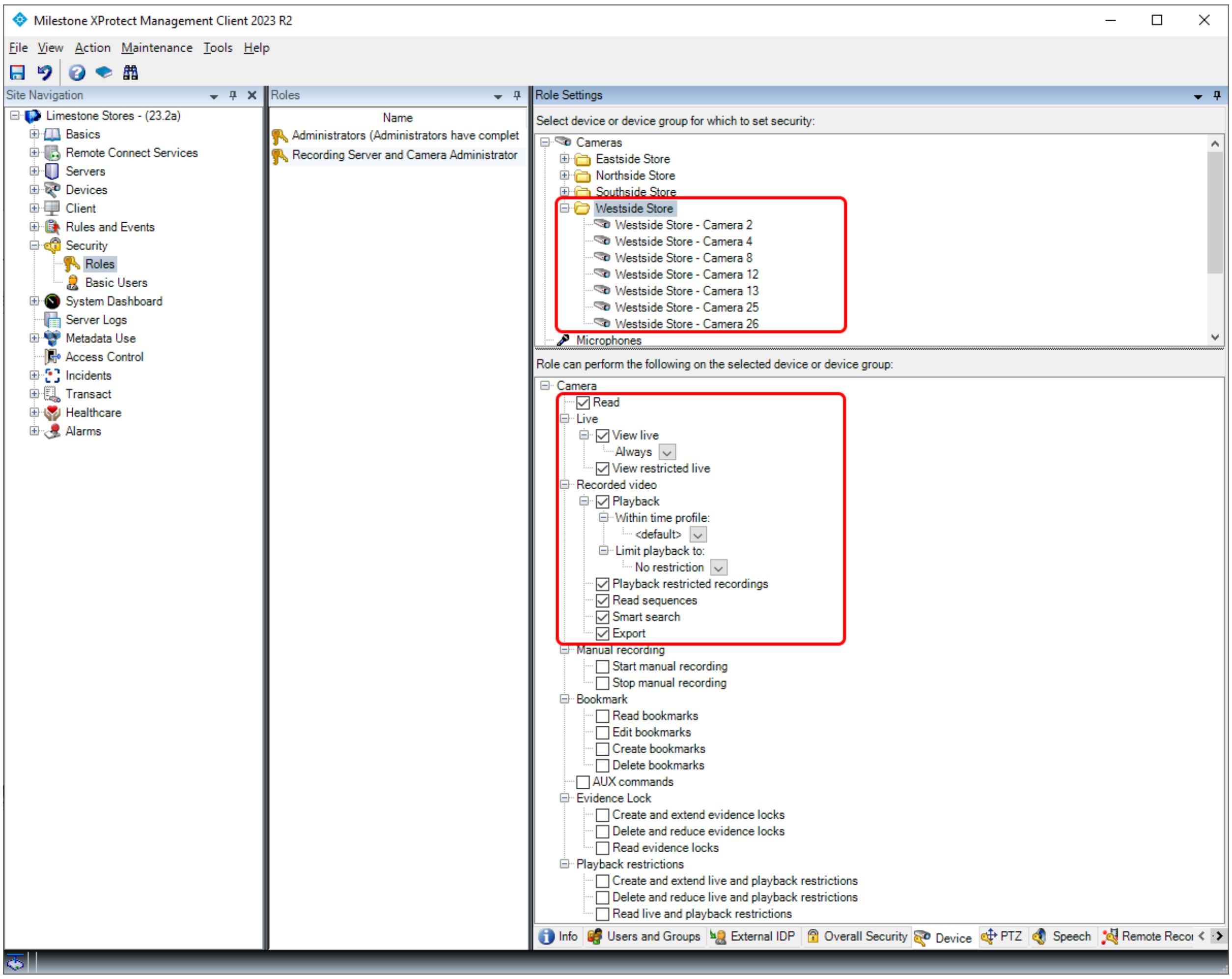
Description: This is the Smart Wall in the Control Room

You do not have sufficient permissions to complete the operation.

XProtect Management Client
Missing permissions to edit (and thus also create) Smart Walls

Individual device permission

In addition to setting the device permission on the '*Overall Security*' tab, it is also possible to set permissions for viewing and managing individual devices. This is done on the '*Device*' tab. Here permissions can be set for a group of devices or for an individual device.



Select device or device group for which to set security:

- Cameras
  - Eastside Store
  - Northside Store
  - Southside Store
  - Westside Store
    - Westside Store - Camera 2
    - Westside Store - Camera 4
    - Westside Store - Camera 8
    - Westside Store - Camera 12
    - Westside Store - Camera 13
    - Westside Store - Camera 25
    - Westside Store - Camera 26
- Microphones

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

- Camera
  - ☑ Read
  - Live
    - ☑ View live
      - Always
    - ☑ View restricted live
  - Recorded video
    - ☑ Playback
      - Within time profile:
        - <default>
      - Limit playback to:
        - No restriction
    - ☑ 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
    - □ Delete and reduce live and playback restrictions
    - □ Read live and playback restrictions

XProtect Management Client

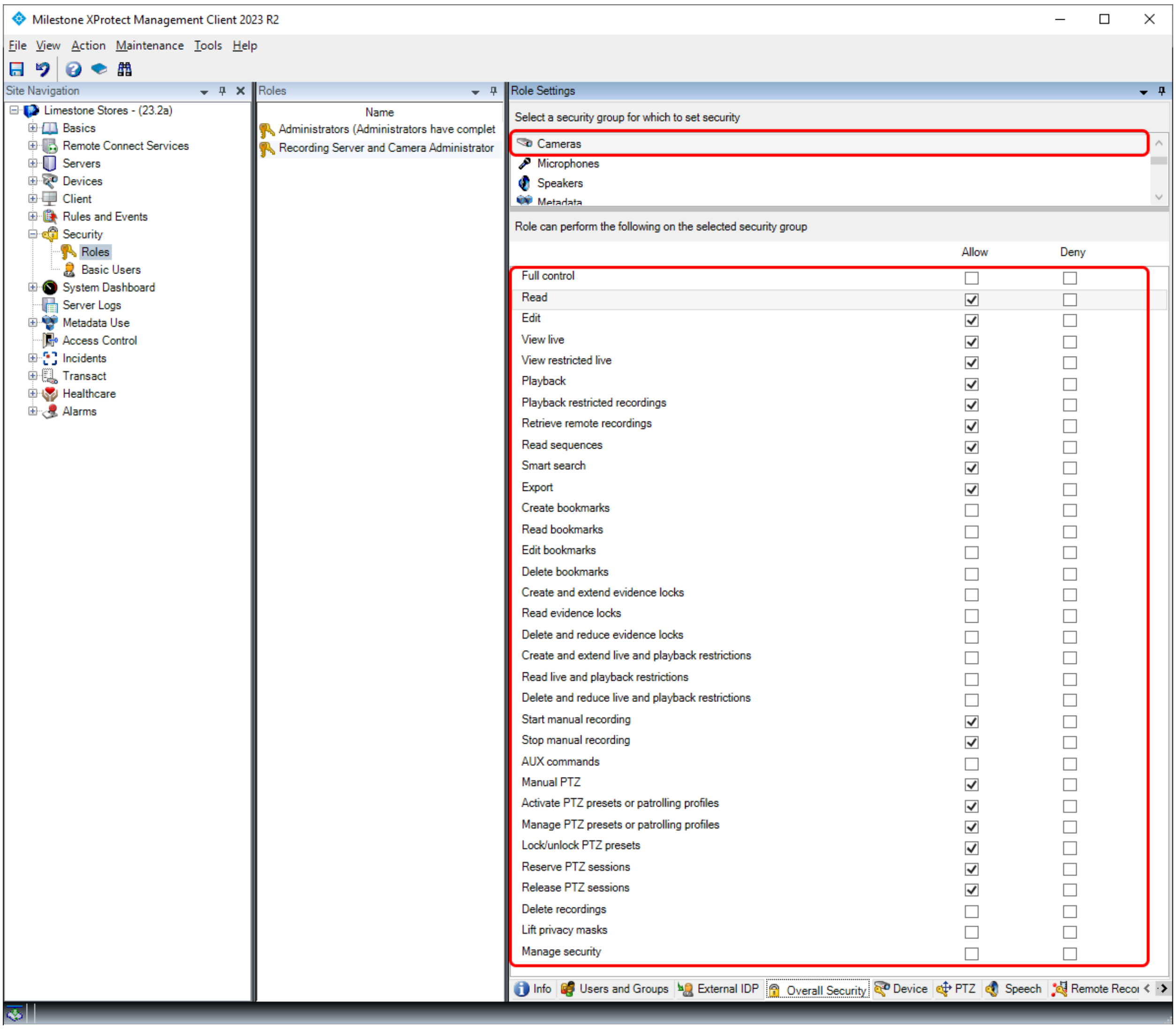
Individual device permissions – '*Read*' and '*View live*' set for a group of cameras

Inherited device permissions

When setting '*Allow*' or '*Deny*' permissions for devices, for instance cameras, on the '*Overall Security*' tab, the permissions are inherited by all devices of this type in the VMS.

Allow permission

In the example below, permissions have been set to '*Allow*' for some of the camera functions.



Select a security group for which to set security

- Cameras
- Microphones
- Speakers
- Metadata

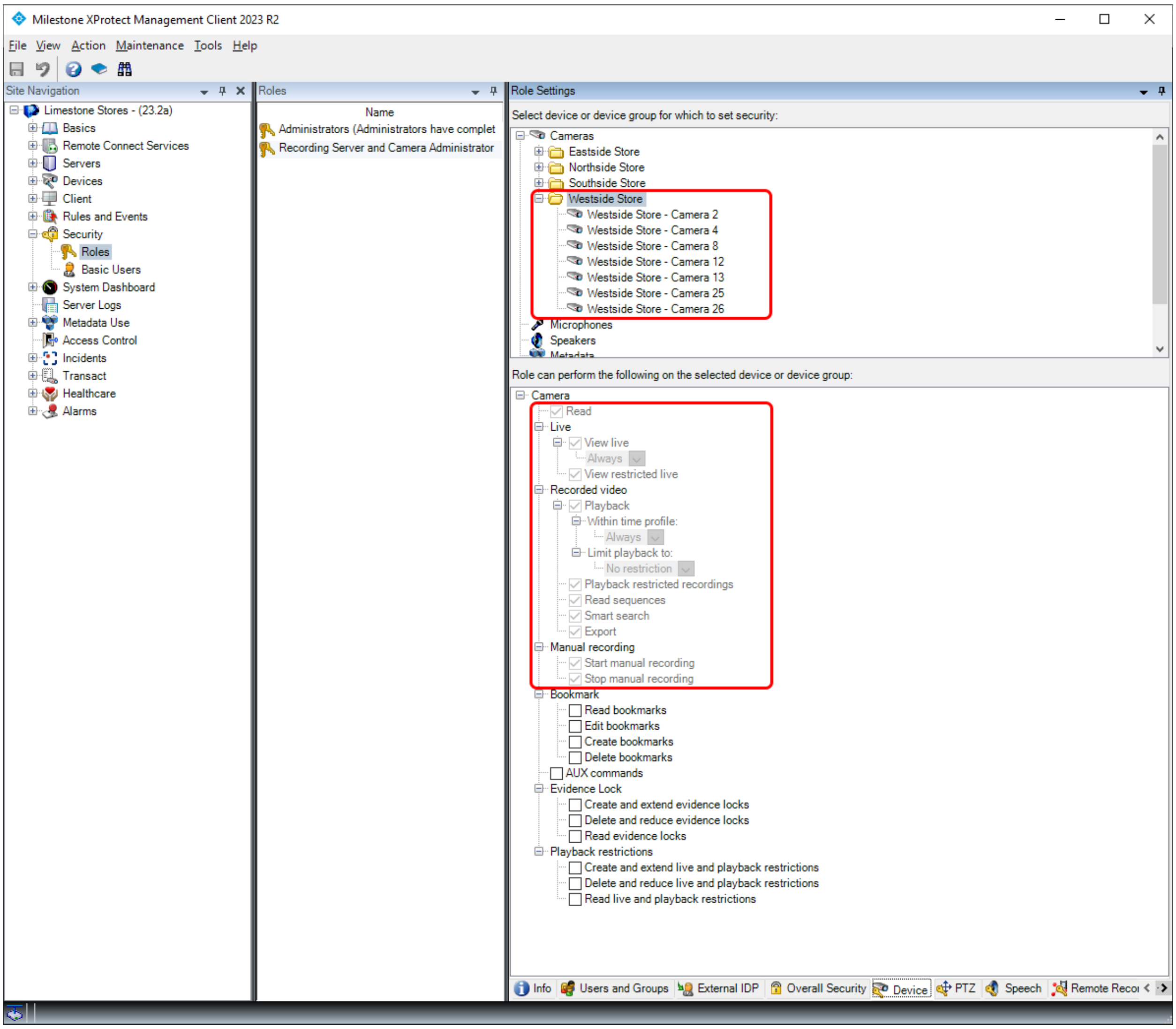
Role can perform the following on the selected security group

	Allow	Deny
Full control	☐	☐
Read	☑	☐
Edit	☑	☐
View live	☑	☐
View restricted live	☑	☐
Playback	☑	☐
Playback restricted recordings	☑	☐
Retrieve remote recordings	☑	☐
Read sequences	☑	☐
Smart search	☑	☐
Export	☑	☐
Create bookmarks	☐	☐
Read bookmarks	☐	☐
Edit bookmarks	☐	☐
Delete bookmarks	☐	☐
Create and extend evidence locks	☐	☐
Read evidence locks	☐	☐
Delete and reduce evidence locks	☐	☐
Create and extend live and playback restrictions	☐	☐
Read live and playback restrictions	☐	☐
Delete and reduce live and playback restrictions	☐	☐
Start manual recording	☑	☐
Stop manual recording	☑	☐
AUX commands	☐	☐
Manual PTZ	☑	☐
Activate PTZ presets or patrolling profiles	☑	☐
Manage PTZ presets or patrolling profiles	☑	☐
Lock/unlock PTZ presets	☑	☐
Reserve PTZ sessions	☑	☐
Release PTZ sessions	☑	☐
Delete recordings	☐	☐
Lift privacy masks	☐	☐
Manage security	☐	☐

XProtect Management Client
Overall Security – '*Allow*' set for some of the camera functions

Having set the camera permissions for the role in the '*Overall Security*' tab. The '*Allow*' permissions are now inherited by all cameras currently added to the VMS as well as cameras that may be added to the VMS later.

This can be seen by selecting the '*Device*' tab, where the camera permissions set to '*Allow*' on the '*Overall Security*' tab, are now checked and greyed out for all cameras.



Select device or device group for which to set security:

- Cameras
  - Eastside Store
  - Northside Store
  - Southside Store
  - Westside Store
    - Westside Store - Camera 2
    - Westside Store - Camera 4
    - Westside Store - Camera 8
    - Westside Store - Camera 12
    - Westside Store - Camera 13
    - Westside Store - Camera 25
    - Westside Store - Camera 26
- Microphones
- Speakers
- Metadata

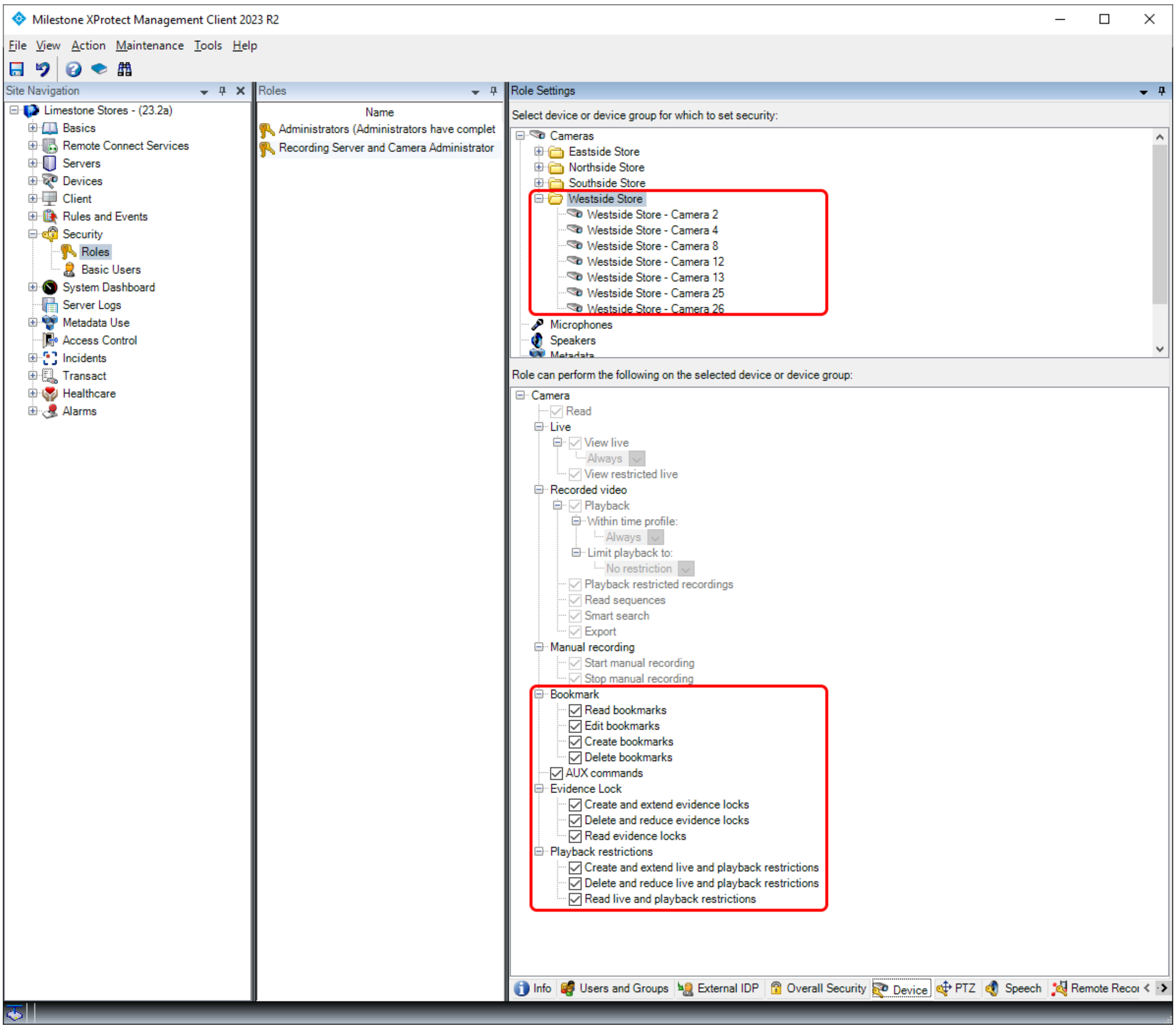
Role can perform the following on the selected device or device group:

- Camera
  - ☑ Read
  - Live
    - ☑ View live
      - Always
    - ☑ View restricted live
  - Recorded video
    - ☑ Playback
      - Within time profile:
        - Always
      - Limit playback to:
        - No restriction
    - ☑ 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
    - □ Delete and reduce live and playback restrictions
    - □ Read live and playback restrictions

XProtect Management Client

Allow permissions inherited by the cameras and shown as checked and read only

Settings not defined as either '*Allow*' or '*Deny*' on the '*Overall Security*' tab can be set individually per group or per individual camera.



Site Navigation:

- Limestone Stores - (23.2a)
  - Basics
  - Remote Connect Services
  - Servers
  - Devices
  - Client
  - Rules and Events
  - Security
    - Roles
    - Basic Users
  - System Dashboard
  - Server Logs
  - Metadata Use
  - Access Control
  - Incidents
  - Transact
  - Healthcare
  - Alarms

Roles (Name):

- Administrators (Administrators have complet
- Recording Server and Camera Administrator

Select device or device group for which to set security:

- Cameras
  - Eastside Store
  - Northside Store
  - Southside Store
  - Westside Store
    - Westside Store - Camera 2
    - Westside Store - Camera 4
    - Westside Store - Camera 8
    - Westside Store - Camera 12
    - Westside Store - Camera 13
    - Westside Store - Camera 25
    - Westside Store - Camera 26
- Microphones
- Speakers
- Metadata

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

- Camera
  - ☑ Read
  - Live
    - ☑ View live
      - Always
    - ☑ View restricted live
  - Recorded video
    - ☑ Playback
      - Within time profile:
        - Always
      - Limit playback to:
        - No restriction
    - ☑ 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
    - ☑ Delete and reduce live and playback restrictions
    - ☑ Read live and playback restrictions

XProtect Management Client
Permissions not set to either '*Allow*' or '*Deny*' can be set individually per group or per camera

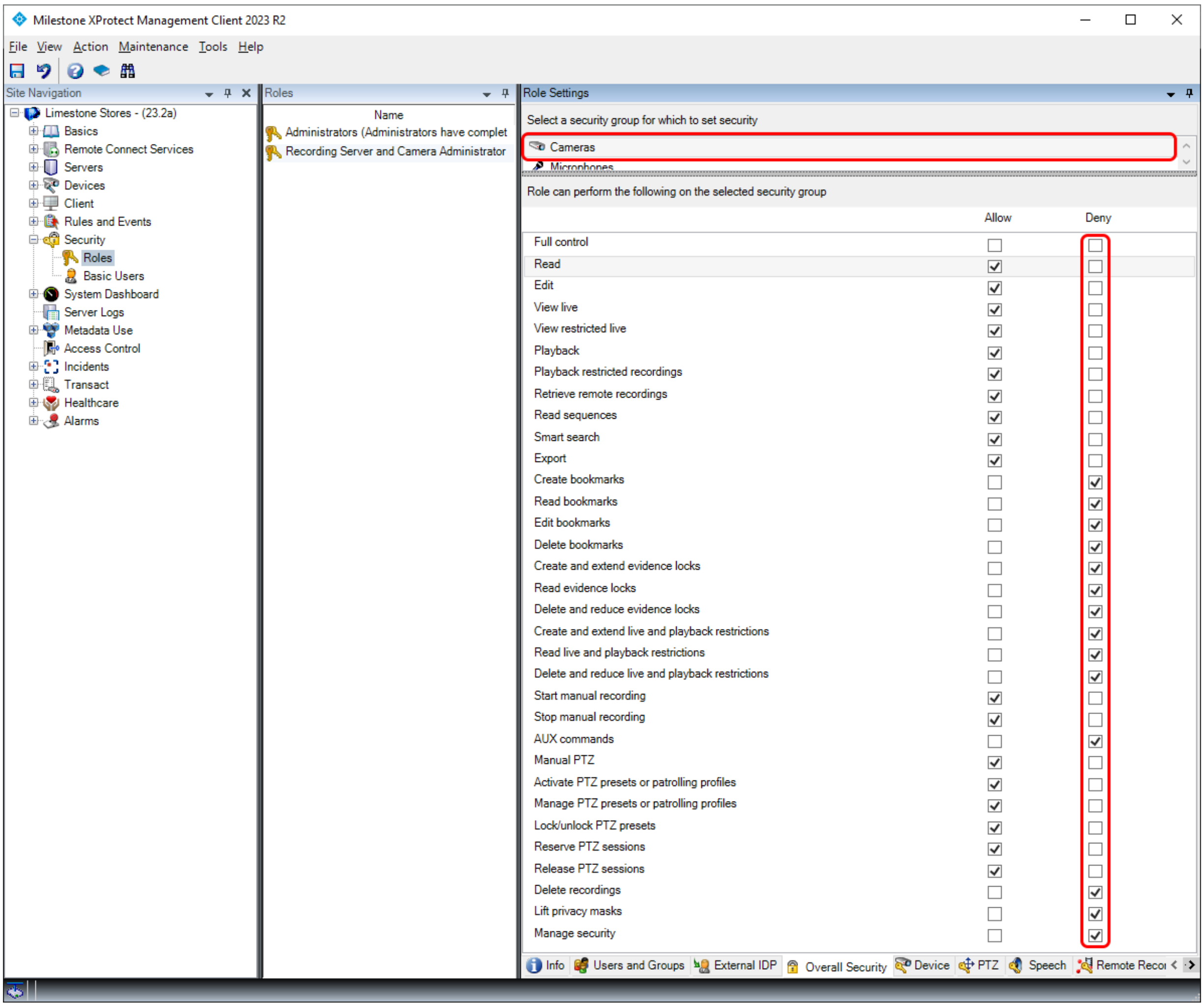
Deny permission and multiple roles

In addition to the '*Allow*' permission, XProtect Corporate supports a '*Deny*' permission. The '*Deny*' permission can be used to override the '*Allow*' permission in cases where users or administrators are members of multiple roles and, via the combined '*Allow*' permissions in the roles, gain access to more functions than they should.

To make it easier to understand how permissions across roles are combined for users or administrators that are members of multiple roles, the following examples will illustrate it for various scenarios:

- If the '*Allow*' permission is set for some specific cameras on the '*Device*' tab in one role and nothing is selected in another role, the users or administrators will be able to access the cameras for which the '*Allow*' permission is set
- If the '*Allow*' permission is set for '*Cameras*' on the '*Overall* Security' tab in one role and nothing is selected in another role, the users or administrators will be able to access all cameras
- If the '*Allow*' permission is set for '*Cameras*' on the '*Overall* Security' tab in one role, but set to '*Deny*' on the '*Overall* Security' tab in another role, the users or administrators will not be able to access any cameras, as '*Deny*' overrides the '*Allow*' permission
- If the 'Allow' permission is set for some specific cameras on the 'Device' tab in one role, but set to 'Deny' on the 'Overall Security' tab in another role, the users or administrators will not be able to access any cameras, as 'Deny' overrides the 'Allow' permission

Therefore, by creating an extra role with '*Deny*' set for the unwanted permissions and by adding the users or administrators to this role, the unwanted permissions can be removed for the users or administrators. This can be utilized to permanently or temporarily deny users or administrators access to functions and device types, that they would otherwise be able to access.



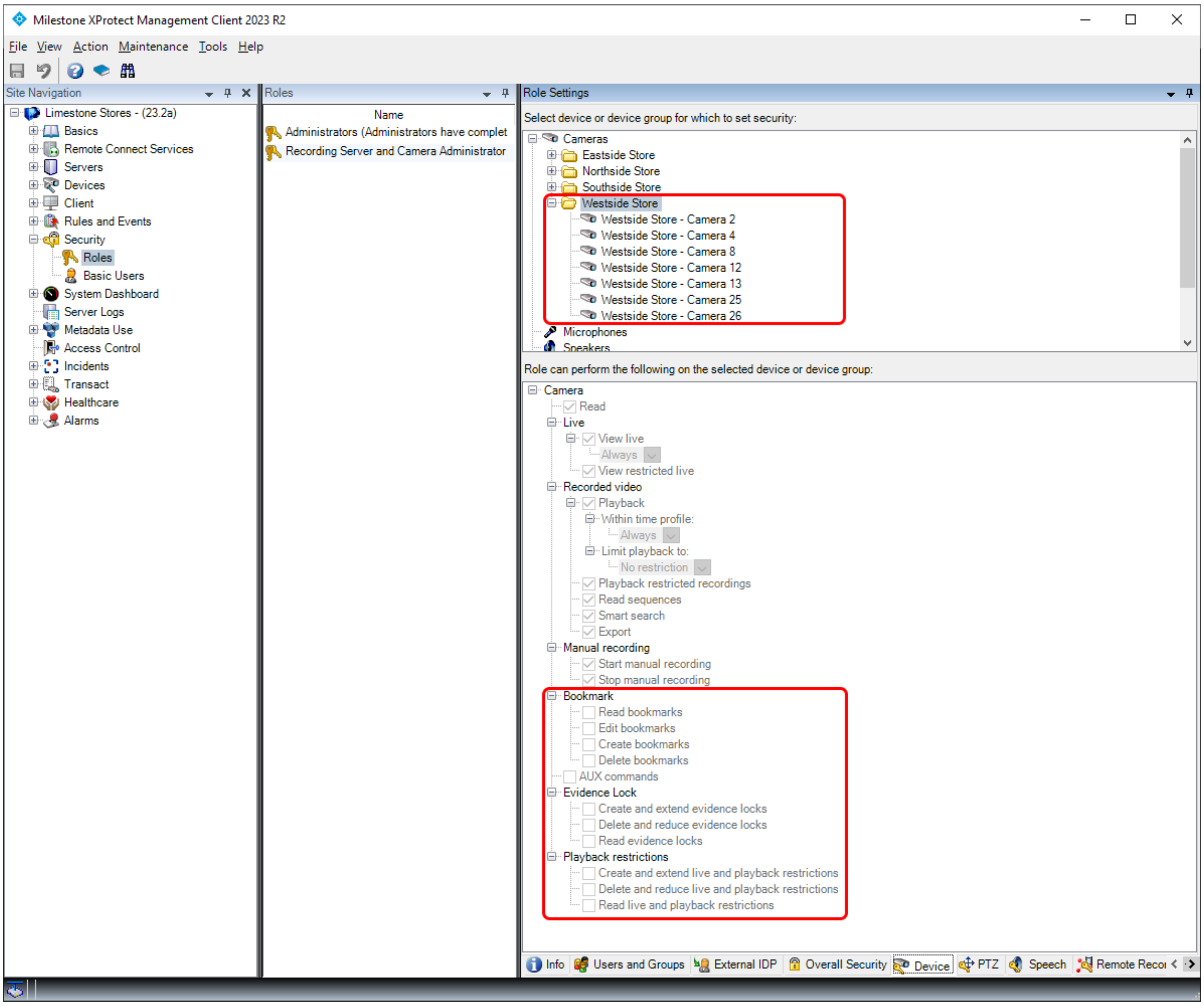
Select a security group for which to set security: Cameras

Role can perform the following on the selected security group

	Allow	Deny
Full control	□	□
Read	☑	□
Edit	☑	□
View live	☑	□
View restricted live	☑	□
Playback	☑	□
Playback restricted recordings	☑	□
Retrieve remote recordings	☑	□
Read sequences	☑	□
Smart search	☑	□
Export	☑	□
Create bookmarks	□	☑
Read bookmarks	□	☑
Edit bookmarks	□	☑
Delete bookmarks	□	☑
Create and extend evidence locks	□	☑
Read evidence locks	□	☑
Delete and reduce evidence locks	□	☑
Create and extend live and playback restrictions	□	☑
Read live and playback restrictions	□	☑
Delete and reduce live and playback restrictions	□	☑
Start manual recording	☑	□
Stop manual recording	☑	□
AUX commands	□	☑
Manual PTZ	☑	□
Activate PTZ presets or patrolling profiles	☑	□
Manage PTZ presets or patrolling profiles	☑	□
Lock/unlock PTZ presets	☑	□
Reserve PTZ sessions	☑	□
Release PTZ sessions	☑	□
Delete recordings	□	☑
Lift privacy masks	□	☑
Manage security	□	☑

XProtect Management Client
Overall Security – '*Deny*' set for some of the camera functions

When selecting the device tab, the camera permissions set to '*Deny*' on the '*Overall Security*' tab, are displayed as unchecked and greyed out as they are inherited from the '*Overall Security*' tab.



Select device or device group for which to set security:

- Cameras
  - Eastside Store
  - Northside Store
  - Southside Store
  - Westside Store
    - Westside Store - Camera 2
    - Westside Store - Camera 4
    - Westside Store - Camera 8
    - Westside Store - Camera 12
    - Westside Store - Camera 13
    - Westside Store - Camera 25
    - Westside Store - Camera 26
- Microphones
- Speakers

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

- Camera
  - ☑ Read
  - Live
    - ☑ View live
      - Always
    - ☑ View restricted live
  - Recorded video
    - ☑ Playback
      - Within time profile:
        - Always
      - Limit playback to:
        - No restriction
    - ☑ 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
    - □ Delete and reduce live and playback restrictions
    - □ Read live and playback restrictions

XProtect Management Client
'*Deny*' permissions inherited by the cameras are shown as unchecked and read-only

Documentation – Role Settings

For detailed information about configuration of roles and permissions, please refer to the documentation which can be found by selecting the '*Roles*' node in the XProtect Management Client and pressing '*F1*' on the keyboard. Alternatively, visit Milestone – Documentation; Roles

Dual Authorization

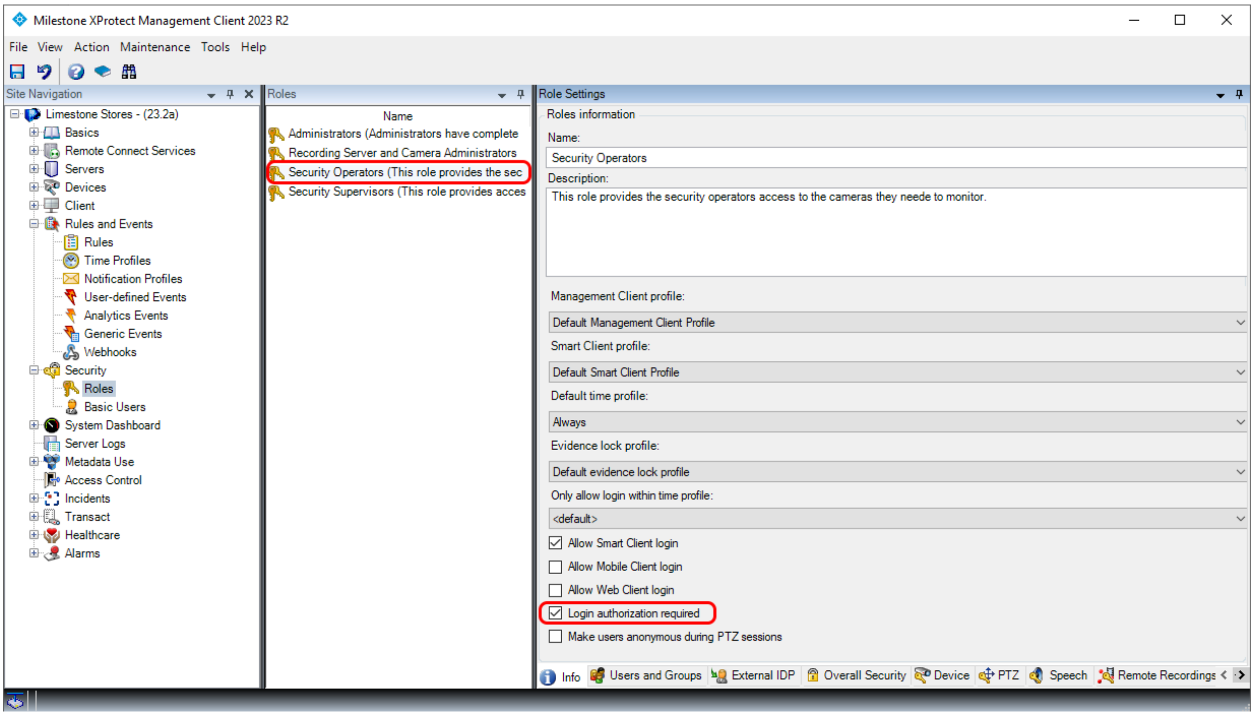
In addition to supporting profiles and permissions for viewing and managing devices and VMS functionality, XProtect Corporate also offers an additional layer of security via the Dual Authorization feature.

Dual Authorization is a feature whereby a user or administrator wishing to log in to the VMS must be authorized manually by a second privileged user or administrator.

Dual authorization has been implemented as a role setting and is supported for both the XProtect Smart Client and for the XProtect Management Client. If the XProtect Mobile client, the XProtect Web Client or MIP SDK integrations are used for a role that requires dual authorization, access will be denied as these clients and MIP SDK integrations do not support dual authorization.

Configuration

Dual authorization is enabled for a role by checking the '*Login authorization required*' checkbox on the role's '*Info*' tab. When this is done, all users with this role will be prompted to have a second privileged user authorize their login to the VMS.



Name: Security Operators

Description: This role provides the security operators access to the cameras they neede to monitor.

Management Client profile: Default Management Client Profile

Smart Client profile: Default Smart Client Profile

Default time profile: Always

Evidence lock profile: Default evidence lock profile

Only allow login within time profile: <default>

☑ Allow Smart Client login

☐ Allow Mobile Client login

☐ Allow Web Client login

☑ Login authorization required

☐ Make users anonymous during PTZ sessions

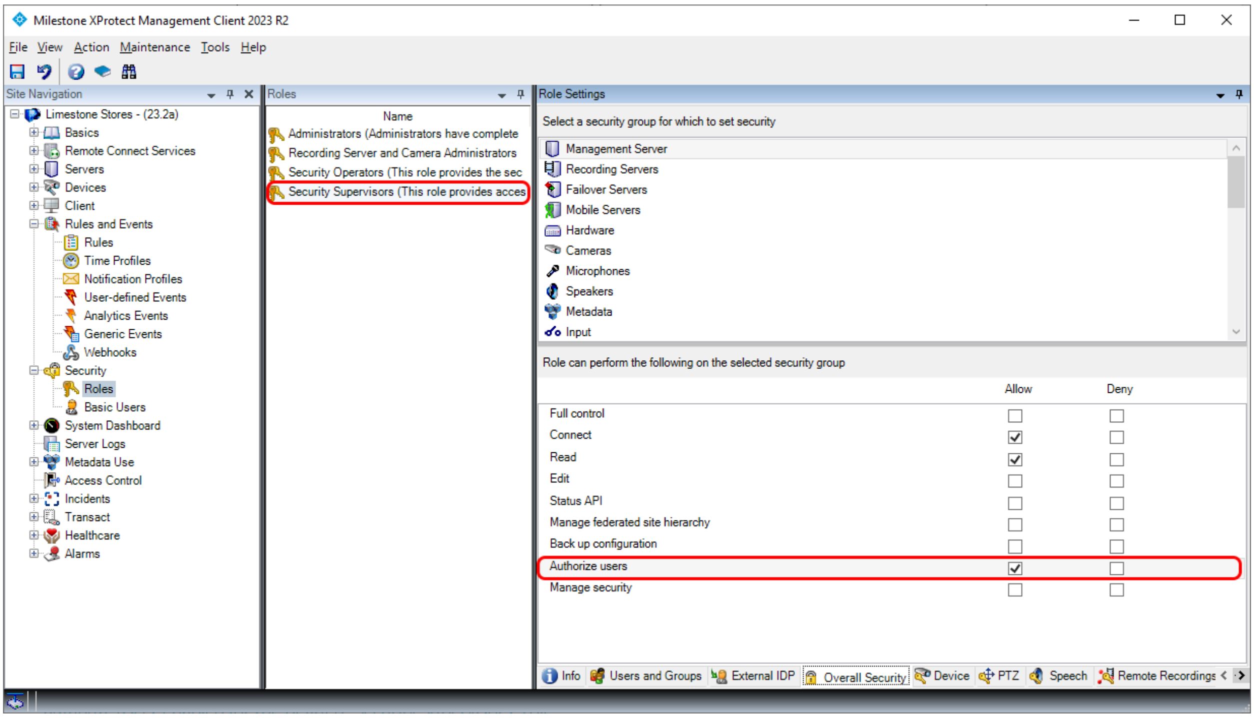
XProtect Management Client

'*Login authorization required*' enabled for the defined "Security Operators" role

Permission to authorize login is configured by enabling '*Authorize users*' in a second role. This second role does not need to be an administrator role with management permissions. Any role with '*Authorize users*' permission can authorize login. It could for instance be enabled for a "Supervisors" role that otherwise just has access to viewing cameras in the XProtect Smart Client. With '*Authorize users*' enabled for this role, the “Supervisors” can authorize user login - even for administrators using the XProtect Management Client.

Note: The Dual Authorization function is not supported for the built-in ‘*Administrators*’ role. Members of this role will always be able to log in without any further authorization. Therefore, if the Dual Authorization should be used for administrators of the VMS, a new administrator role must be created and configured with the right set of permissions.

The ‘*Authorize users*’ permission is found under the ‘*Management Server*’ node in the ‘*Overall Security*’ tab.



Name
- Administrators (Administrators have complete
- Recording Server and Camera Administrators
- Security Operators (This role provides the sec
- Security Supervisors (This role provides acces

Select a security group for which to set security
- Management Server
- Recording Servers
- Failover Servers
- Mobile Servers
- Hardware
- Cameras
- Microphones
- Speakers
- Metadata
- Input

Role can perform the following on the selected security group

	Allow	Deny
Full control	□	□
Connect	☑	□
Read	☑	□
Edit	□	□
Status API	□	□
Manage federated site hierarchy	□	□
Back up configuration	□	□
Authorize users	☑	□
Manage security	□	□

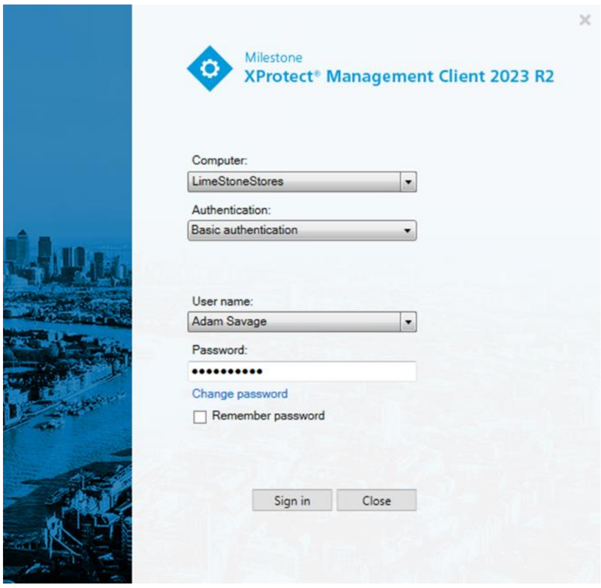
XProtect Management Client
‘*Authorize users*’ enabled for the defined “Security Supervisors” role

Login authorization

When a user or administrator, who is a member of a role that requires authorization, tries to log in with the XProtect Smart Client or the XProtect Management Client, the user is authenticated as usual. However, once successfully authenticated, the user is presented with a second login dialog prompting for login authorization by another user. The second user must enter his or her username and password to authorize the login.

In both XProtect Smart Client and XProtect Management Client, the user authorizing the login can see who is requesting to be authorized as the name of the user is displayed in the authorization dialog.

Initial user authentication using the XProtect Management Client or the XProtect Smart Client.



Milestone XProtect® Management Client 2023 R2

Computer: LimeStoneStores

Authentication: Basic authentication

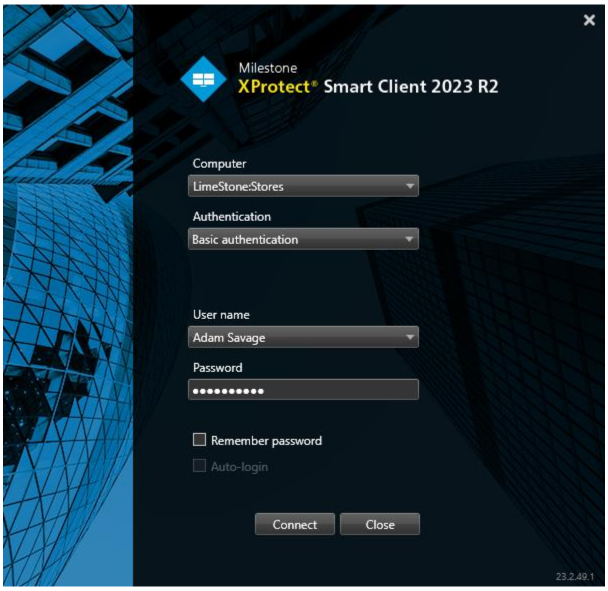
User name: Adam Savage

Password: ••••••••••

Change password

□ Remember password

XProtect Management Client
Login dialog



Milestone XProtect® Smart Client 2023 R2

Computer: LimeStone:Stores

Authentication: Basic authentication

User name: Adam Savage

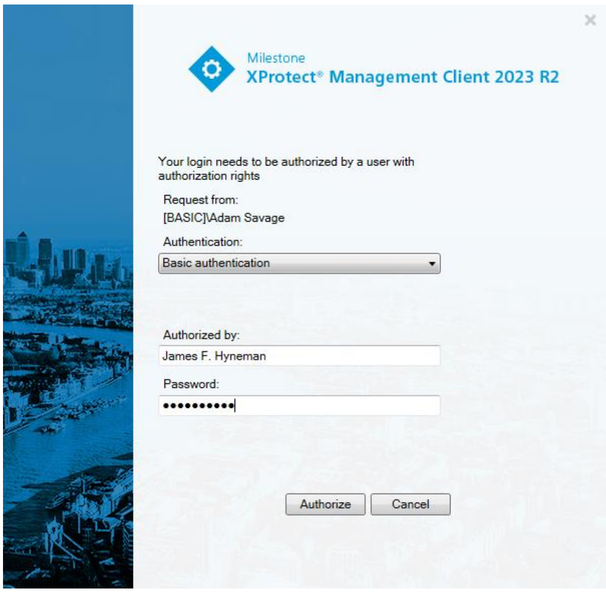
Password: ••••••••••

□ Remember password

□ Auto-login

XProtect Smart Client
Login dialog

Second user authentication and authorization using the XProtect Management Client or the XProtect Smart Client.



Milestone XProtect® Management Client 2023 R2

Your login needs to be authorized by a user with authorization rights

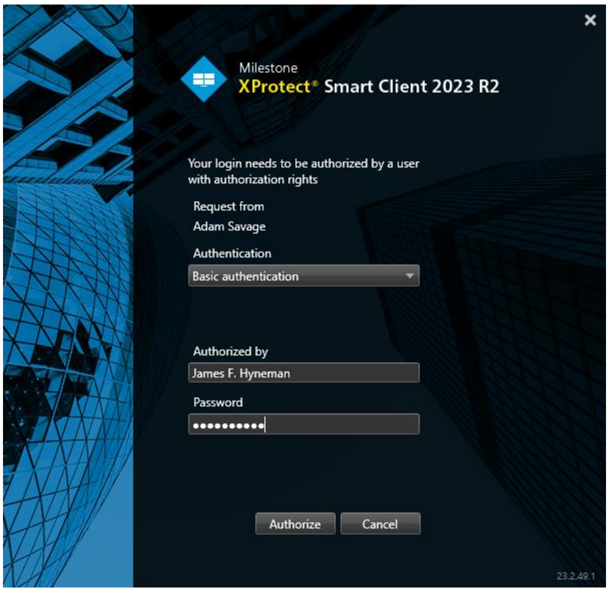
Request from: [BASIC]\Adam Savage

Authentication: Basic authentication

Authorized by: James F. Hyneman

Password: ••••••••••

XProtect Management Client
Authorization dialog shown after initial login



Milestone XProtect® Smart Client 2023 R2

Your login needs to be authorized by a user with authorization rights

Request from Adam Savage

Authentication: Basic authentication

Authorized by: James F. Hyneman

Password: ••••••••••

XProtect Smart Client
Authorization dialog shown after initial login

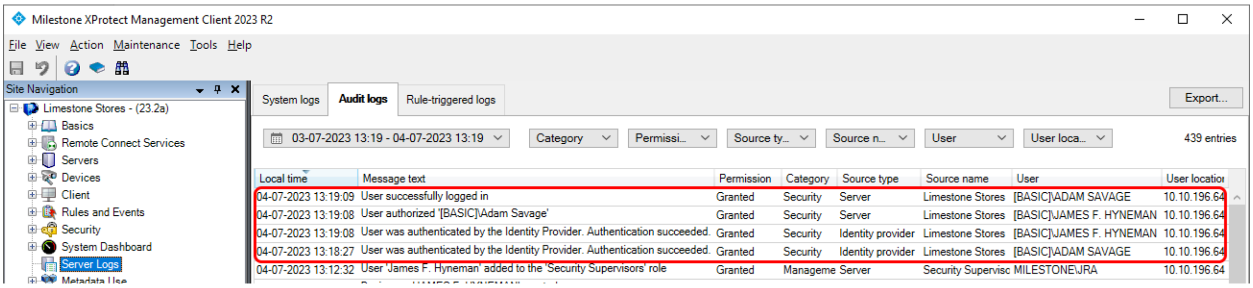
When the second user has been authenticated, the login is authorized and the normal client interface is shown. The client can now be used as usual until closed or logged out.

Audit log

When Dual Authorization is used, several audit log entries are registered describing the sequence of actions made by the two users.

Reading the audit logs from the bottom up the following is documented:

- Adam got authenticated by the Identity Provider in the VMS
- Using the authorization dialog, James got authenticated by the Identity Provider in the VMS
- Having been authenticated, James authorized Adam's login
- Login for Adam was completed and Adam got access to the VMS with the client used



Local time	Message text	Permission	Category	Source type	Source name	User	User locatior
04-07-2023 13:19:09	User successfully logged in	Granted	Security	Server	Limestone Stores	[BASIC]\ADAM SAVAGE	10.10.196.64
04-07-2023 13:19:08	User authorized '[BASIC]\Adam Savage'	Granted	Security	Server	Limestone Stores	[BASIC]\JAMES F. HYNEMAN	10.10.196.64
04-07-2023 13:19:08	User was authenticated by the Identity Provider. Authentication succeeded.	Granted	Security	Identity provider	Limestone Stores	[BASIC]\JAMES F. HYNEMAN	10.10.196.64
04-07-2023 13:18:27	User was authenticated by the Identity Provider. Authentication succeeded.	Granted	Security	Identity provider	Limestone Stores	[BASIC]\ADAM SAVAGE	10.10.196.64
04-07-2023 13:12:32	User 'James F. Hyneman' added to the 'Security Supervisors' role	Granted	Manageme	Server	Security Supervisc	MILESTONE\JRA	10.10.196.64

XProtect Management Client
Audit log – showing the Dual Authorization flow

Additional security functionality

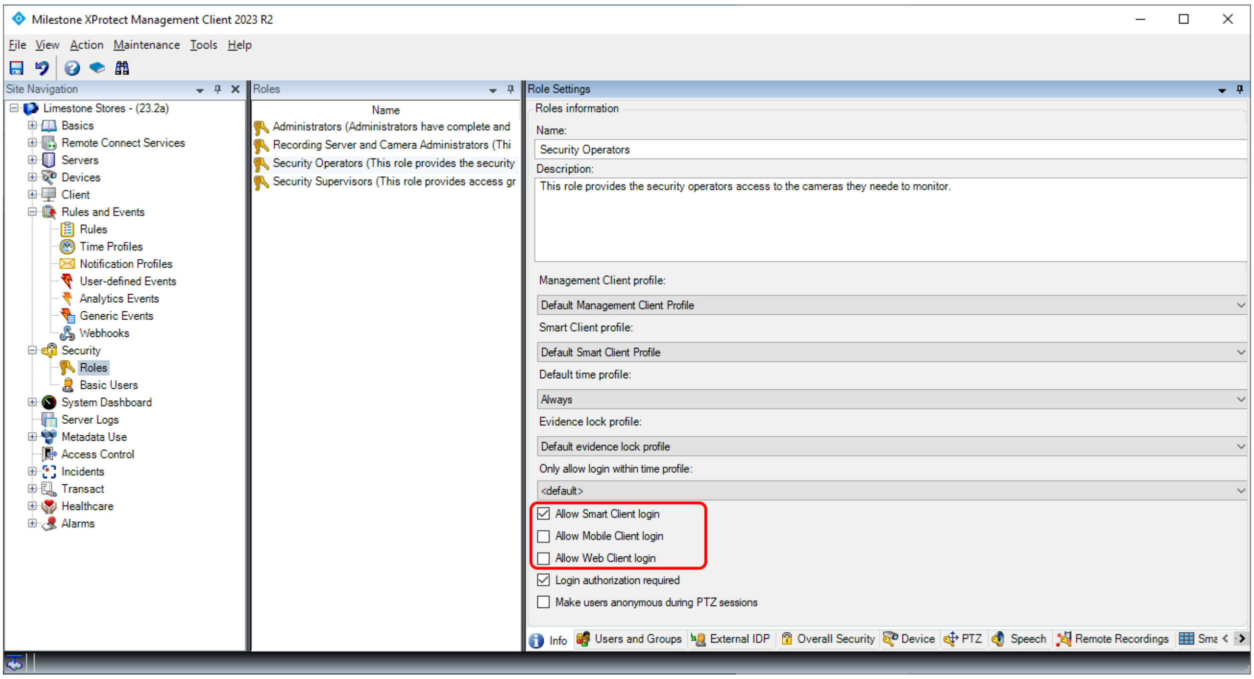
In addition to the Management Client profiles, Role options and Dual Authorization previously covered, XProtect Corporate offers a few additional security functions.

Client login

In addition to the previously covered profile and permission functions, roles can be configured to control if the XProtect Smart Client, XProtect Mobile client or XProtect Web Client can be used to log in to the VMS.

Controlling what clients users can use enables the VMS administrator to lock down access to the VMS for certain clients so only the client fitting the user's tasks are allowed. This could for instance be:

- Roaming security guards that only may use the XProtect Mobile client
- Control room users that only may use the XProtect Smart Client
- Administrators that only may use the XProtect Management Client



Administrators (Administrators have complete and
Recording Server and Camera Administrators (Thi
Security Operators (This role provides the security
Security Supervisors (This role provides access gr

Roles information

Name:
Security Operators

Description:
This role provides the security operators access to the cameras they neede to monitor.

Management Client profile: Default Management Client Profile

Smart Client profile: Default Smart Client Profile

Default time profile: Always

Evidence lock profile: Default evidence lock profile

Only allow login within time profile: <default>

☑ Allow Smart Client login
☐ Allow Mobile Client login
☐ Allow Web Client login
☑ Login authorization required
☐ Make users anonymous during PTZ sessions

XProtect Management Client
Role – XProtect Smart Client login allowed. Mobile Client and Web Client login not allowed.

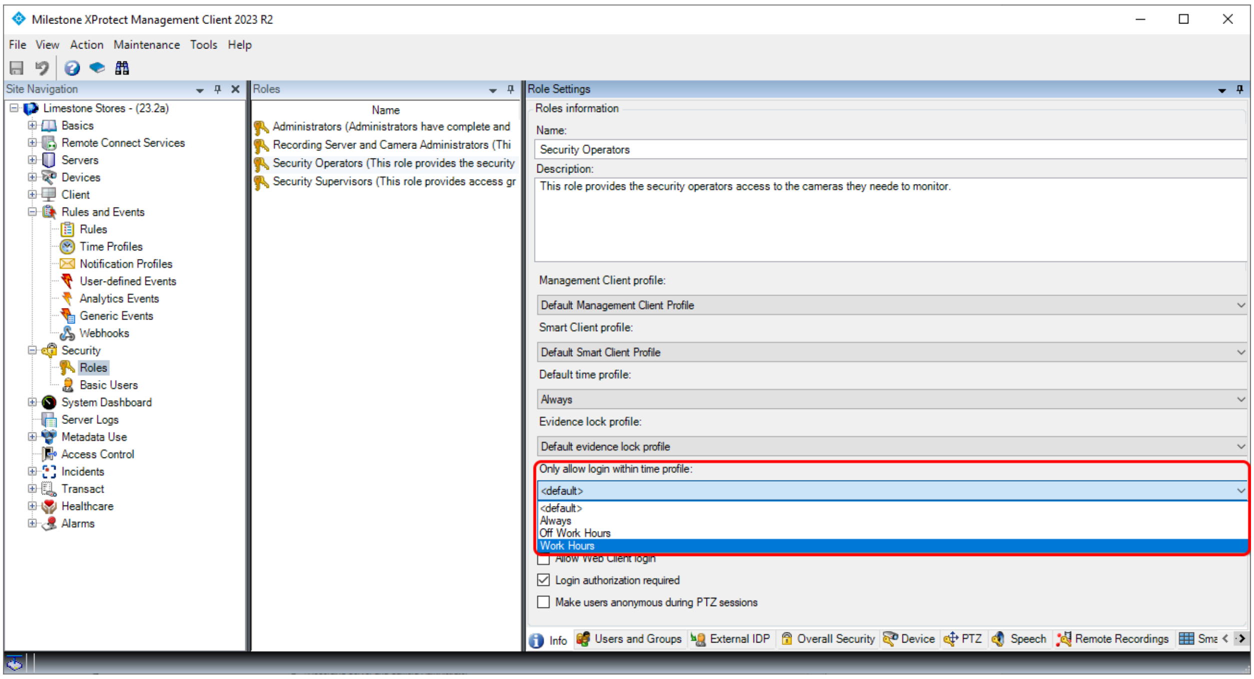
Regardless of which client(s) the users have login permissions for, the functions and devices they can access are the same per the permissions otherwise configured in the role.

Multiple roles

In case users are members of multiple roles with different client permissions, the permissions experienced by the users will be the sum of the permissions from their roles. For example, if just one of the two roles that a user is a member of has the '*Allow Mobile Client login*' enabled, the user can log in with the XProtect Mobile client.

Time-controlled login

In addition to controlling which clients the users and administrators can use to access the VMS, it is possible to limit the time period where they can log in and access the VMS.



Name: Security Operators

Description: This role provides the security operators access to the cameras they neede to monitor.

Management Client profile: Default Management Client Profile

Smart Client profile: Default Smart Client Profile

Default time profile: Always

Evidence lock profile: Default evidence lock profile

Only allow login within time profile: <default>

<default>
Always
Off Work Hours
Work Hours

☐ Allow Web Client login

☑ Login authorization required

☐ Make users anonymous during PTZ sessions

XProtect Management Client
Role – time-controlled login

Time-controlled login is configured by creating a time profile wherein the time to be used for controlling login and access has been configured, and then selecting the time profile in the role.

Users in this role are now restricted to only log in and access the VMS during the time periods specified in the selected time profile. This is also enforced for users already logged in when the time exceeds the time selected in the time profile. In this case, any user in this role still logged in will be logged out and cannot log in again until the time reaches the time period again that is specified in the selected time profile.

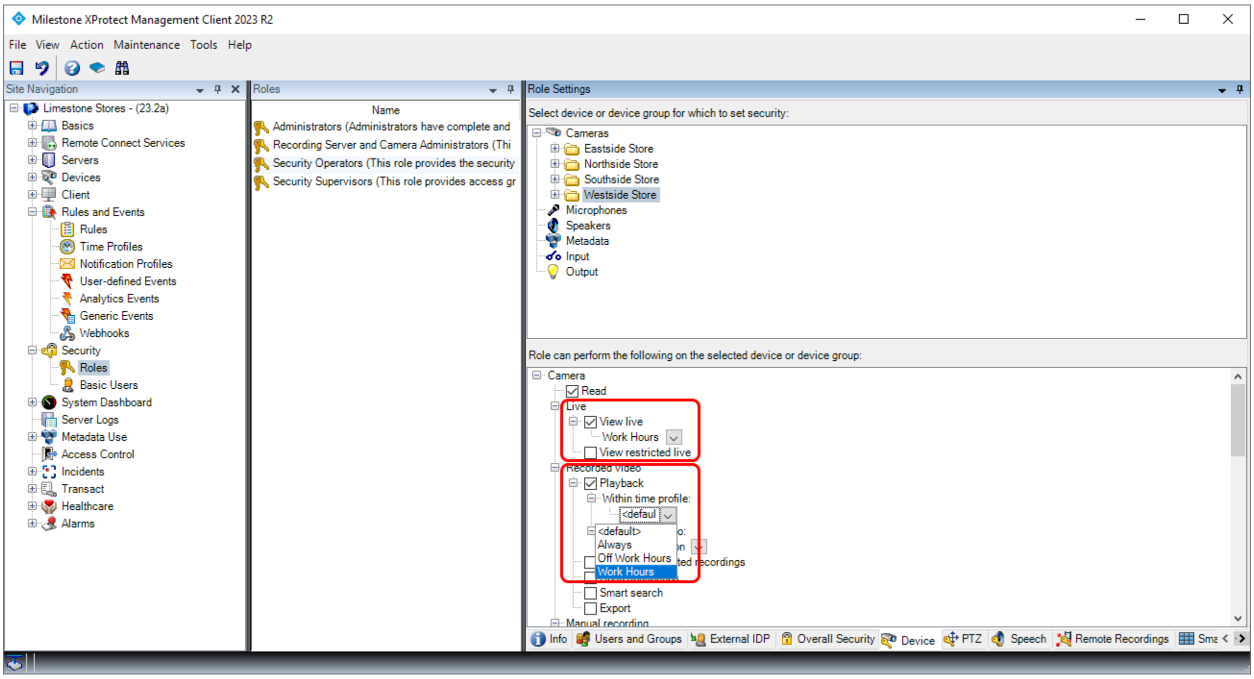
Multiple roles

In case the users are a members of multiple roles where login is restricted by different time profiles, the users can log in and access the VMS during the sum of the selected time in the time profiles used in the roles. For example, if uses are members of two roles and role one's time profile allows login on Mondays, and role two's time profile allows login on Tuesdays, the user can log in and access the VMS on both Mondays and Tuesdays.

Time-controlled device permissions

In addition to controlling login and access to the entire VMS per selected time profile, it is also possible to control access to various functions and devices per time profile. In this case, access to the functions and devices is allowed while the time is within the time periods specified in the selected time profile for the device or function in question.

For example, it is possible to allow access to viewing live and playing back recordings for a group of cameras while the current time is within the time in the selected time profile, as shown in the screenshot below.



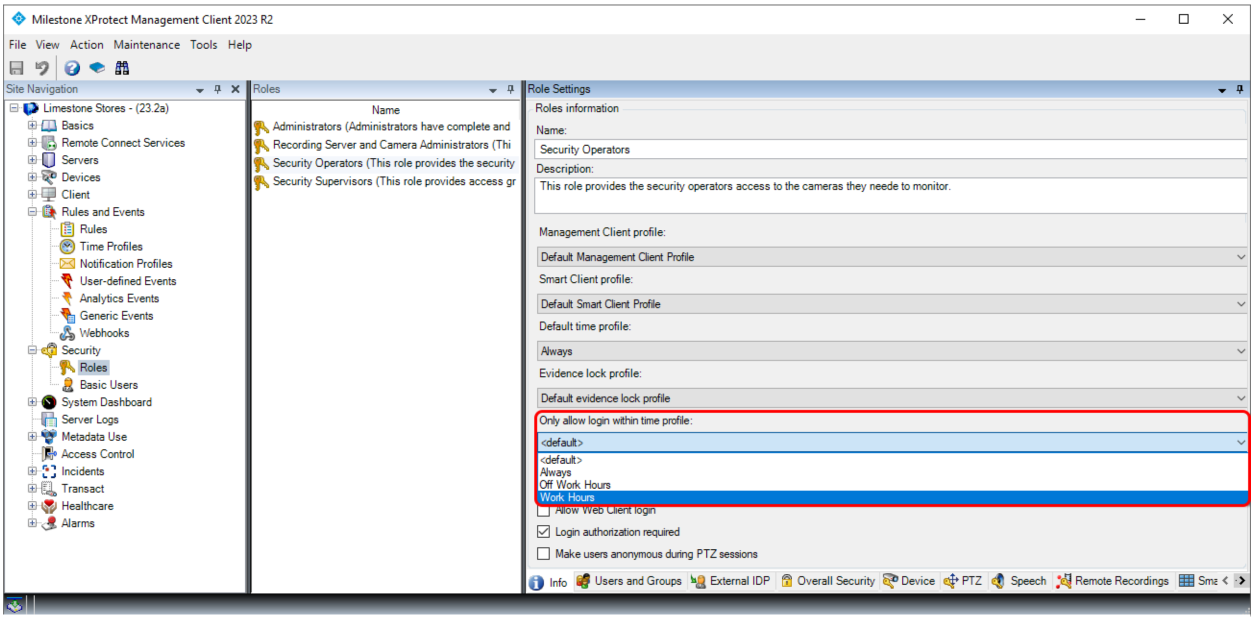
XProtect Management Client
Role – time-controlled permissions

Examples of other devices and functions that can be configured with time-based permissions include:

- Listening to live and recorded audio
- Speaking to speakers
- Controlling PTZ cameras
- Activating outputs and events
- Controlling Smart Walls

Default time profile

In case the same time profile should be applied across all devices and functions that support time-based permissions, a time profile can be applied across all devices. This is done by leaving the time profile setting on the devices and functions set to '*<default>*', and then simply selecting the desired time profile in the '*Default time profile:*' dropdown on the role's '*info*' tab, as shown in the screenshot below.



Administrators (Administrators have complete and
Recording Server and Camera Administrators (Thi
Security Operators (This role provides the security
Security Supervisors (This role provides access gr

Roles information

Name: Security Operators

Description: This role provides the security operators access to the cameras they neede to monitor.

Management Client profile: Default Management Client Profile

Smart Client profile: Default Smart Client Profile

Default time profile: Always

Evidence lock profile: Default evidence lock profile

Only allow login within time profile: <default>

<default>
Always
Off Work Hours
Work Hours

□ Allow Web Client login

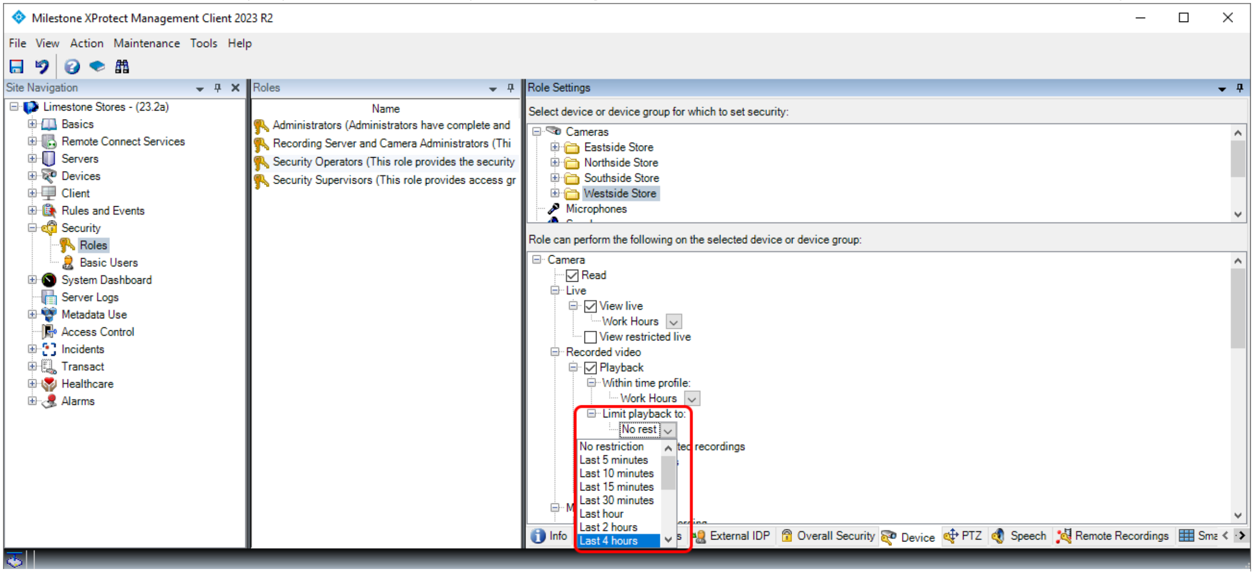
☑ Login authorization required

□ Make users anonymous during PTZ sessions

XProtect Management Client
Role – Selecting default time profile

Limiting playback

Access to playback of recordings a can further be limited so only last n- minutes, hours or days from the current time can be played back. The options range from the last 5 minutes to the last 180 days.



Administrators (Administrators have complete and
Recording Server and Camera Administrators (Thi
Security Operators (This role provides the security
Security Supervisors (This role provides access gr

Select device or device group for which to set security:

Cameras
Eastside Store
Northside Store
Southside Store
Westside Store
Microphones

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

Camera
☑ Read
Live
☑ View live
Work Hours
□ View restricted live
Recorded video
☑ Playback
Within time profile:
Work Hours
Limit playback to:
No rest
No restriction
Last 5 minutes
Last 10 minutes
Last 15 minutes
Last 30 minutes
Last hour
Last 2 hours
Last 4 hours
...ted recordings

XProtect Management Client
Role – Limit playback to last n-minutes, hours, days

Multiple roles

In case the users are members of multiple roles where access to playback is limited to last n- time, the users can play back recordings according to the role with the longest time allowed. For example, if a user is a member of two roles and the two roles limit playback to the last one hour and last 8 hours for the same device, the user can play back recordings from the last 8 hours for this device.

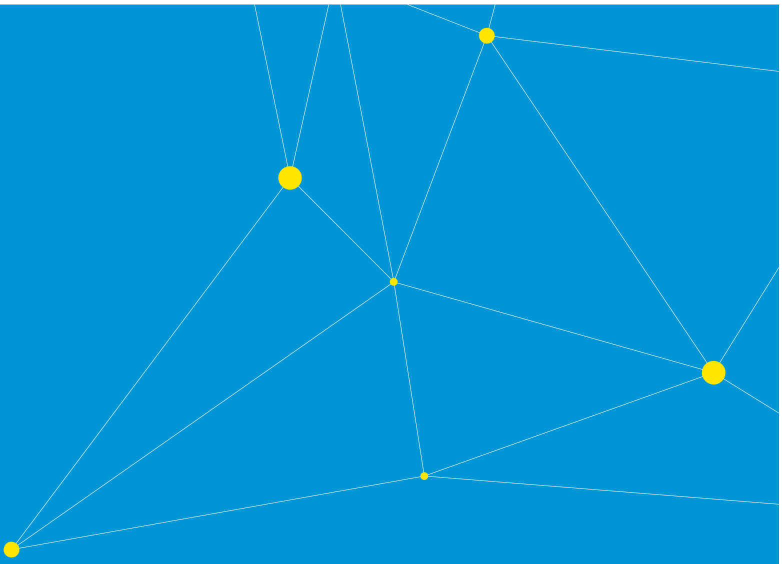
Benefits and summary

Designed to meet demands from customers requiring the highest level of customization, control and security for their surveillance installation, XProtect Corporate offers a broad range of security functionality and permission options to secure the VMS against unauthorized access and to control user and administrator abilities in detail.

The foundation for the security control is the roles where individual users and administrators are assigned one or more roles, each configured with a detailed set of permissions. Utilizing the roles and the detailed permission options, the VMS servers will ensure strict control of both users and administrators, enforcing that they can only access devices and VMS functionality that they have specifically been assigned permissions for.

With the Dual Authorization feature, security is taken to an even higher level where even administrators can be required to have their access to the VMS authorized by a second privileged user or administrator, thereby ensuring that no one person alone can access and manage, or even tamper with or disable, the VMS.

With XProtect Management Client profiles, XProtect Corporate offers a possibility to customize the XProtect Management Client user interface. The customization options provide a strict security control of the VMS and in addition, the XProtect Management Client can be tailored to match the administrators' security permissions and responsibility in the VMS. This makes it easier for the administrators to navigate and manage the VMS and furthermore it may reduce the cost of training administrators in managing the VMS, as well as reduce the risk of unintentional misconfiguration of the VMS.



Milestone Systems is a leading provider of open platform video management software; technology that helps the world see how to ensure safety, protect assets and increase business efficiency. Milestone enables an open platform community that drives collaboration and innovation in the development and use of network video technology, with reliable and scalable solutions that are proven in more than 500,000 sites worldwide. Founded in 1998, Milestone is a stand-alone company in the Canon Group.