White paper

XProtect® Corporate – Advanced Security Management

Prepared by:

John Rasmussen, Senior Technical Product Manager, Corporate Business Unit, Milestone Systems

Date: November 17, 2014

Table of Contents

Introduction

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

Advanced and/or large scale installations often have more than one administrator managing the system and in some cases have external contractors handling specific maintenance and management functions such as replacing cameras or managing recording servers.

To further increase the manageability and security of these large systems, XProtect Corporate 2014 introduces two new important capabilities: *Management Client profiles* and *advanced management rights*.

Management Client profiles allows for customization of XProtect Management Client to optimize it for different functional responsibility area and skill levels. *Advanced management rights* enables tiered assignment of rights to system administrators, providing the ability to create sub-management domains where management of a specific set of devices can be assigned to a specific system administrator.

In high security installations, access to managing the system can be protected even greater by applying dual authentication – which requires two verified persons to gain system access.

Purpose and target audience

The purpose of this whitepaper is to provide insight to the benefits of advanced management rights and the ease of configuring them in conjunction with Management Client profiles and how to use inherited device permissions and dual authorization. This whitepaper will also show examples of the configuration and use of these new features.

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

- Management Client profiles
- Advanced management rights
- Inherited device rights
- Dual authorization

The primary audience is individuals with projects where the customer needs advanced management rights (which may include):

- Video surveillance system architects and designers
- Project consultants
- IT and video surveillance administrators

The reader should have a general understanding of XProtect Corporate - in particular the *Roles* concept in the XProtect Management Client.

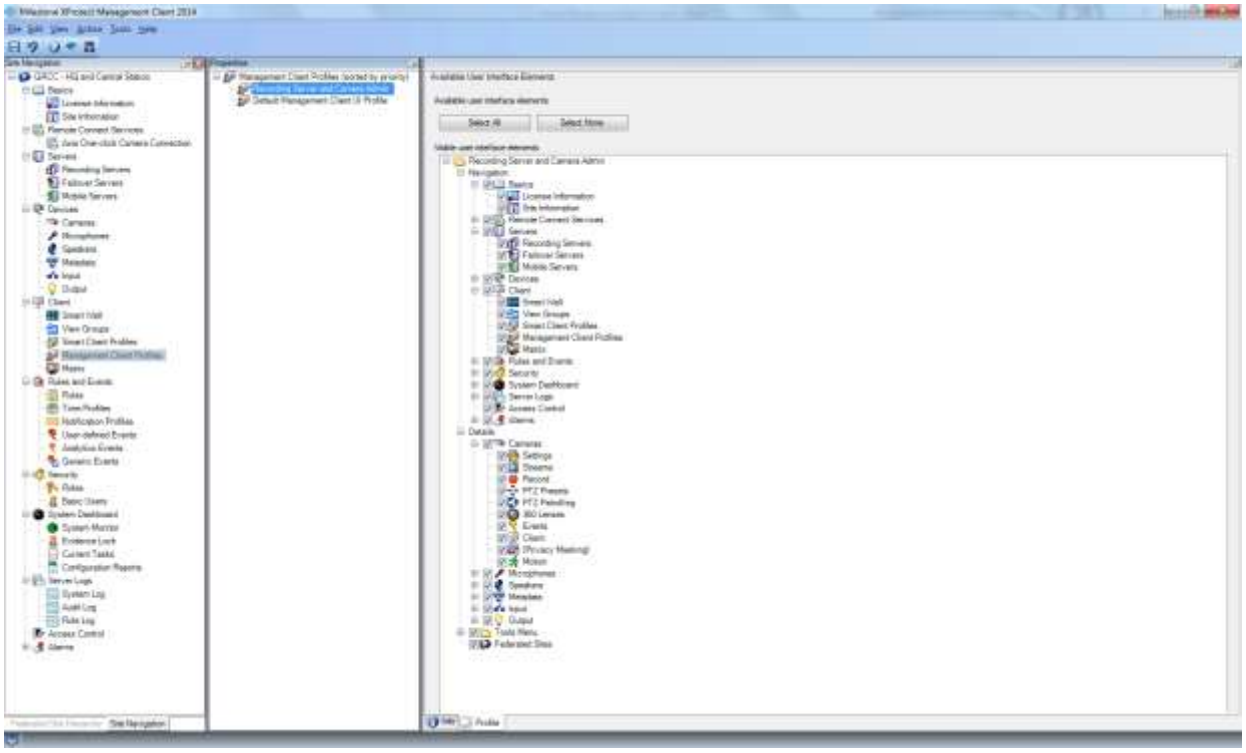
Management Client profiles

XProtect Corporate 2014 supports customization of the XProtect Management Client user interface (UI) to make it simpler to navigate and use by:

- Removing functions that are not used in the current system or
- Optimizing the user interface to match an administrator's specific role, function or area of responsibility

The XProtect Management Client user interface is customized by creating a *Management Client* profile and matching it to a specific role. When an administrator logs in (and the administrator's *Role* is configured with a modified *Management Client* profile) XProtect Management Client will only display areas of the user interface that are relevant to their predetermined role. Areas that have been determined as inaccessible to the user according to their respective *Management Client* profile will be hidden from view. This function will make the XProtect Management Client easier to use and more friendly to navigate.

Management Client profiles are managed under the *Client/Management Client Profiles* node in the XProtect Management Client.



Management Client Profiles setup dialog.

Several nodes can be expanded showing further detailed options – for example the *Cameras* node under which access to each of the camera setting tabs can be set.

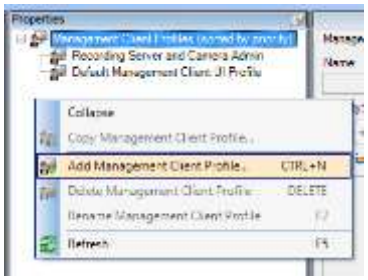
For details on individual XProtect Management Client options, please refer to the Administrator's Manual which can be found by pressing "F1" on the keyboard on the PC running the XProtect Management Client. If the *Management Client Profile* node is selected before pressing the "F1" key, the right content will be displayed immediately.

Alternatively, download the XProtect Corporate Administrator's manual on the Milestone website at http://www.milestonesys.com/downloads/?type=13

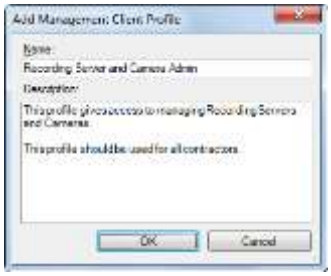
Configuration

New profiles are created by:

1) Right-clicking in the "Properties" pane and selecting *Add Management Client Profile* then,
2) Assigning it a name and optionally enter a description.



Management Client Profiles, right-click menu.



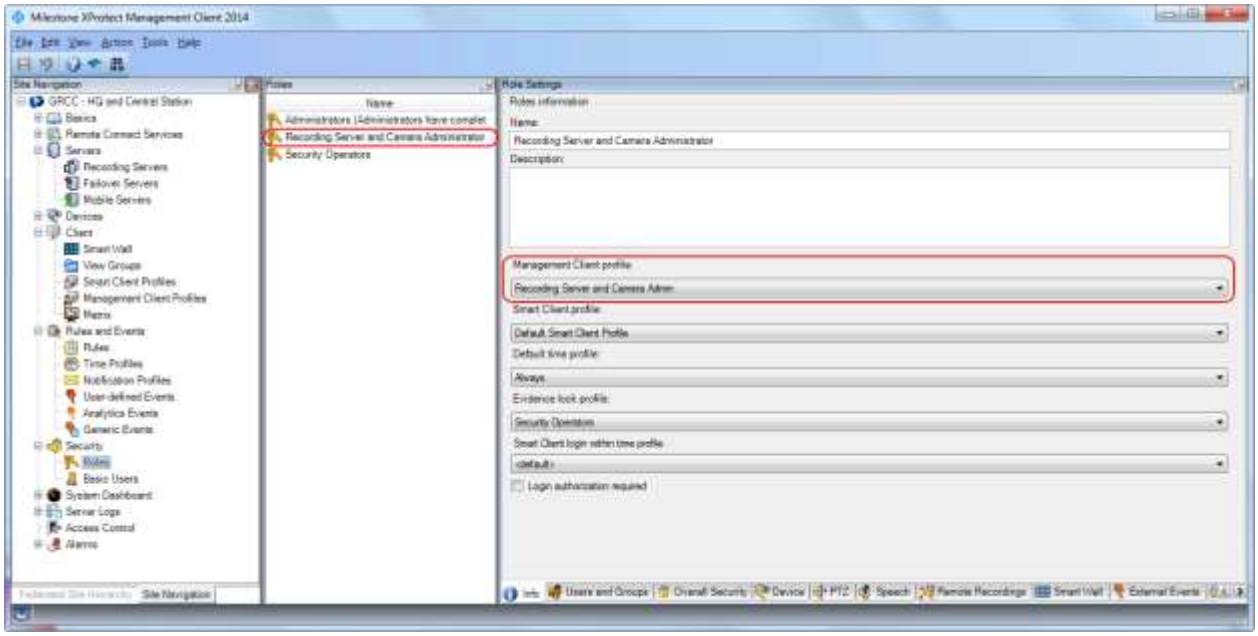
Add Management Client Profile dialog.

By default the new profile will provide access to all functions in XProtect Management Client. To limit access to various functions and features simply uncheck the relevant checkboxes.

When the permissions have been set in the profile, the next step is to use the *Management Client profile* in a role.

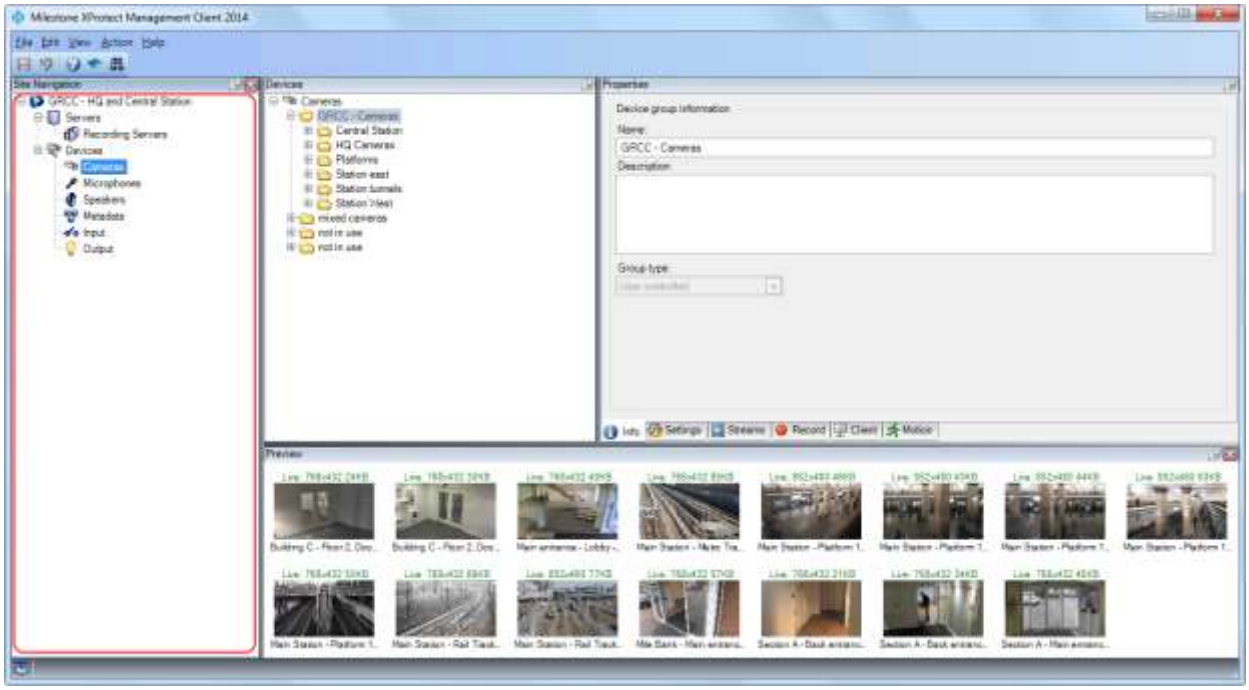
This is done by:

1) Selecting a role with management rights
2) In the *Info* tab's *Management Client profile* dropdown select the *Management Client Profile*.



Selecting the *Management Client profile* on the *Info* tab for a role.

When users (administrators) in this role login with the XProtect Management Client they are now restricted to only manage selected functions - as the user interface elements for all other functions have been removed (as seen in the screenshot below where all other UI elements than devices and recording servers have been removed).

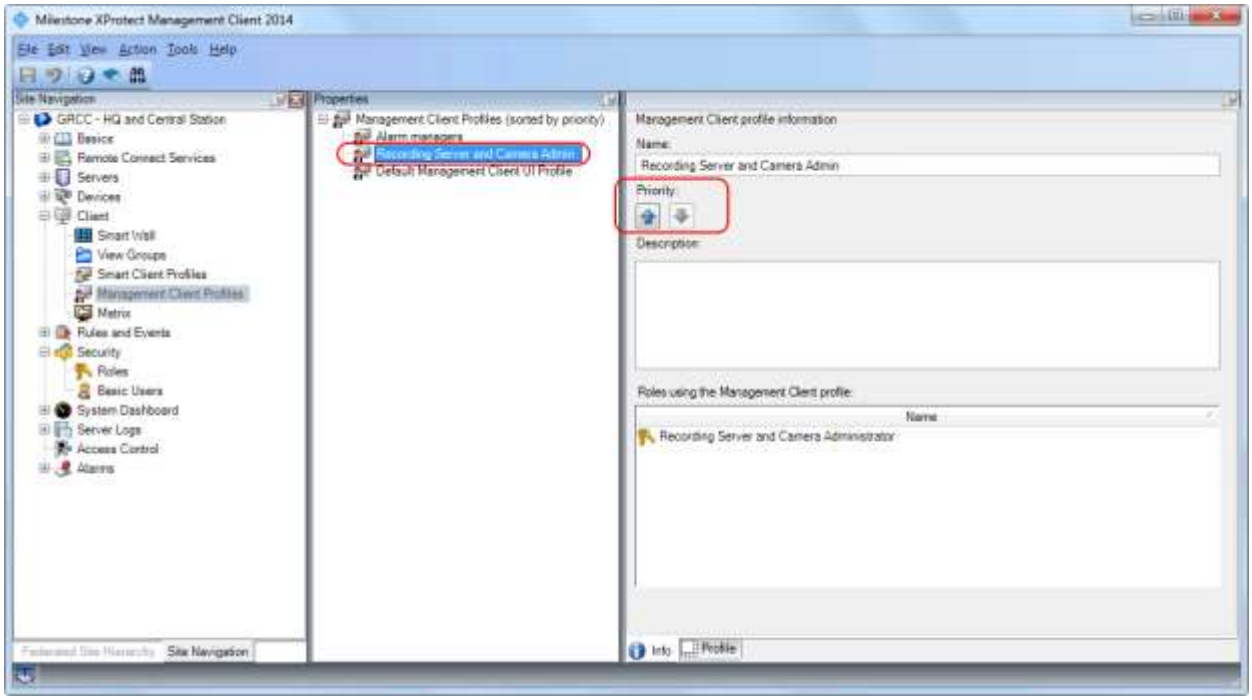


Example of the XProtect Management Client experience when a *Management Client Profile* is applied.

Multiple Management Client profiles

If the administrator logging in with XProtect Management Client is a member of multiple *Roles* configured with different *Management Client profiles*, he or she will be assigned the *Management Client profiles* with the highest priority.

Management Client profiles priority is set by the order that each profile is listed in the *Properties* pane with the highest priority at the top. The priority can be changed by clicking the *Priority up/down* buttons on the *Management Client profiles' Info* tab.



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

Security notice

Although the appearance in XProtect Management Client (when using *Management Client profiles* or setting security permissions) can be very similar, it is important to distinguish between *Management Client profiles* and security permissions. The two features are not related to each other in any way.

Management Client profiles, is solely a user-interface configuration feature and does not in any way limit the user's access to the disabled features. It only removes user-interface elements so they cannot be used. If the user for instance uses the Milestone Integration Platform Software Development Kit

(MIP SDK) or a "hacked" XProtect Management Client that disregards the *Management Client profiles* settings, the user will be able to access all functions allowed by the security permissions.

Security permissions are (on the other hand) true security enforced by the system servers no matter how the system is accessed.

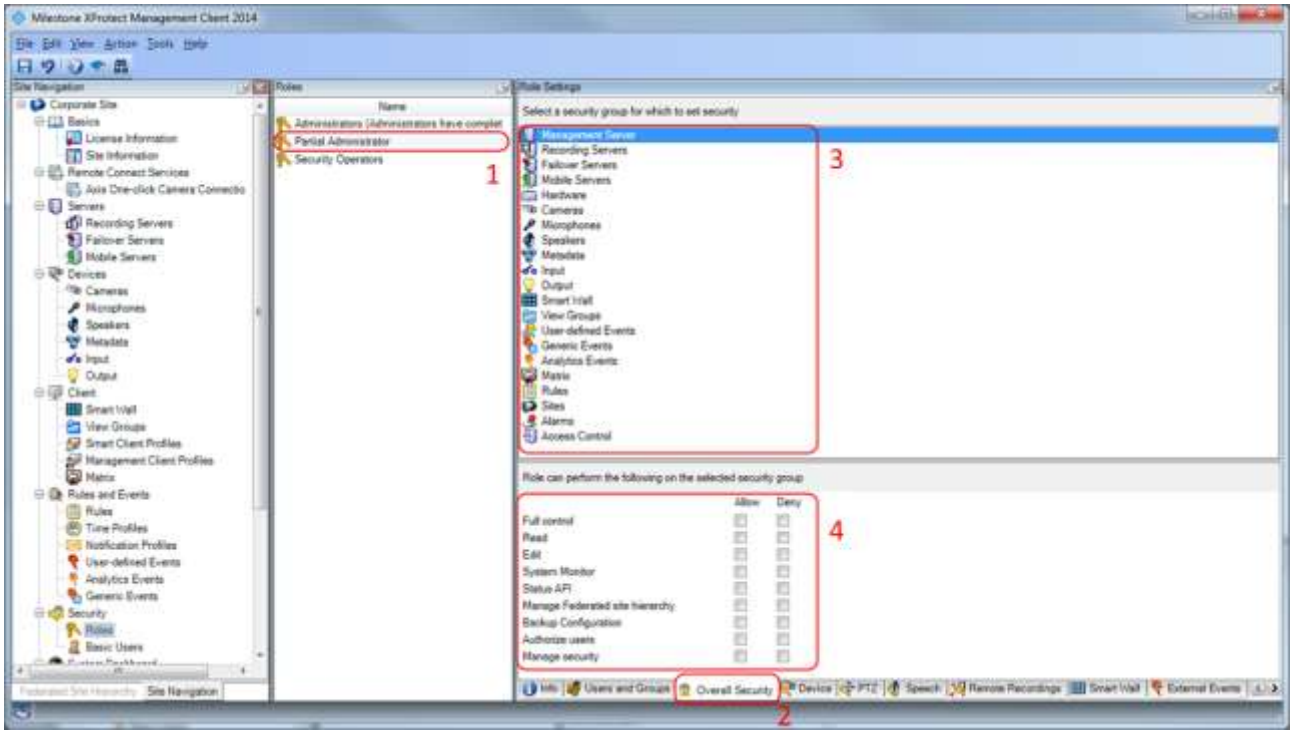
This means that security concerns of using the *Management Client profiles* to control access to the system can be addressed by setting the actual security permissions in the user's *Role* so it matches what the administrator should be able to do. When this is done the server side components will ensure that the administrator cannot access anything other than what he or she has security permission to access - no matter if using a hacked XProtect Management Client or the MIP SDK.

Management Rights

In addition to the *Management Client profiles*, XProtect Corporate 2014 supports tiered management rights, which is the ability to set management rights on individual functions, features and devices in the system. In contrast to *Management Client profiles* (which control the appearance of the XProtect Management Client user interface), management rights controls system permissions and are enforced by the surveillance system servers.

The screenshot below highlights how *Overall Security* is configured for a role.

1. *Roles* list - *Partial Administrator* role selected
2. *Overall Security* tab selected
    - The *Overall Security* settings are divided into logical system components and functions like - *Management Server, Recording Server, Rules, Roles*, etc.
3. *Role Settings – Management Server* selected
4. Security group settings
    - Lists the security permissions for the selected security group
    - The security permissions will vary depending on the selected security group
    - Checking *Allow* will grant access to the selected function
    - Checking *Deny* will deny access to the selected function
    - *Allow* and *Deny* permissions set on the *Overall Security* tab are inherited by the device permissions



Overall Security settings for a role.

For details on individual security options, please refer to the administrator manual which can be found by pressing "F1" on the keyboard on the PC running the XProtect Management Client. If the *Overall Security* tab is selected before pressing the "F1" key, the manual displays the right content immediately.

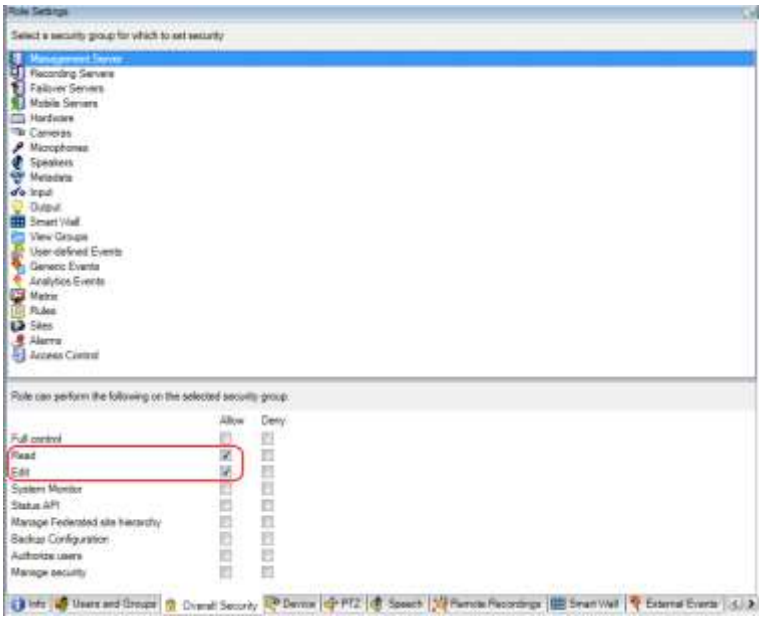
Alternatively, download the XProtect Corporate Administrator's manual on the Milestone website at http://www.milestonesys.com/downloads/?type=13

Configuration

Following the example in the *Management Client profiles* section (of an administrator having the access capability to manage recording servers and devices) the actual server side enforced security must be configured as shown in the following dialogs:

1) On the *Management Server* node the *Read* and *Edit* permissions must at a minimum be set to provide XProtect Management Client login

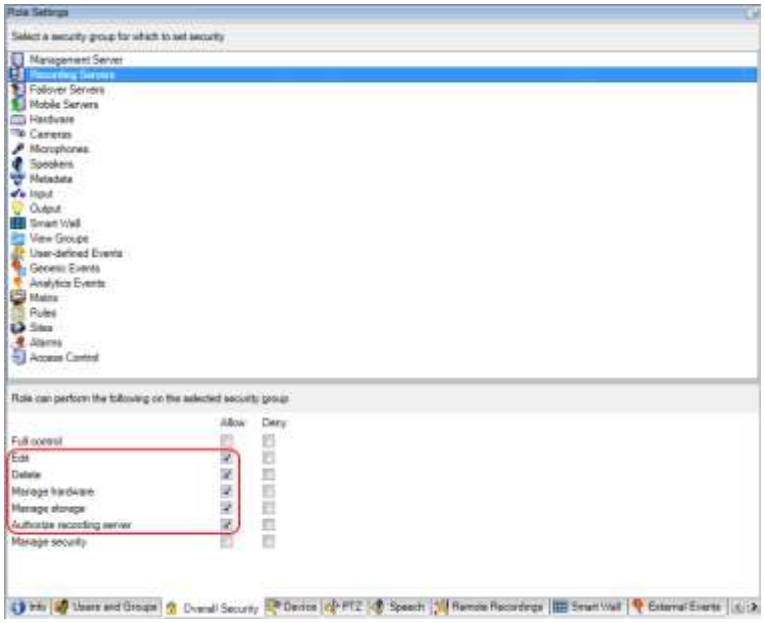
permission (*Read* and *Edit*).



Read and Edit permissions allowed for the *Management Server* security group.

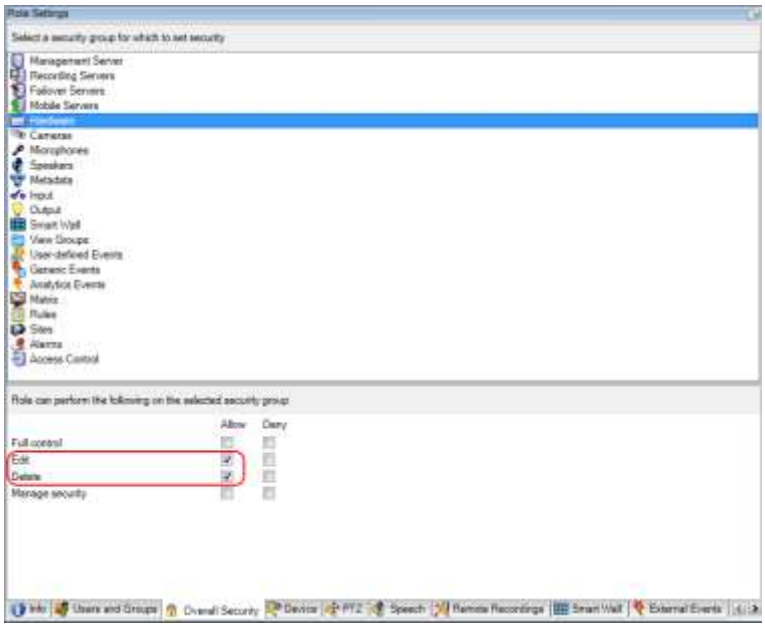
2). To manage recording servers the following permissions are needed under the *Recording Servers* node:

- *Edit*
- *Delete*
- *Manage Hardware*
- *Manage Storage*
- *Authorize recording servers*



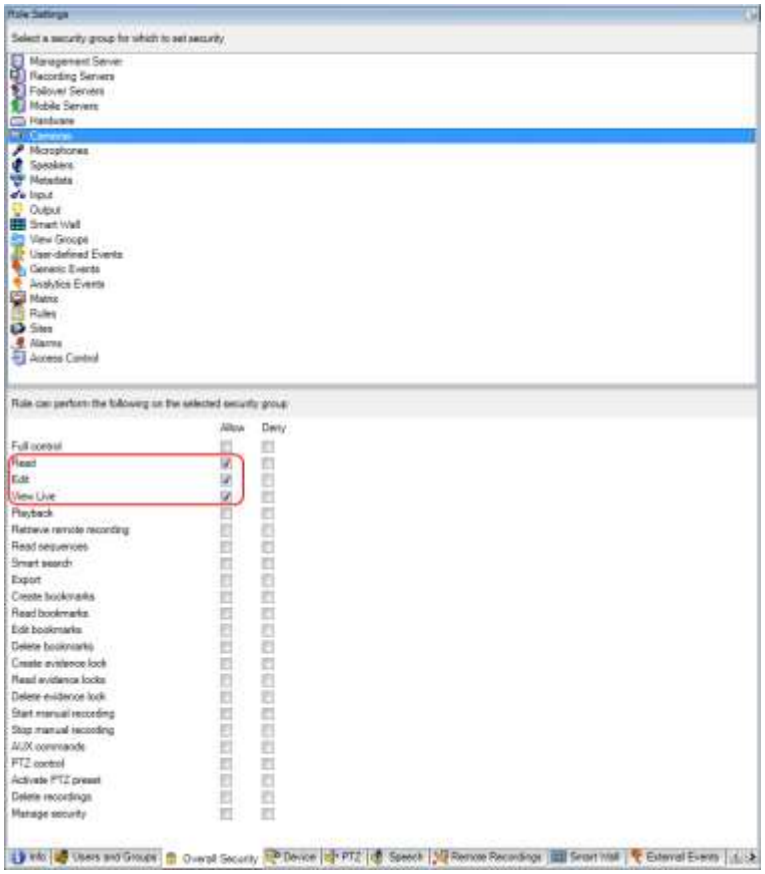
Edit, Delete, Manage hardware, Manage storage and *Authorize recording server* permissions allowed for the *Recording Server* security group.

In order to work with the hardware devices on the recording servers the *Edit* and *Delete* permissions must be selected.



Edit and *Delete* permissions allowed for the *Hardware* security group.

To work with the devices (cameras, microphones, speakers, metadata, input, output) the *Read, Edit and View Live* (for XProtect Management Client preview permissions) are required.



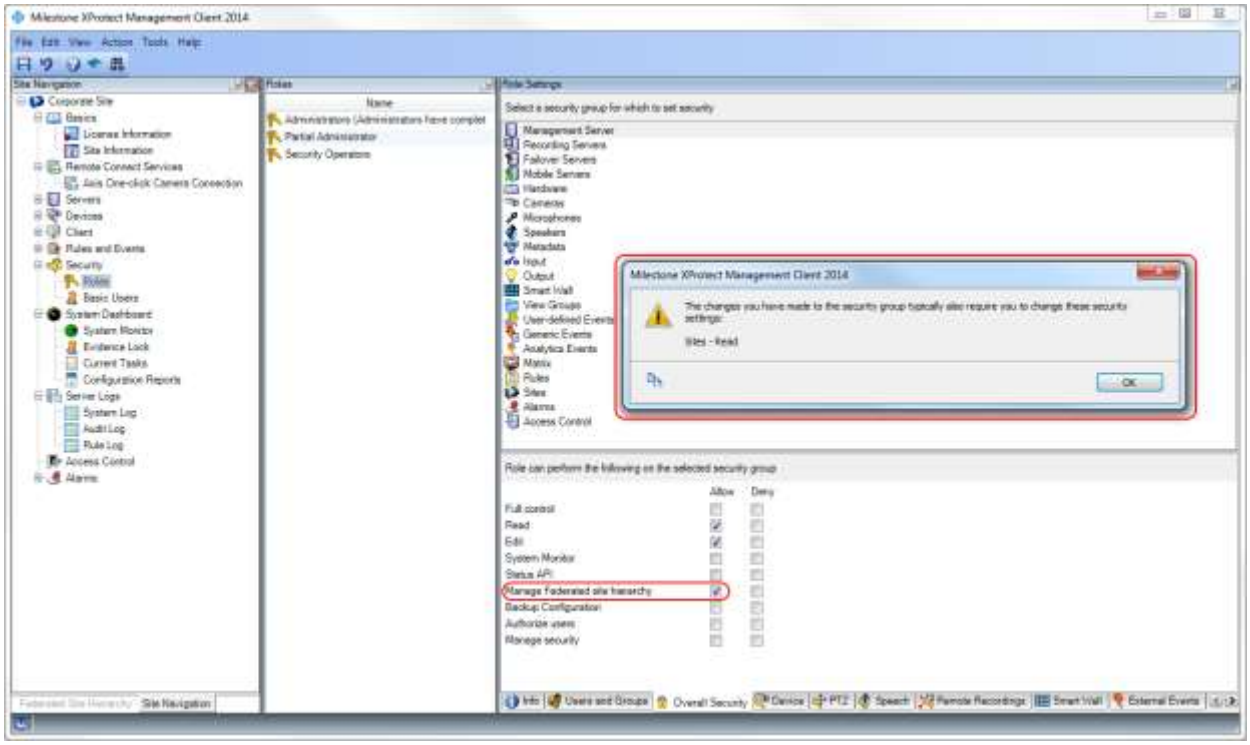
Read, Edit and *View Live* permissions allowed for the *Cameras* security group.

With the above settings set, the security will be enforced server side and the administrator will only be able to manage these sections of the system, even if using a hacked XProtect Management Client or integrations done with the MIP SDK.

Permission requirements and advices

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

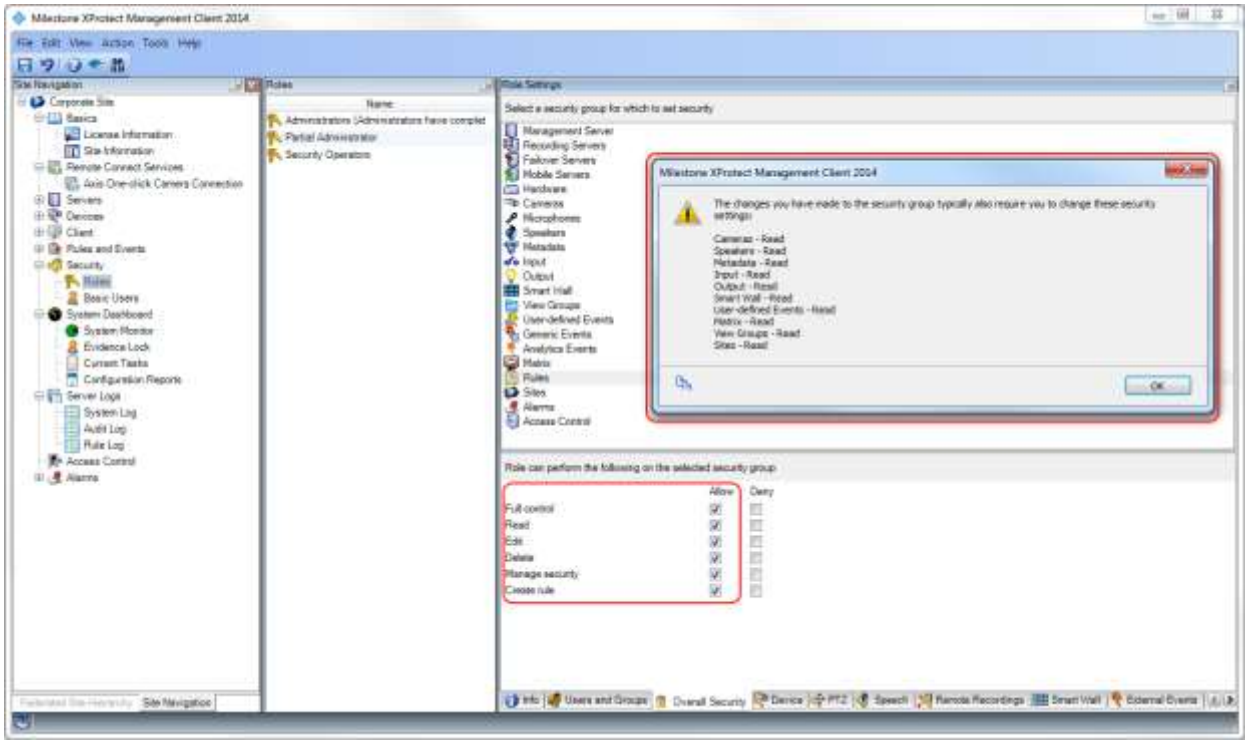
In the below example *Manage Federated site hierarchy* has been selected on the *Management Server* element, but in order for this to work the administrator must also enable access to read the federated sites. If access to read sites is not given, the administrator technically has permission to manage the federated hierarchy - but it will be impossible as the information from the federated sites cannot be read.



Example of XProtect Management Client notifying (the administrator) that additional permissions are required to obtain access as expected.

Another example of XProtect Management Client notifying the administrator that more permissions may be needed is when setting permissions to work with rules.

In this case, the administrator needs access to multiple item types to configure the rules, as rules can be defined to be trigged on events from several different source types and to perform actions on several system features and device types.

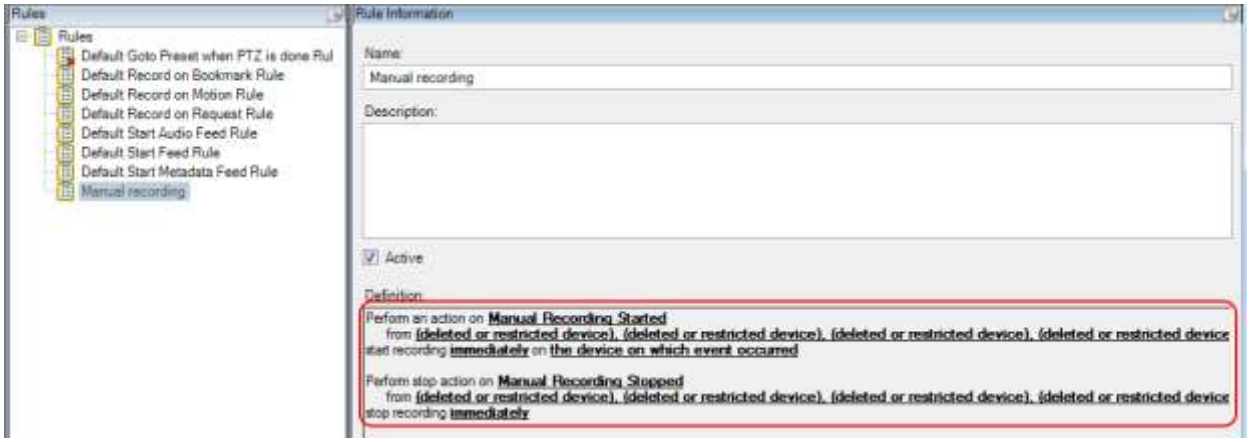


Example of XProtect Management Client suggesting that more permissions may be needed to obtain access as expected.

In contrast to the previous example, this notification is not a requirement but a recommendation to grant permission to some or all of the listed items, as the administrator working with rules needs to be able to select triggering sources and features and/or sources to perform actions on.

It may though be desired to only grant the administrator rights to a subset of sources and features, as it then is possible to limit the sources and actions the administrator can work with in the rule.

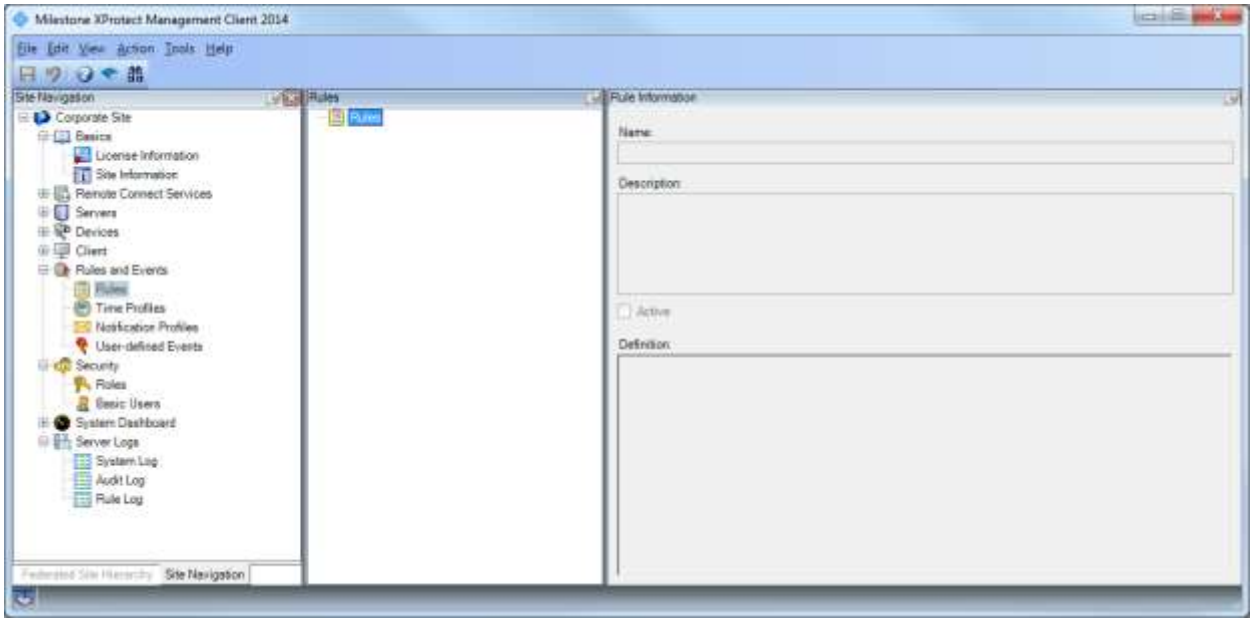
If an administrator (with one set of rules permissions) attempts to work with a rule that includes sources he or she does not have permission to view, the sources are listed as: *(deleted or restricted device)*.



Example of a rule where the administrator either does not have permission to the device or the device itself has been deleted.

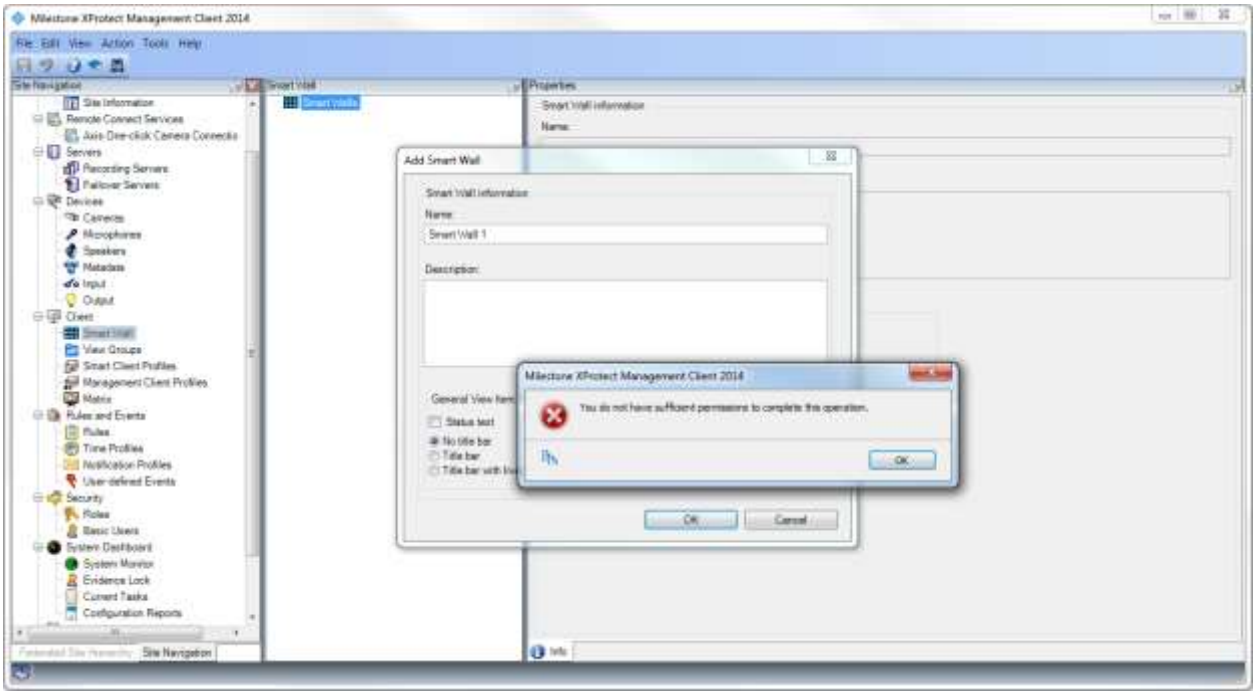
Missing permission handling

If there is a difference between the defined *Management Client profile* controlling the XProtect Management Client UI and the security permissions (that control access to the functions on the servers) the administrator will see empty dialogs, lists or settings in the XProtect Management Client as shown in the below example.



Example of a mismatch between security permissions and *Management Client profiles* where the administrator has access to the *Rules* user interface, but does not have *Rules* read permission.

When trying to administrate settings or features beyond configured permissions for the administrator the XProtect Management Client will display error messages informing that he or she has insufficient access permission.

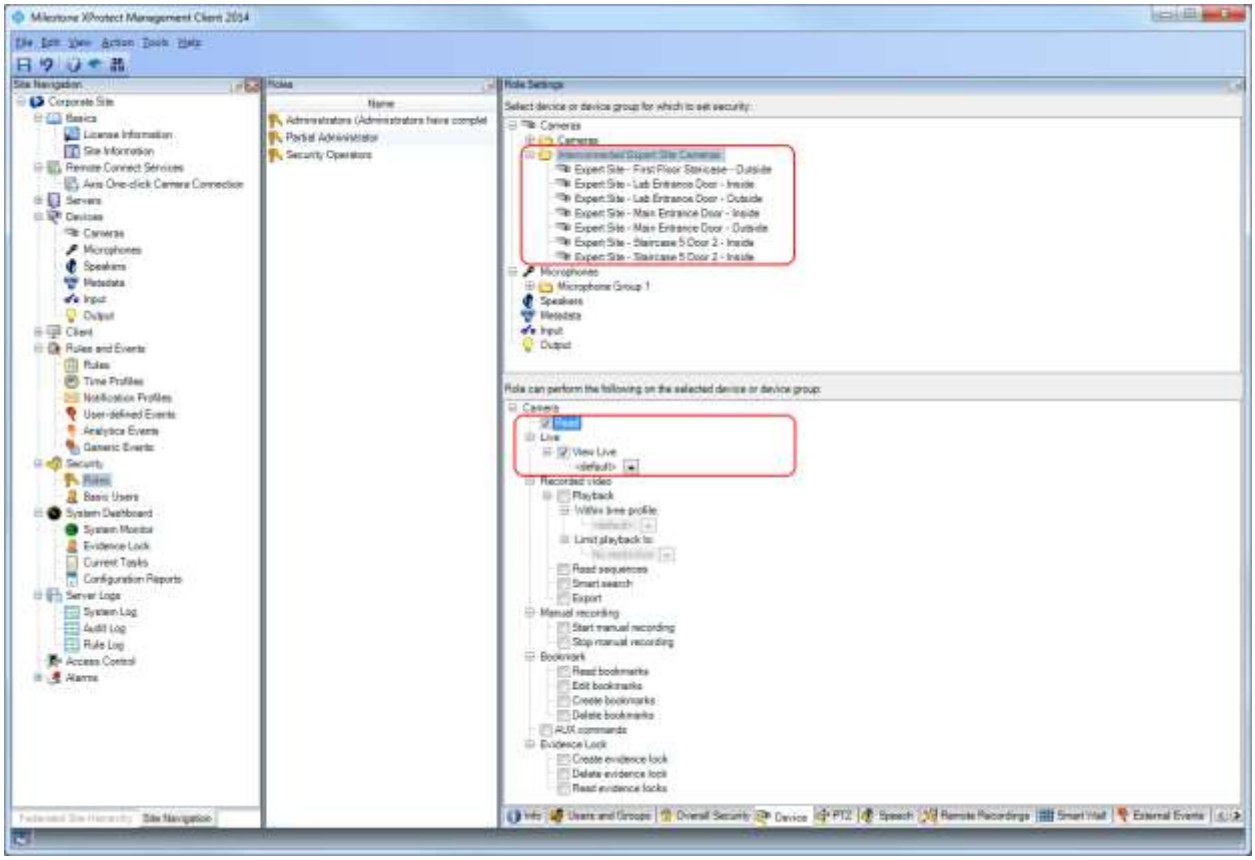


Example of XProtect Management Client notifying the administrator that permission to perform a function is missing.

Individual device permission

In addition to setting the device permission on the *Overall Security* tab, it is also possible to set permissions on the *Device* tab as known from previous versions of XProtect Corporate.

In XProtect Corporate 2014 the permissions set in the *Device* tab do not only apply to users accessing the system with the XProtect® Smart Client, XProtect® Web Client or Milestone Mobile, but also to administrators using XProtect Management Client. This makes it possible to select specific devices the administrator can work with in the XProtect Management Client - for example, only cameras within a specific device group as illustrated below:



Read and *View Live* permissions set for a group of cameras.

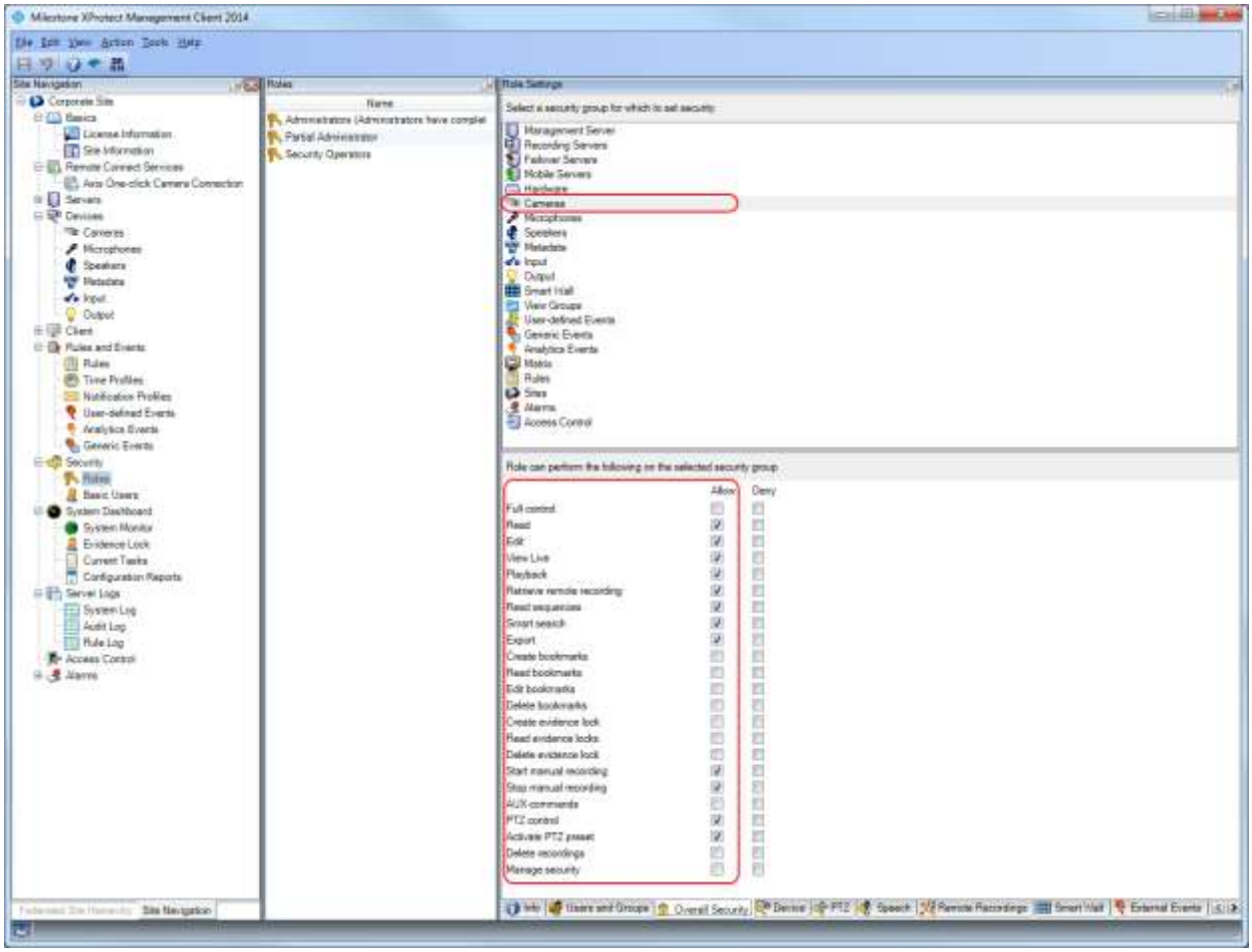
Inherited device permissions

When setting permissions for devices on the *Overall Security* tab the selected permissions are inherited by all existing devices of the same type in the system.

Allow permission

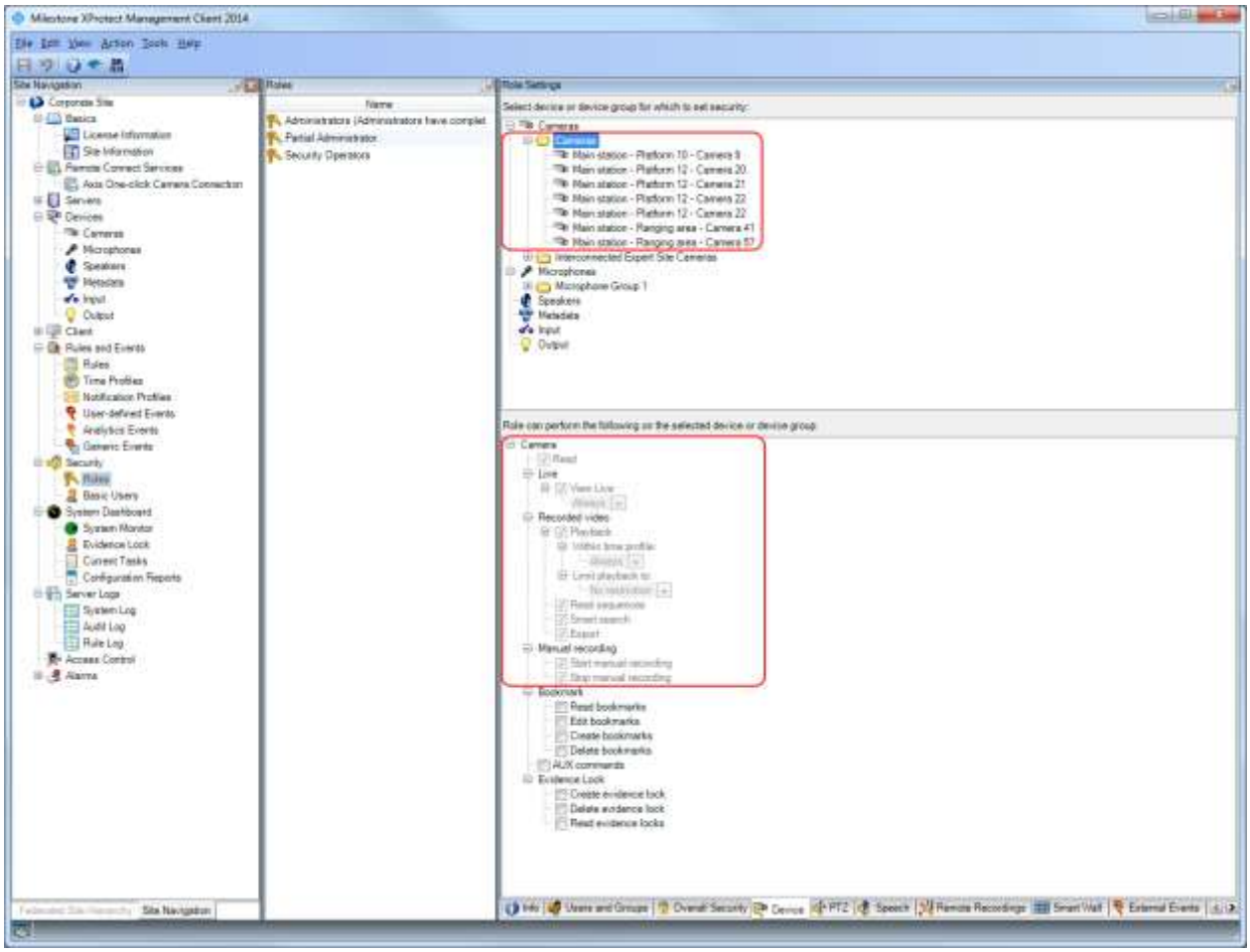
In the below example, permissions have been granted to a sub set of camera functions by checking the *Allow* checkboxes.

Note:
If the role already has been configured with access rights to either groups or individual devices, any change to the *Overall Security* settings will override these individual settings.



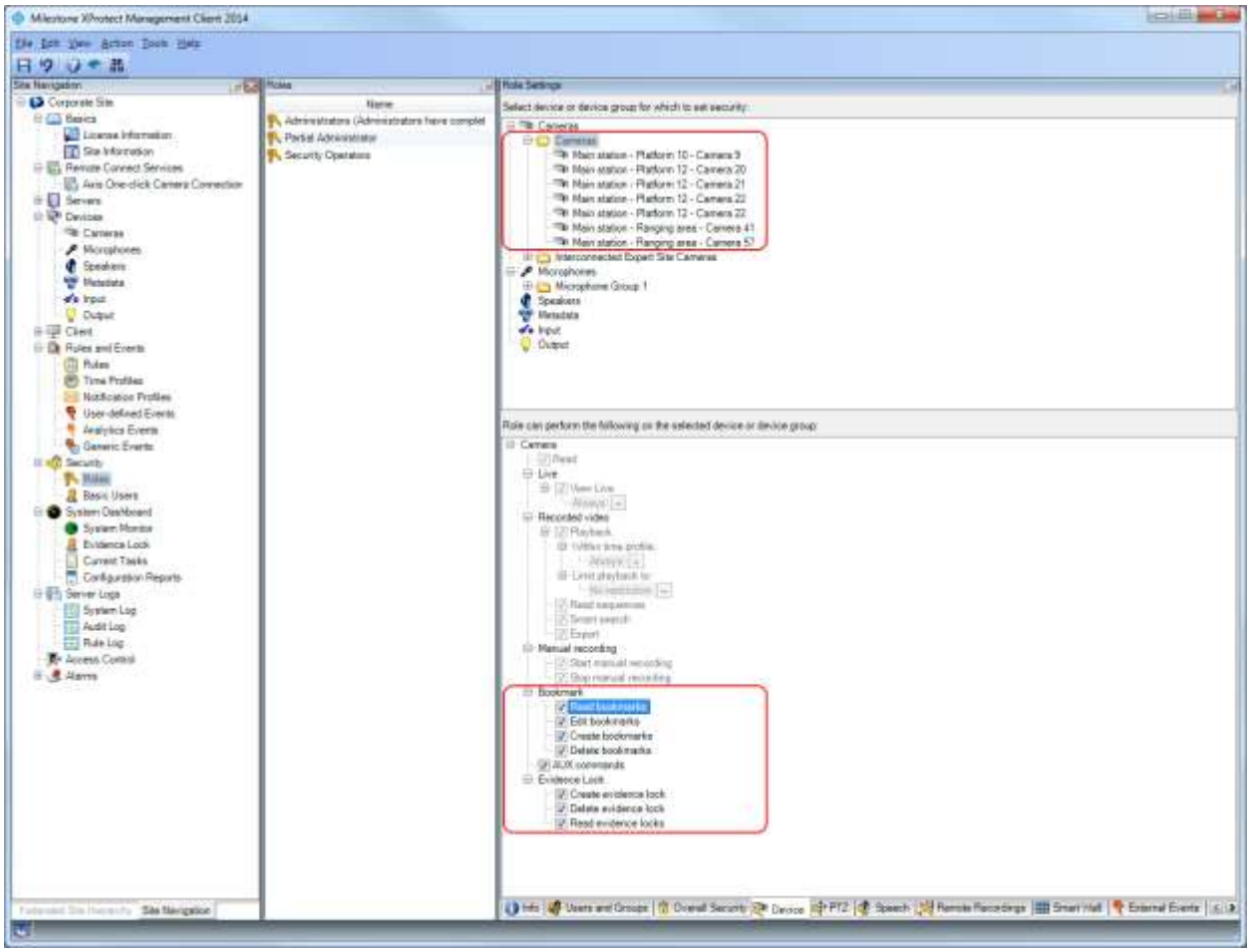
Several permissions set to *Allow* for the *Cameras* security group.

Selecting the *Device* tab, the camera permissions set to *Allow* on the *Overall Security* tab, are checked and greyed out as they are inherited from the *Overall Security* tab.



Allow permissions inherited by the cameras in the group and shown as read-only.

The settings not defined as either *Allow* or *Deny* on the *Overall Security* tab can be set individually per device, as shown in the screenshot below:



Permissions not set to either *Allow* or *Deny* can be set individually on the cameras.

Deny permission

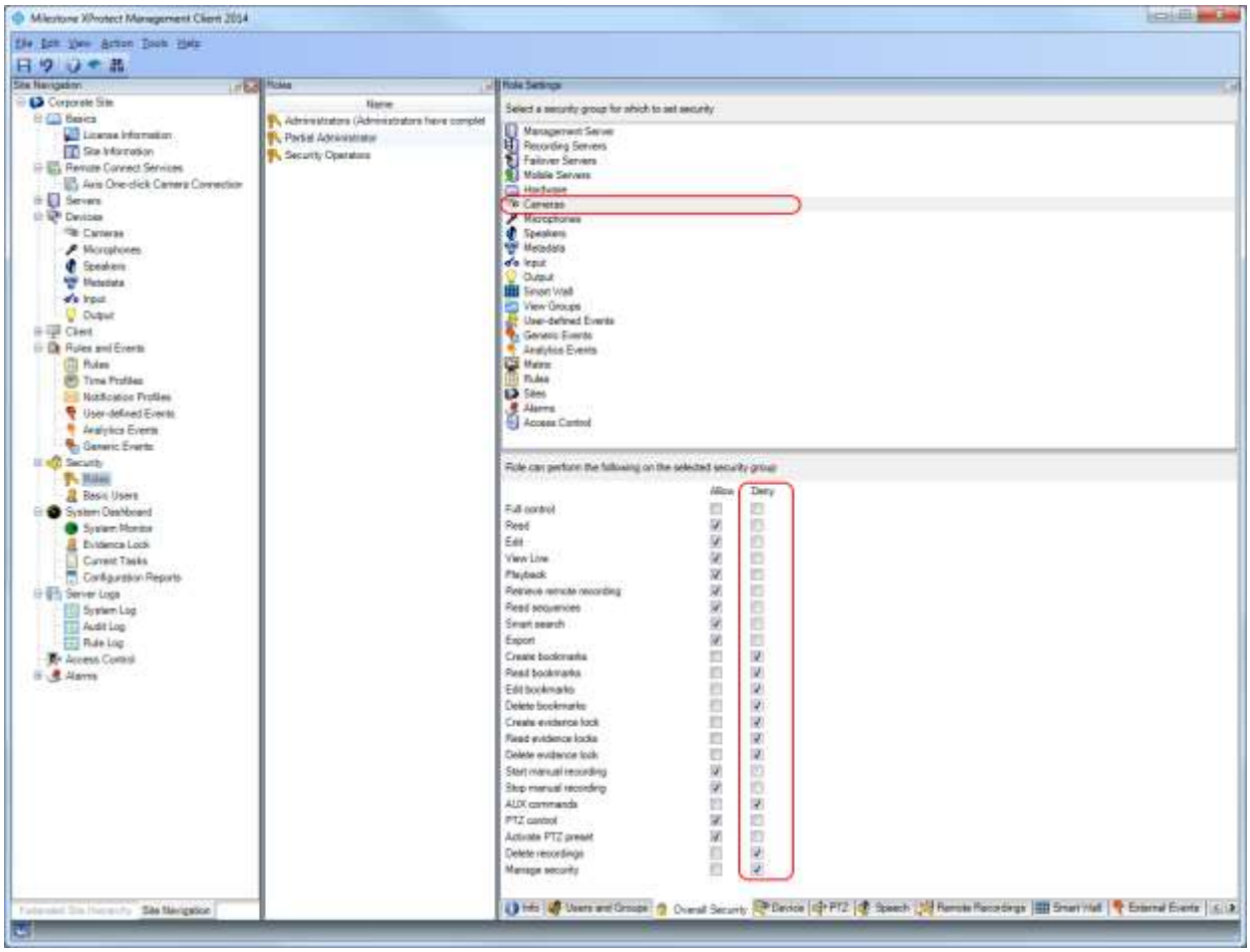
In addition to the *Allow* permission, XProtect Corporate 2014 also supports a *Deny* permission. The *Deny* permission can be used to control permissions for users that are members of two or more roles. In this case the user's actual permission will be a combination of the permissions in all roles the user is a member of with the *Deny* permission taking precedence over the *Allow* permission.

A few examples:

- If the *Allow* permission is set for cameras in one role and nothing is selected in another role, the user will be able to access the cameras.

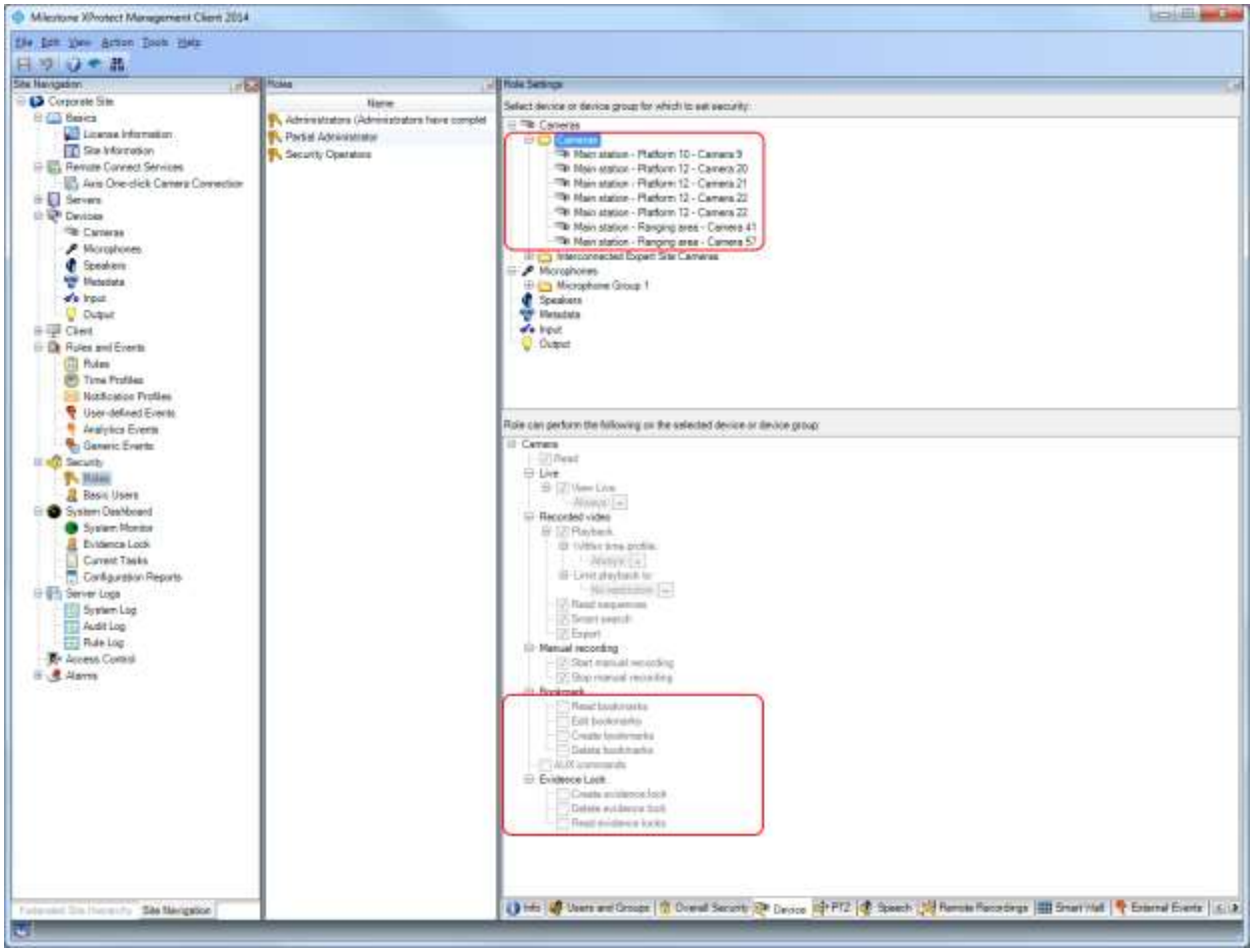
- If the *Allow* permission is set for cameras in one role, but set to *Deny* in another role, the user will not be able to access the cameras, as the *Deny* permission takes precedence.
- If permission is enabled for the cameras on the *Device* tab in one role, but set to *Deny* in another role, the user will not be able to access the cameras, as the *Deny* permission takes precedence.

This means that the *Deny* permission can be utilized to permanently or temporarily deny users' access (to for instance cameras) by creating a second role with *Deny* permission set. All users added to this group will then be denied access.



Several permissions set to *Deny* for the *Cameras* security group

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.



Deny permissions inherited by the cameras in the group and shown as read-only.

Dual Authorization

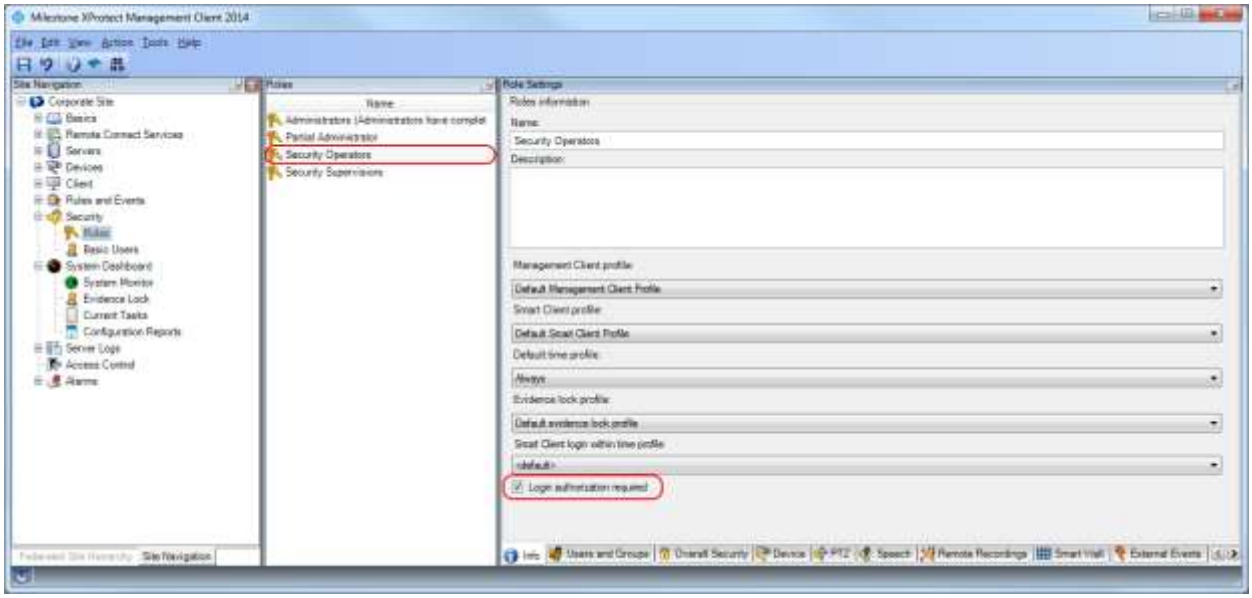
In addition to extending the XProtect Corporate 2014 administration and device permissions, XProtect Corporate 2014 also offers increased security by introducing dual authorization.

Dual authorization is a method whereby a user must be authorized by another supervising user to get access to the system.

Dual authorization has been implemented as an option per role and is supported by both the XProtect Smart Client and the XProtect Management Client. If the Milestone Mobile Client, the XProtect Web Client or MIP SDK integrations are used with a role that requires dual authorization, access will

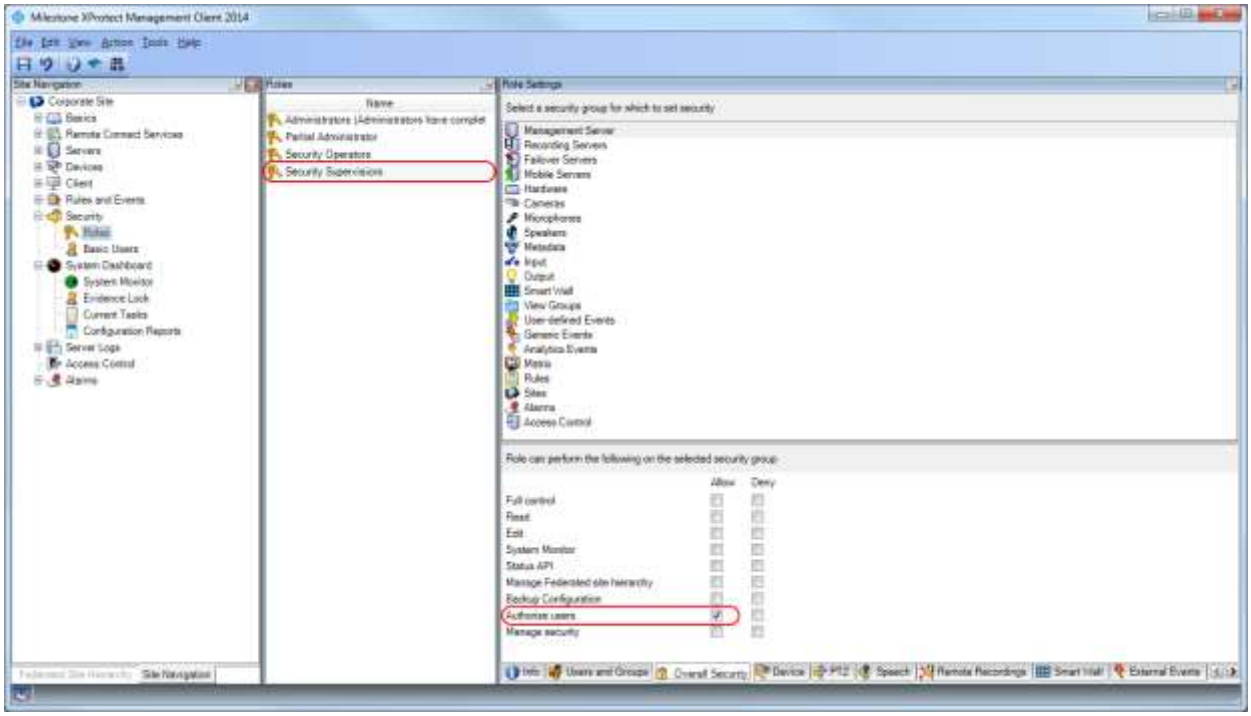
be denied as these clients and MIP SDK integrations do not yet support dual authorization.

Dual authorization is enabled for a selected role by checking the *Login authorization required* checkbox on the roles *Info* tab. When this is done all users in this role will be prompted for a second user (supervisor) to authorize their access to the system.



Login authorization required checked for a role.

Users (supervisors) that can do the authorization are configured by creating a second role and in this role give permission to authorize access by checking the *Authorize users* checkbox found under the *Management Server* node in the *Overall Security* tab.



Authorize users' permission checked in the *Management Server* security group for a role.

When a user or administrator (in a role requiring authorization) tries to login with the XProtect Smart Client or XProtect Management Client, he or she is presented with a second authentication dialog prompt (for a second user or supervisor) to authorize access.

In both XProtect Smart Client and XProtect Management Client the user doing the authorizing can see who is being authorized as the name of the first user is displayed in the dialog.

XProtect Management Client login and authorization dialogs:

Initial login dialog.

Authorization dialog.

Audit log

When a user is authorized and granted access two log entries are made, one for the user being authorized (*User successfully logged into the system from the…)* and one for the user (supervisor) authorizing access (*User authorized '[Basic]\Tom Kristensen')*.

Login and authorization audit log messages.

Benefits and summary

Designed to meet strict demands to system security from customers operating in high security and sensitive surveillance installations, XProtect Corporate offers an array of security mechanisms to protect the system for both external and internal tampering.

The foundation of this security control is role-based user rights management, where individual users are assigned different roles and each role is granted full or partial permission to make use of certain functionality and access different cameras and other security peripherals connected to the system.

XProtect Corporate 2014 introduces a number of additional system security concepts - that optionally can be applied to increase security even further. With regard to user access:

- *Dual authorization* only allow users to access the system once a second co-worker or supervisor has validated the login. This capability prevents individual users from illegally accessing sensitive information and is considered a critical function in any high security operation.

This white paper also elaborates on a new tiered management user rights concept that makes it possible to assign partial permission(s) to system administrators. This access permission makes it possible to limit specific administrator rights to only perform certain actions in the system - or limit the user to be able to configure only a specific subset of cameras and/or other security peripherals within the system a powerful capability for any large system with multiple system administrators or in installations where contractors need access to certain management functionality.

Another important new security concept discussed in this white paper is the *Overall Security* settings, which enables definition of common permission settings for all functions and devices connected to the system for a given user role. Since these common settings are automatically inherited by new devices added to the system it streamlines both the initial setup and the daily management of the system.

XProtect Corporate 2014 also introduces the ability to customize available functions in the administrator user interface, XProtect Management Client. This means that the user interface can be optimized for different administrator's responsibility areas and skill levels - by simply removing functions in the user interface that are not relevant to a specific role. This capability can reduce the cost of training and the potential risk of unintentional misconfiguration of the system.

About Milestone Systems

Founded in 1998, Milestone Systems is the global industry leader in open platform IP video management software. The XProtect platform delivers powerful surveillance that is easy to manage, reliable and proven in thousands of customer installations around the world. With support for the widest choice in network hardware and integration with other systems, XProtect provides best-in-class solutions to video enable organizations – managing risks, protecting people and assets, optimizing processes and reducing costs. Milestone software is sold through authorized and certified partners. For more information, visit **www.milestonesys.com**

Milestone Systems Headquarters, DK
Tel: +45 88 300 300

Milestone Systems US
Tel: +1 503 350 1100