Connecting SINEC NMS to UMC

SIMATIC, SCALANCE

https://support.industry.siemens.com/cs/ww/en/view/109780337

Siemens Industry Online Support

Legal information

Use of application examples

Application examples illustrate the solution of automation tasks through an interaction of several components in the form of text, graphics and/or software modules. The application examples are a free service by Siemens AG and/or a subsidiary of Siemens AG ("Siemens"). They are non-binding and make no claim to completeness or functionality regarding configuration and equipment. The application examples merely offer help with typical tasks; they do not constitute customer-specific solutions. You yourself are responsible for the proper and safe operation of the products in accordance with applicable regulations and must also check the function of the respective application example and customize it for your system.
Siemens grants you the non-exclusive, non-sublicensable and non-transferable right to have the application examples used by technically trained personnel. Any change to the application examples is your responsibility. Sharing the application examples with third parties or copying the application examples or excerpts thereof is permitted only in combination with your own products. The application examples are not required to undergo the customary tests and quality inspections of a chargeable product; they may have functional and performance defects as well as errors. It is your responsibility to use them in such a manner that any malfunctions that may occur do not result in property damage or injury to persons.

Disclaimer of liability

Siemens shall not assume any liability, for any legal reason whatsoever, including, without limitation, liability for the usability, availability, completeness and freedom from defects of the application examples as well as for related information, configuration and performance data and any damage caused thereby. This shall not apply in cases of mandatory liability, for example under the German Product Liability Act, or in cases of intent, gross negligence, or culpable loss of life, bodily injury or damage to health, non-compliance with a guarantee, fraudulent non-disclosure of a defect, or culpable breach of material contractual obligations. Claims for damages arising from a breach of material contractual obligations shall however be limited to the foreseeable damage typical of the type of agreement, unless liability arises from intent or gross negligence or is based on loss of life, bodily injury or damage to health. The foregoing provisions do not imply any change in the burden of proof to your detriment. You shall indemnify Siemens against existing or future claims of third parties in this connection except where Siemens is mandatorily liable.
By using the application examples you acknowledge that Siemens cannot be held liable for any damage beyond the liability provisions described.

Other information

Siemens reserves the right to make changes to the application examples at any time without notice. In case of discrepancies between the suggestions in the application examples and other Siemens publications such as catalogs, the content of the other documentation shall have precedence.
The Siemens terms of use (https://support.industry.siemens.com) shall also apply.

Security information

Siemens provides products and solutions with Industrial Security functions that support the secure operation of plants, systems, machines and networks.
In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens' products and solutions constitute one element of such a concept.
Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the Internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.
For additional information on industrial security measures that may be implemented, please visit https://www.siemens.com/industrialsecurity.
Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats.
To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed at: https://www.siemens.com/industrialsecurity.

Table of contents

1 Introduction

1.1 Overview

Efficient user management is an essential part of every security concept. The User Management Component (UMC) enables for system-wide central maintenance of users with an optional connection to Microsoft Active Directory. Person-specific assignment of roles and permissions minimizes maintenance effort while achieving a high level of transparency. Central user management thus represents the basis for an efficient, thorough administration of personalized access permissions within the system. This can significantly reduce security risks.

UMC allows the establishment of a central user management. This means that you can define and manage users and user groups across software and devices. Users and user groups can also be transferred from a Microsoft Active Directory (AD).

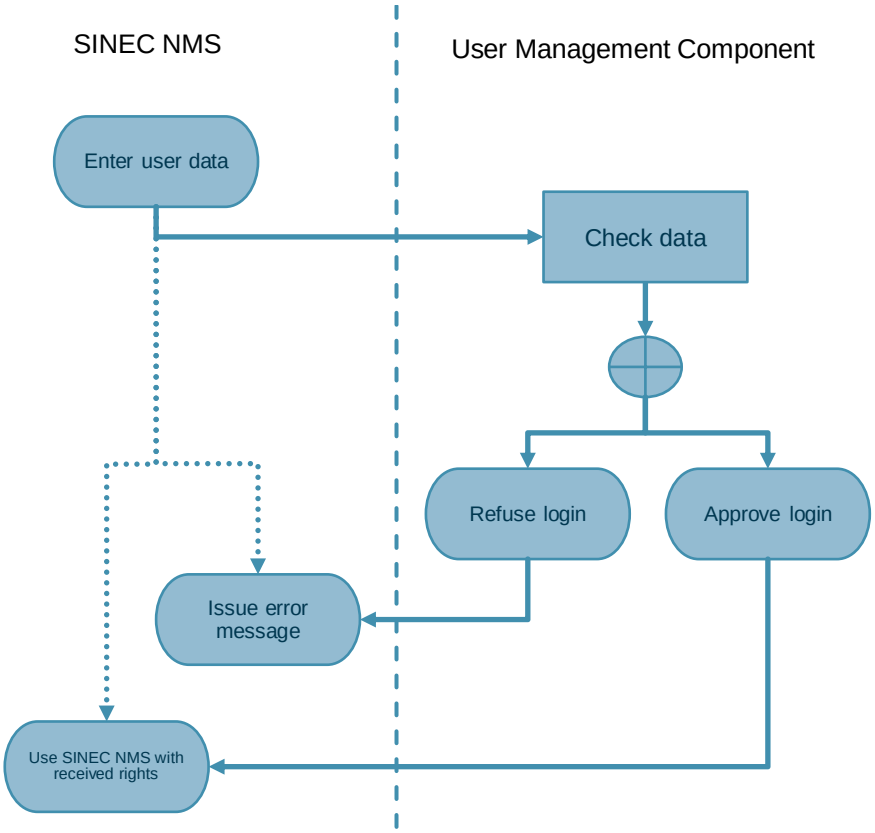
You can import the global users and user groups into the various applications or use them as temporary users.

This document builds on the base document under the same article ID. In the base document, you will find a description of the installation and setup of the UMC.

In this document, you will learn how to connect the network management system SINEC NMS to UMC and how to log in with a UMC user or a user from the AD.

1.2 Principle of Operation

The UMC server receives the login requests of the connected applications and checks the entered user data. Then the application receives a response whether the logon credentials are correct and the logon is approved.



Note

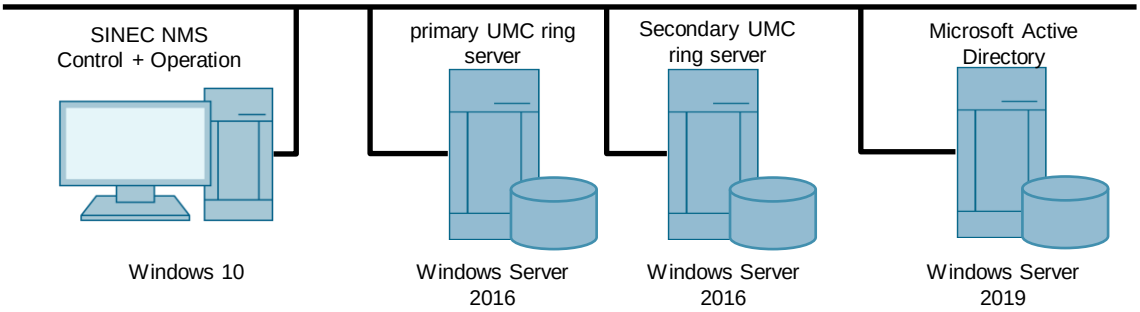
The exchange between SINEC NMS and UMC server takes place in the web browser of the client.

2 Engineering

2.1 Hardware setup

The following Figure shows the hardware setup in this example.

Figure 2-1



Requirement

This application example builds on the base document. Ensure that the UMC and Microsoft AD are set up appropriately.

Example users and groups

The following UMC users with their associated groups are used in the example.

Table 2-1

Users	Groups
Admin	Administrator (UMC)
MYCORP\John.Doe	Administrators, domain admins, SINEC_NMS_Admin_Group, UM service accounts
MYCORP\UmcUser	UM_Users, Domain Users
MYCORP\ServiceEngineer	Engineers, Domain Users
MYCORP\Administrator	Administrators, Domain Admins
Bob	SINEC_NMS_Admin_Group (UMC)

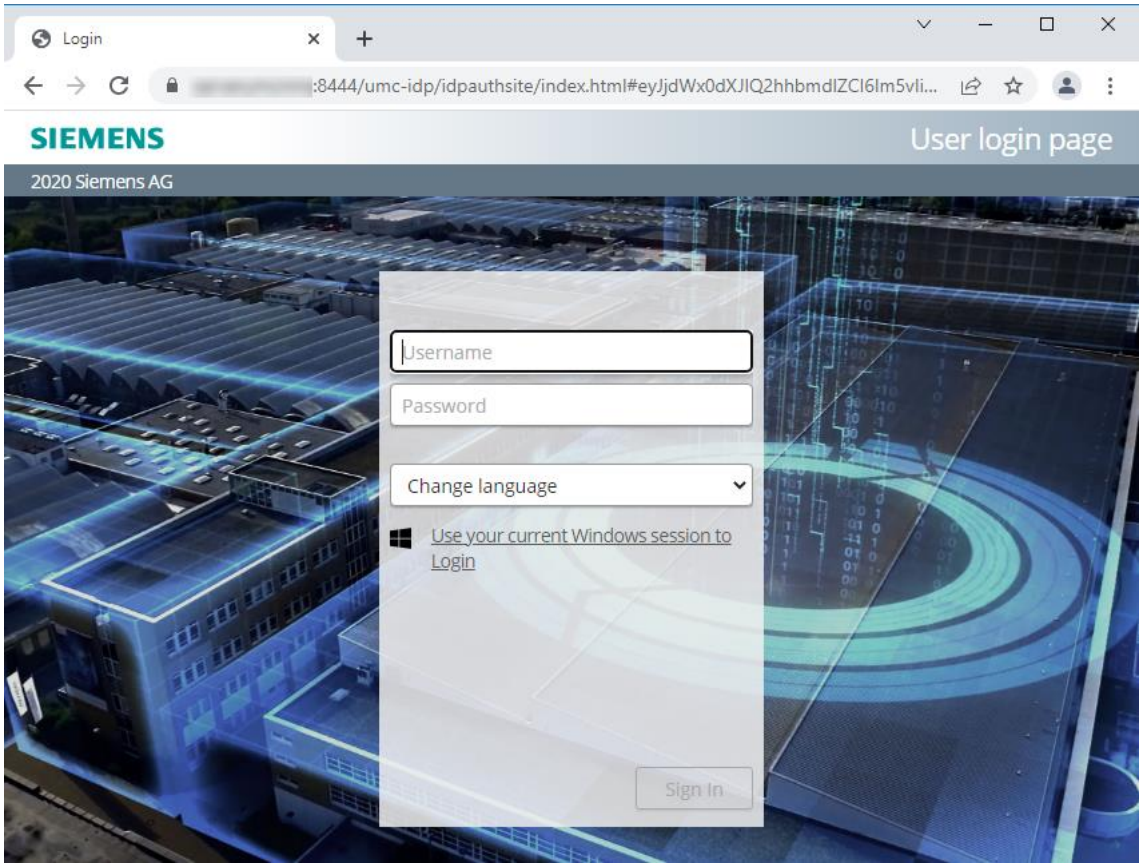
2.2 Adjusting Settings in the UMC

To use a UMC user in SINEC NMS, the user must be a member of a special group that is created in the UMC and linked to a role in SINEC NMS.

Logon to the UMC WBM

When UMC is installed with the SINEC NMS setup, it can be accessed via the following web page. Open a web browser and enter the URL "https://<IP address>:8444/UMC". When logging in, use the user that you specified during installation.

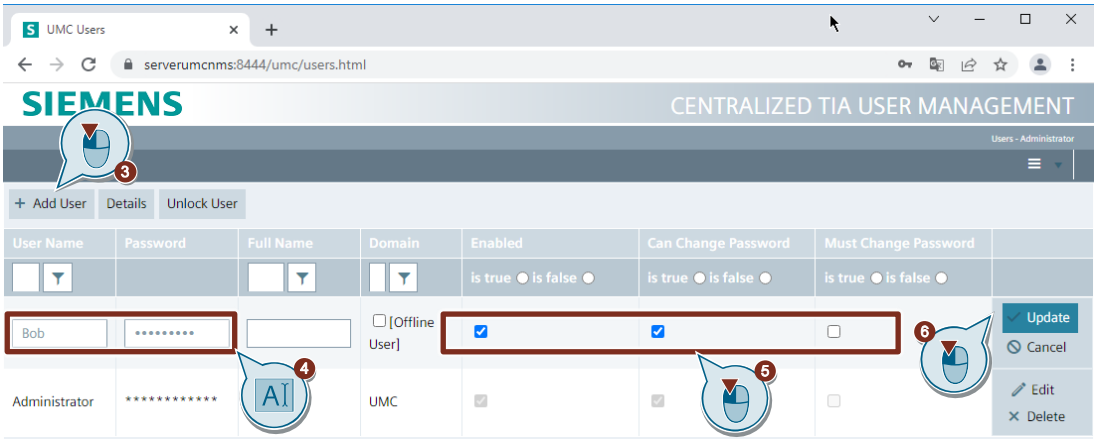
Figure 2-2



Create users

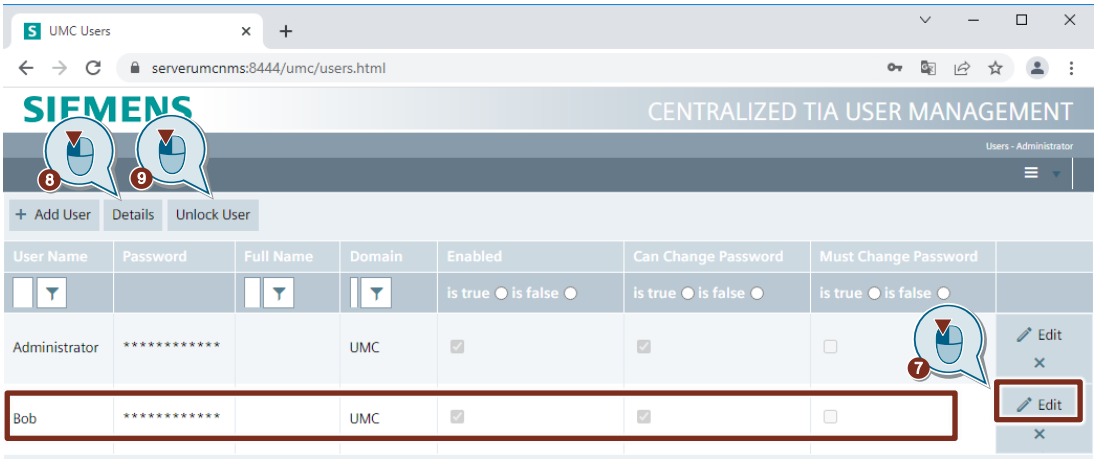
1. Click the "Menu" button (3 bars).
2. Open the "Users" menu. Users are created and permissions assigned in this menu.

3. Click the "Add Users" button to create a new user.
4. Enter a username and a password for the new user.
5. Make the following settings for the user:
   - Enable the user.
   - Give permission to change the password. Because the password will expire after 60 days according to the default configuration, it is advisable to modify the permission for new users to match the company policies.
   - It is also possible to require the new user to change the password after logging in for the first time.
6. Click "Update" to apply the settings.
   The user will be created with the settings you have specified.



7. Click the "Edit" button to modify the user's settings.

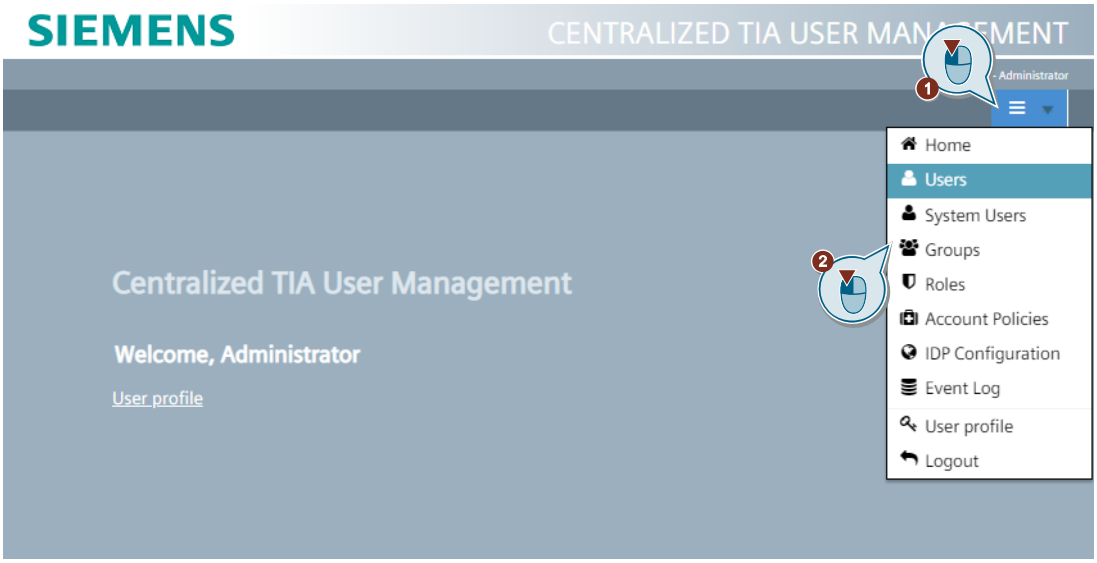
8. Select the user and click "Details" to set the details of the user. Details of a user are e. g.
   - Attributes such as email address
   - Roles for the UMC server
9. Click "Unlock User" to unlock a user if it has been locked. This happens if the wrong password was entered too many times, for example.



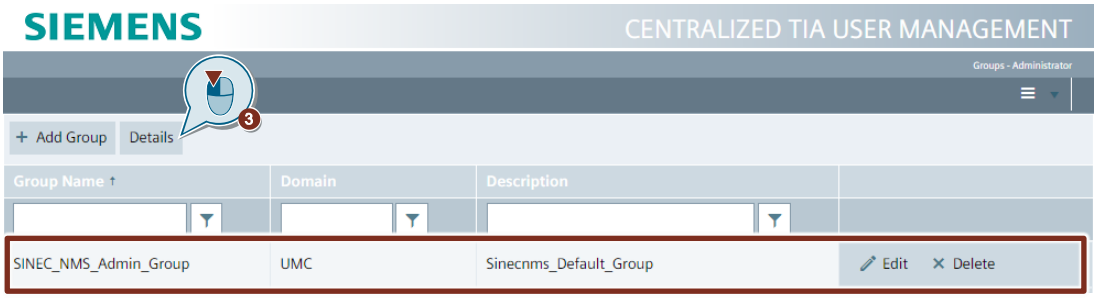
Assign user to a group

Access rights to SINEC NMS are assigned with groups. The group "SINEC_NMS_Admin_Group" is the default UMC group in SINEC NMS for allowing the UMC users administrative access to SINEC NMS.

1. Click the "Menu" button (3 bars).
2. Open the "Groups" menu. This is the menu where new users can be added to existing groups or new groups can be created. New groups are necessary if a new role in SINEC NMS needs to be linked with UMC users.



3. Select the group "SINEC_NMS_Admin_Group", already created when UMC was installed, then click the "Details" button to add the users to this group.
   The detail view of the group will open.



Note

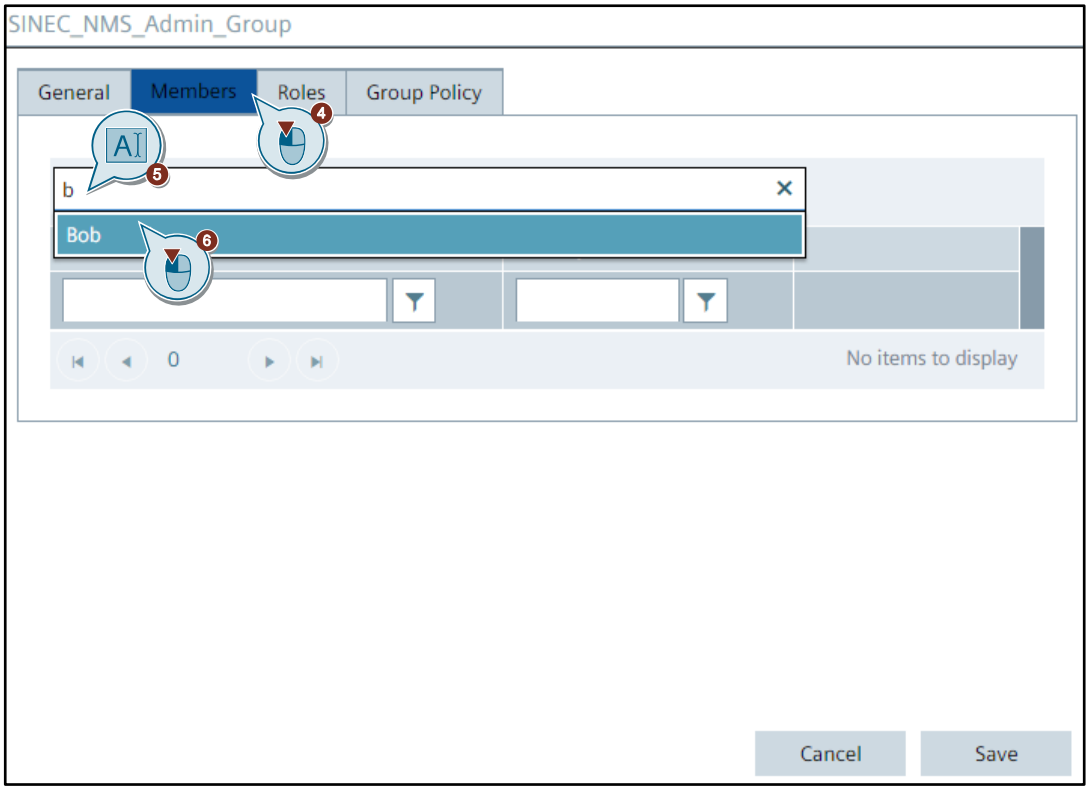
If the group "SINEC_NMS_ Admin_Group" does not exist in UMC, create it.

If you wish to use a different group name, create it in SINEC NMS (see chapter 2.3.1).

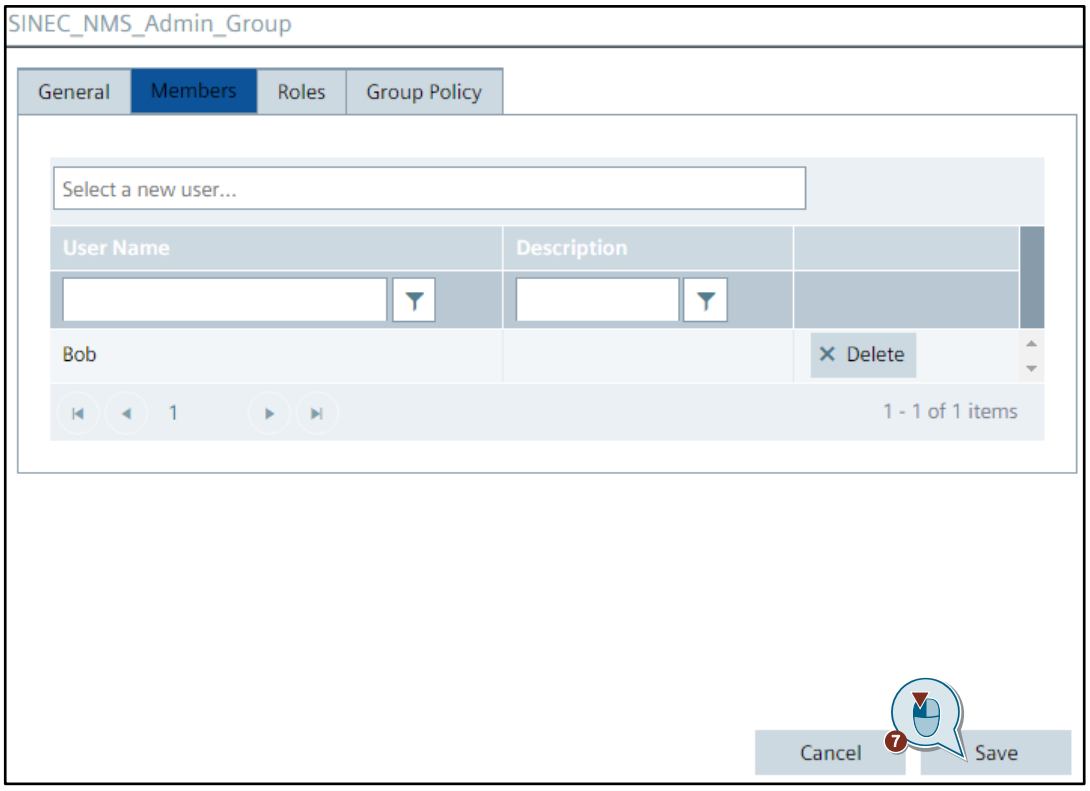
4. Open the "Members" tab.
   All current group members will be displayed.
5. Enter the first letters of a user who will later need to have administrative access to SINEC NMS.
   All users with the initial letters you entered will be displayed in a list.
6. Select the desired user to assign it to the group as a group member.

Note

You can assign additional users to the group as group members.



7. Click "Save" to save the group members you have entered.



8. If you need additional SINEC NMS users who should not have administrative access, create additional groups and add the desired members to them.

Result

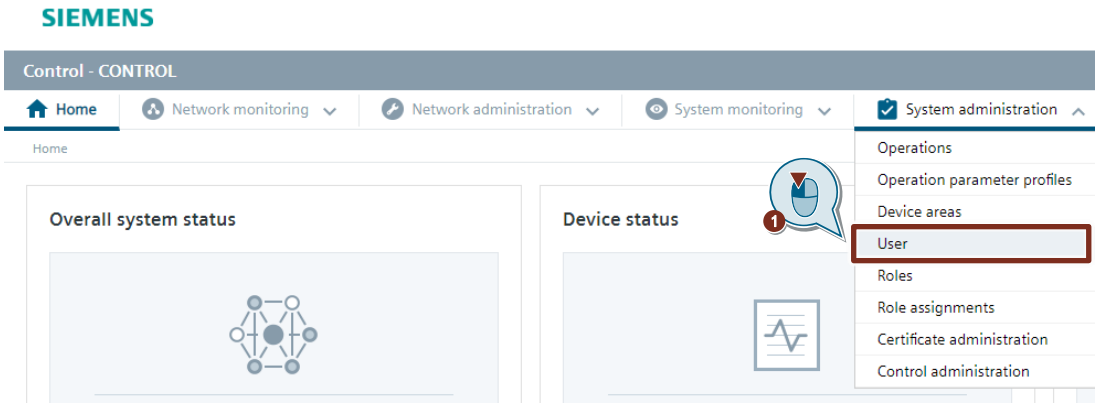
The modifications in the UMC ring server are complete.

2.3 Configuring SINEC NMS

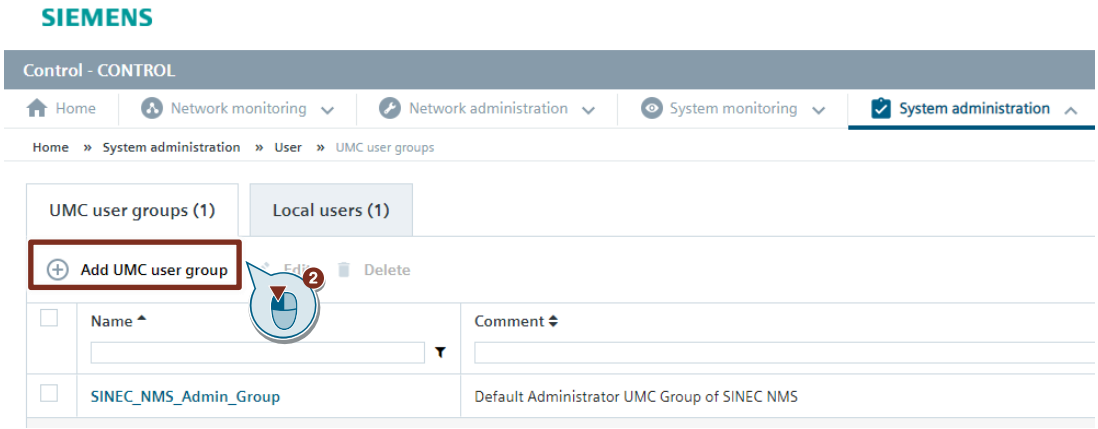
This example assumes that the basic setup of SINEC NMS has already been completed. Only the UMC-relevant setup will be addressed.

2.3.1 Create UMC user group

1. Open the menu "System administration > User" in the Control to create UMC user groups in SINEC NMS.



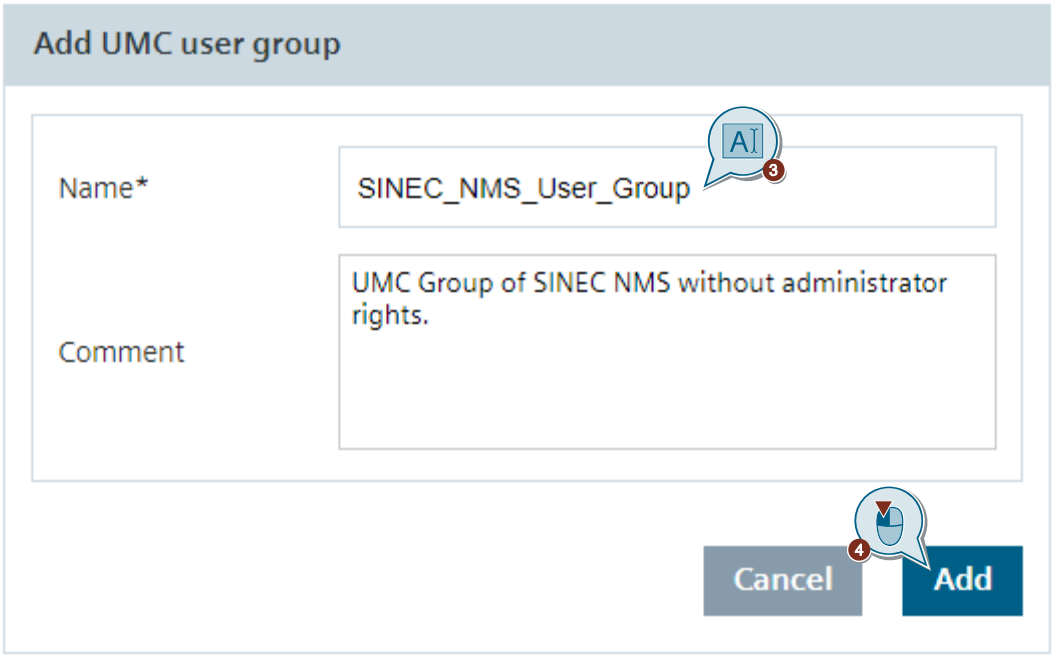
2. In the "UMC user groups" tab, click on "Add UMC user group".
The "Add UMC user group" dialog will open.



Note

The group "SINEC_NMS_Admin_Group" is the default UMC group in SINEC NMS for allowing the UMC users administrative access to SINEC NMS.

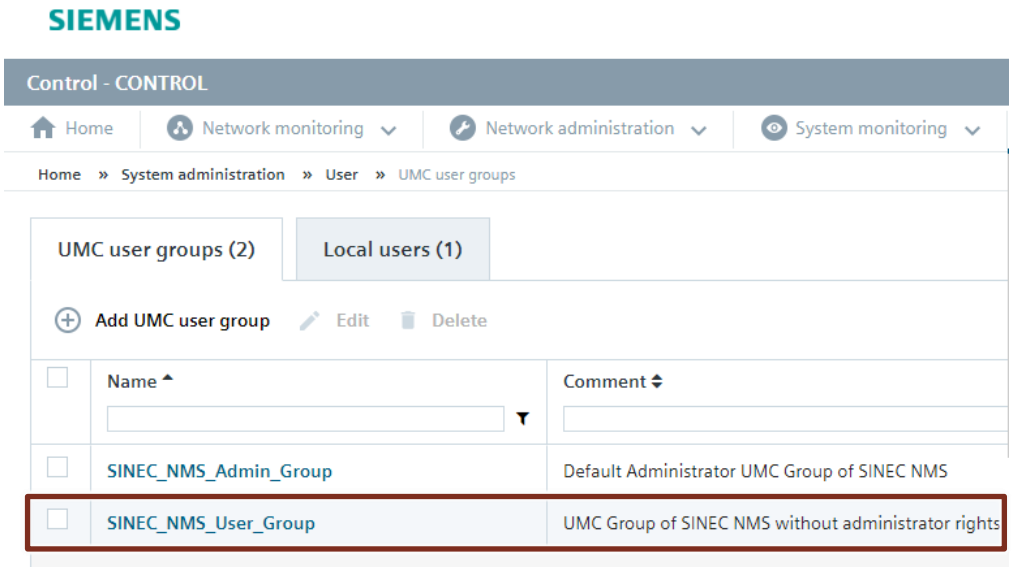
3. Enter a name for the UMC user group.
   Use exactly the same name as in UMC. In SINEC NMS, the user is assigned the rights based on the name of the UMC user group.
4. Click the "Add" button.



Result

The new UMC user group has been created in SINEC NMS.

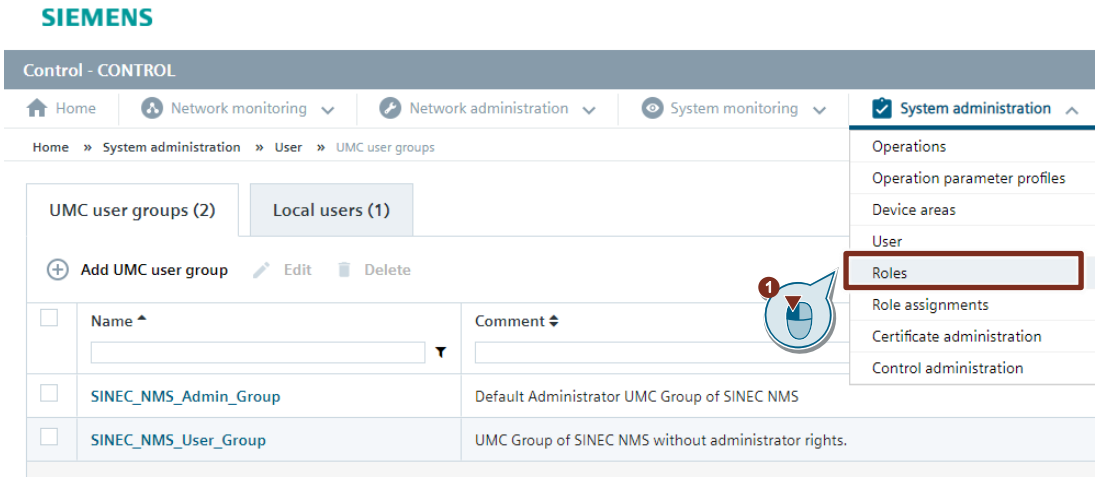
Figure 2-3



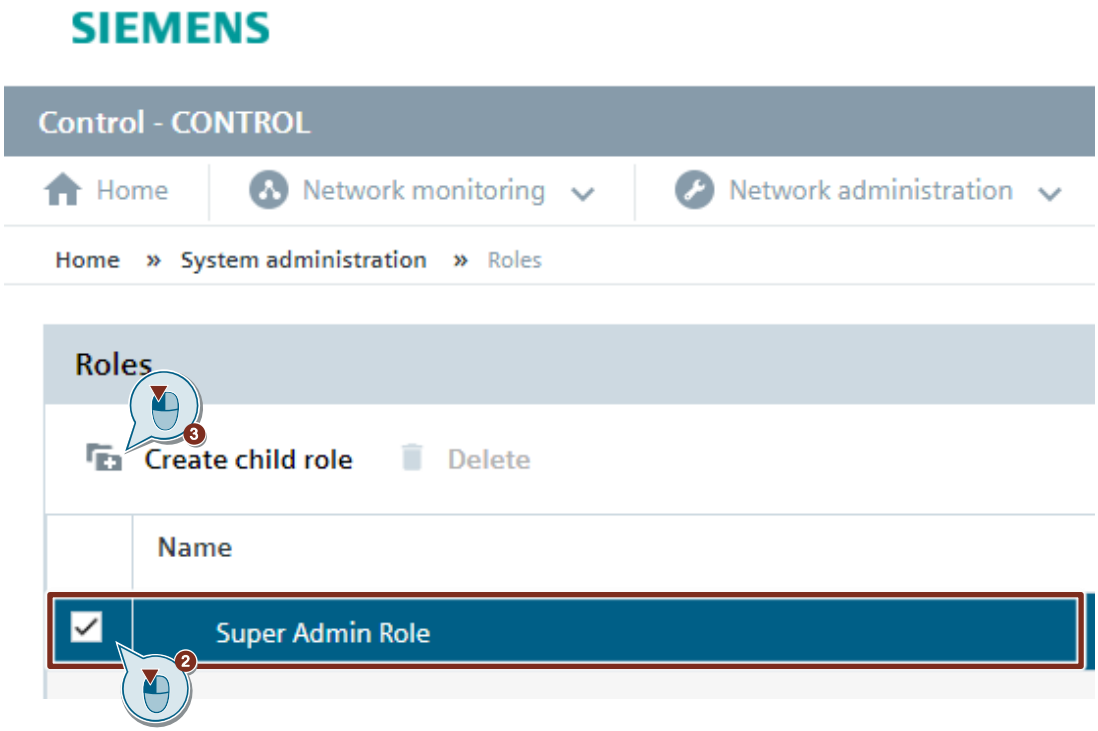
Assign the new UMC user group to an existing role in SINEC NMS or create a new role. A new role is necessary if a restriction in permissions or device areas is required.

2.3.2 Create role

1. Open the menu "System administration > Role" to add roles in SINEC NMS.

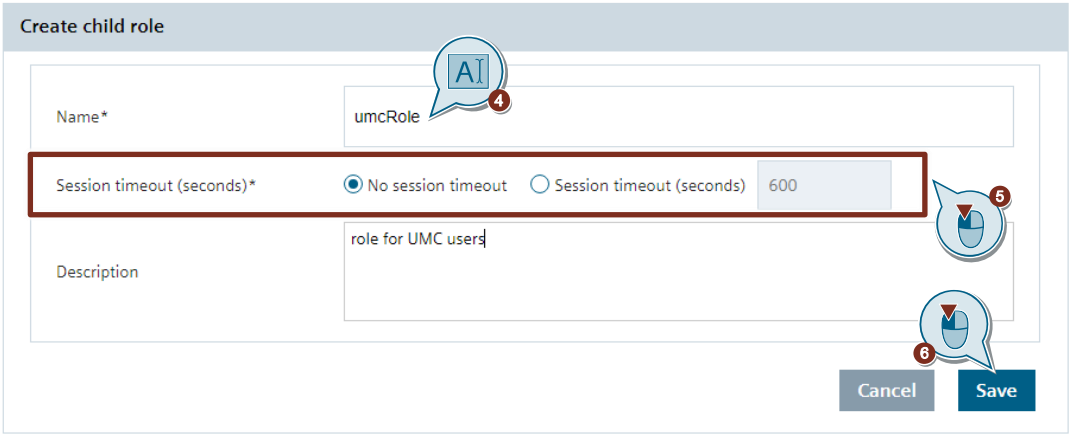


2. Select an existing role, e. g. the default role "Super Admin Role" with administrator privileges.
3. Click "Create child role". New roles will be created as child roles. In this case, the settings are inherited from the parent role.
   The "Create child role" dialog will open.



Note The group "SINEC_NMS_Admin_Group" is already assigned to the role "Super Admin Role".

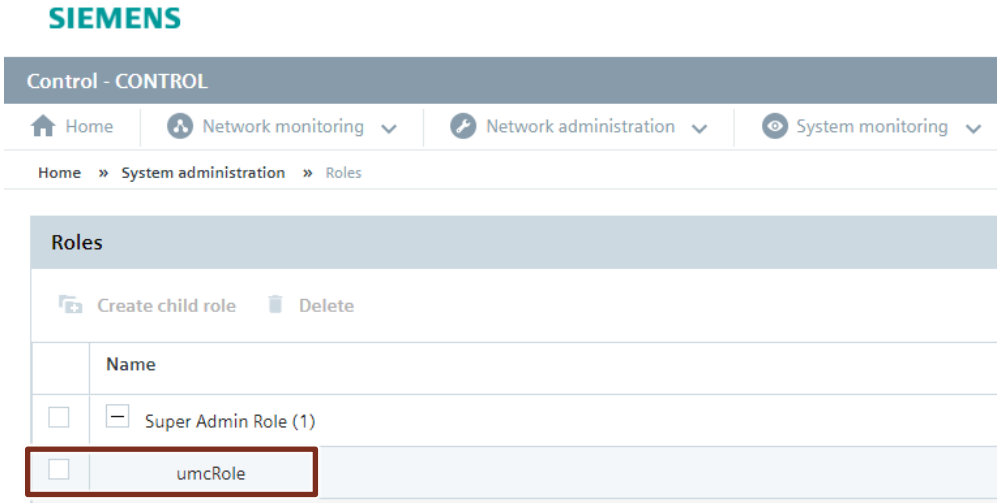
4. Enter a name for the role.
5. Set the session timeout.
6. Click the "Save" button.



Result

The new role has been created in SINEC NMS.

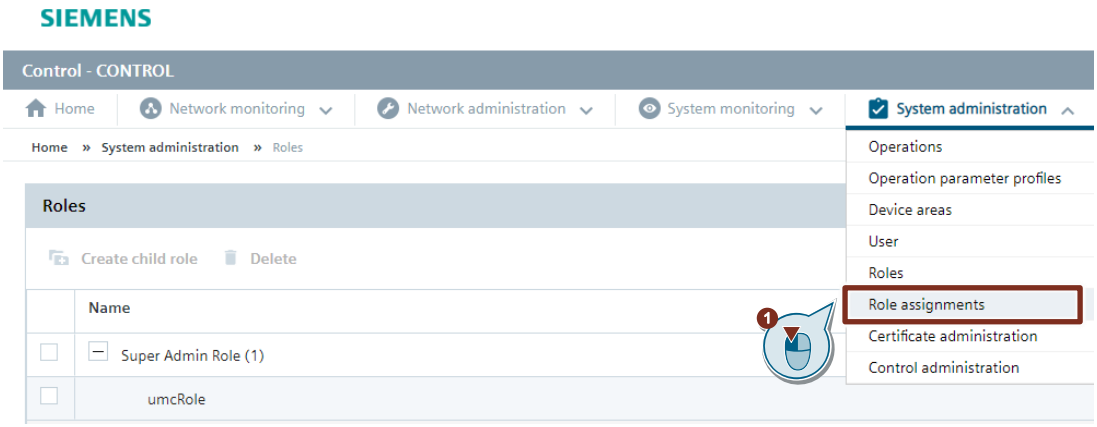
Figure 2-4



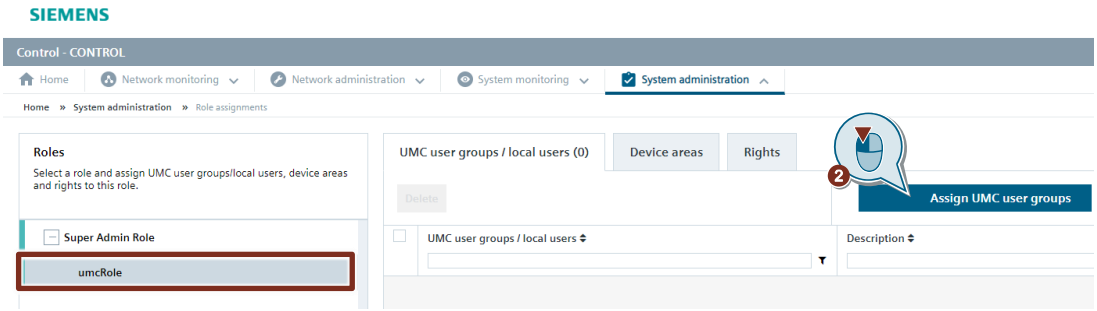
2.3.3 Assign UMC user group and rights to the role

Assign UMC user group

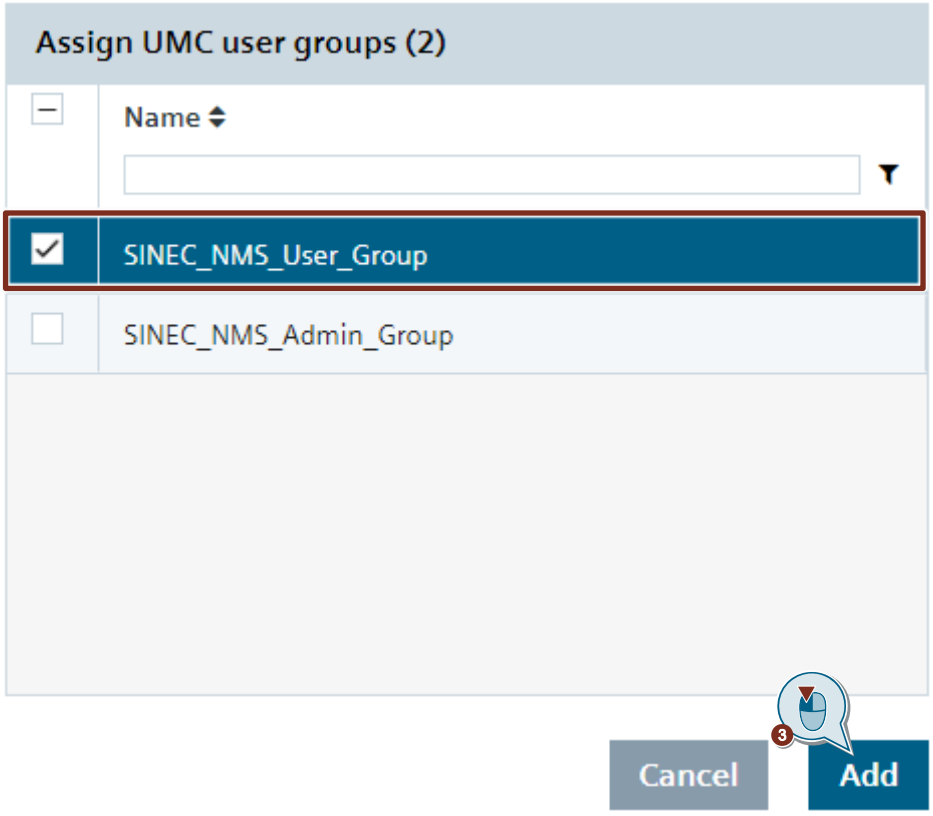
1. Open the menu "System administration > Role assignments" to add roles in SINEC NMS.



2. Select the role you wish to edit. Then click on "Assign UMC user groups" in the "UMC user groups / local users" tab.
The "Assign UMC user groups" dialog will open.

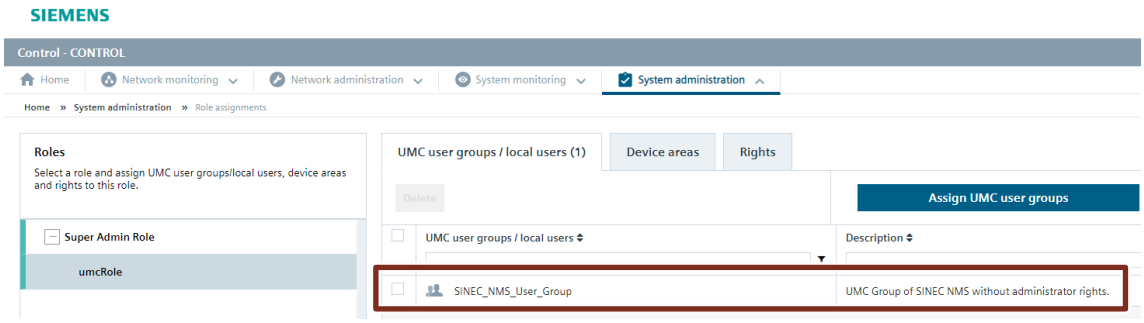


3. Select the desired UMC user group and click the "Add" button.



The UMC user group is assigned to the role.

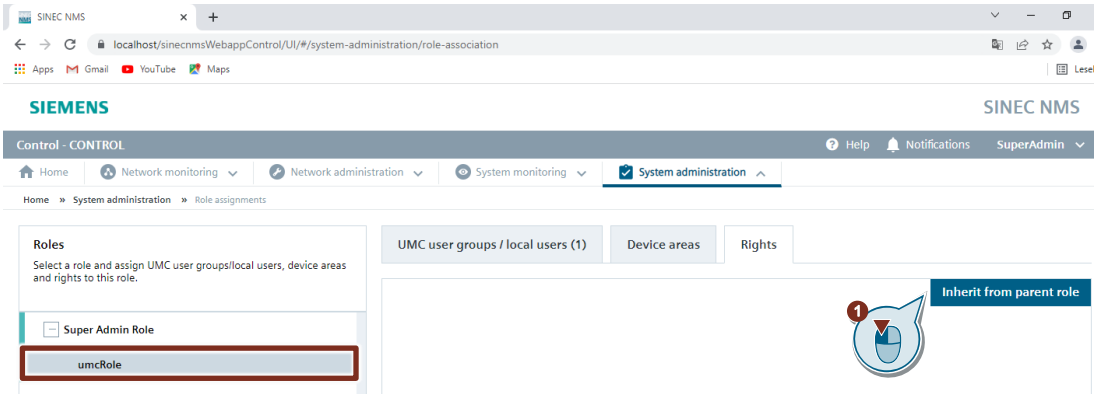
Figure 2-5



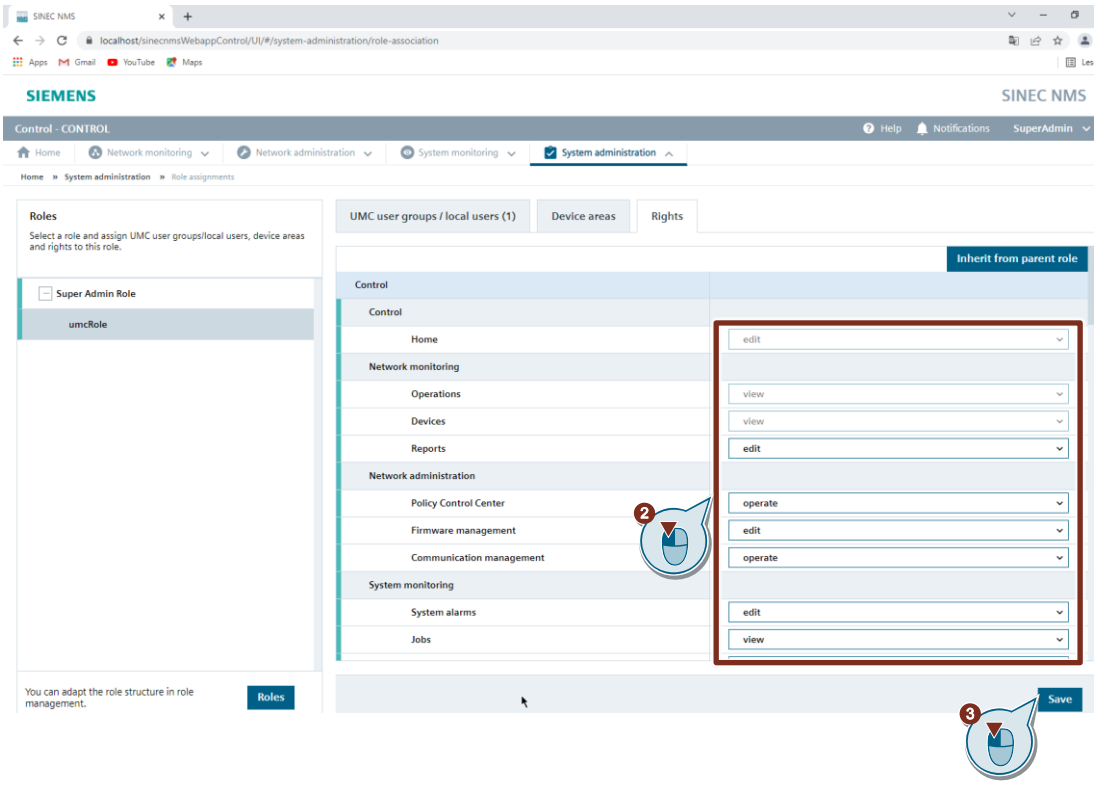
Assign rights to the role

1. Select the role you wish to edit, then click "Inherit from parent role" in the "Rights" tab. The newly created role receives the same rights as the higher-level role.

   Figure 2-6



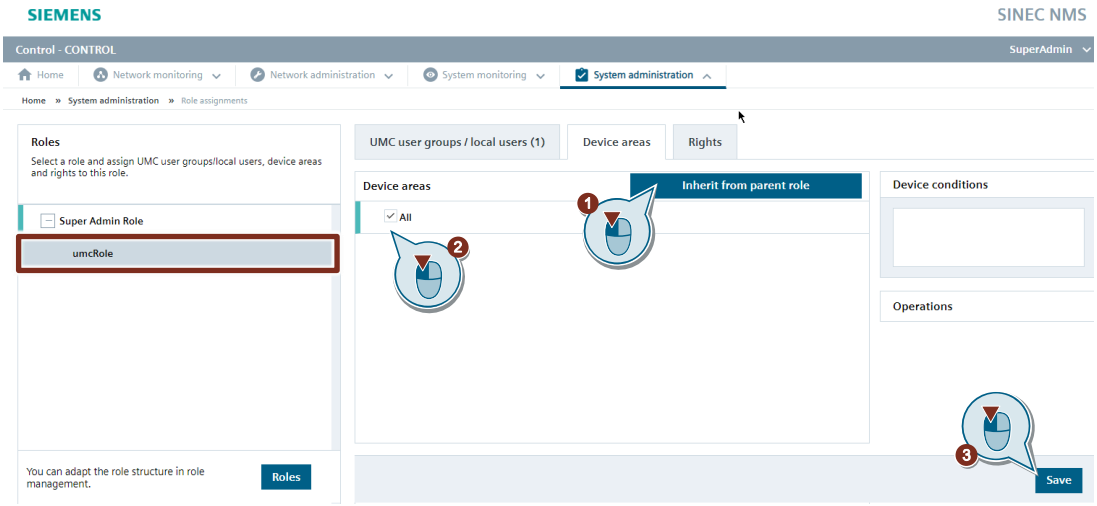
2. Modify the rights of the newly created role if necessary.
3. Click the "Save" button.



The rights are assigned to the role.

Assign device areas to the role

1. Select the role you wish to edit, then click "Inherit from parent role" in the "Device areas" tab to assign the desire device areas to the role.
2. Tick the checkbox associated with the device area.
   A role may be assigned all device areas of the parent role or fewer device areas.
3. Click the "Save" button.



The device areas are assigned to the role.

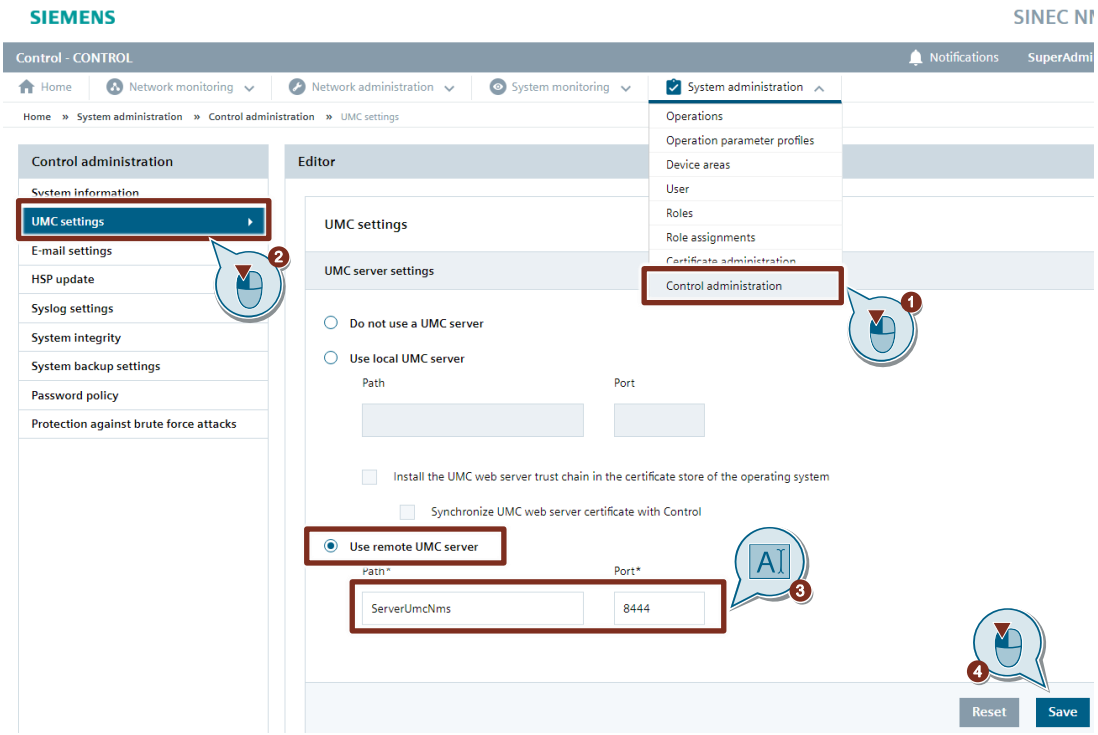
2.3.4 UMC settings

If the UMC ring server is not installed on the SINEC NMS Control PC, you must specify which address and port SINEC NMS can reach UMC at. By default, the settings are preset when installing SINEC NMS for UMC have been configured.

1. Open the menu "System administration > Control administration" in the Control.
2. Open the "UMC settings" page.
   Because the UMC server is located elsewhere in the network, the following option is enabled:
   - "Use remote UMC server"
3. Enter the address parameters of the UMC server.
   - IP address or device name
   - Port
4. Click the "Save" button.

Note

With this option, you must synchronize the certificates between the two systems (SINEC NMS and UMC) yourself.



If the UMC server is installed on the same PC as the SINEC NMS Control, the following option is enabled:

- "Use local UMC server"

The address of the UMC server will be displayed. The default port is 8444.

During the installation of SINEC NMS with the "UMC" option, the SINEC NMS EE certificates for UMC are stored in the certificate manager of the Control.

If the option "Install the UMC web server trust chain in the certificate store of the operating system" is enabled, the SINEC NMS EE certificate for UMC communication and the Microsoft Internet Information Server will be stored in the certificate store of the operating system.

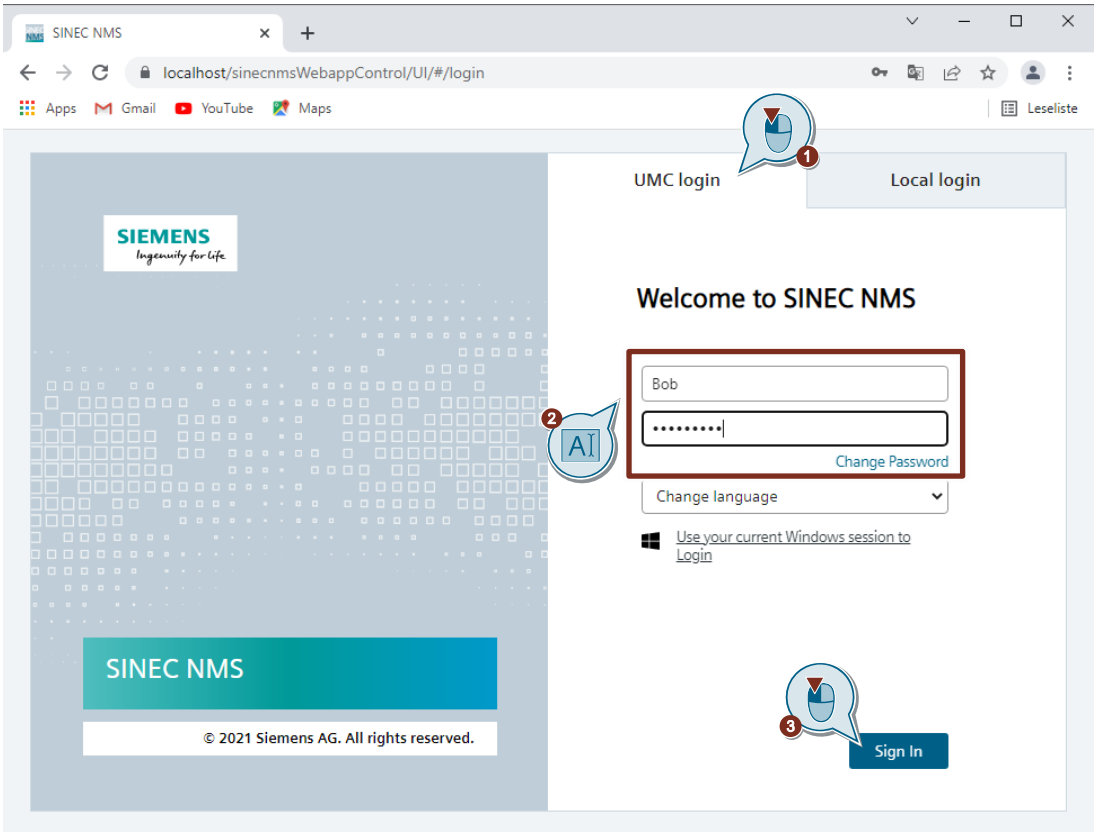
If the "Synchronize UMC web server certificate with Control" option is enabled, the UMC server certificate will be automatically synchronized with the Control. This is recommended in case you are refreshing a certificate.

2.4 Function test

Once you have adjusted the settings in UMC and SINEC NMS and you have set up the corresponding groups, you can log in to SINEC NMS with the UMC users.

Follow the instructions below to log in with a UMC user to the Web Based Management of the SINEC NMS Control:

1. Open the Web Based Management of the SINEC NMS Control and select "UMC login" as a login method.
2. Enter the login credentials of a user who is a member of the UMC group you created. In this application example, the UMC user "Bob" is a member of the UMC group.
3. Click the "Sign In" button.



Note

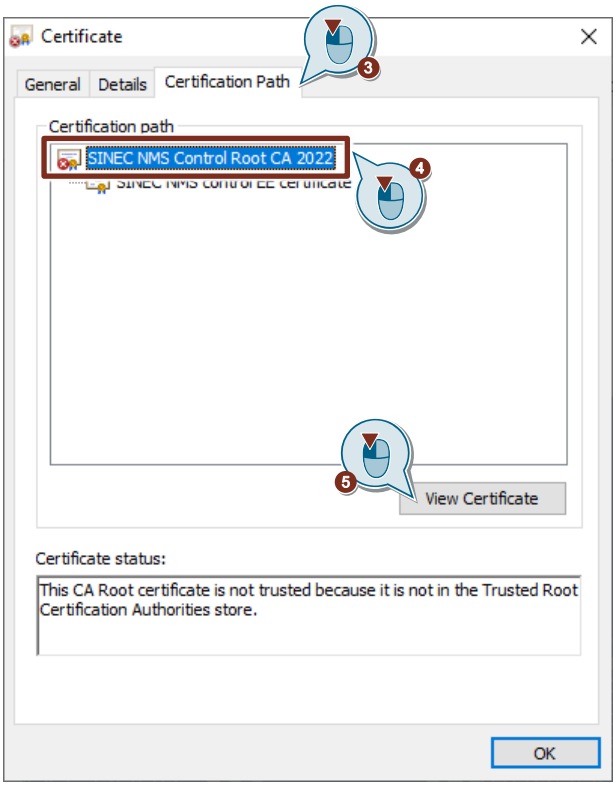
At the initial UMC login to the SINEC NMS WBM, you will enter the login credentials of the UMC administrator.

3 Useful information

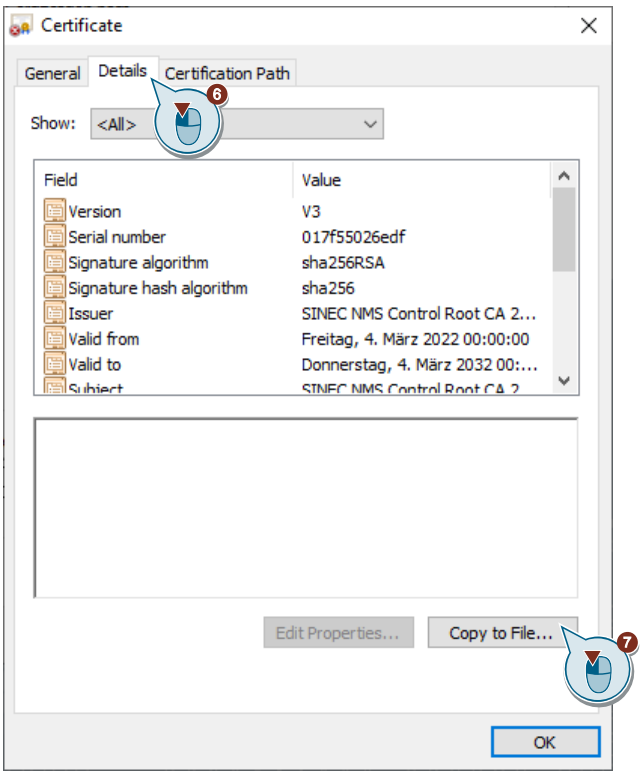
3.1 Trusting the SINEC NMS Root Certification Authority

Trust the SINEC NMS Root Certification Authority.

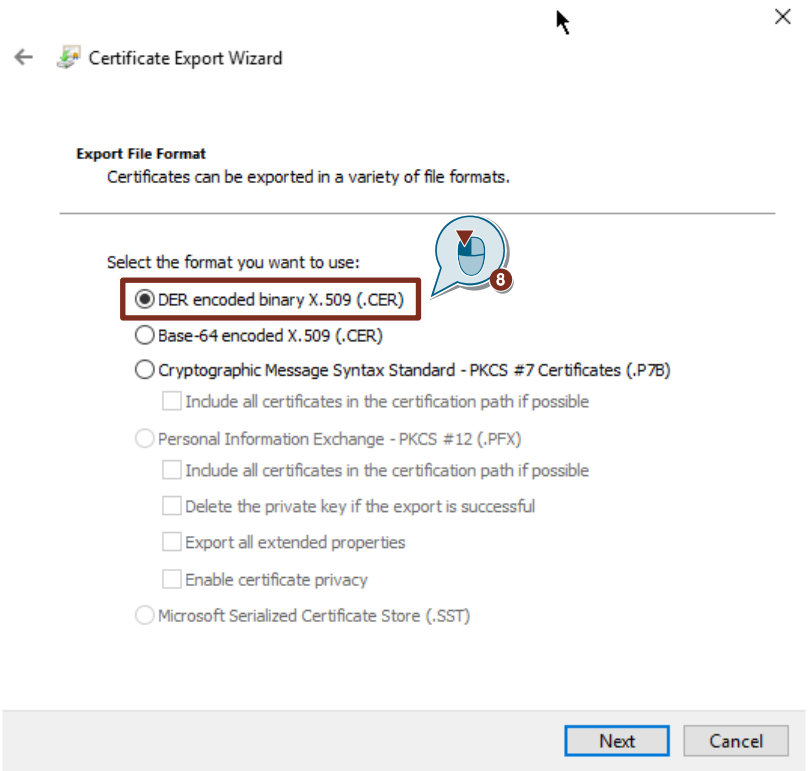
1. Open the SINEC NMS Control in a web browser (https://<IP address> or <Host name>).
2. Click on the security warning in the address bar of the web browser and select the certificate.
3. In the "Certificate" dialog, open the "Certification Path" tab.
4. Select the Root CA certificate (SINEC NMS Control Root CA <Year>).
5. Click "View Certificate".



6. Open the "Details" tab.
7. Click the "Copy to File" button.
   The "Certificate Export Wizard" will open.

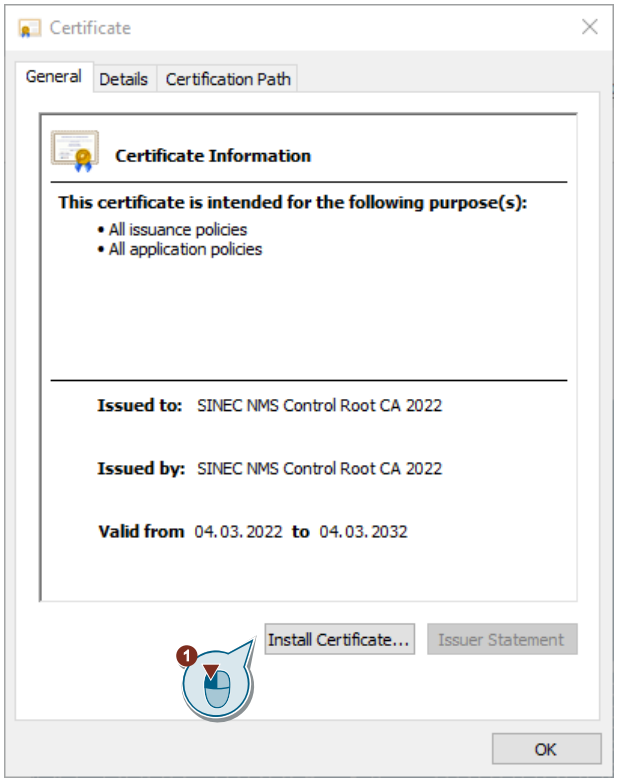


8. In the "Certificate Export Wizard", select the format "DER encoded binary X.509 (.CER)" for saving the certificate.

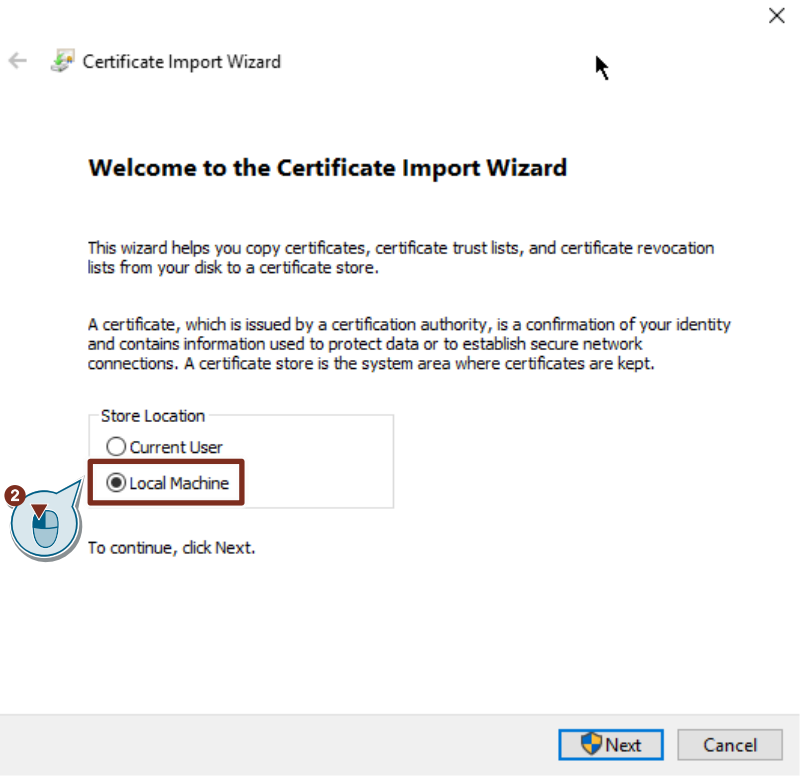


For Google Chrome or Internet Explorer to have access to the Root CA of SINEC NMS, it must be stored in the certificate store for "Trusted Root Certification Authorities" on the desired PC. Proceed as follows for each individual PC.

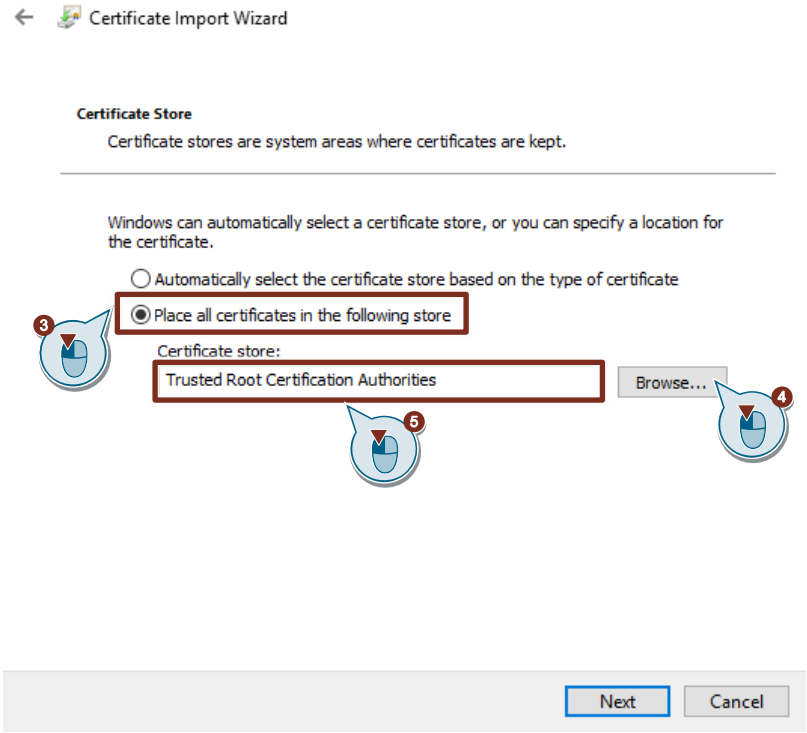
1. Open the new file and click "Install certificate".
   The "Certificate Import Wizard" will open.



2. Install the certificate on the local machine.



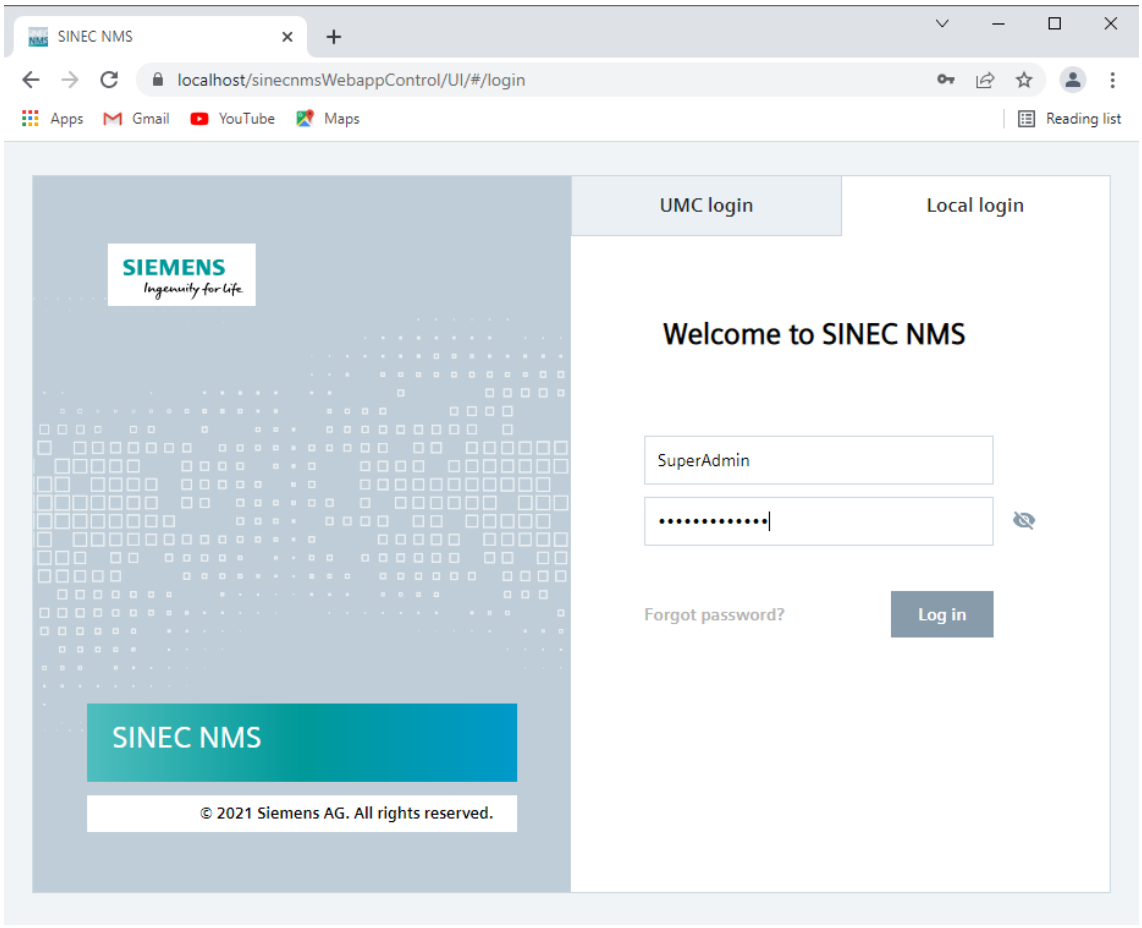
3. Select "Place all certificates in the following store" as the target location.
4. Click "Browse".
5. Select the "Trusted Root Certification Authorities" certificate store.



6. Finish installing the certificate.
7. Close all web browser windows and reopen the Web Based Management of the SINEC NMS Control.

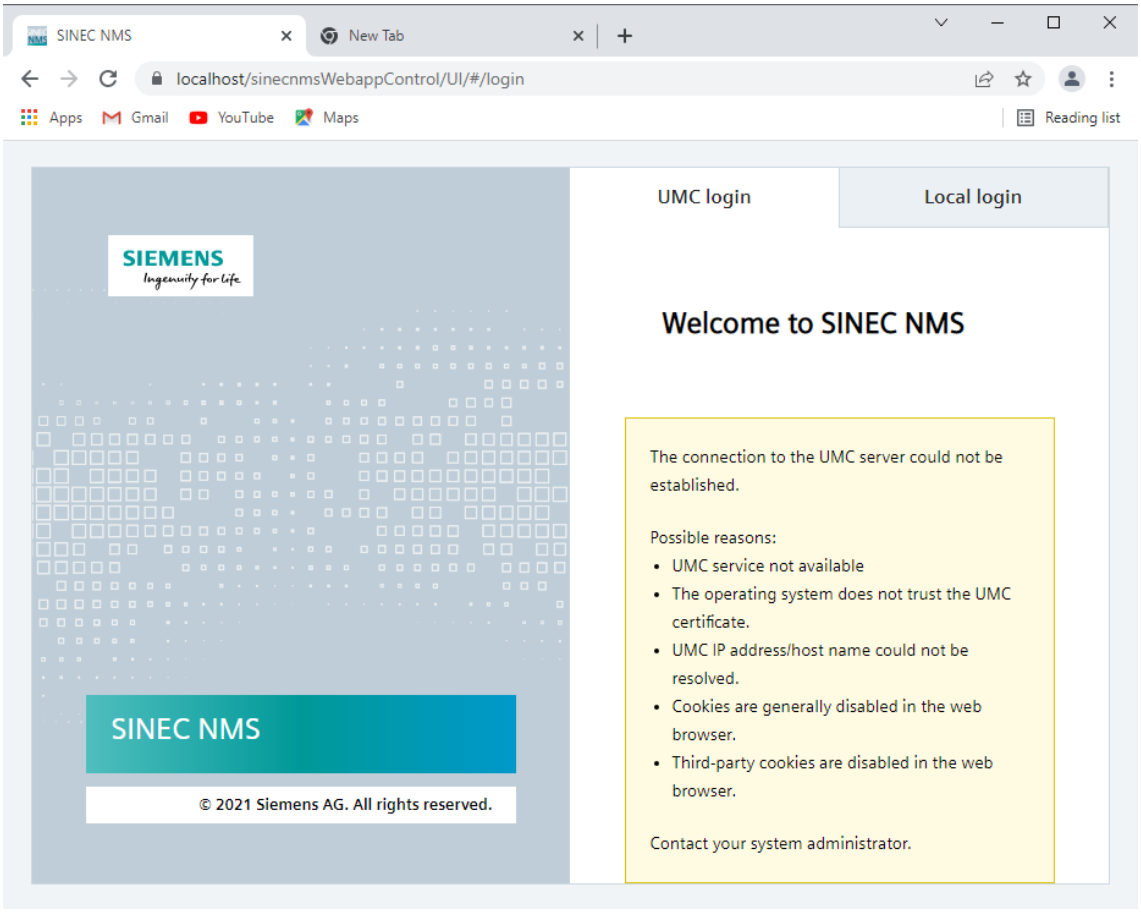
The connection to the Web Based Management of the SINEC NMS Control is secure.

Figure 3-1

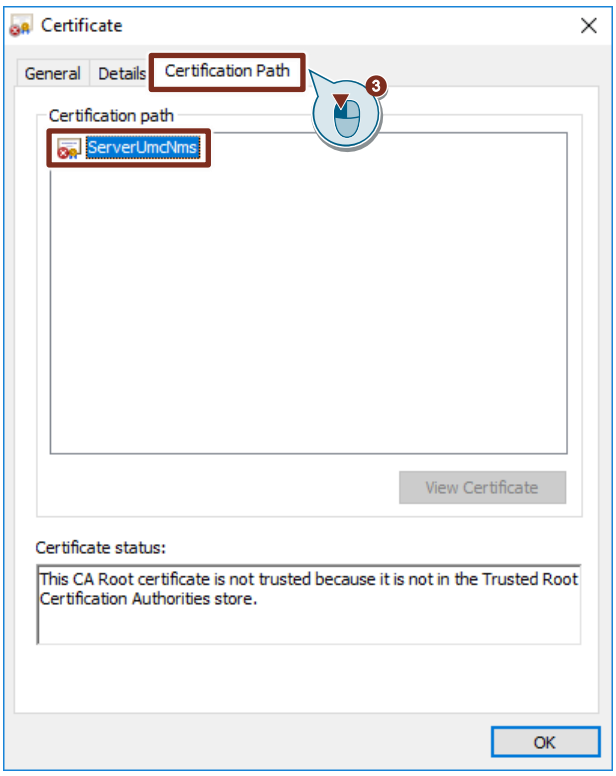


3.2 Trusting a UMC certificate

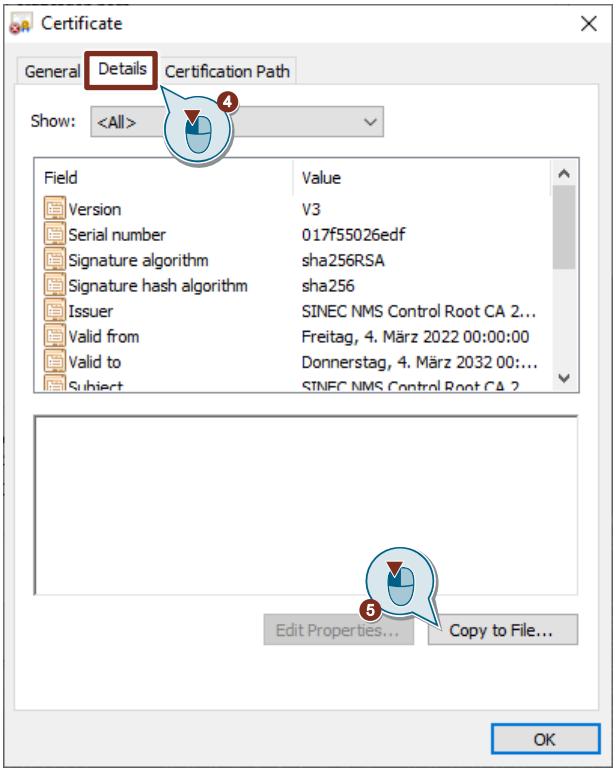
If the UMC server and SINEC NMS are installed on different PCs in the network, it will also be necessary to trust the UMC certificate. If the UMC certificate is not trusted, then the following message will appear when logging on to UMC.



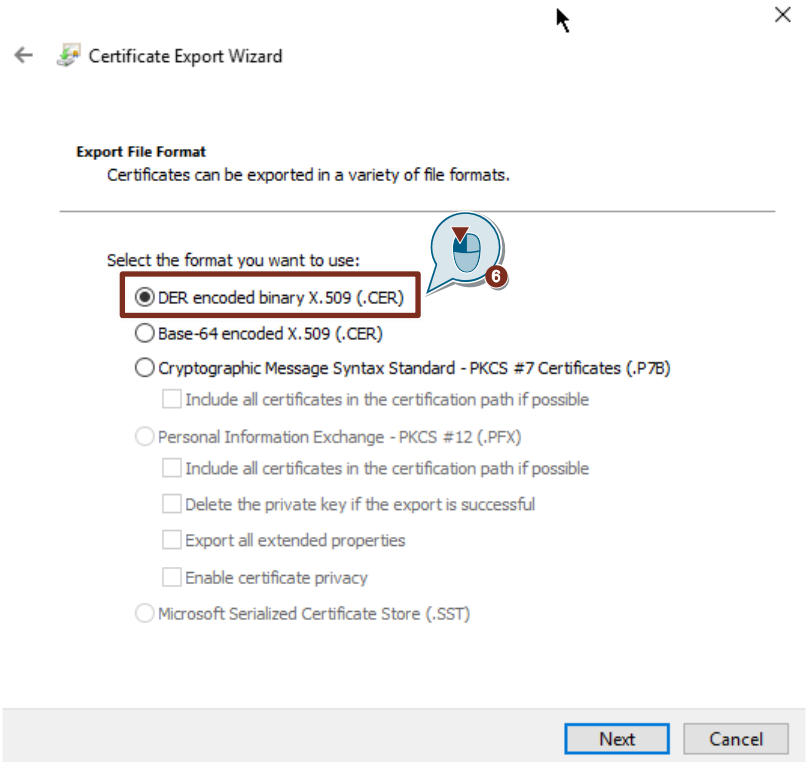
1. In a web browser, open the UMC WBM (https://<IP address> or <Host name>:8444/umc).
2. Click on the security warning in the address bar of the web browser and select the certificate.
3. Open the "Certification Path" tab in the "Certificates" dialog and check whether a root CA certificate is present.



4. Open the "Details" tab in the "Certificate" dialog.
5. Click the "Copy to File" button.
   The "Certificate Export Wizard" will open.

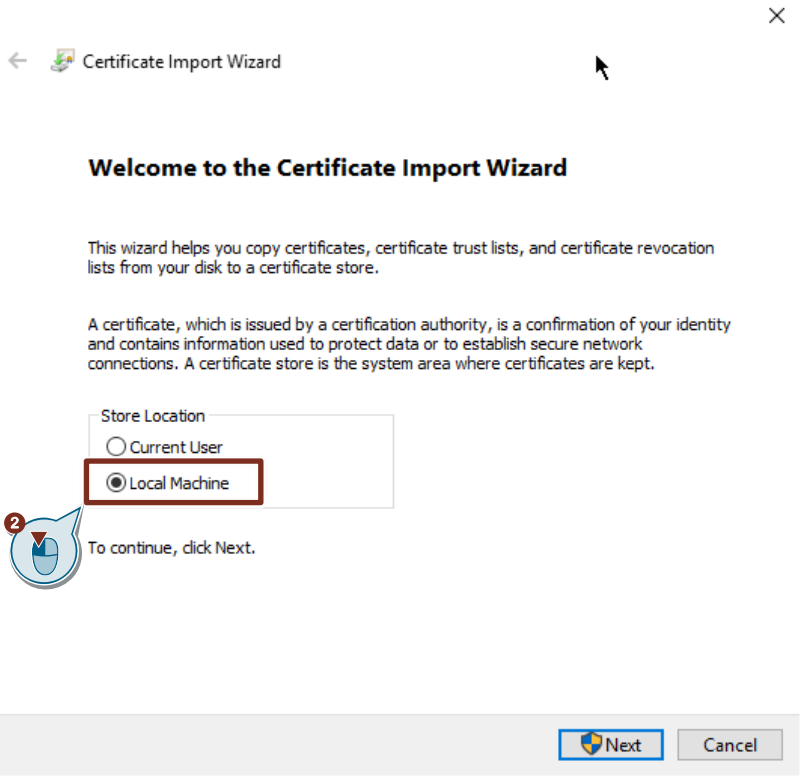


6. In the "Certificate Export Wizard", select the format "DER encoded binary X.509 (.CER)" for saving the certificate.

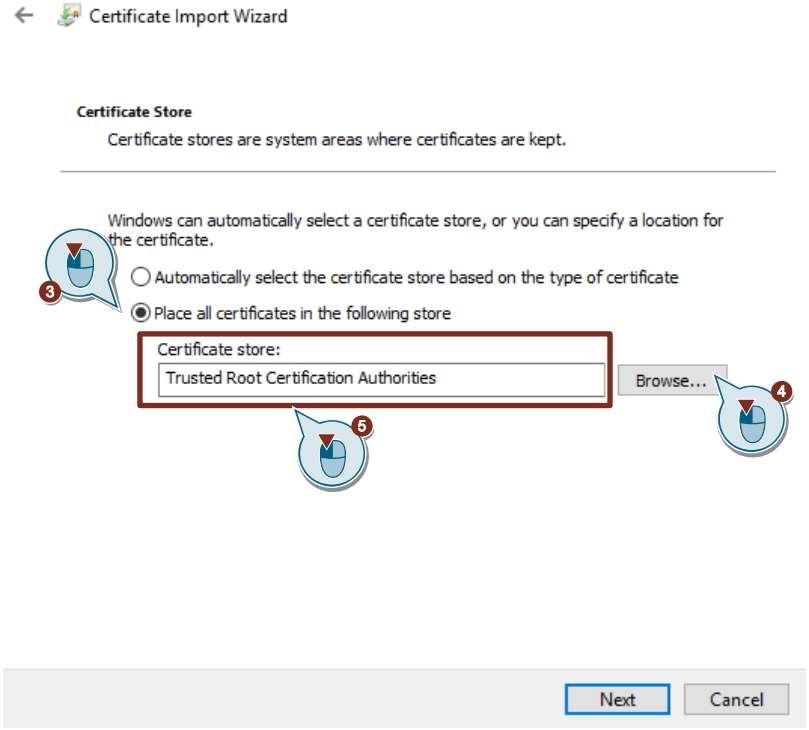


For Google Chrome or Internet Explorer to have access to the certificate of UMC, it must be stored in the certificate store for "Trusted Root Certification Authorities" on the desired PC. Proceed as follows for each individual PC.

1. Open the new file and click "Install certificate".
   The "Certificate Import Wizard" will open.
2. Install the certificate on the local machine.



3. Select "Place all certificates in the following store" as the target location.
4. Click "Browse".
5. Select the "Trusted Root Certification Authorities" certificate store.



6. Finish installing the certificate.
7. Close all web browser windows and reopen the Web Based Management of the SINEC NMS Control.

The connection to the Web Based Management of UMC is secure.

Troubleshooting

If it is not possible to access the certificate on the UMC web page even though the certificate was imported, perform the following troubleshooting steps.

The UMC server is reached via the PC name. If there is no DNS server or AD server and Net BIOS is not possible, you must enter the PC name in the host file of the PC. The host file is located in "C:\Windows\System32\drivers\etc".

3.3 Importing groups from a Microsoft Active Directory (AD) into UMC

Requirement

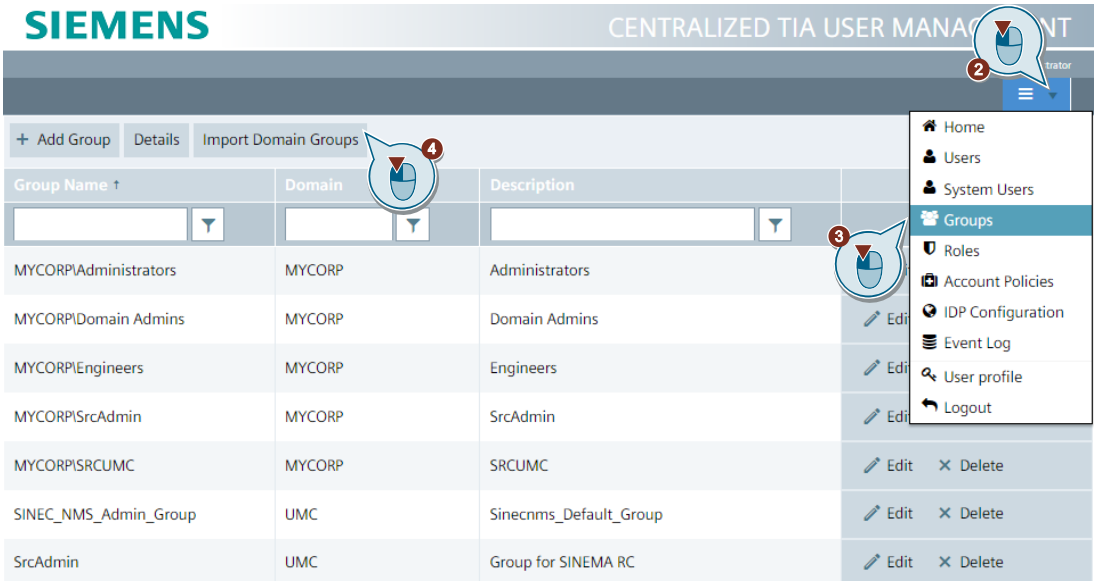
The AD has been connected to UMC.

Note The base document describes how to link an AD to UMC.

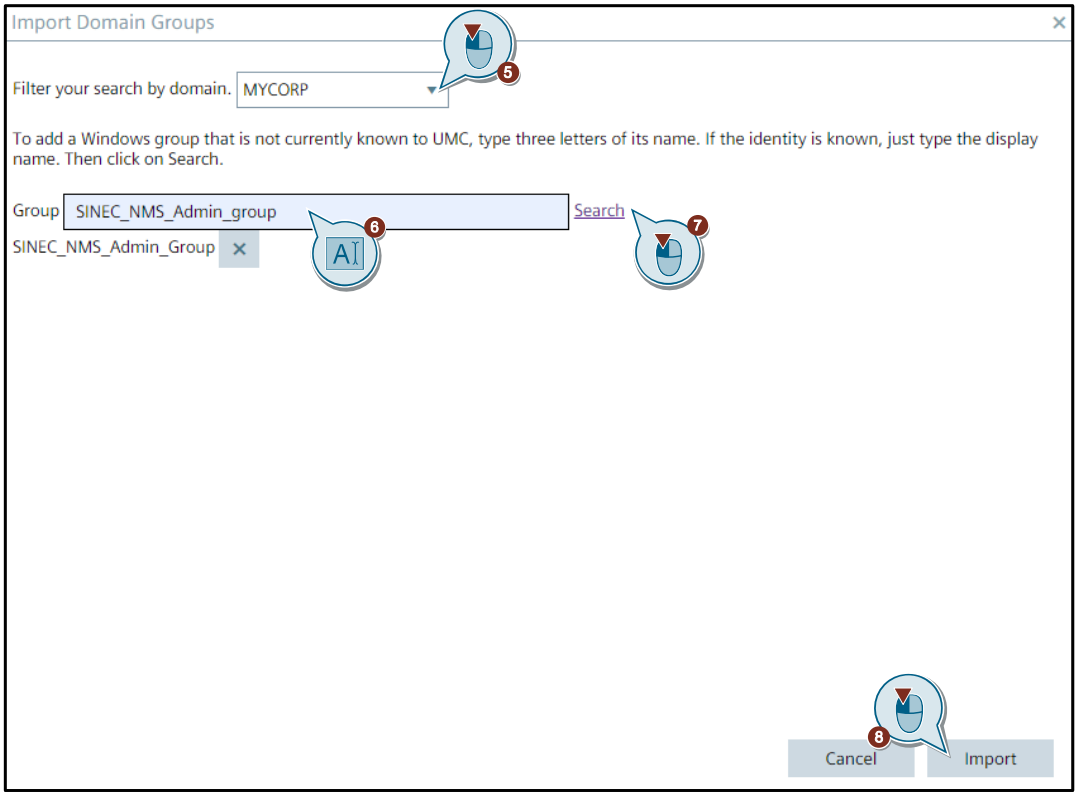
Instructions

If a Microsoft Active Directory (AD) is linked to UMC, proceed according to the instructions below to import groups from the AD. The advantage of these groups is that users are managed centrally in the AD and not locally in UMC.

1. Sign in to the UMC WBM with the login credentials of the UMC administrator.
2. Click the "Menu" button (3 bars).
3. Open the "Groups" menu. This menu allows you to import domain groups.
4. Click the "Import Domain Groups" button.
   The "Import Domain Groups" dialog will open.



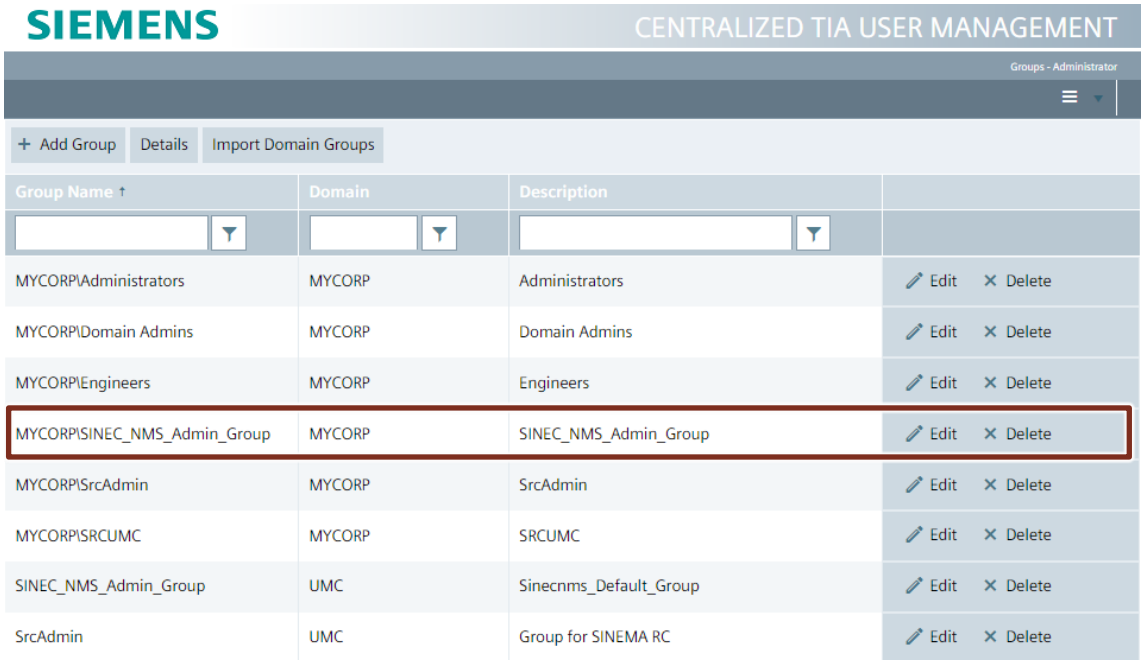
5. Select the domain of the AD.
6. To add a domain group that is not known to UMC, enter three letters from the name of that group's name. If the identity is known, enter the display name.
7. Click on "Search".
   The desired domain group will be displayed.
8. Click the "Import" button.



Result

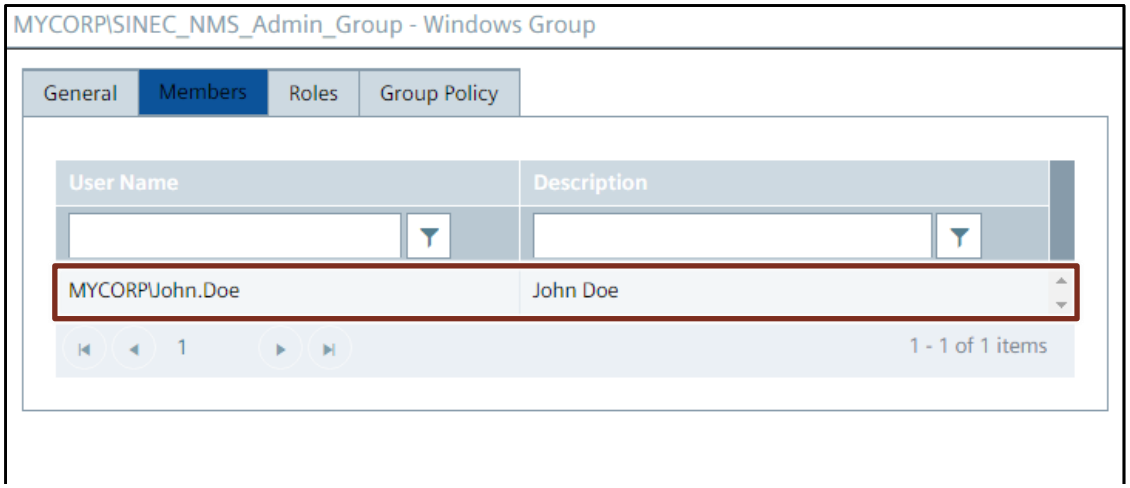
The desired domain group is imported into UMC.

Figure 3-2



The "Members" tab of the group's detail view displays all users assigned to the domain group in the AD.

Figure 3-3



The imported domain groups can then be created in SINEC NMS and assigned to a role.

Figure 3-4

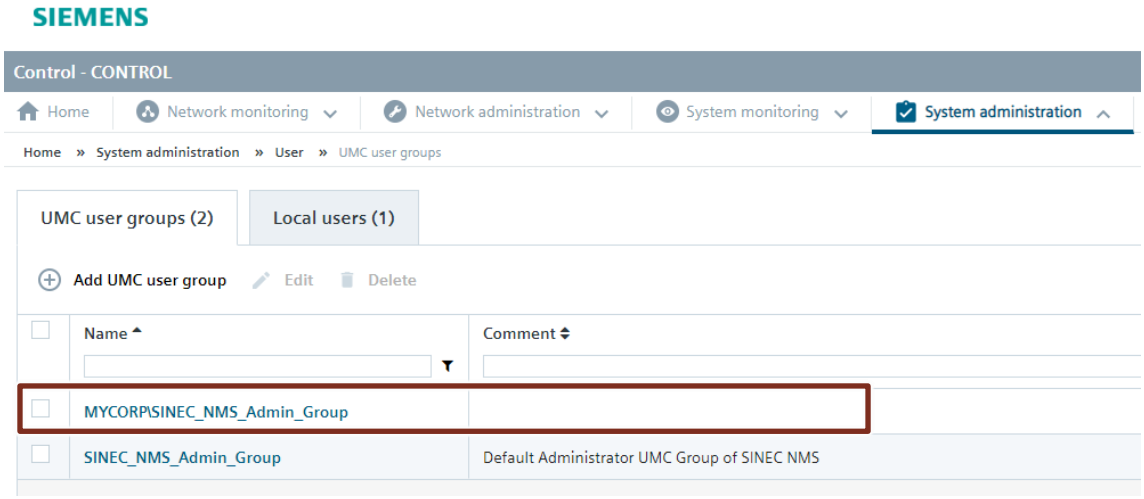
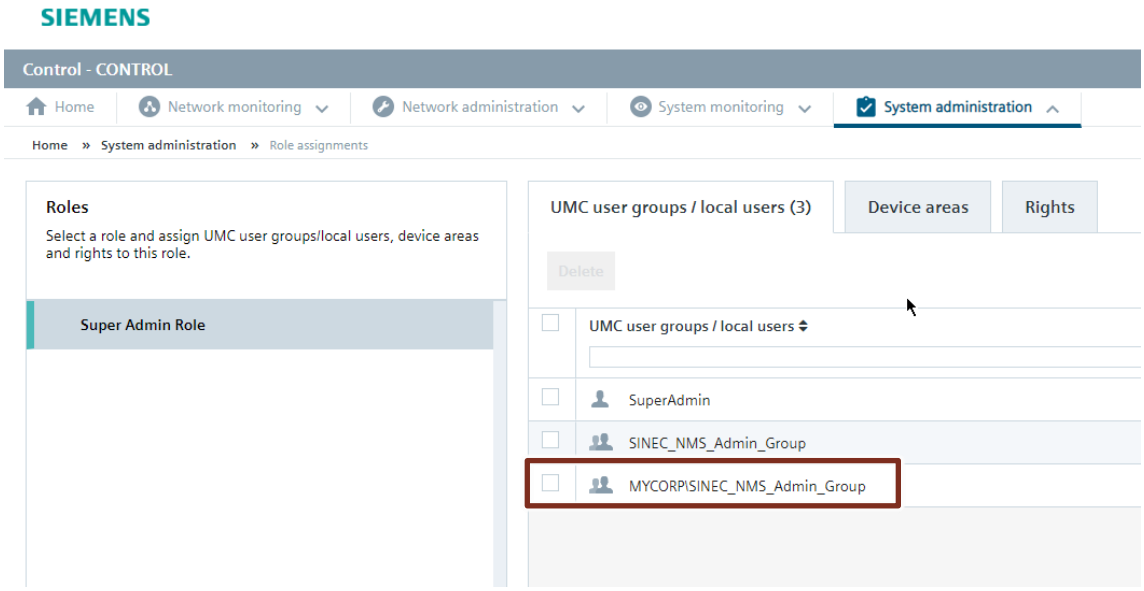
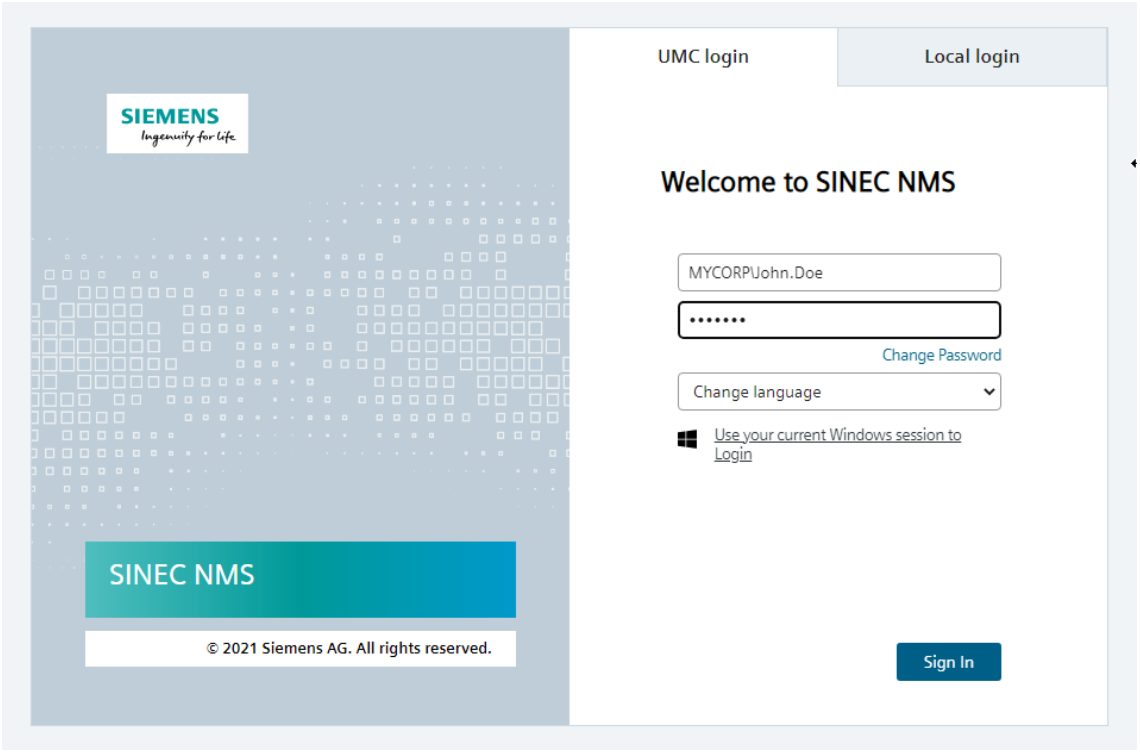


Figure 3-5



The domain user "MYCORP\John.Doe", assigned to the domain group "MYCORP\SINEC_NMS_Admin_Group", can sign in as a UMC user to the WBM of SINEC NMS.

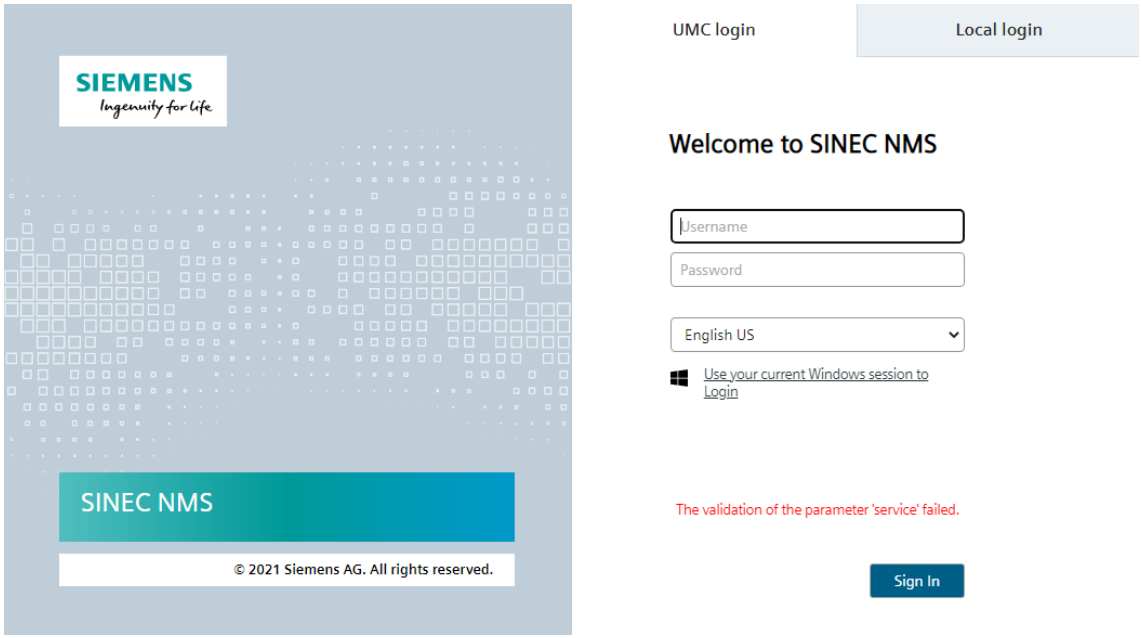
Figure 3-6



3.4 Adding SINEC NMS to the UMC whitelist

If you receive the following error message when signing in to the SINEC NMS WBM, SINEC NMS has not yet been added to the UMC whitelist.

Figure 3-7

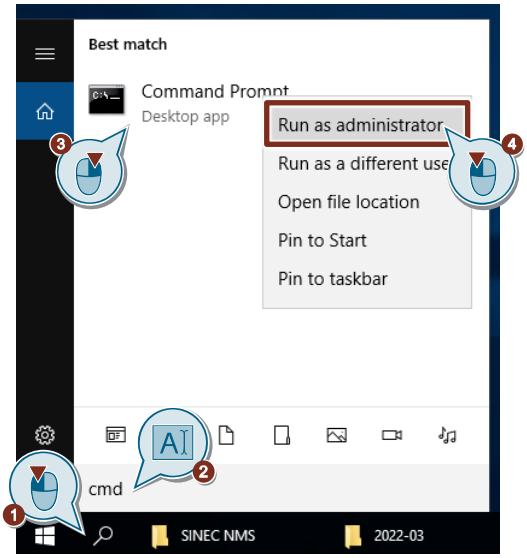


Proceed according to the instructions below to add SINEC NMS to the UMC whitelist.

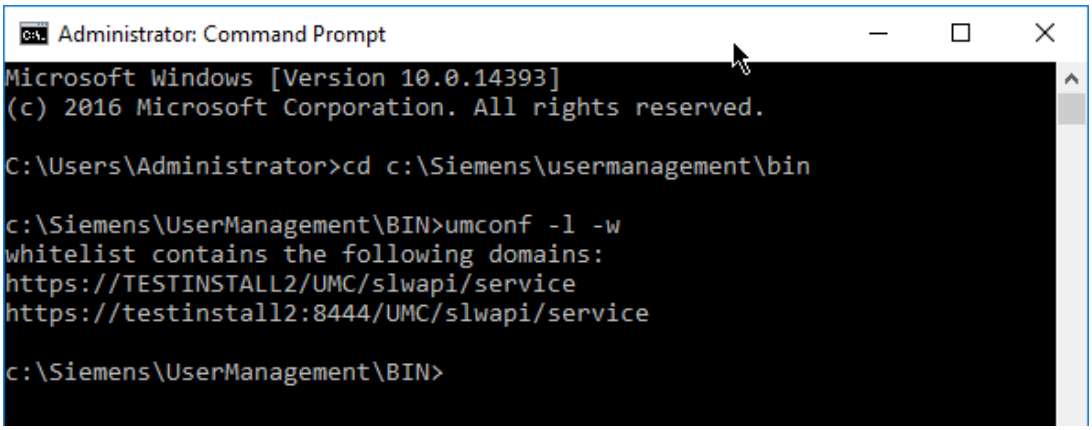
Note

If the first login is made with the UMC administrator, then the hostname will be automatically added to the UMC whitelist.

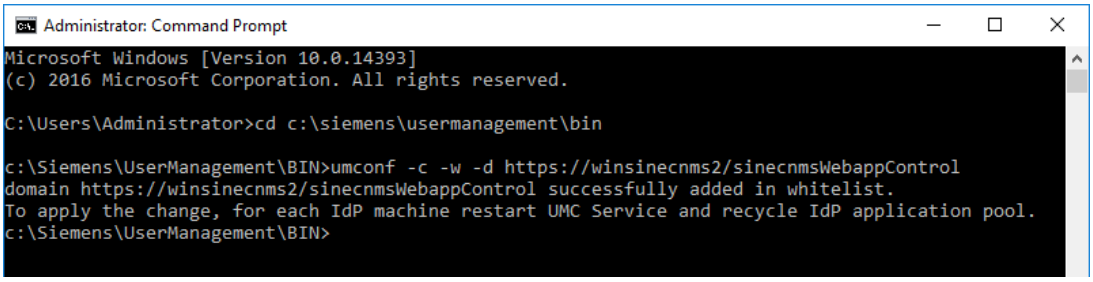
1. Run the "Command Prompt" as an administrator on the UMC ring server.



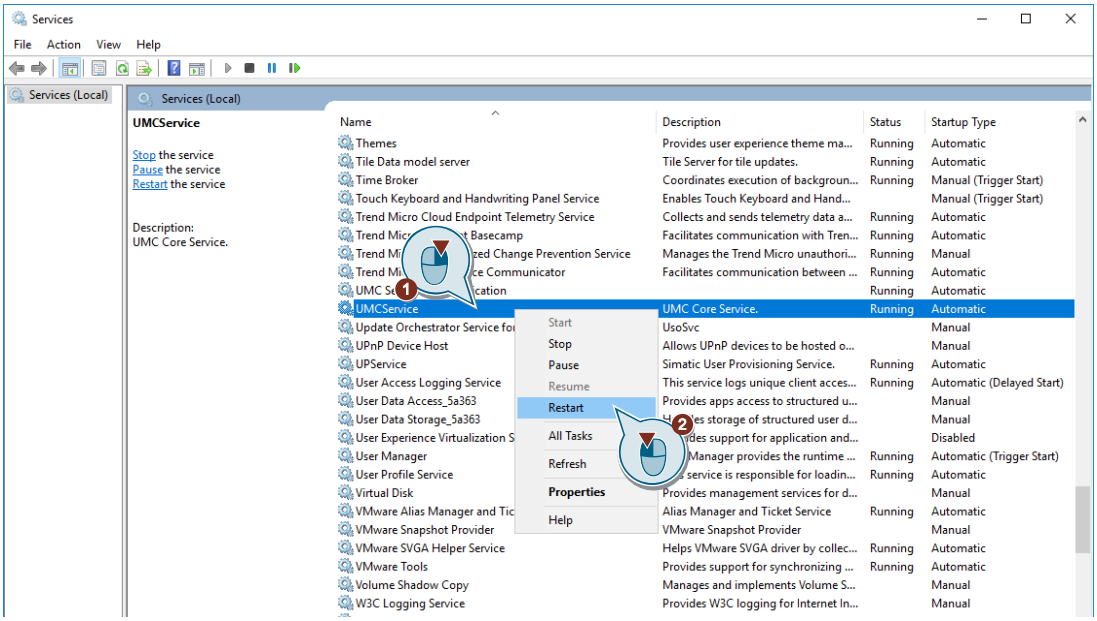
2. Change the directory using the following command:
   `cd C:\Program Files\Siemens\UserManagement\BIN`
3. With the following command you get all whitelist entries:
   `umconf -l -w`



4. The entry "https://<hostname>/sinecnmsWebappControl" is required to log in with SINEC NMS.
5. You can add the PC name of the SINEC NMS Control to the UMC whitelist with the following command.
   `umconf -c -w -d https://<Hostname>/sinecnmsWebappControl`



6. Restart the UMC service on the PC that is acting as the identity verification location for SINEC NMS.



The entry has been successfully added to the UMC whitelist.

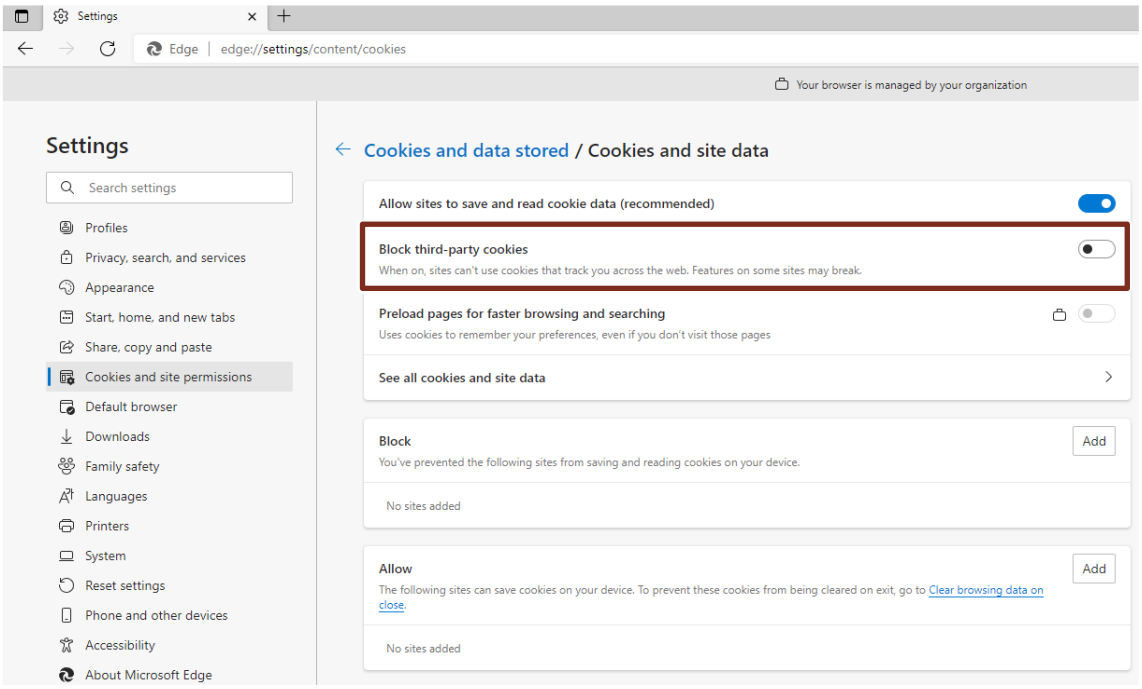
3.5 Allowing third-party cookies

Third-party cookies must be allowed in the web browser to log in with a UMC user to the WBM of the SINEC NMS Control.

Check the web browser settings to make sure that third-party cookies are not blocked.

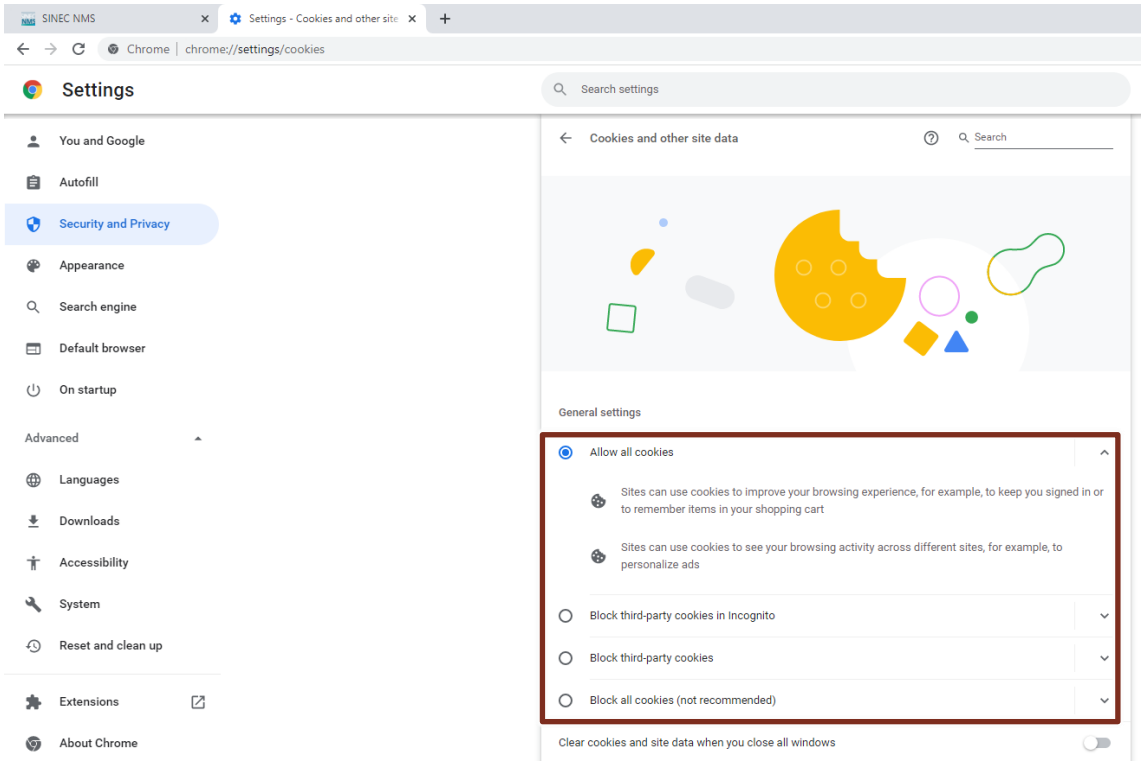
Settings in Microsoft Edge

Figure 3-8



Settings in Google Chrome

Figure 3-9

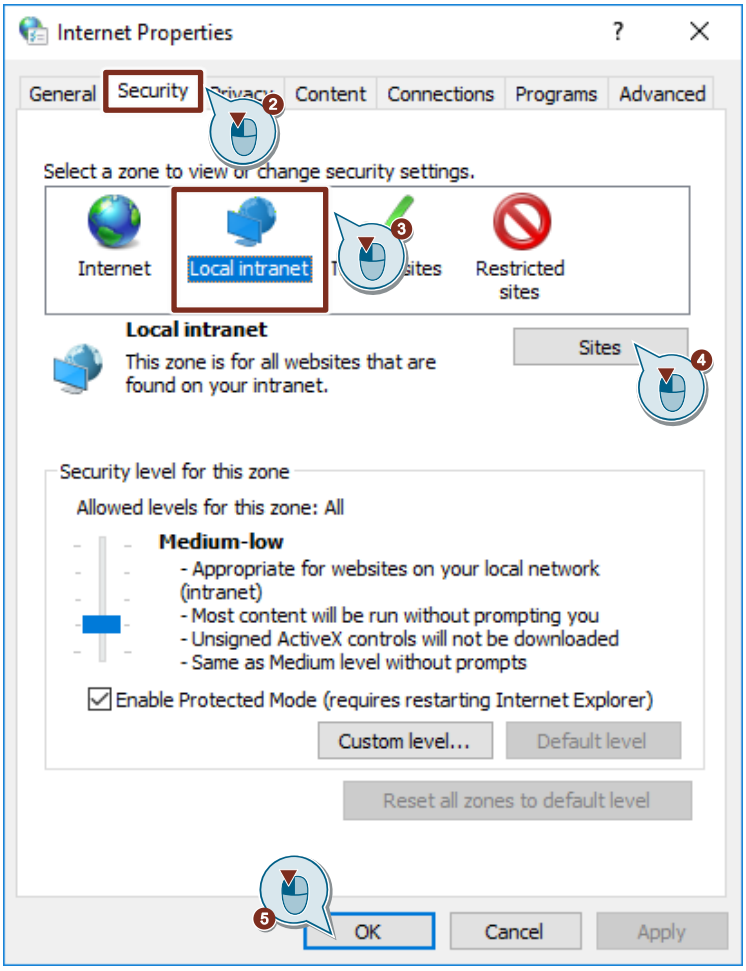


3.6 Using the current Windows session for the login

Perform the following steps to use the current Windows session for the UMC login:

1. In the Windows "Control Panel", open the "Internet options" menu in the "Network and Internet" category.
   The "Internet Properties" dialog will open.
2. Open the "Security" tab.
3. Select "Local intranet" for the security zone.
4. Click the "Sites" button and add the UMC web page and the SINEC NMS web page to the selected security zone.
5. Click "OK" to apply the settings.

Figure 3-10



Result

You can now use the current Windows session to sign in to UMC or SINEC NMS.

4 Appendix

4.1 Service and support

Industry Online Support

Do you have any questions or need assistance?

Siemens Industry Online Support offers round the clock access to our entire service and support know-how and portfolio.

The Industry Online Support is the central address for information about our products, solutions and services.

Product information, manuals, downloads, FAQs, application examples and videos – all information is accessible with just a few mouse clicks:

support.industry.siemens.com

Technical Support

The Technical Support of Siemens Industry provides you fast and competent support regarding all technical queries with numerous tailor-made offers
– ranging from basic support to individual support contracts.

Please send queries to Technical Support via Web form:

support.industry.siemens.com/cs/my/src

SITRAIN – Digital Industry Academy

We support you with our globally available training courses for industry with practical experience, innovative learning methods and a concept that’s tailored to the customer’s specific needs.

For more information on our offered trainings and courses, as well as their locations and dates, refer to our web page:

siemens.com/sitrain

Service offer

Our range of services includes the following:

- Plant data services
- Spare parts services
- Repair services
- On-site and maintenance services
- Retrofitting and modernization services
- Service programs and contracts

You can find detailed information on our range of services in the service catalog web page:

support.industry.siemens.com/cs/sc

Industry Online Support app

You will receive optimum support wherever you are with the "Siemens Industry Online Support" app. The app is available for iOS and Android:

support.industry.siemens.com/cs/ww/en/sc/2067

4.2 Industry Mall

The Siemens Industry Mall is the platform on which the entire siemens Industry product portfolio is accessible. From the selection of products to the order and the delivery tracking, the Industry Mall enables the complete purchasing processing – directly and independently of time and location:
mall.industry.siemens.com

4.3 Links and literature

Table 4-1

No.	Topic
\1\	Siemens Industry Online Support https://support.industry.siemens.com
\2\	Link to the article page of the application example https://support.industry.siemens.com/cs/ww/en/view/109780337

4.4 Change documentation

Table 4-2

Version	Date	Change
V1.0	02/2021	First edition
V2.0	04/2022	Complete revision