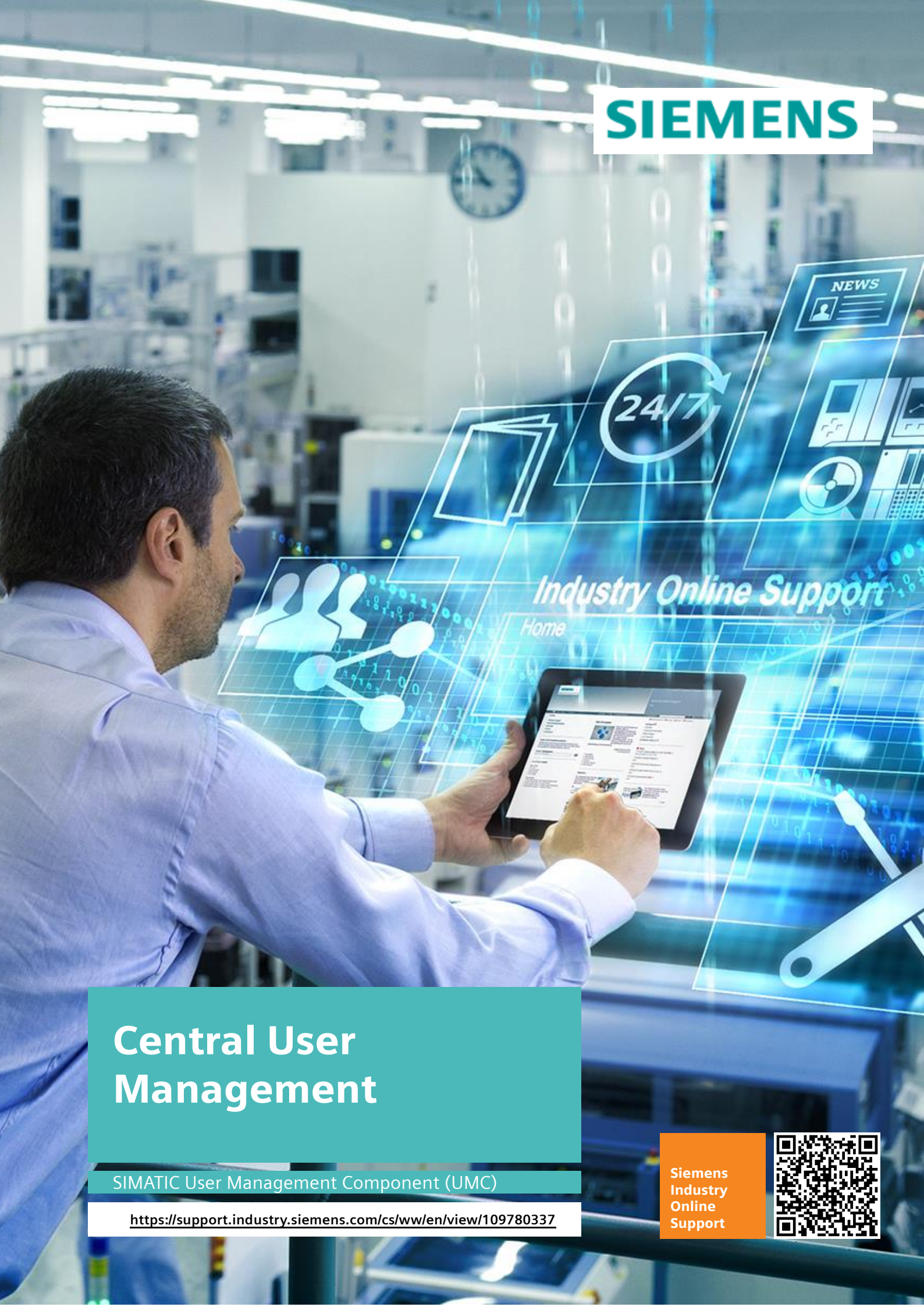


Central User Management

SIMATIC User Management Component (UMC)

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

Overview

Efficient user management is an essential part of every security concept. The User Management Component (UMC) enables the system-wide, central maintenance of users with an optional connection to Microsoft Active Directories. 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 efficient, thorough administration of personalized access permissions within the system. This can significantly reduce security risks.

UMC allows the establishment of 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 central users and user groups into the various applications or use them as temporary users.

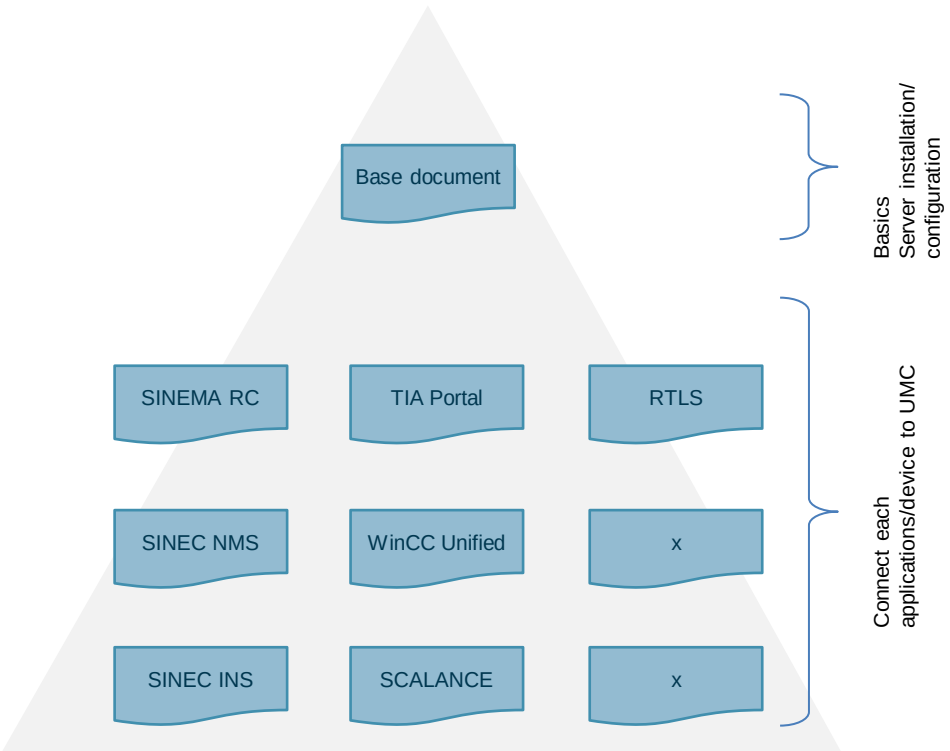
What we show in this document

In this application example, you will learn the functions and usage of UMC. You will get a general overview of UMC, as well as how to install and set up this component.

Further documents describe how the following applications are connected to UMC:

- SINEMA RC
- SINEC NMS
- WinCC Unified
- TIA Portal
- WinCC Runtime Advanced

Figure 1-1



2 Principle of Operation

2.1 Advantages and Benefits of Central User Management

The international standard IEC 62443 deals with cyber security in industrial automation systems. In the standard system, the following topics, among others, are of decisive importance:

- Authentication
- Authorization
- Central User Management

It must be possible to identify users (authentication) and to grant appropriate permissions on the system depending on the person (authorization).

Decentralized user management, where users are stored locally on each system or component, is inefficient for larger systems and cannot be managed in the long run. Therefore, Central User Management is of utmost importance.

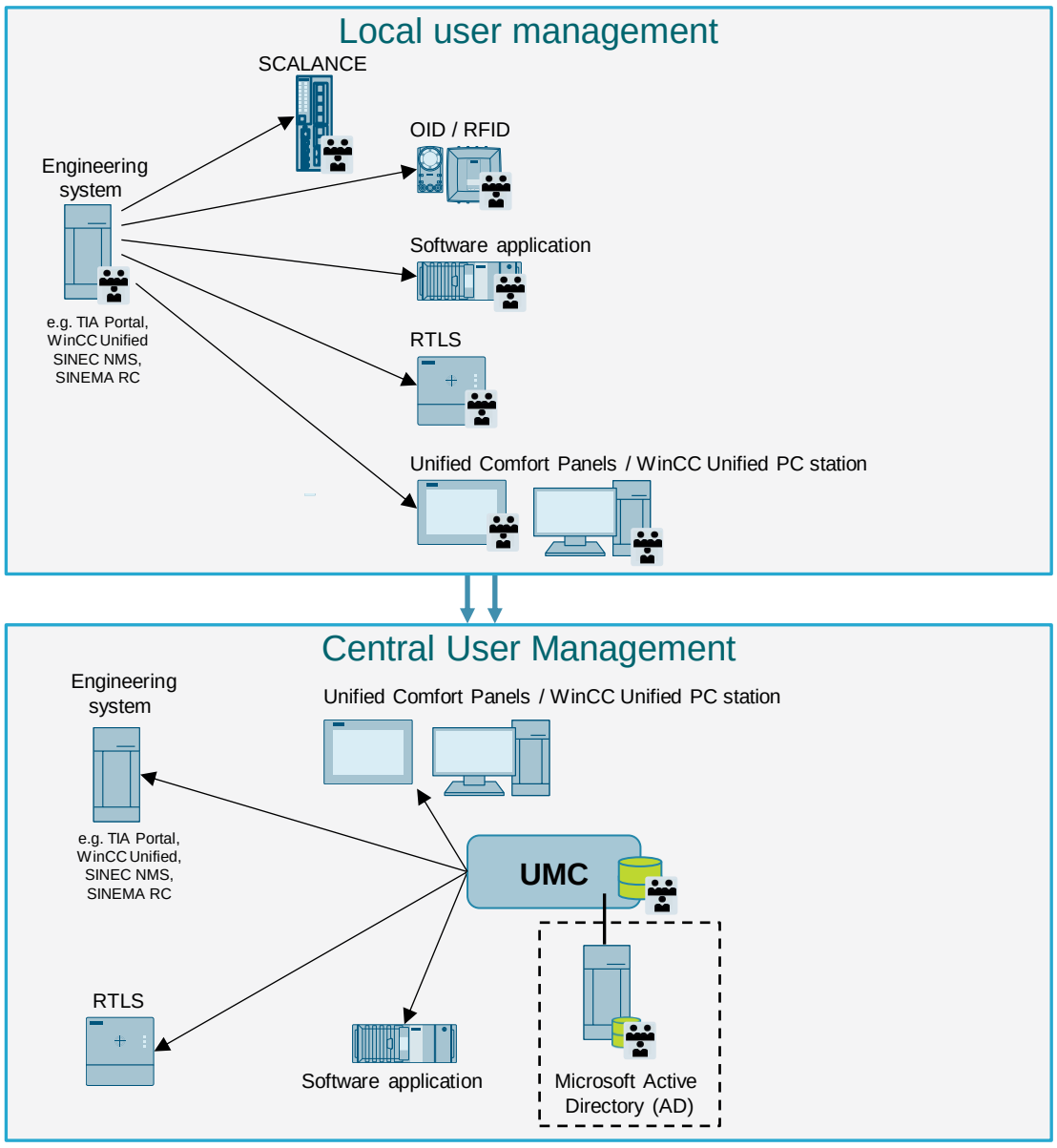
With Central User Management, the components need only forward the authentication request to the control center and, if the response is successful, grant access from the control center (depending on authorization).

Note

The User Management and Access Control concept (UMAC) states that user management takes place in UMC, but permissions management happens locally in the application.

The following graphic explains these two approaches.

Figure 2-1



2.2 Central user management for SIEMENS Digital Industries

A sample of the components that can be operated with UMC is shown in the following Table:

Table 2-1

Product	UMC function
TIA Portal	The TIA Portal imports the required users and user groups from the UMC and enables the assignment of roles with functional permissions for Engineering and Runtime.
WinCC Unified	The Engineering System imports the required users and user groups from the UMC and enables the assignment of roles with functional permissions for Engineering and Runtime. It is possible to use these users for Runtime, on Unified Comfort Panels, and on WinCC Unified PCs.
WinCC Runtime Advanced	WinCC Advanced Runtime can be connected to UMC via SIMATIC Logon Remote Authentication (SLRA) or via the additional software PM-Logon. The Engineering System imports the users and user groups from UMC and enables the assignment of roles with function permissions for Runtime.
SINEC NMS / INS	SINEC imports the users and assigns them the desired configuration permissions.
SINEMA Remote Connect Server	With SINEMA Remote Connect Server, access to remote components and system sections is controlled. The users can be divided into groups.
SIMATIC PCS neo	The use of UMC is mandatory for SIMATIC PCS neo and is installed automatically. The UMC is integrated in the "Administration Console".
SIMATIC RTLS	The SIMATIC RTLS Locating Manager is connected to the UMC using the "User Configuration" client and imports the desired users and groups.

The detailed description of the connection of the individual components can be found in the entry 109780337. Detailed descriptions will be available successively.

2.3 UMC fundamentals and terminology

Important UMC terms

In the following Table, you will find the most important UMC terms.

Table 2-2

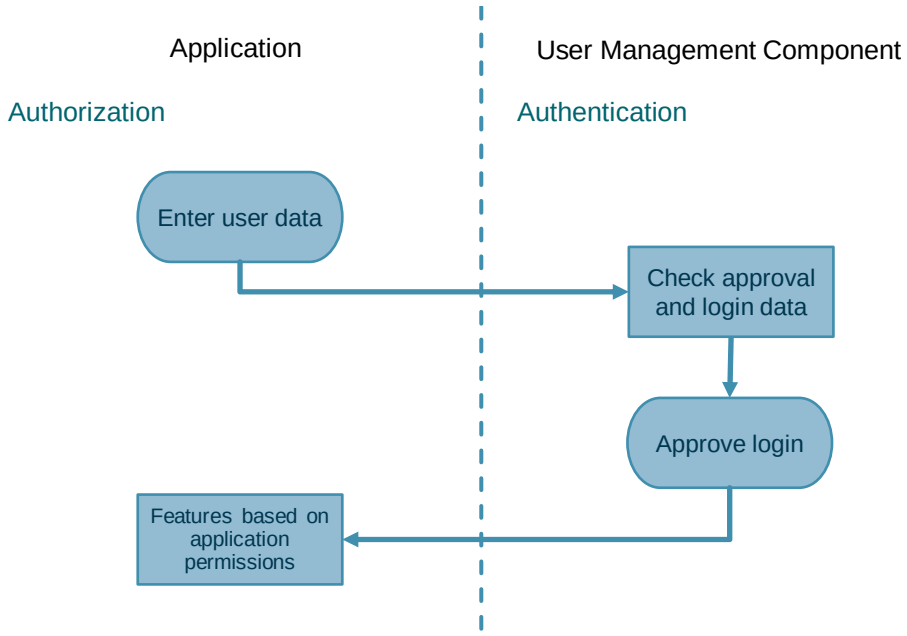
UMC term	Description
UMC ring server	This is the domain server that manages all logins. Users and groups are created in UMC via a web interface or imported from a Microsoft Active Directory into UMC. The users created in UMC are imported into the desired applications. In the application, the roles and permissions for the application are created and assigned to the imported user. A UMC ring server is configured by default with the console application "umconf.exe".
UMC server	This is a server that works in "deprecated" mode when it is not connected to a UMC ring server. The deprecated mode still allows for authentication functions, but not user management. In addition, it offers the option of performing authentication offline in the event of a connection failure. The UMC server is also available with the "Run Time" feature as a UMC "Run Time" Server.
UMC Agent	This is a client that is connected to the UMC server. With each login, it checks the login data on the server.
Microsoft Active Directory	For example, a Microsoft Active Directory manages the users associated with all the employees in a company. These users can later be imported into the UMC server. A Microsoft Active Directory is specifically for Windows operating systems.
UMAC	UMAC stands for "User Management & Access Control" and describes not only user management but also access management.

Login process via UMC

The UMC server receives the login requests of the connected applications and checks the entered user data. The application then receives a response on whether the login data is correct. If this is the case, it will approve the login.

Permissions management is not performed in UMC. In UMC, it is decided whether a user has access to the desired component and whether the access data is correct. In the application or component, permissions management remains as normal.

Figure 2-2

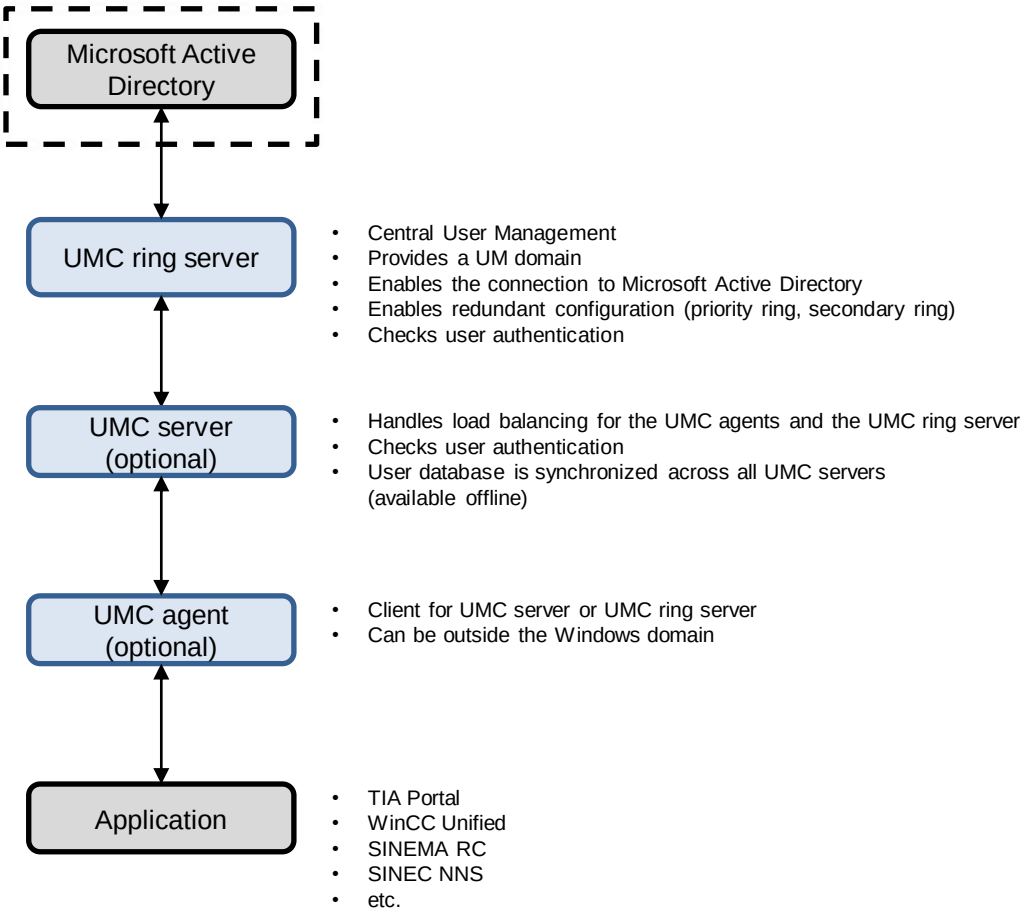


UMC architecture

The UMC structure consists of at least one UMC ring server and one UMC Agent. Any redundancy between UMC ring servers is possible. The use of UMC servers in the network serves to distribute the load during logins.

The setup with redundant servers can also be used for load distribution. In this way, load spikes in large domains can be distributed across different UMC servers.

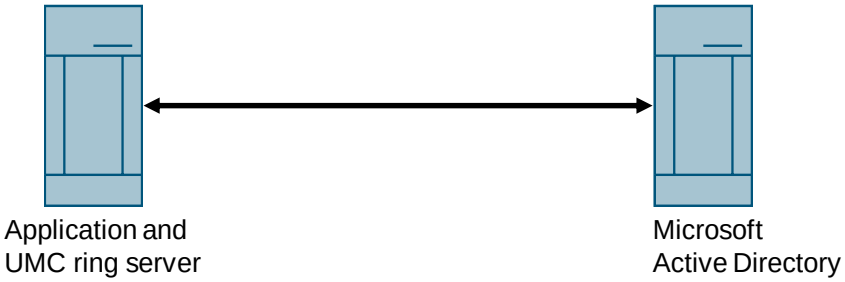
Figure 2-3



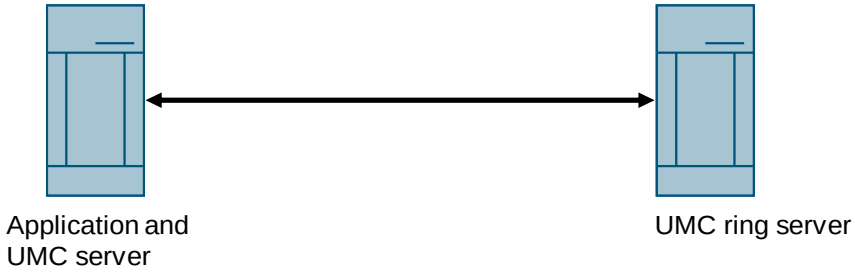
Connecting the application to UMC

The application can be connected to UMC in various ways:

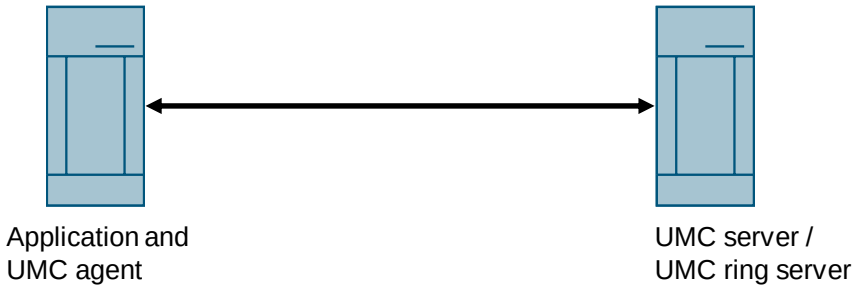
- Application, UMC ring server and Microsoft Active Directory



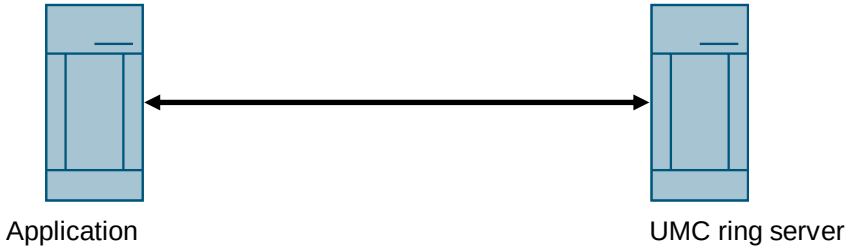
- Application, UMC server and UMC ring server



- Application, UMC agent, UMC server or UMC ring server



- Application and UMC ring server

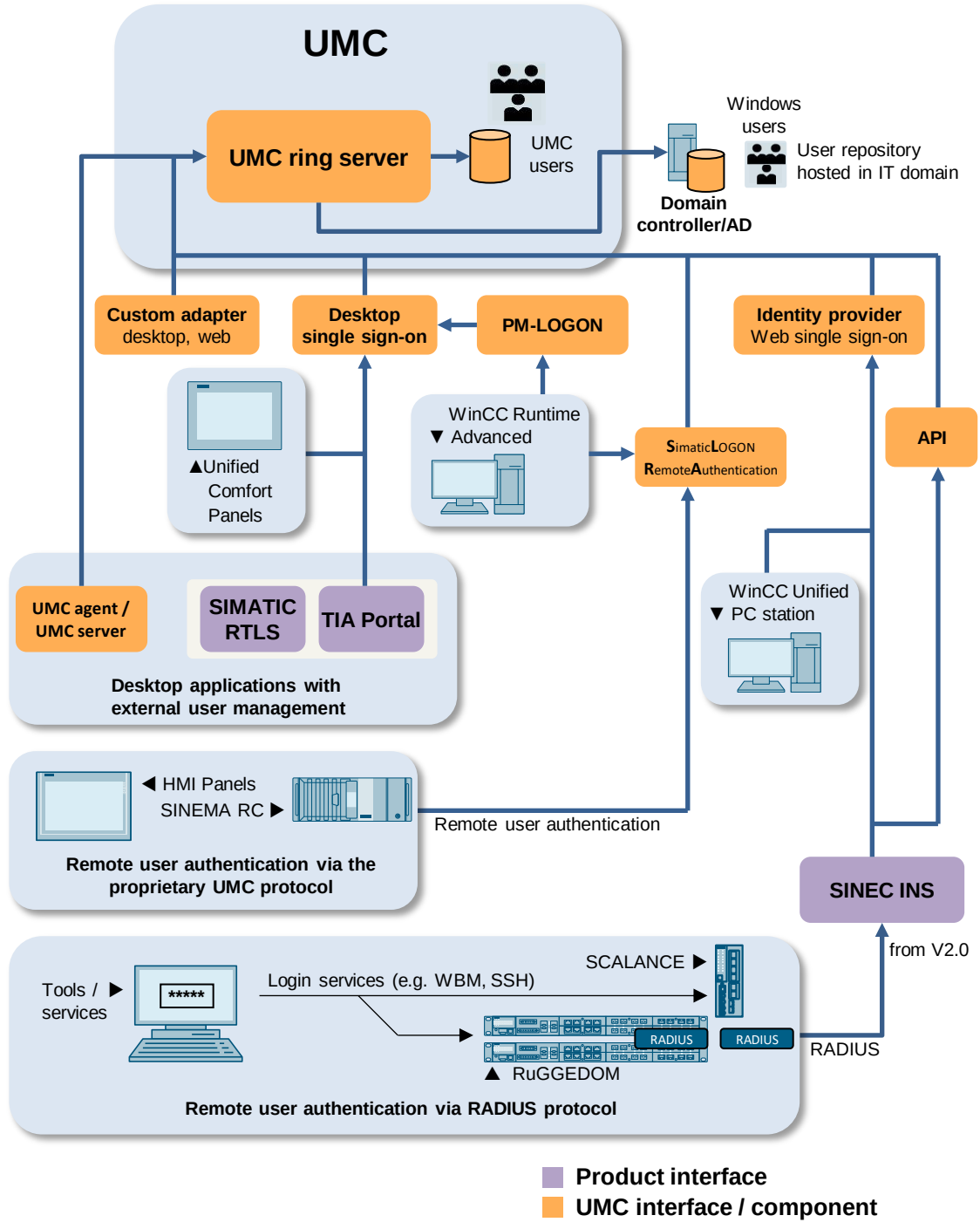


Note The UMC component belonging to the application must be installed on the same PC as the application.

UMC interfaces

The following graphic shows an overview of the available UMC interfaces and which components from the SIMATIC product range use them.

Figure 2-4



License information

Licenses are required for the use of UMC. Up to 10 user accounts can be managed without a license. This allows you to test the UMC included in your product at no additional cost.

Additional user accounts are licensed per Rental License (e. g. up to 100 user accounts), which includes royalty-free usage (e. g. 10 users), etc.

Table 2-3

License	Item number
User Management Component (UMC) with 10 or fewer user accounts	license-free
Rental License for 100 user accounts and 365 days Certificate of License to download	6ES7823-1UE30-0YA0
Rental License for 4000 user accounts and 365 days Certificate of License to download	6ES7823-1UE10-0YA0

Note

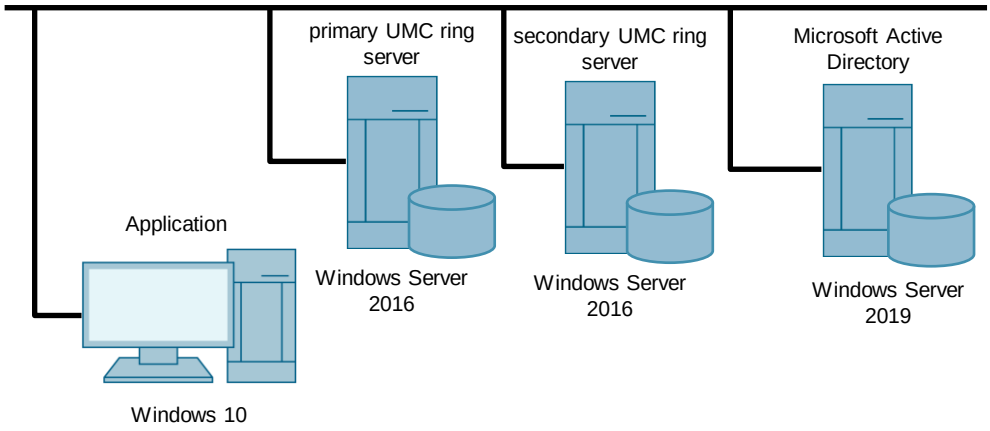
You may need additional licenses to connect an application. This is the case with SINEMA Remote Connect Server, for example.

3 Engineering

Introduction

In the following section, we show you the complete installation and configuration of a redundant UMC ring server with a Microsoft Active Directory (AD) connection.
This structure is used in the descriptions of the individual components.

Figure 3-1



Example users and groups

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

Table 3-1

Users	Groups
Admin	Administrator (UMC)
MYCORP\John.Doe	Administrators, Domain Admins
MYCORP\UmcUser	UM_Users, Domain Users
MYCORP\ServiceEngineer	Engineers, Domain Users
MYCORP\Administrator	Administrators, Domain Admins
Bob	UMC_User (UMC)

3.1 Installation

Installation files for the UMC server

The installation files for the User Management Component (UMC) can be found in the following installation packages:

- TIA Portal
  A stand-alone installation of UMC is possible. The installation file "TIA_UMC_V2.exe" for UMC and the English documentation for UMC can be found on the TIA Portal installation disk (DVD 2) in the folders "Support" and "Documentation".
  When TIA Portal is installed, UMC is installed automatically.
- WinCC Unified
  A stand-alone installation of UMC is possible. The installation file "TIA_UMC_V2.exe" for UMC and the English documentation for UMC can be found on the TIA Portal installation disk (DVD 2) in the "Support" and "Documents" folders.
  When installing WinCC Unified, UMC is installed automatically.
- SINEMA RC Client Installation Package
  The installation package includes the UMC server.
- SINEC NMS
  The UMC can be optionally selected during the installation of SINEC NMS.
- PCS neo
  The UMC is automatically installed and integrated into the Administration Console.

Used installation file

In this example, we install the UMC ring server as a stand-alone version. This installation is demonstrated using two examples because there are differences in the installation between the TIA Portal and SINEC NMS installation packages.

3.2 Configuration

Overview

If a Microsoft Active Directory exists in your network, the UMC can be linked to it.

After you have installed and set up the Microsoft Active Directory, carry out the basic configuration of the UMC ring server using the respective console.

Requirements

The following devices are used in this application example:

- 1 PC with Windows Server 2019 for the Microsoft Active Directory
- 2 PCs with Windows Server 2016 for the redundant UMC ring servers
- Network construction as in the introduction in Figure 3-1 is shown.

3.2.1 Integrating UMC ring server PC into the domain

Requirements

- You have installed a Microsoft Active Directory on a PC and created a domain (e. g., "mycorp.com").
- You have created the required users and groups.
  In the example, the following domain users are used in the corresponding domain groups:

  Table 3-2

User "MYCORP\"	Groups
John Doe	Administrators, Domain Admins
Service engineer	Engineers
UmcUser	UM_USERS
Administrator	Administrators, Domain Admins

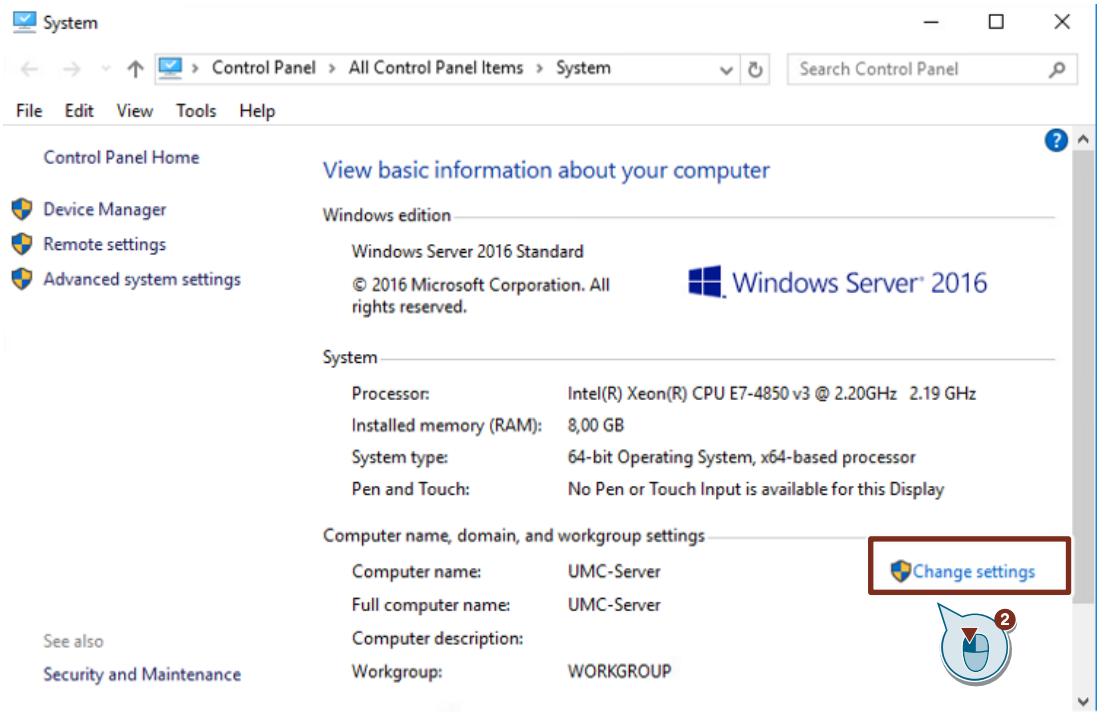
Note

So that the UMC Ring Server PC can connect to the Microsoft Active Directory, it is necessary for the UMC Ring Server PC to be in the same domain as the PC on which the Microsoft Active Directory is installed.

Instructions

After installing the operating system on the UMC ring server PC, perform the following steps to join it to the domain of the PC where Microsoft Active Directory is installed.

1. Open the menu "Control Panel > System" on the UMC server PC in Windows.
2. Click "Change settings".
   The "System Properties" dialog opens.

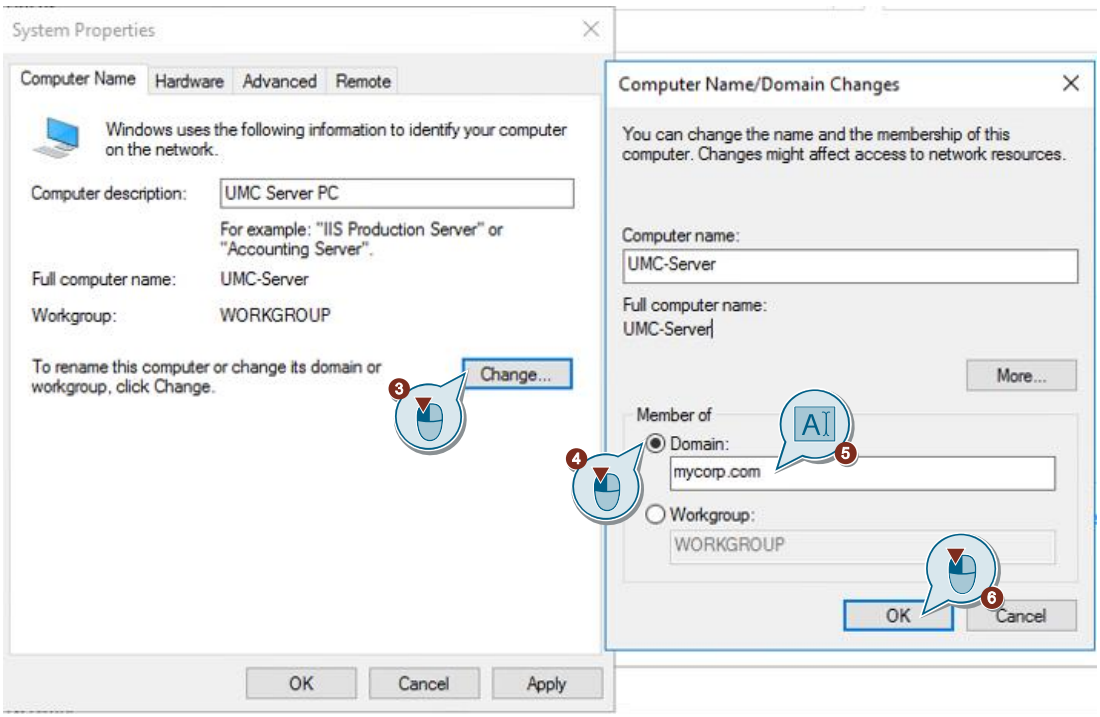


3. Click the "Change" button.
   The "Computer Name/Domain Changes" dialog opens.
4. Select the option for the UMC ring server PC to be a member of the "domain".
5. Enter the name of the domain (e.g., "mycorp.com").

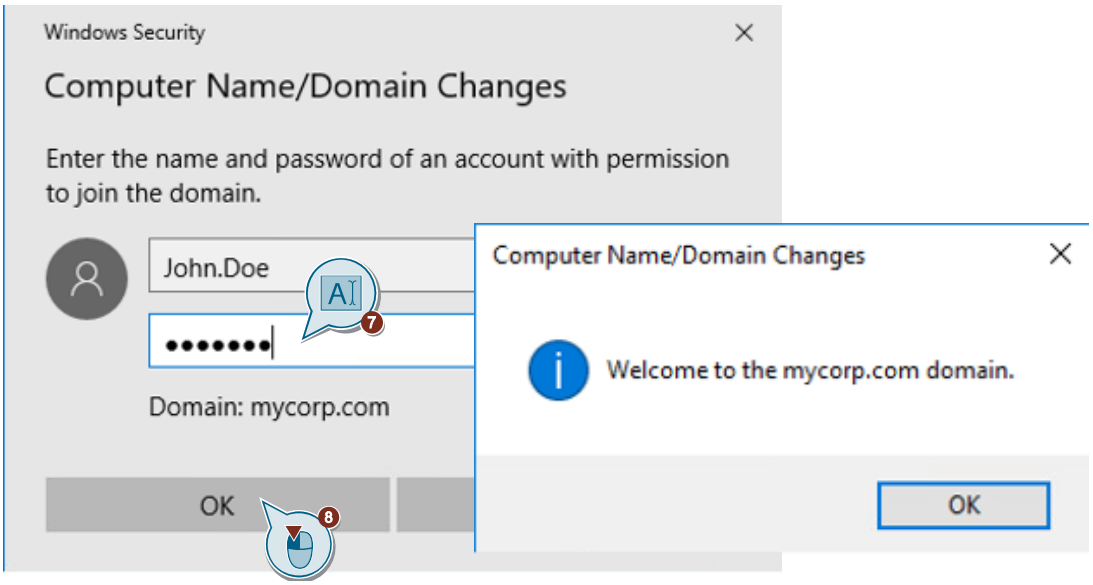
Note

The UMC ring server PC must be a member of the domain of the PC on which Microsoft Active Directory is installed.

6. Apply this setting with "OK".
   A login dialog appears.



7. Enter the login data of the user "John Doe".
8. Click on "OK".
   A message appears stating that the user "John Doe" successfully logged into the "myCorp.com" domain.



9. Restart your UMC ring server PC. If the domain user "John.Doe" can log in on the UMC ring server PC, then the UMC ring server PC is successfully logged in to the domain.

Result

The UMC ring server PC is integrated into the domain "mycorp.com" and it can import users and groups from the Microsoft Active Directory.

Next, set up the UMC ring server.

3.2.2 Install UMC and configure UMC ring server

Use the UMC installation file provided by TIA Portal or SINEC NMS.

The installation and setup of UMC depends on the UMC installation file used.

3.2.2.1 Variant for TIA Portal installation

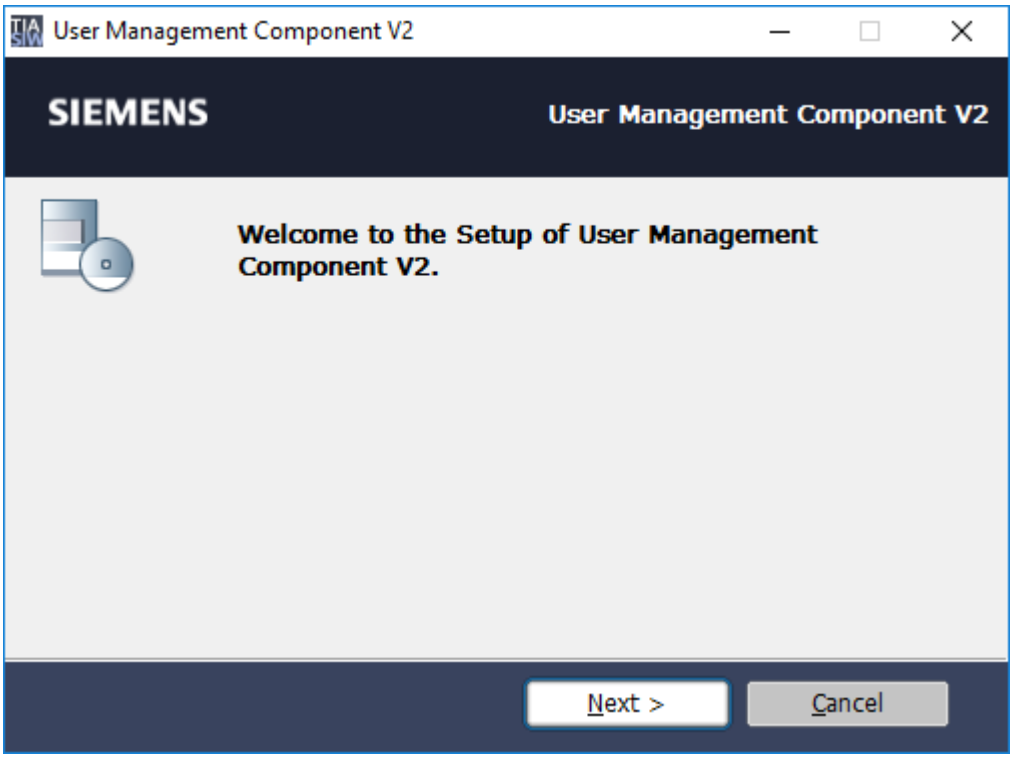
Note

The IIS configuration, as well as the IIS components necessary for the UMC installation are described in the manual "UMC_InstallationManual".

The manual "UMC_InstallationManual" can be found in the installation path "...\UserManagement\Documentation".

Installation

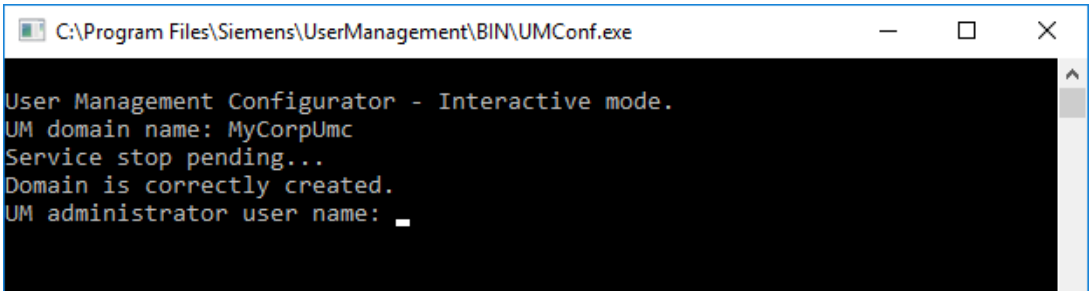
1. Run the installation file "TIA_UMC_V2.exe".
2. Unzip the installation file and run the setup.



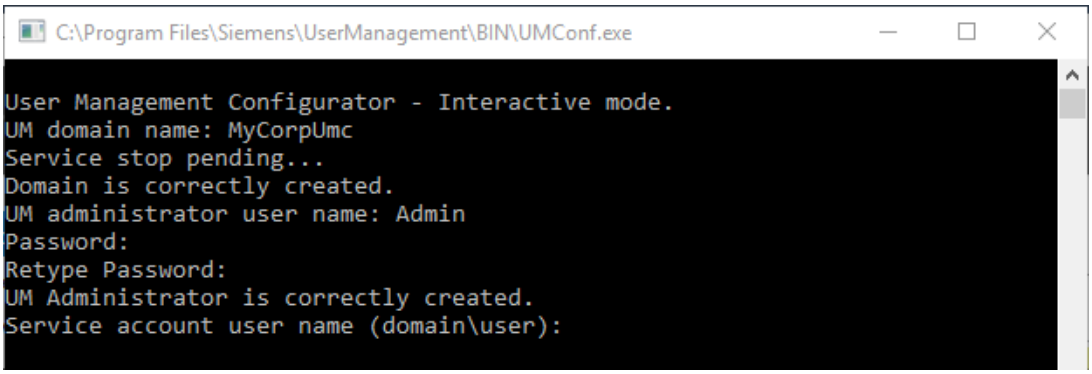
After installing the User Management Component, you must configure it. Follow these steps:

Configuration

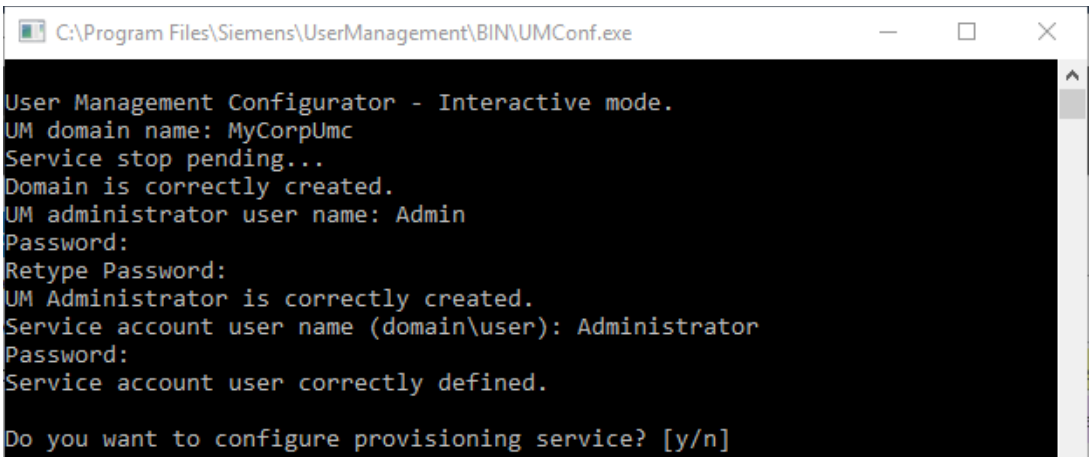
1. Start the executable file "UMConf.exe" as Administrator. The default installation path is "C:\Program Files\Siemens\Automation\UserManagement\BIN".
2. Create a unique user management domain name ("UM domain name"). Enter the desired name and confirm with <Enter>.



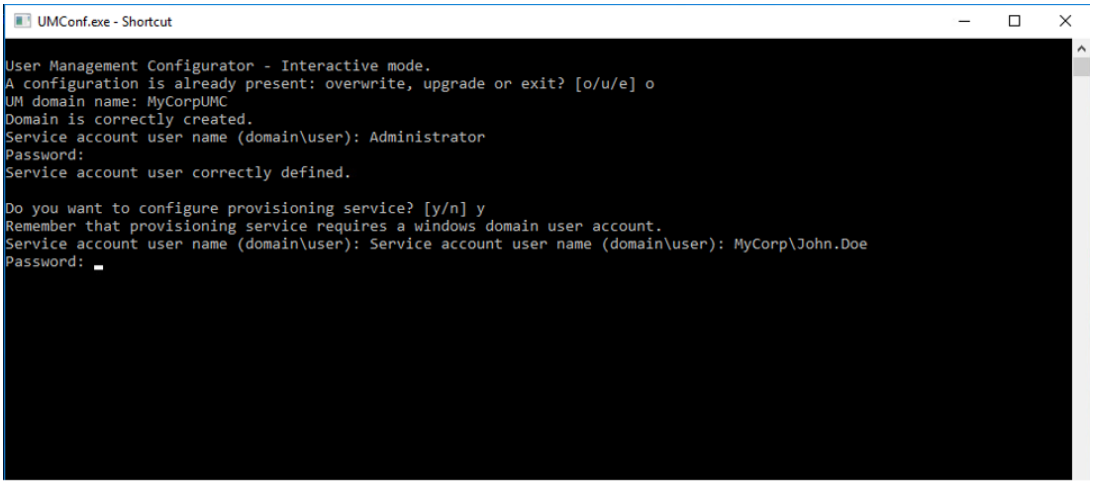
3. Create a username and a password for the UMC administrator. Confirm your entries with <Enter>.



4. Create a service account for managing the UM services. The service account must be a Windows user that either belongs to the group "UM Service Accounts" or has administrator privileges for the UM service "UMCService". This could be the default Windows administrator, for example. Confirm your entries with <Enter>.
5. Configure the UMC provisioning service to connect a Microsoft Active Directory to UMC. In this case, enter "y".

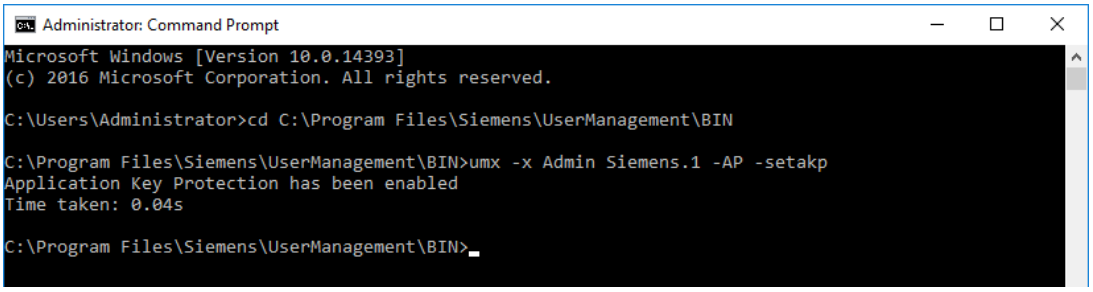


6. Enter a domain user as a service account (e. g. MYCORP\John.Doe). The domain user is linked with the UMC provisioning service. After entering the password, the console closes.



To enable the import of users into TIA Portal, you must configure another setting.

1. Open a new console as Administrator.
2. Change the directory using the following command:
   `cd C:\Program Files\Siemens\UserManagement\BIN`
3. Enter the following command. Replace "User" and "Password" with the login data of the UMC administrator.
   `umx -x [User] [Password] -AP -setakp`



4. Enable Desktop single sign-on for WinCC Unified Panels and TIA Portal.
   `umconf -dsso enable -f`
5. Close the console.

The initial setup is complete.

Note

The connection of UMC to a Microsoft Active Directory is only possible if this PC is already integrated in the corresponding domain.

The specified service account must be a user of the domain.

Note

Further help and command instructions for user management can be found on the UMC ring server PC in the following path:
"C:\Program Files\Siemens\Automation\UserManagement\Documentation"

The manual "UMC_InstallationManual" contains further information about installation, requirements, and Windows settings.

The manual "UMC_UMCONFUserManual" contains all commands for the configuration of UMC. For example, here are the commands and parameters to attach a UMC Agent to a UMC ring server (e.g., "attached").

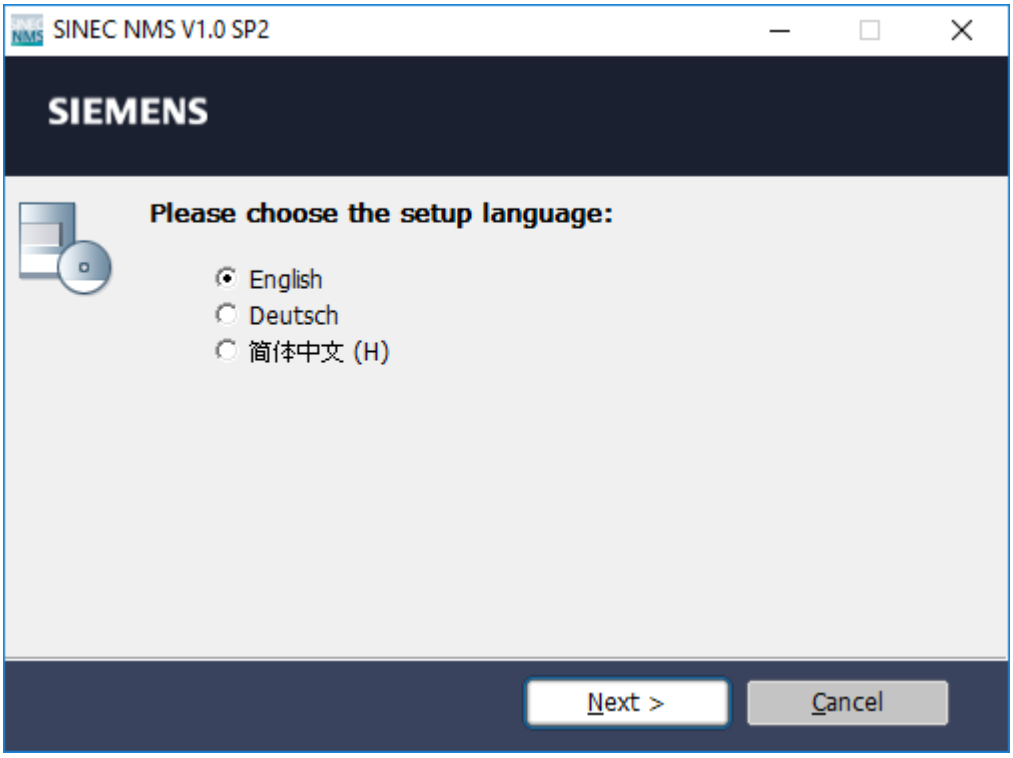
The manual "UMC_UMXUserManual" contains all commands, including the parameters for user management. For example, it describes how to create, edit, or delete users or user groups using the command line.

3.2.2.2 Variant for the SINEC NMS installation

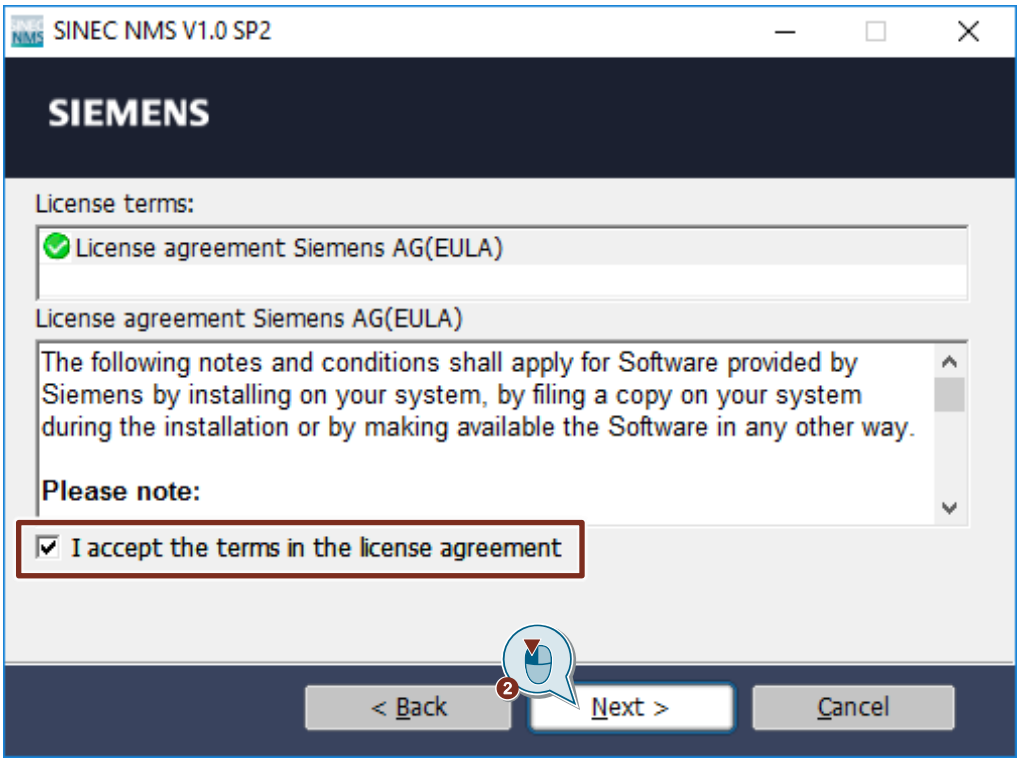
This example uses the SINEC NMS installation file

Installation

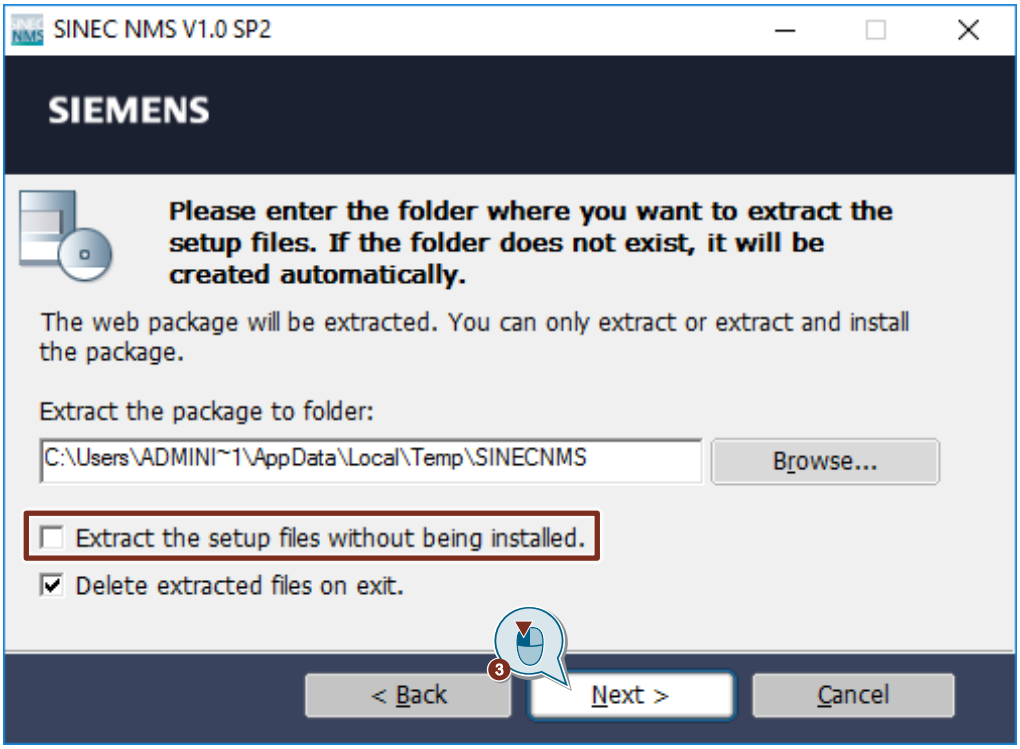
1. Launch the file "SINECNMS_V1.0_SP2.exe".



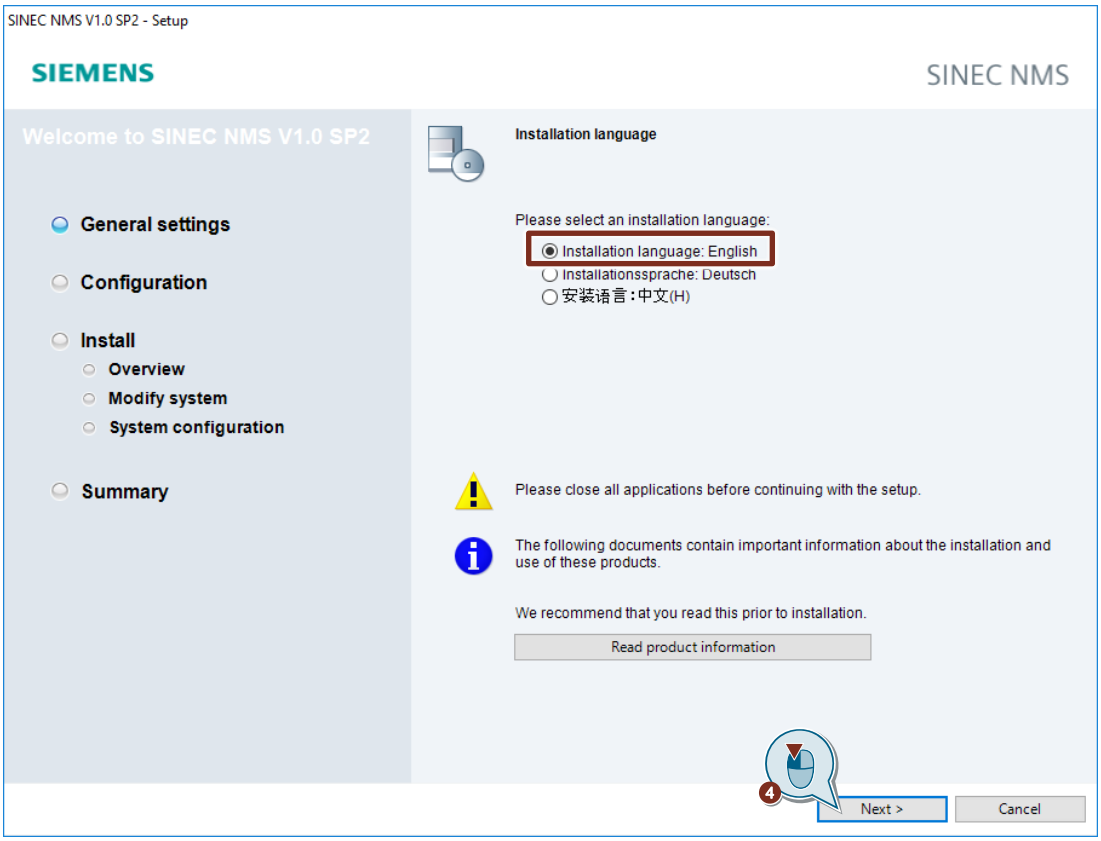
2. Accept the license agreement and click "Next".



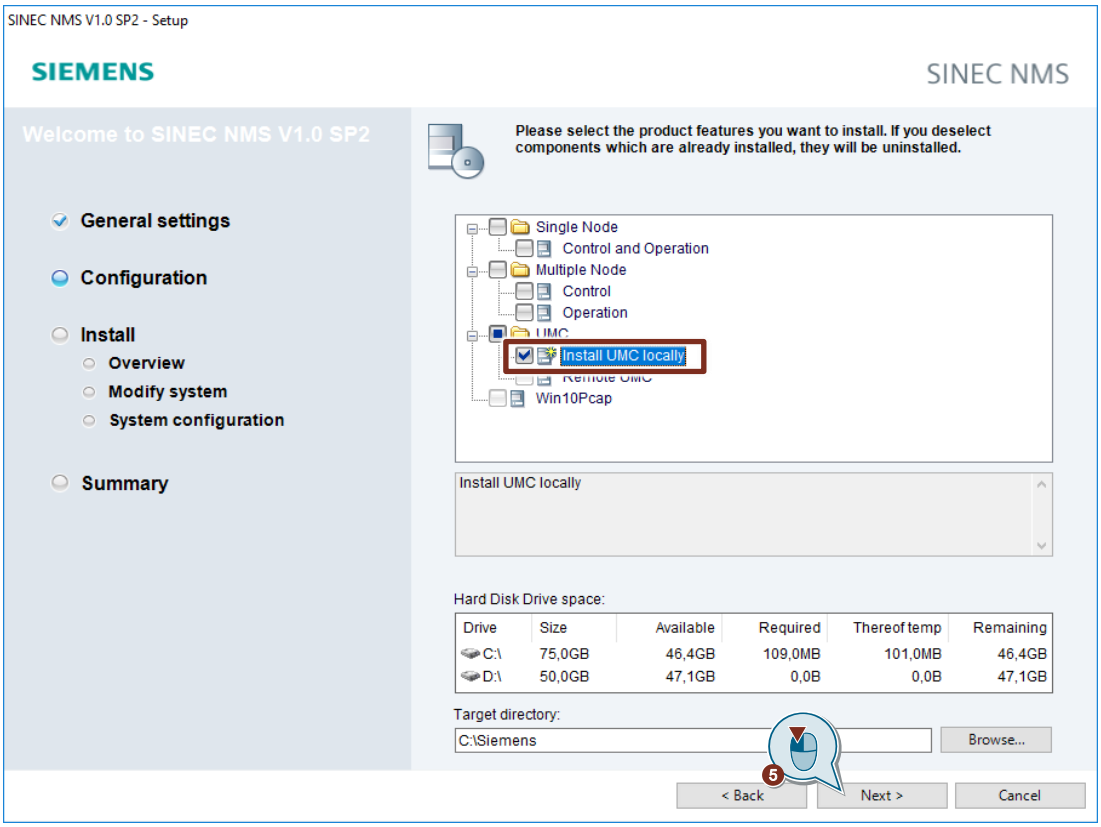
3. Extract and install the installation files. Click on "Next".



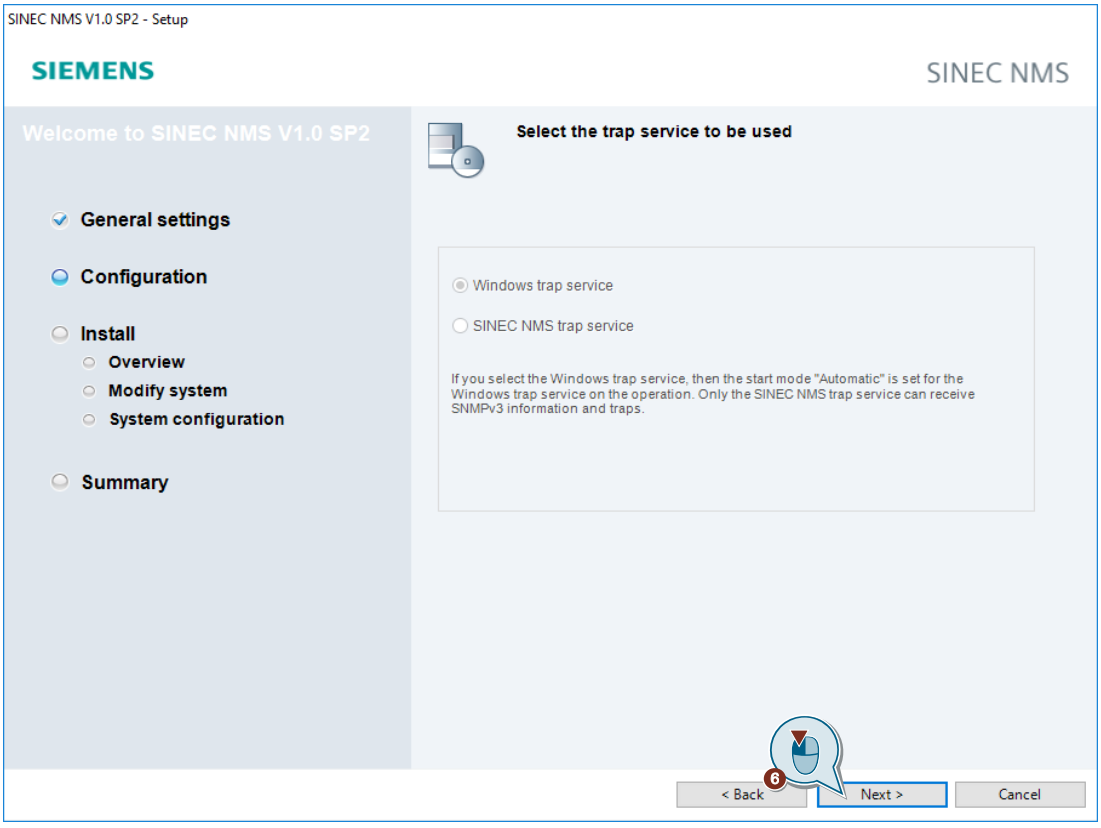
4. Select the installation language and click the "Next" button.



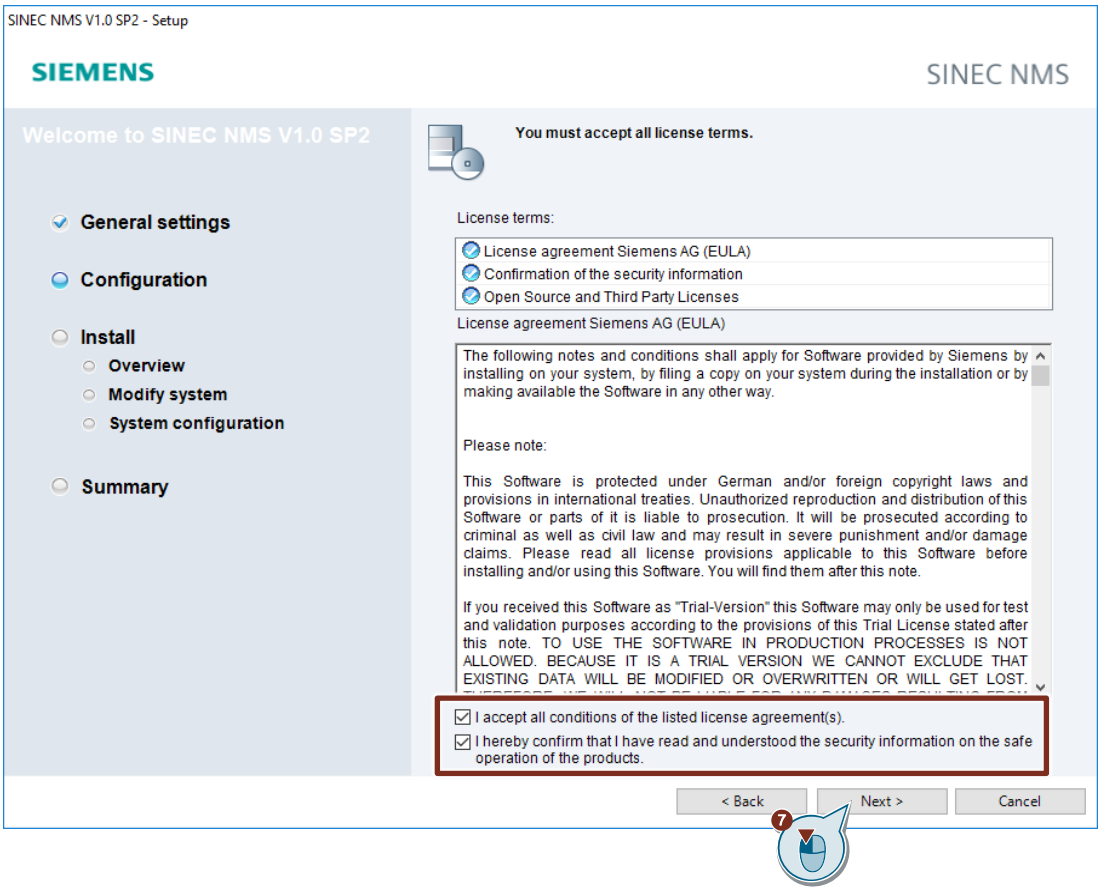
5. Select "Install UMC locally" for the product configuration and click "Next".



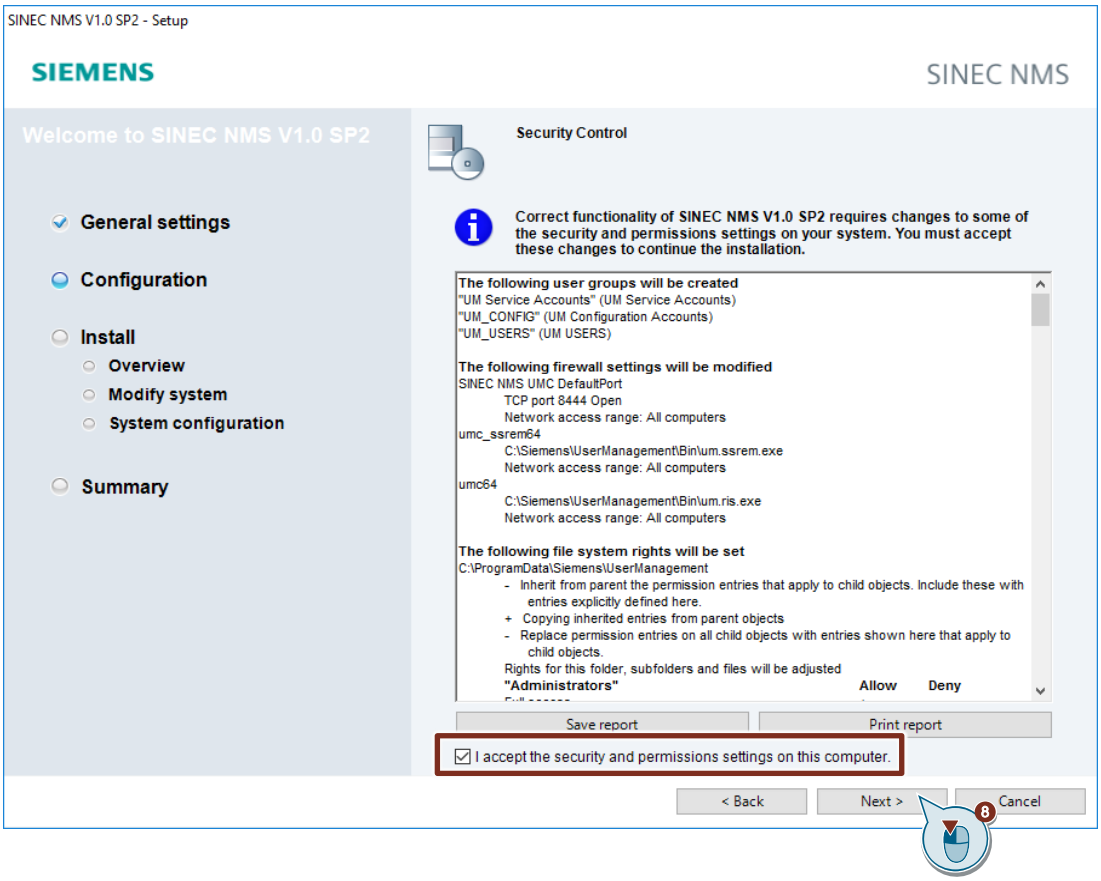
6. Click on "Next".



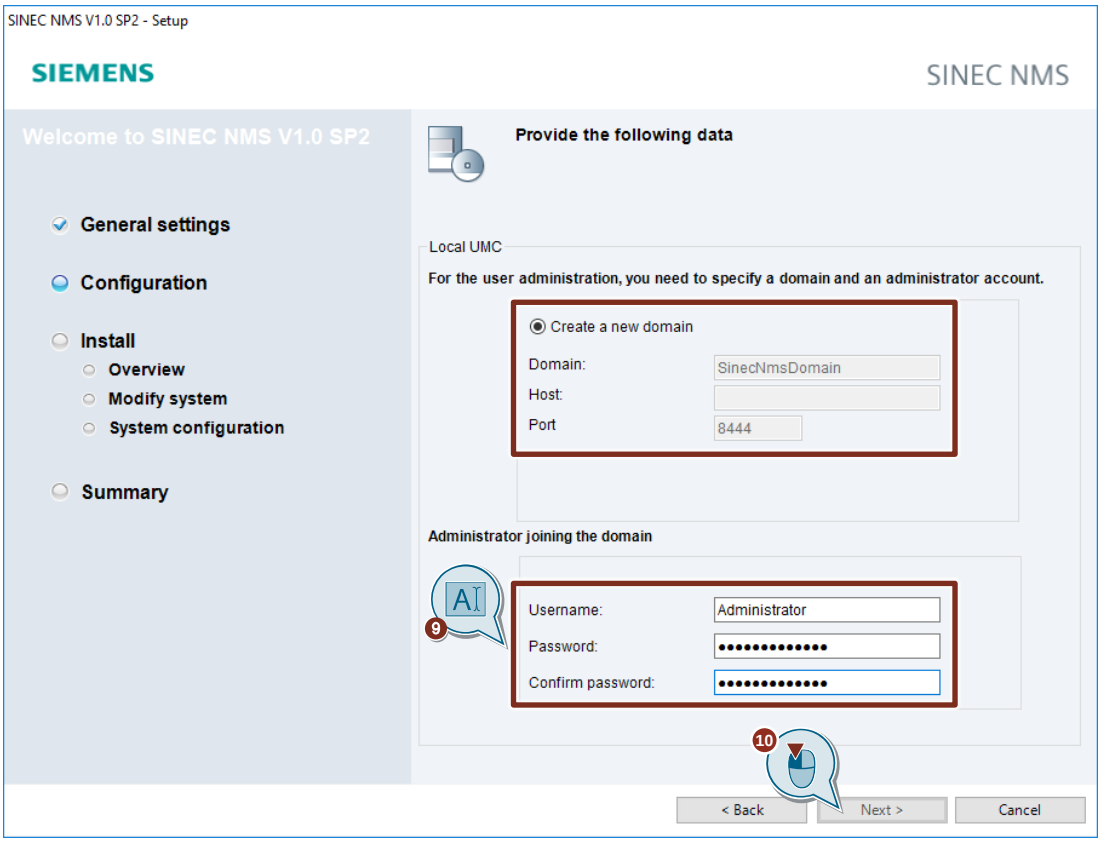
7. Accept the license agreement and confirm that you have read the security information.



8. Accept the security settings and click "Next".



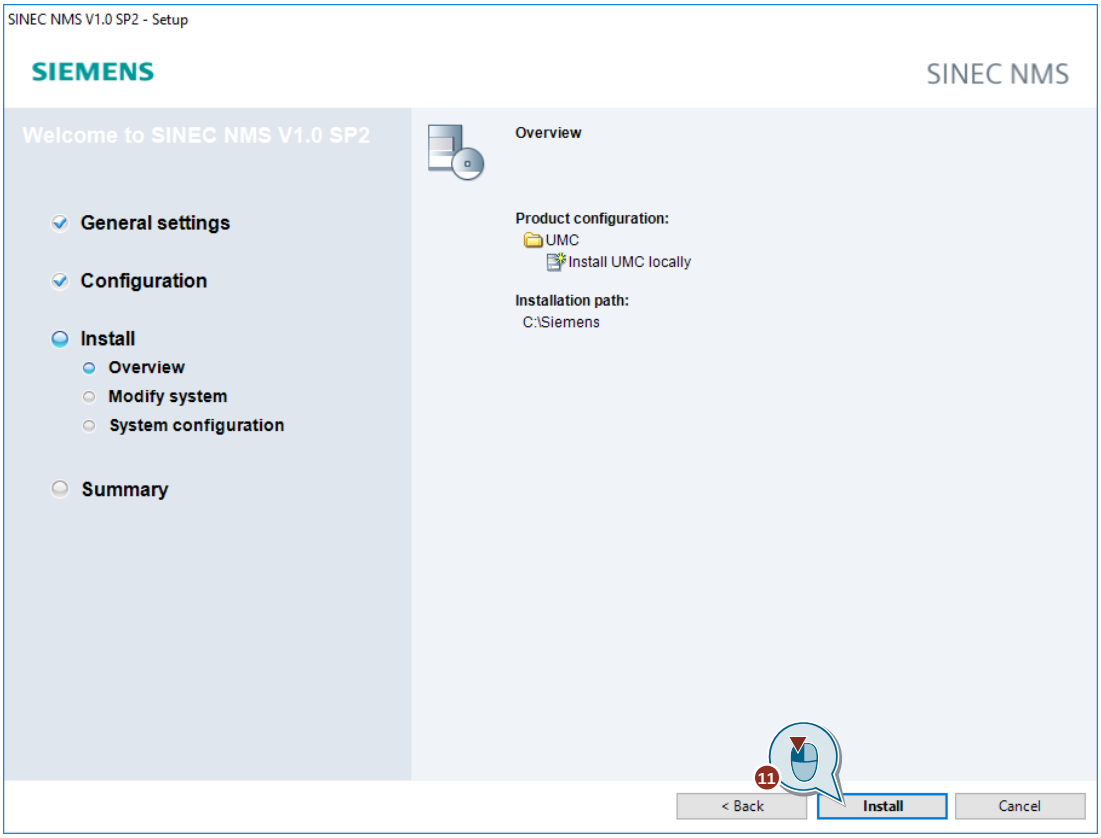
9. Enter the login information of the administrator to log in to UMC.
10. Click on "Next".



Note

During installation, a new user management domain will be created automatically, e. g. "SinecNmsDomain". The user management website uses port 8444.

11. Click "Install" to begin the installation.



12. Restart the PC.

Note The administrator account is created as a service account.

Link UMC ring server to AD

Perform the following configuration steps to link the UMC ring server to a Microsoft Active Directory (AD):

1. Open a console with Administrator permissions.
2. Use the following command to navigate to the UMC installation folder:
   `cd C:\Siemens\UserManagement\BIN`
3. Enter the following command to link a specific Windows user from the AD with the UMC provisioning service.
   In this application example, the domain user MYCORP\John.Doe is linked with the UMC provisioning service.
   `umconf -P -u MYCORP\John.Doe -p Admin1! -f`

Note

To allow the import of AD group members into UMC, the Windows user must possess the following permissions:

- Access permissions to the Microsoft Active Directory, i. e. the Windows user is a member of the Domain Admins group or Domain Users group.
- Write permissions to the folder "C:\ProgramData\Siemens\UserManagement\CONF", i. e. the Windows user is an administrator on the local PC. Alternatively, the Windows user must be assigned to the group "UM Service Accounts".

4. Close the console if the linking procedure was successful.
5. Restart the UM service "UMCService".

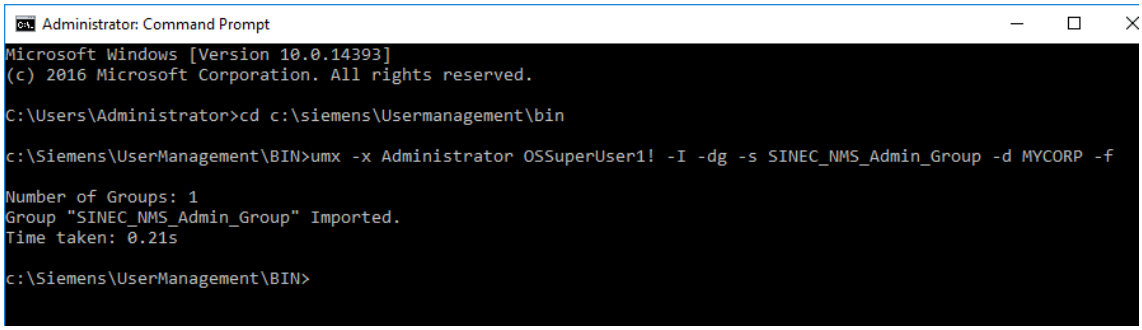
Result

The "Import Users" and "Import Domain Groups" buttons are visible in UMC.

Alternatively, it is possible to navigate to the UMC installation folder with the console and administrator rights and import groups into UMC with the following command:

`umx -x <UmcAdministrator> <Password> -I -dg -s <domainGroup> -d <domain> -f`

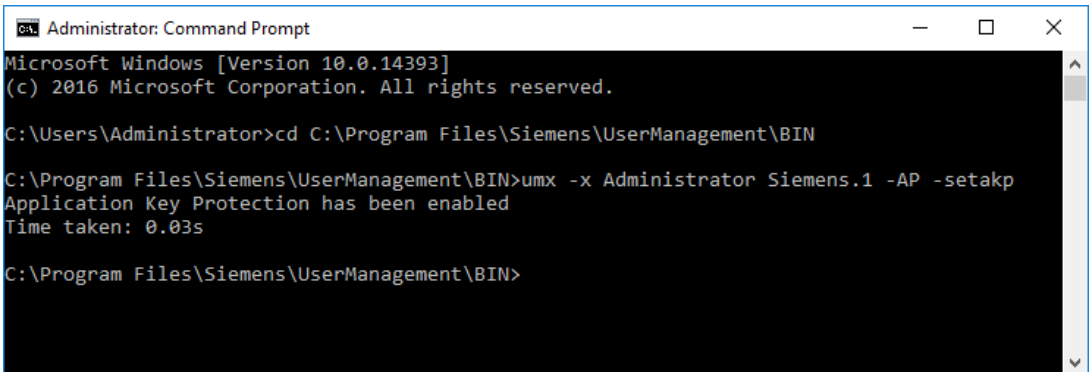
Figure 3-2



Enable users to be imported into TIA Portal

To enable the import of users into TIA Portal, you must configure another setting.

1. Open a console as an Administrator.
2. Change the directory using the following command:
   `cd C:\Program Files\Siemens\UserManagement\BIN`
3. Enter the following command. Replace "User" and "Password" with the user data of the UMC administrator.
   `umx -x [User] [Password] -AP -setakp`



Note

Further help and command instructions for user management can be found on the UMC ring server PC in the following path:
"C:\Program Files\Siemens\UserManagement\Documentation"

The manual "UMC_InstallationManual" contains further information about installation, requirements, and Windows settings.

The manual "UMC_UMCONFUserManual" contains all commands for the configuration of UMC. For example, here are the commands and parameters to attach an UMC Agent to a UMC ring server (e.g., "attached").

The manual "UMC_UMXUserManual" contains all commands, including the parameters for user management. For example, it describes how to create, edit, or delete users or user groups using the command line.

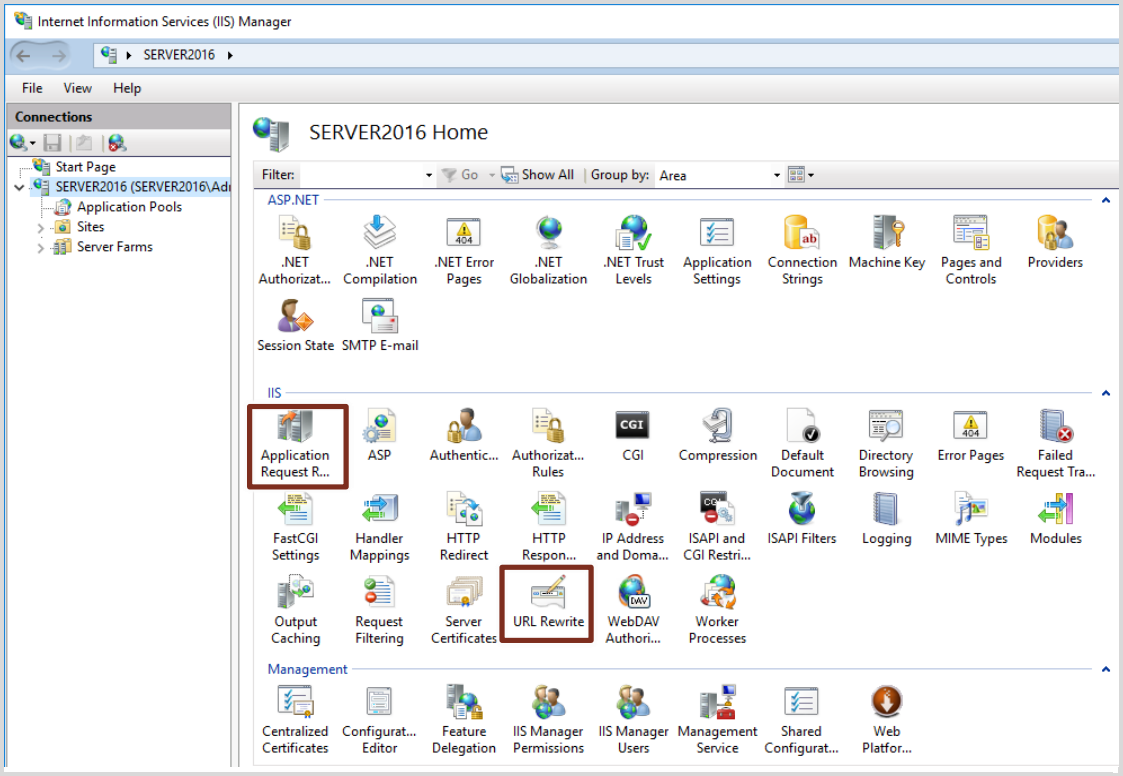
3.2.2.3 Set up access to the UMC WBM over HTTPS

Note

For detailed information on setting up Web Based Management over HTTPS, refer to the UMC installation manual.

Verify that the following IIS components are installed. These are required for accessing the UMC Web-Based Management via HTTPS.

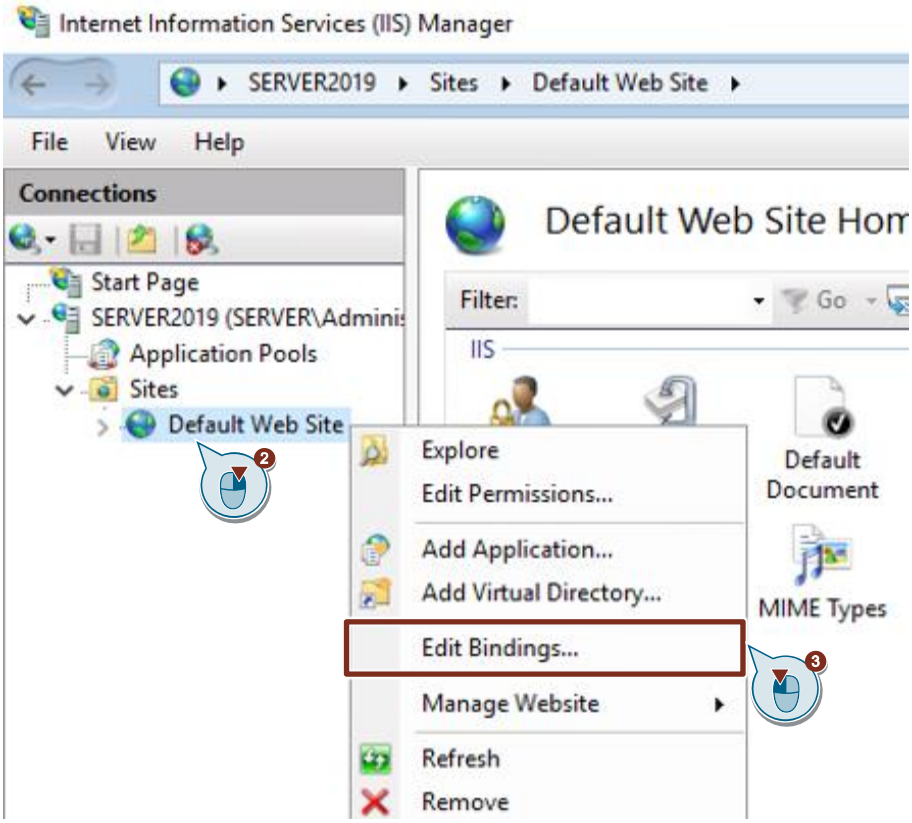
- Application Request Routing
  https://www.iis.net/downloads/microsoft/application-request-routing
- URL Rewrite
  https://www.iis.net/downloads/microsoft/url-rewrite



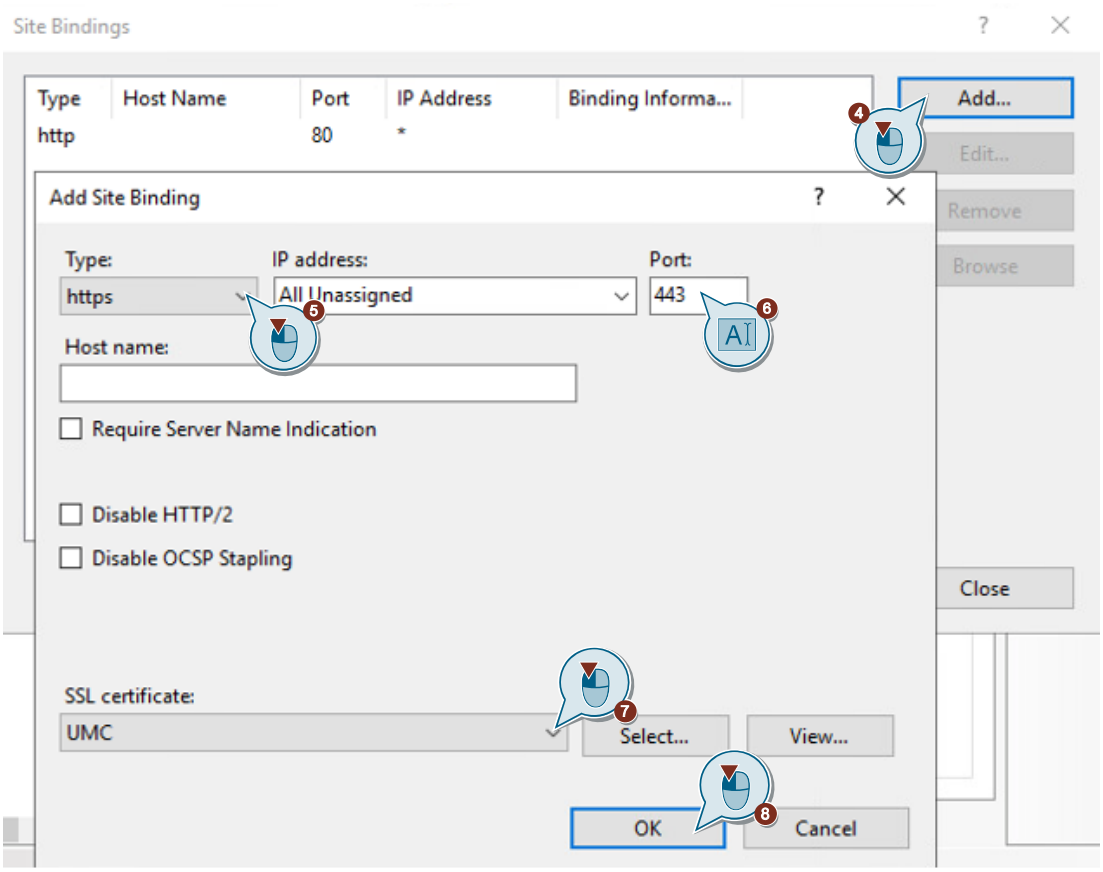
Proceed according to the instructions below to configure the Internet Information Services (IIS) Manager to work with the HTTPS protocol.

Set up the Internet Information Services (IIS) Manager on your UMC ring server PC so that you can access the UMC web server via HTTPS. To do this, you must generate your own certificate, which you then import into your browser.

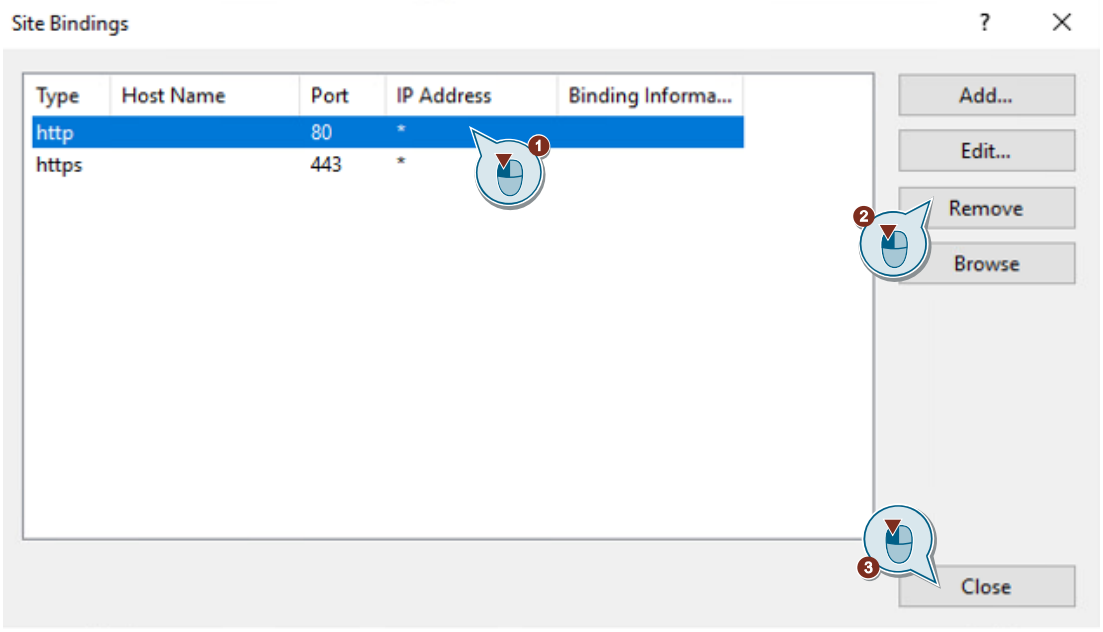
1. Open the Internet Information Services (IIS) Manager. If necessary, you must first install it via the Server Manager.
2. Right-click on "Default Web Site".
   The context menu opens.
3. Select "Edit Bindings..." in the context menu.
   The "Site Bindings" dialog will open.



4. Click the "Add" button to add a new binding or select an already existing binding, then click "Edit" to modify the settings.
   The "Add site binding" or "Edit site binding" dialog will open.
5. Select the "https" type for the binding.
6. Enter the port for the "https" binding. The TIA Portal installation uses port 443. The SINEC NMS installation uses port 8444.
7. Assign the UMC SSL certificate to the "https" binding.
   The following chapters provide more information on SSL certificates:
   - Chapter 5.1
   - Chapter 5.2
   - Chapter 5.3
8. Then confirm the entries with "OK".



9. Delete the "http" binding, as it is not needed in this application example. Close the window.



10. Run the batch file "REMOVE_IdP_WebUi_configuration.bat" as an administrator.
11. Run the batch file "IdP_WebUi_configurator.bat" as an administrator.

Note

The default installation path for these files is:
"C:\Program Files\Siemens\Automation\UserManagement\BIN".

Result

The initial setup of UMC and the Identity Web Provider, which allows access to the Web Based Management (WBM), has been completed. You can now log in to the UMC via the WBM. Install the applied certificate on the PCs that need to have access to the WBM (see chapter 5.4).

To log in to the UMC WBM, open a web browser such as Chrome and enter this address in the address bar:

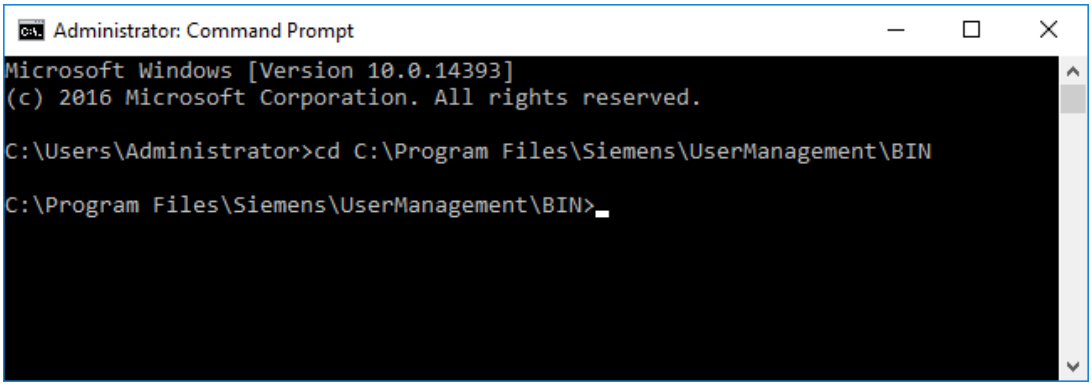
- https://localhost:<Port>/UMC

Note The TIA Portal installation uses port 443. The SINEC NMS installation uses port 8444.

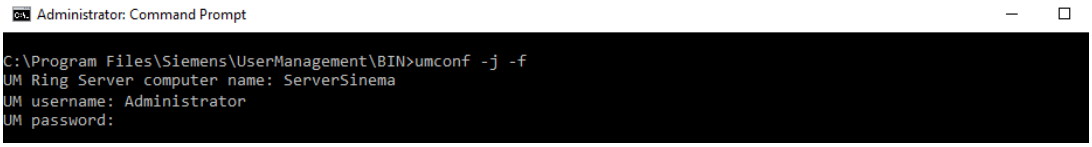
3.2.3 Set up a secondary UMC ring server

If you need redundancy, install UMC on the secondary server PC. Configure the secondary server PC as a UMC ring server. A UMC server is used only for load balancing, not redundancy. When connecting to a Microsoft Active Directory, ensure that the server PC is also a member of the domain.

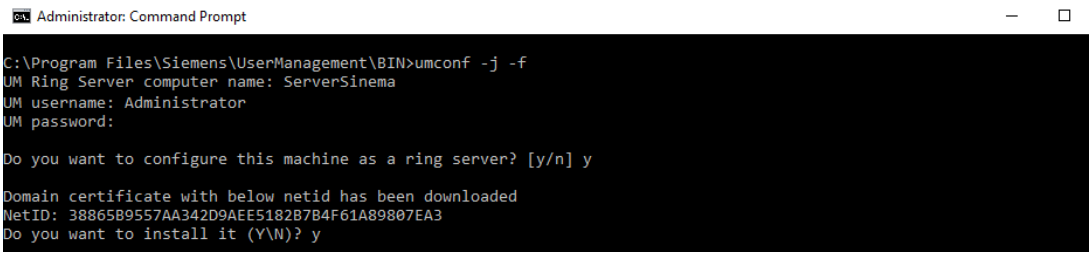
1. Open a console with Administrator permissions.
2. Change to the folder "BIN" in the installation directory of the UMC. The default path is "C:\Program Files\Siemens\UserManagement\BIN". To do this, enter the following command.
   `cd C:\Program Files\Siemens\UserManagement\BIN`



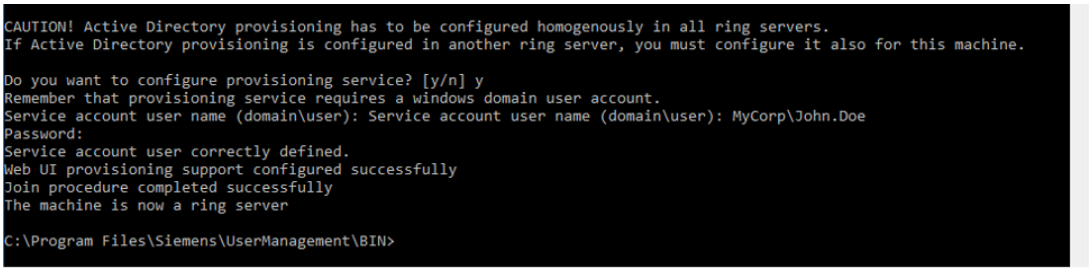
3. Now enter the command "umconf -j". This command causes the current UMC installation to connect to the existing UMC ring server. An additional "-f" is required if the UM service "UMCService" has not yet been stopped. The necessary information is then automatically requested.



4. Enter the PC name of the primary UMC ring server and the credentials of the UMC service account.
   Now you are asked whether the server should be configured as a secondary ring server. Confirm this with "y".
5. The console automatically downloads the certificate from the primary UMC ring server, which must be installed. Confirm this with "y".



6. If you have linked a Microsoft Active Directory to the UMC ring server, you must also do this in the secondary UMC ring server. For this purpose, enter a domain user as the service account (e. g. MYCORP\John.Doe), as already described for the configuration of the "provisioning service".



After the configuration is complete, the secondary UMC ring server is now up and running.

4 UMC Operation

After installing UMC and setting up the web components, you can log into the UMC Web-Based Management (WBM) using a web browser. To do this, open a web browser on the UMC ring server PC and enter the following URL:

- https://localhost:<Port>/UMC

The following URL also allows you to access the WBM from a different PC:

- https://<IP address or host name of the UMC ring server PC>:<Port>/UMC

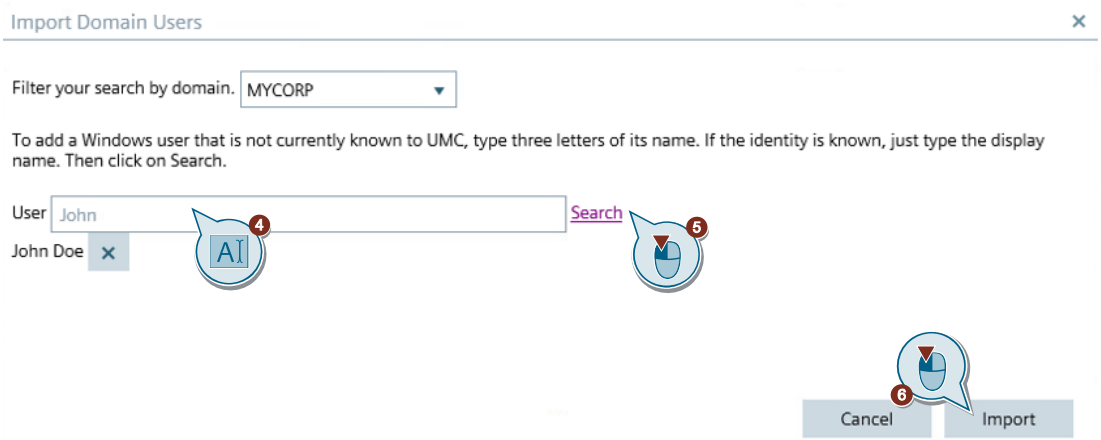
Import or create users

Note To be able to import domain users and domain groups into UMC, you must have logged in once with a domain user on the local UMC ring server PC.

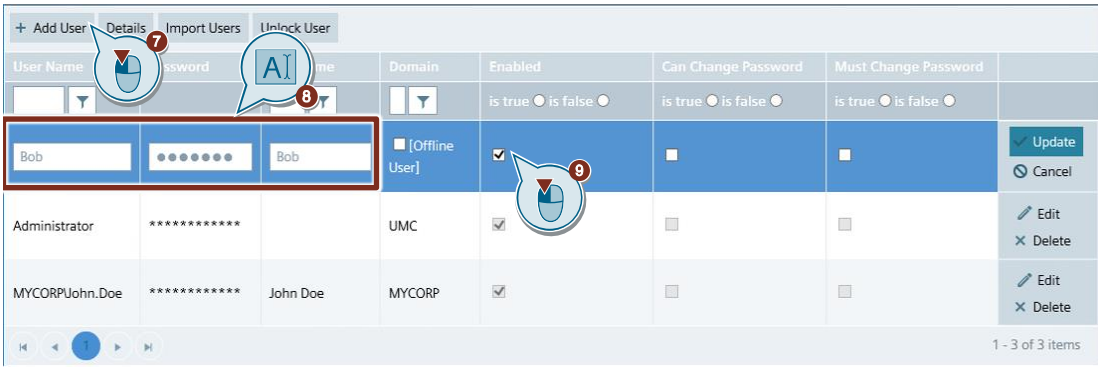
1. Log in to UMC with your administrator account and click the Menu icon .
2. Navigate to "Users".

3. If you have connected UMC to a Microsoft Active Directory, click the "Import Users" button to import users from the Microsoft Active Directory.
The "Import Domain Users" dialog opens.

4. Enter the name of the domain user you want to import from the selected domain.
5. Click on "Search".
6. After the specified domain user is found, click "Import" to import it.



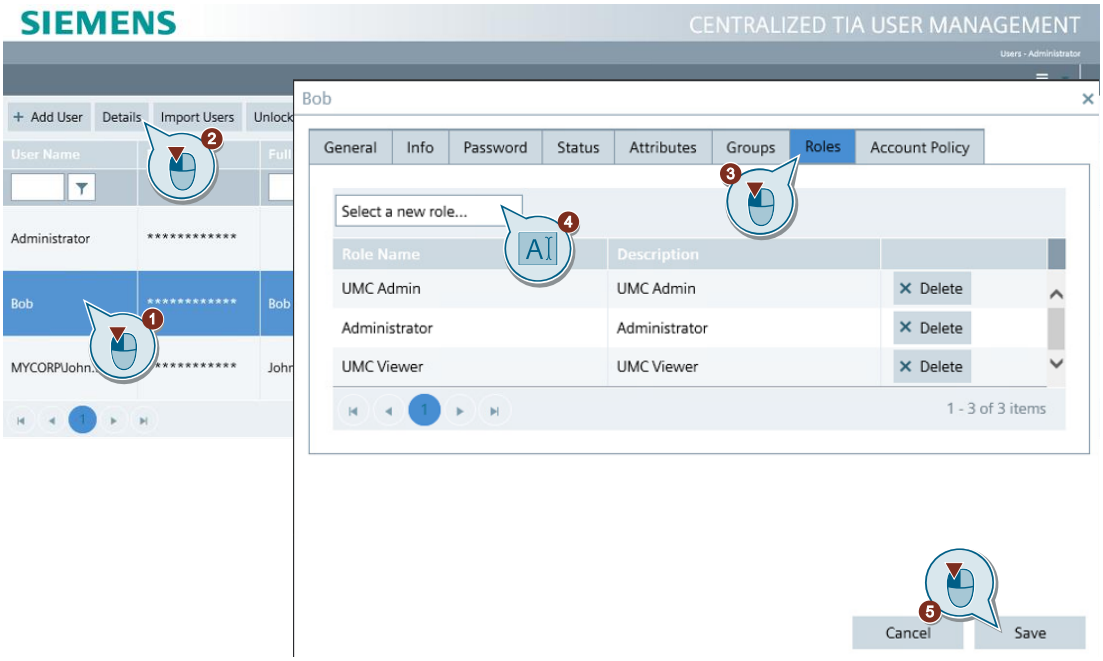
7. Click the "Add User" button to create a new user in UMC.
8. Enter a username and a password for the user.
9. Enable the user.



Note It is necessary to activate the users you have created or imported.

Assign a role to the user

1. Select the newly created or imported user.
2. Click "Details".
   The "Details" dialog for the user will open.
3. Open the "Roles" tab.
4. Enter the name of the role that you wish to assign to the user.
   The roles listed are for UMC only.
5. Save your changes.



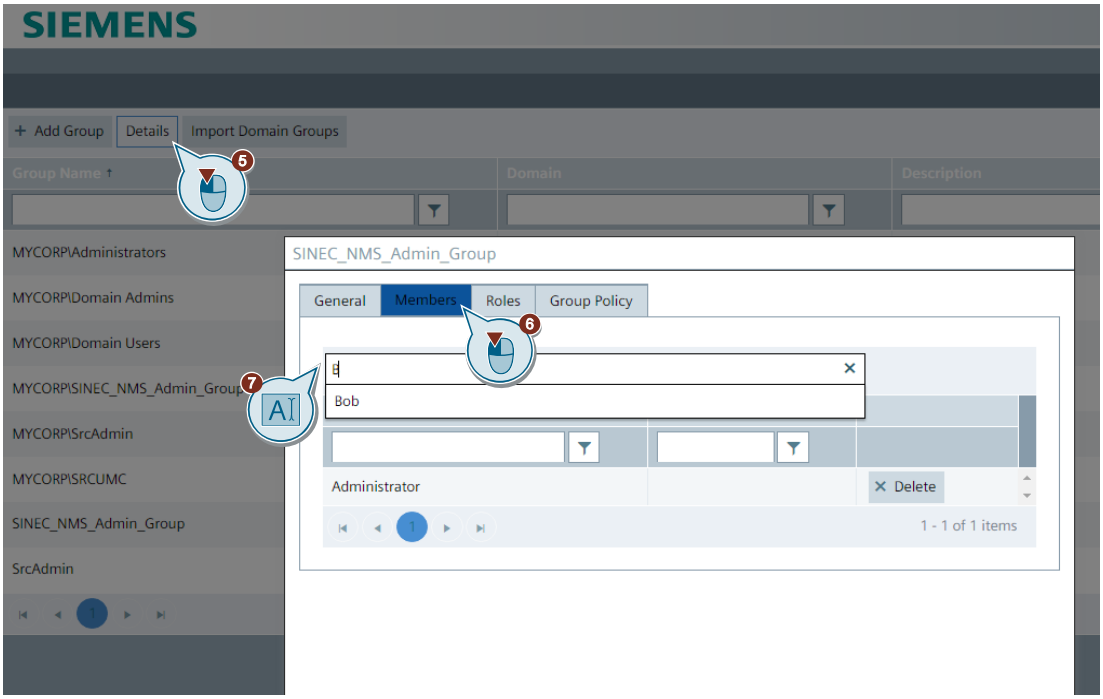
Create groups

1. Click the menu icon  .
2. Navigate to "Groups".
3. Click "Import Domain Groups" to import groups from the linked Microsoft Active Directory.
4. Click "Add Group" to create your own groups.

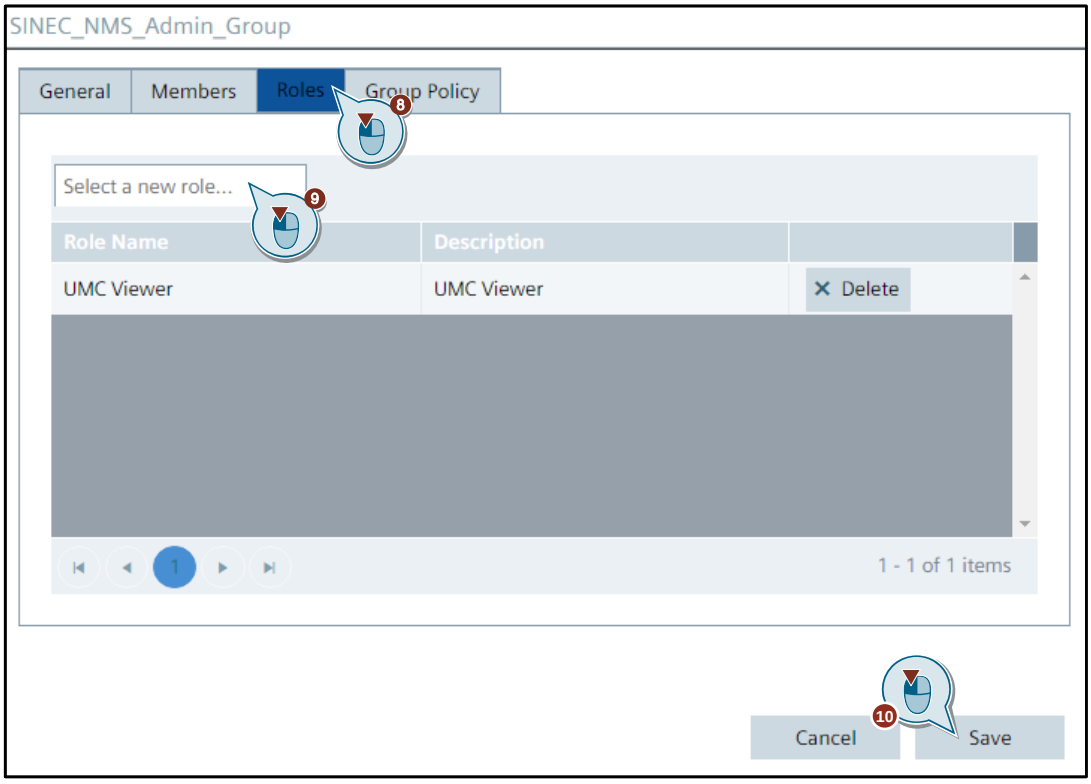
5. Select the newly created or imported groups and click the "Details" button.
   The "Details" dialog for the user will open.
6. Open the "Members" tab.
   All users assigned to the group will be displayed.

Note For domain groups, all users assigned to the group in the AD will be displayed.

7. Enter the name of the user that you wish to assign to the group.



8. Open the "Roles" tab to add the desired permissions to the group.
9. Enter the name of the role that you wish to assign to the group.
10. Save your entries.



Note

NOTE

If a user need be able to link UMC agents to UMC, the user needs the "UM_ATTACH" permission.

If a user should be able to join UMC servers to UMC, they need the "UM_JOIN" permission.

For more information on the functional permissions of users, please refer to the "UMC Web UI User Manual", in Section 1.5.
The "UMC Web UI User Manual" can be found via the following path:
"C:\Program Files\Siemens\UserManagement\Documentation".

Summary

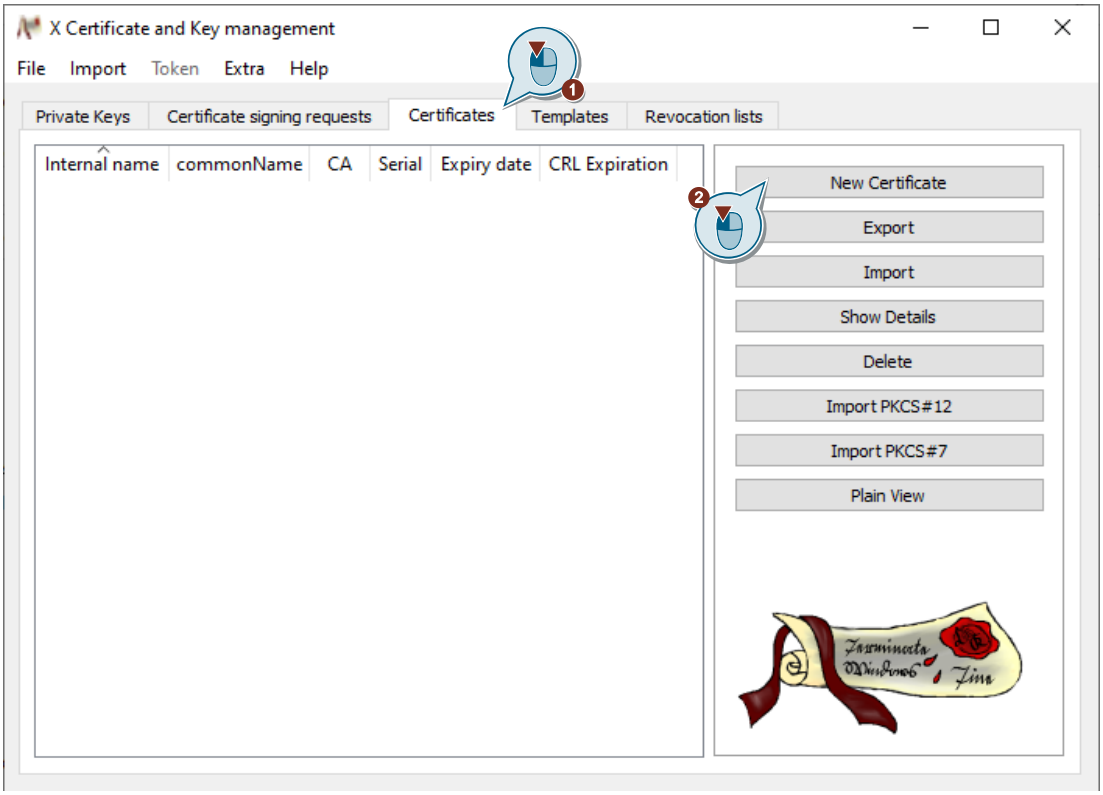
UMC is now fundamentally configured and UMC Agents or UMC servers can be connected. Instructions on how to connect applications from the SIEMENS portfolio can be found in additional documents on the entry page of this application example.

5 Useful information

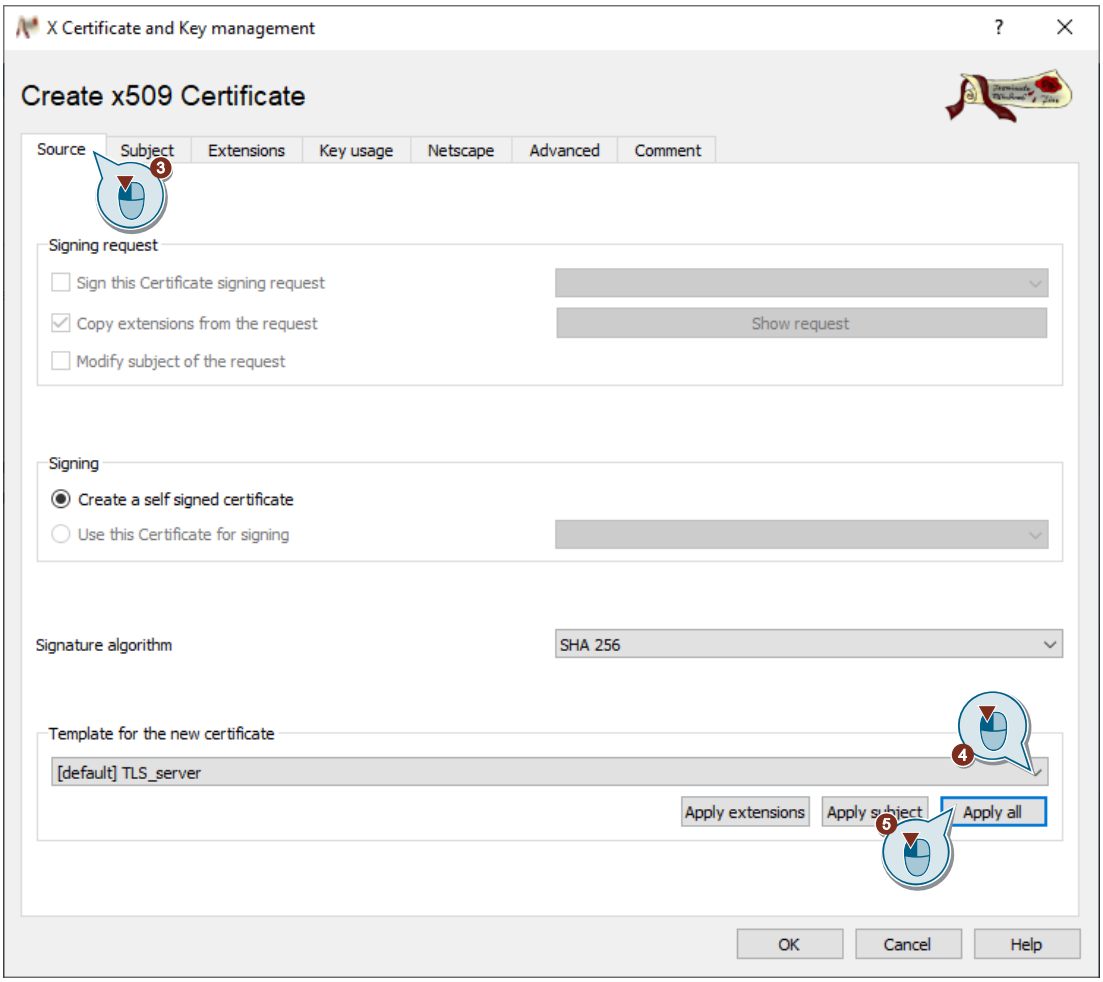
5.1 Creating an SSL certificate in XCA

If the SSL certificate was not automatically installed when installing UMC, you can create an SSL certificate with XCA.

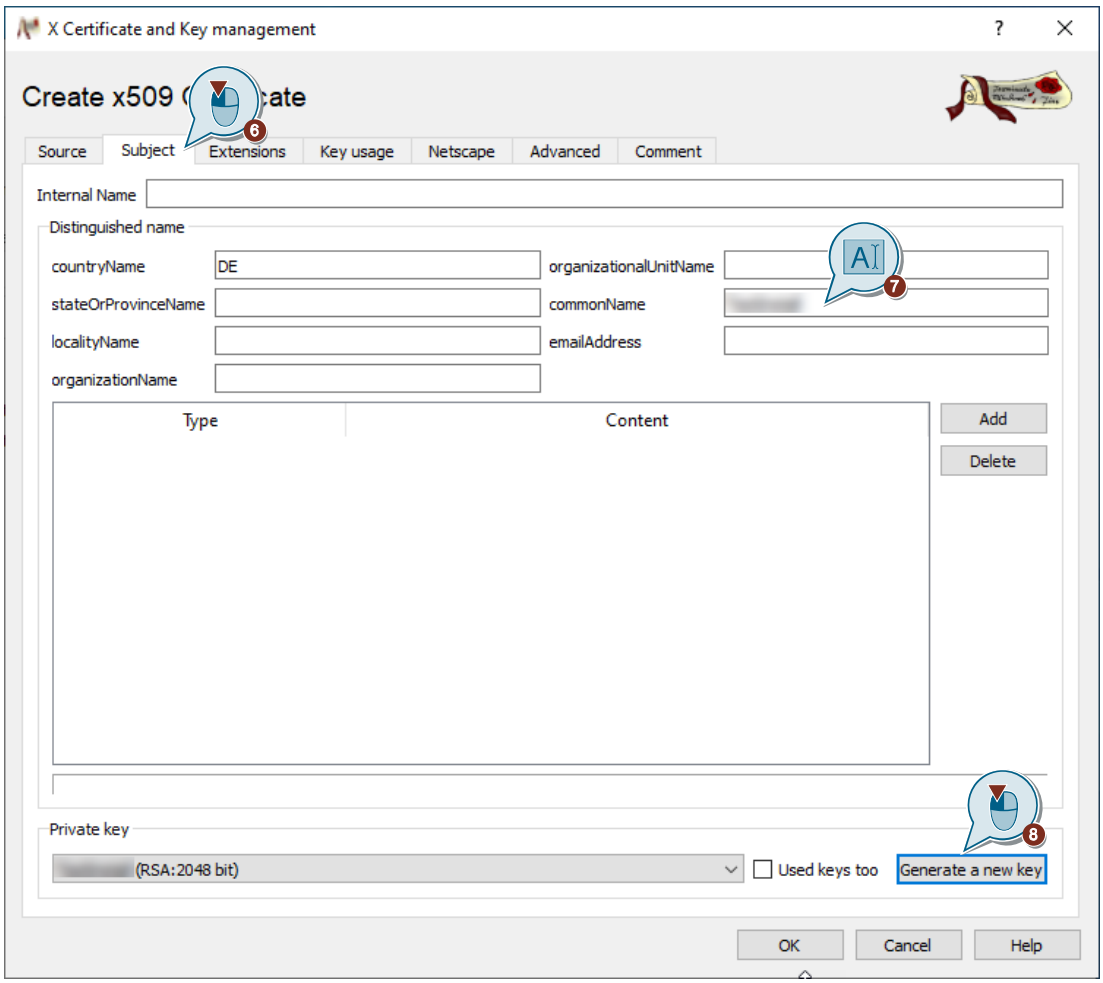
1. Switch to the "Certificates" tab in XCA.
2. Click the "New Certificate" button.
   The "Create x509 Certificate" dialog will open.



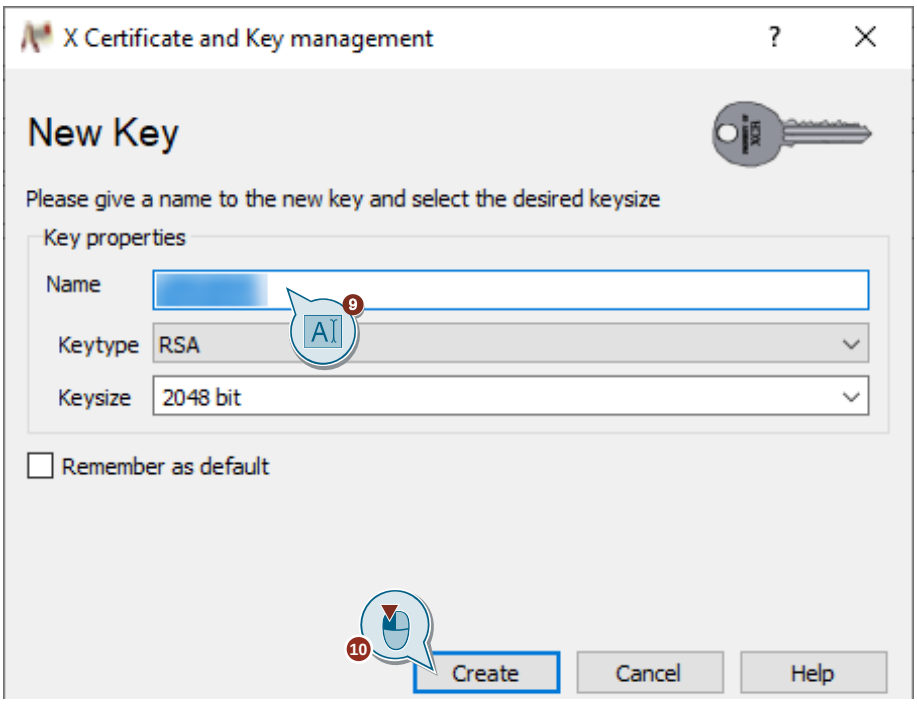
3. Open the "Source" tab.
4. Select the template "TLS_server" for the new certificate.
5. Click "Apply all".



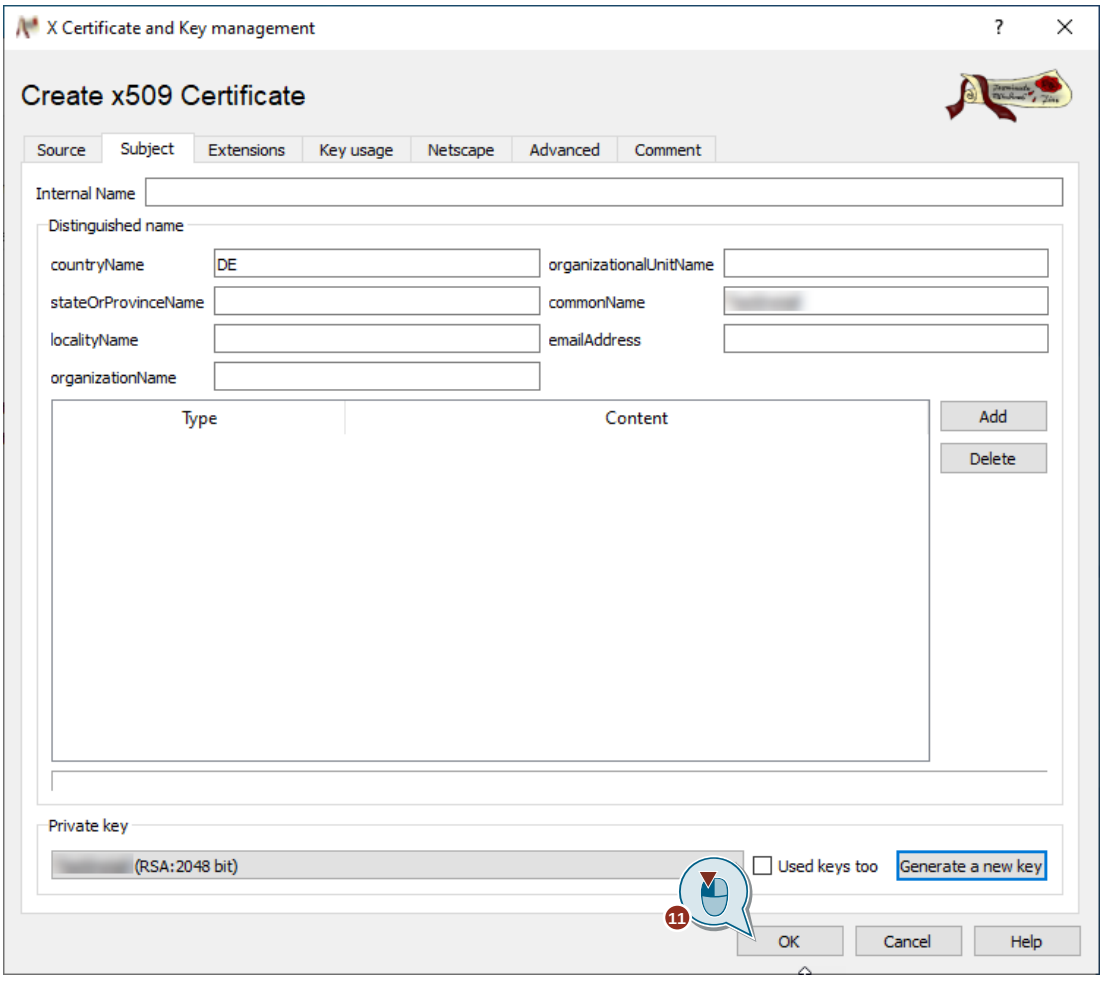
6. Open the "Subject" tab.
7. Under "commonName", enter the PC name of the UMC ring server PC.
8. Click "Create a new key".
   The "New Key" dialog will open.



9. Enter a name for the new key.
10. Click "Create" to create the private key.



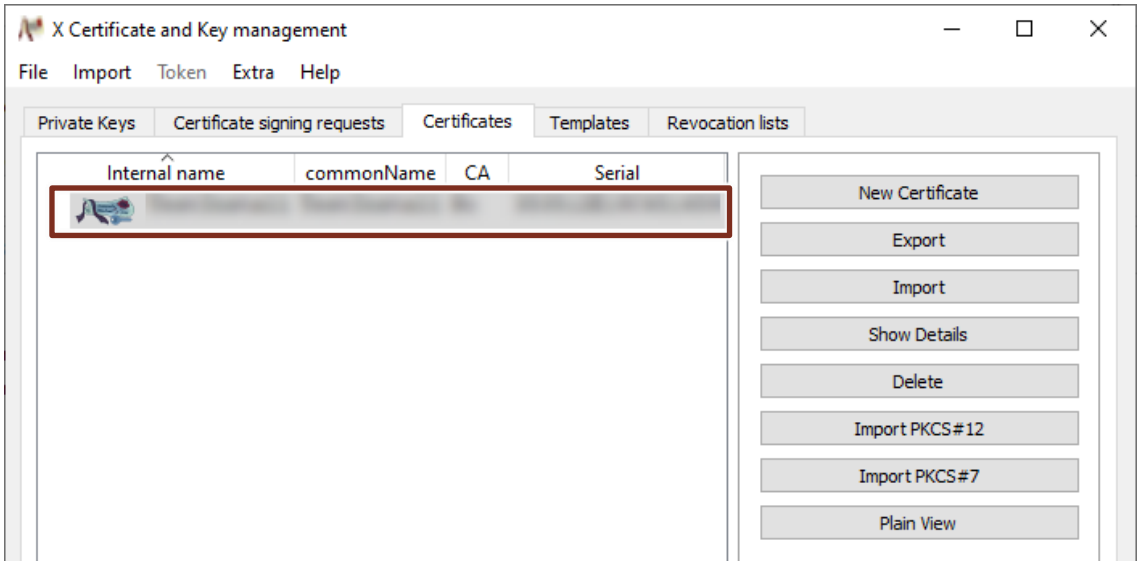
11. In the "Create x509 Certificate" dialog, click "OK" to create the certificate.



Result

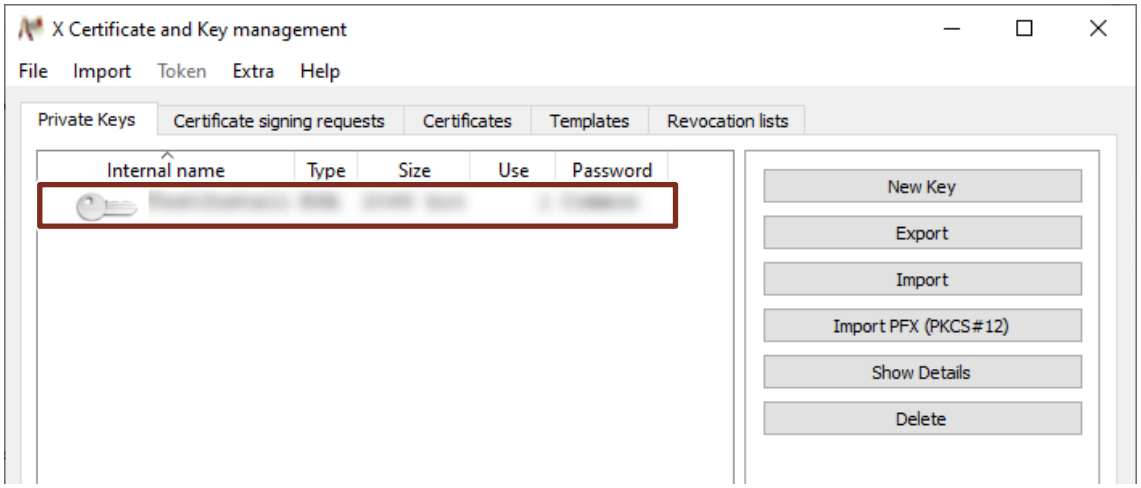
The generated x509 certificate will appear in XCA in the "Certificates" tab.

Figure 5-1



The private key you created will appear in the "Private Keys" tab in XCA.

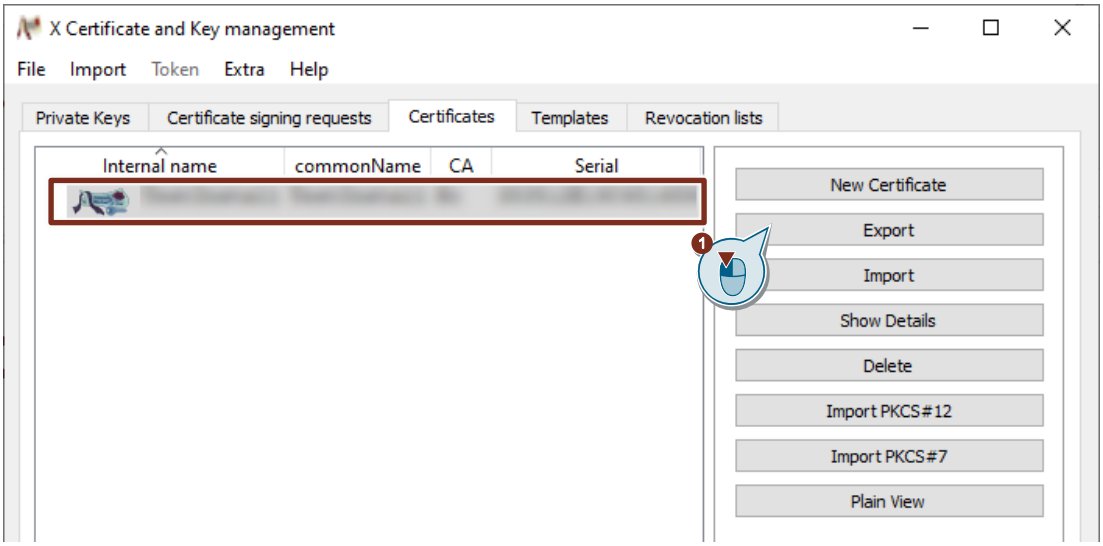
Figure 5-2



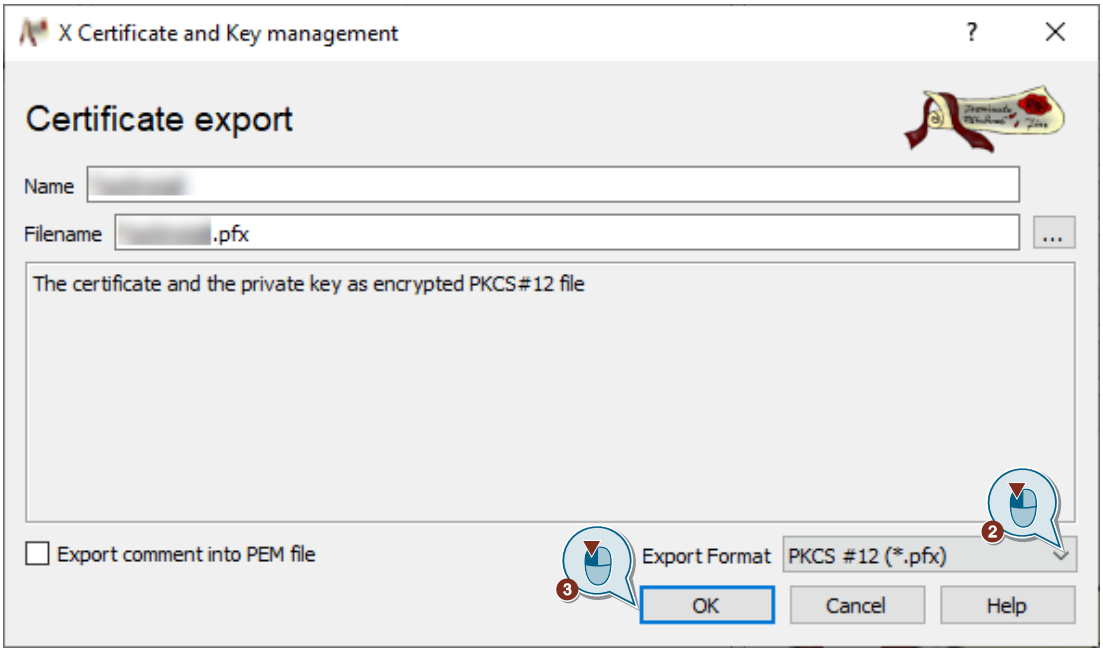
5.2 Exporting SSL certificate from XCA

Export the SSL certificate from XCA to be able to import it later on the UMC ring server PC

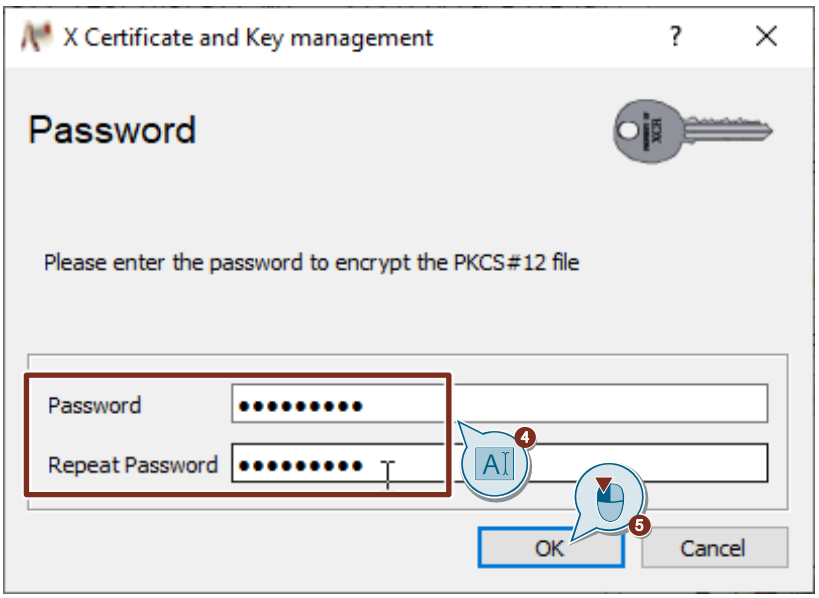
1. In the "Certificates" tab in XCA, select the created certificate and click "Export".
   The "Certificate export" dialog will open.



2. Select the export format "PKCS #12 (*.pfx)".
3. Click "OK".
   The "Password" dialog opens.



4. Enter the password for encrypting the "PKCS #12" file.
5. Click "OK".

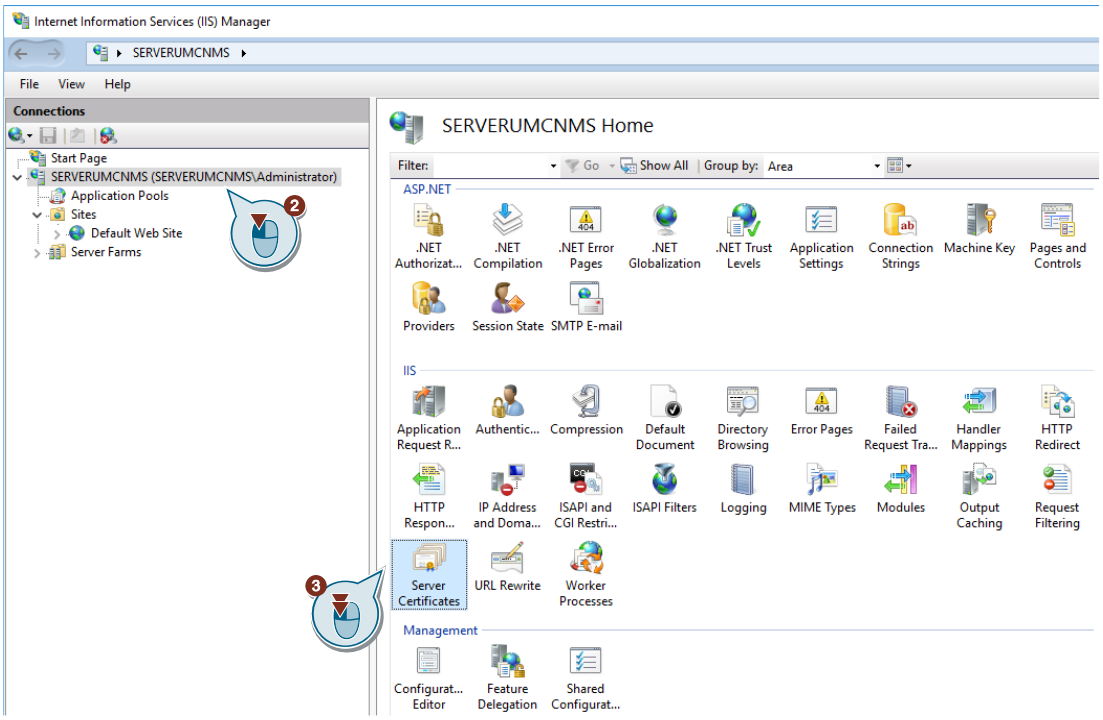


Result

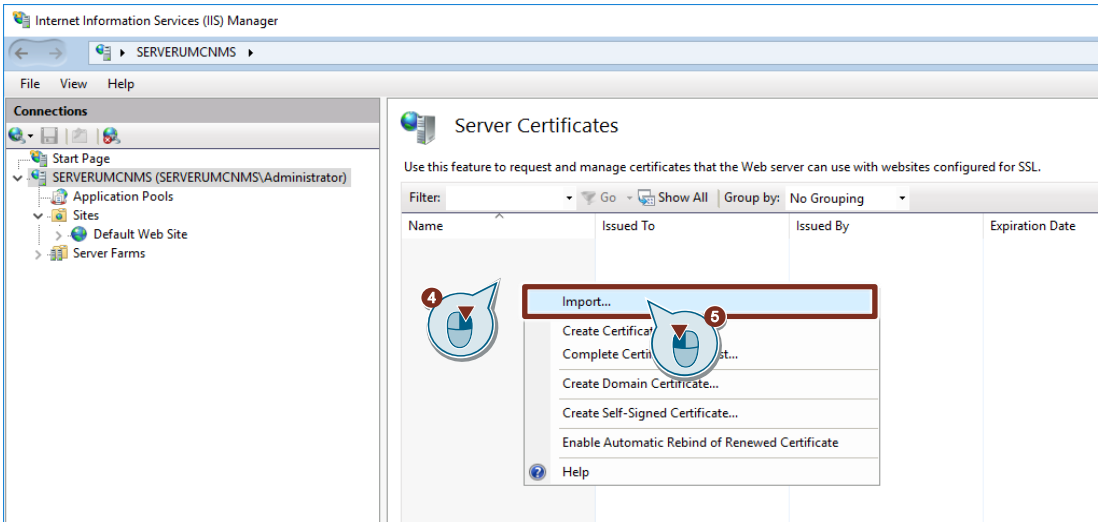
The certificate and private key have been exported.

5.3 Importing SSL certificate on the UMC ring server PC

1. On the UMC ring server PC, open the Internet Information Services (IIS) Manager. If necessary, you must first install it via the Server Manager.
2. Select the UMC ring server PC.
3. Double-click the "Server Certificates" button.
   The "Server Certificates" dialog will open.

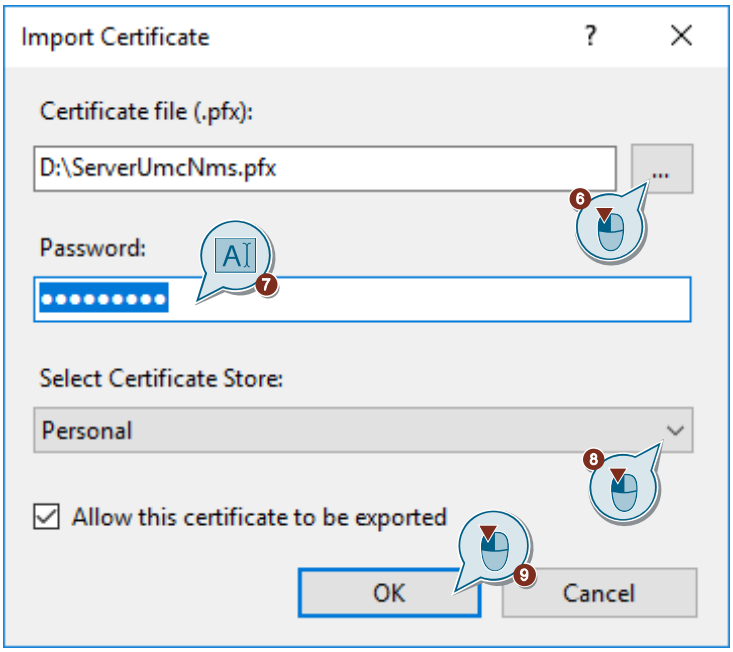


4. Right click in the "Server Certificates" dialog.
   The context menu opens.
5. Select "Import" in the context menu.



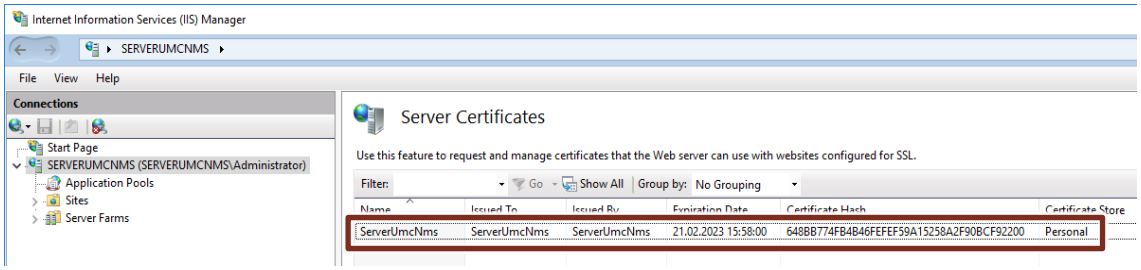
6. Select the certificate file (*.pfx) you exported from XCA in an earlier step.
7. Enter the password that you set when exporting the certificate file (*.pfx).

8. Select the certificate store "Personal".
9. Click "OK".



Result

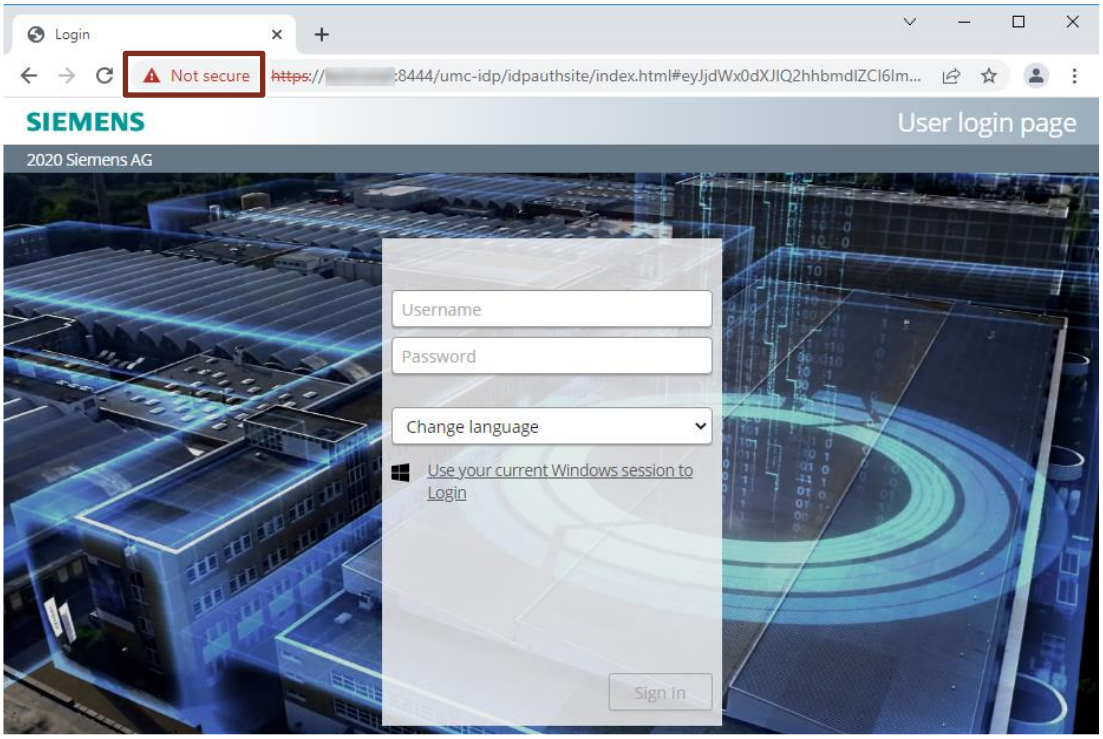
The SSL certificate has been imported into the Internet Information Services (IIS) Manager.



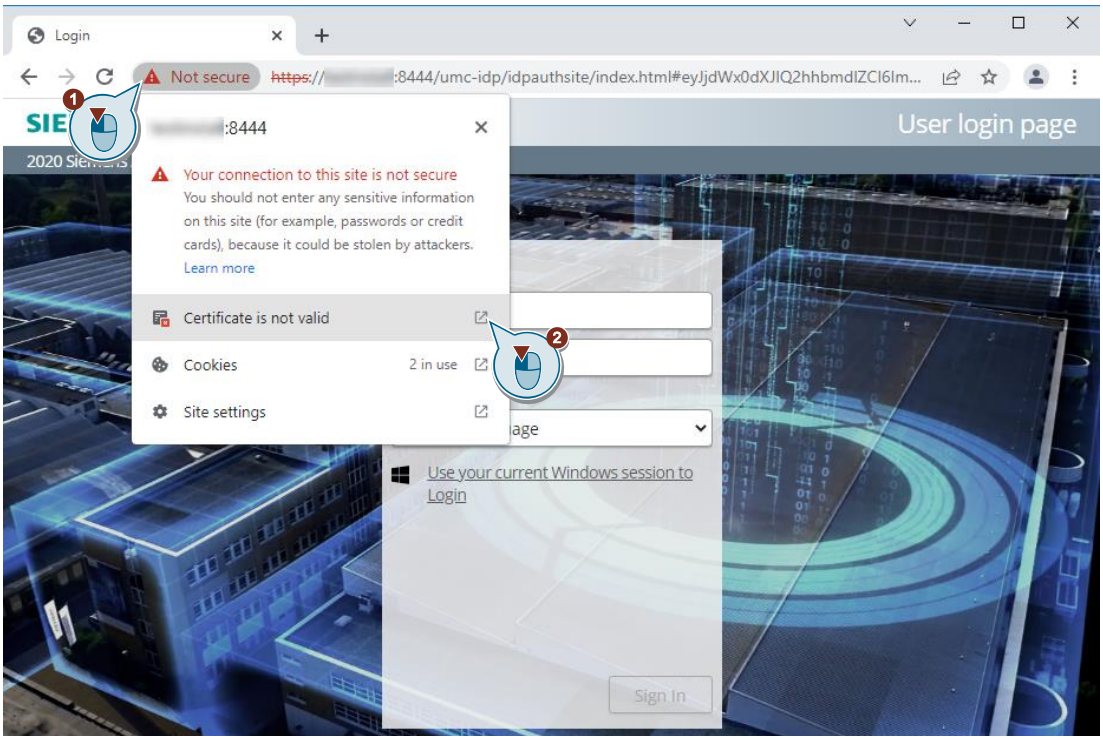
5.4 Installing the SSL certificate on the UMC ring server PC

5.4.1 Export certificate from the web browser

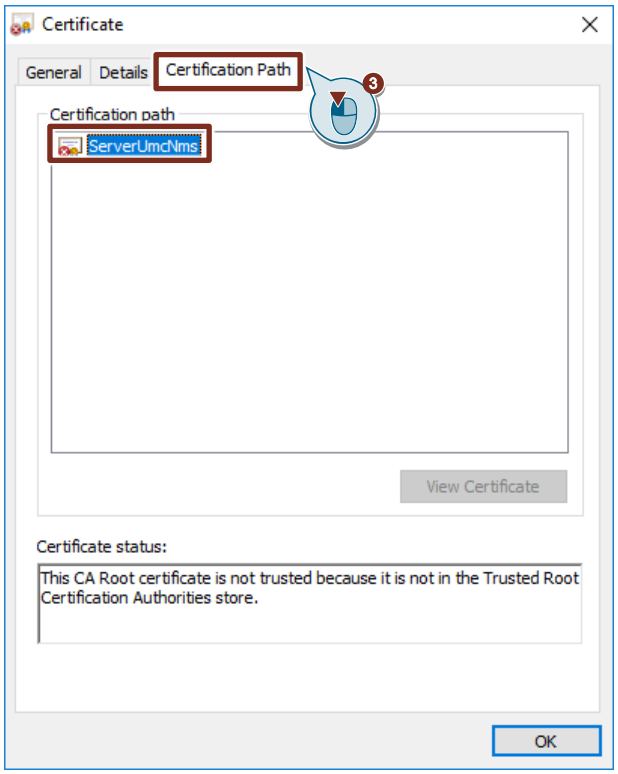
1. On the UMC ring server PC, open the UMC WBM, for example with the following URL:
   https://<IP address> or <PC name>:<Port>/UMC
   The connection is not secure.



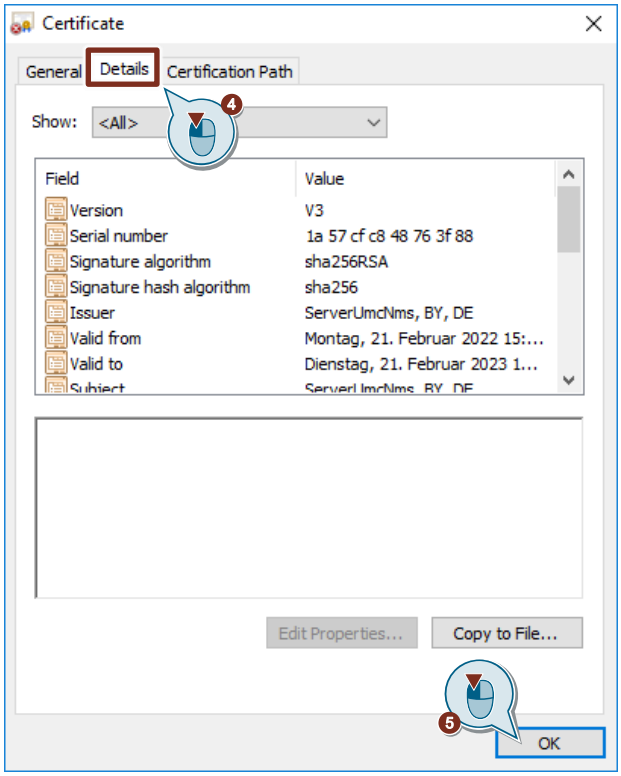
2. In the web browser, open the "Certificate" dialog.



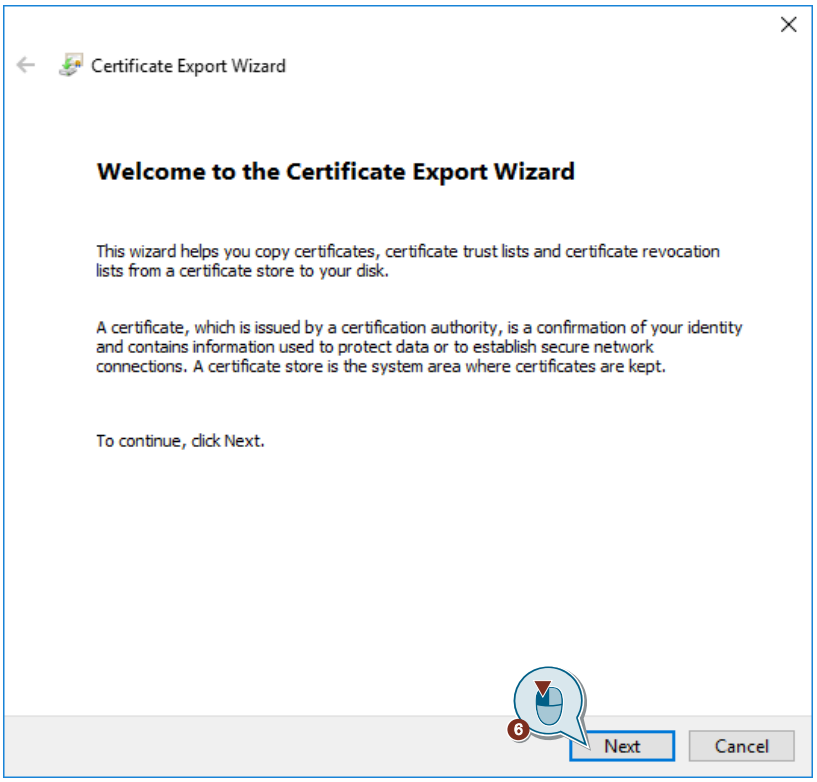
3. Open the "Certification Path" tab and check whether a Root CA certificate is present.



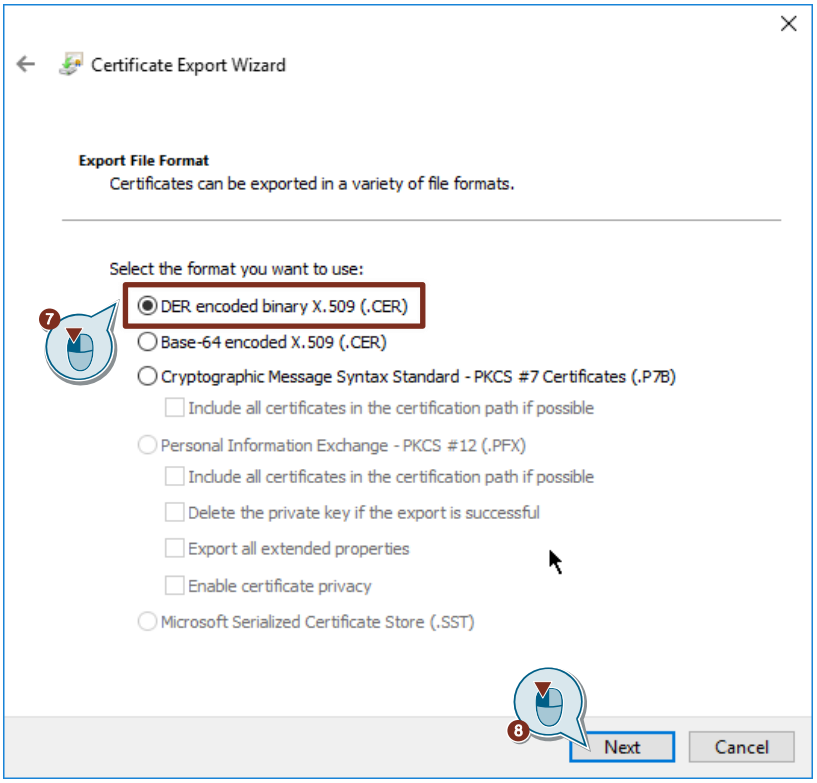
4. Open the "Details" tab.
5. Click the "Copy to File" button.
   The "Certificate Export Wizard" will open.



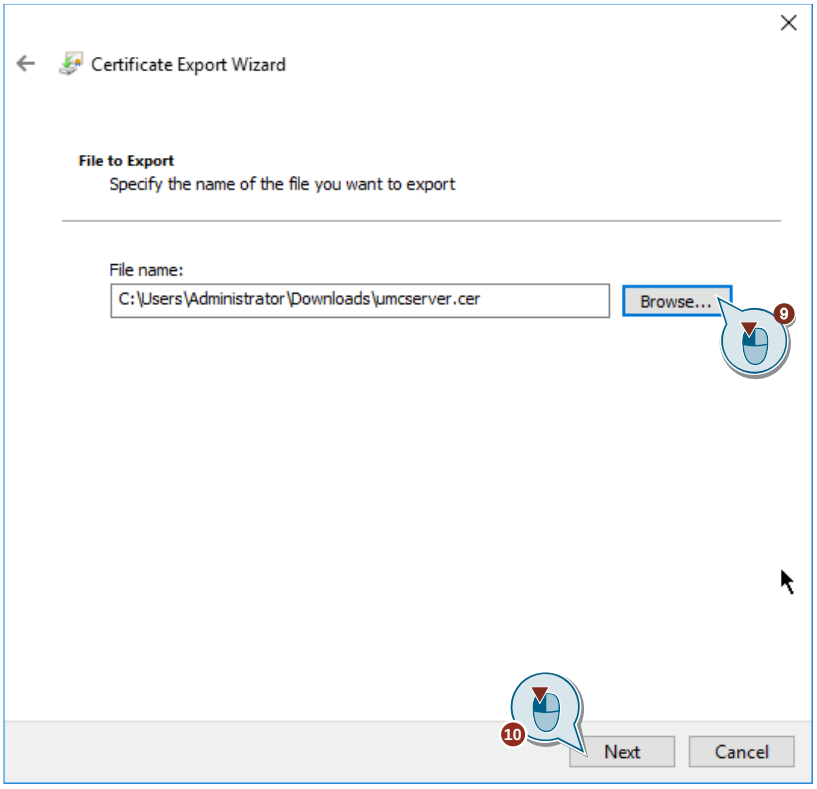
6. Click on "Next".



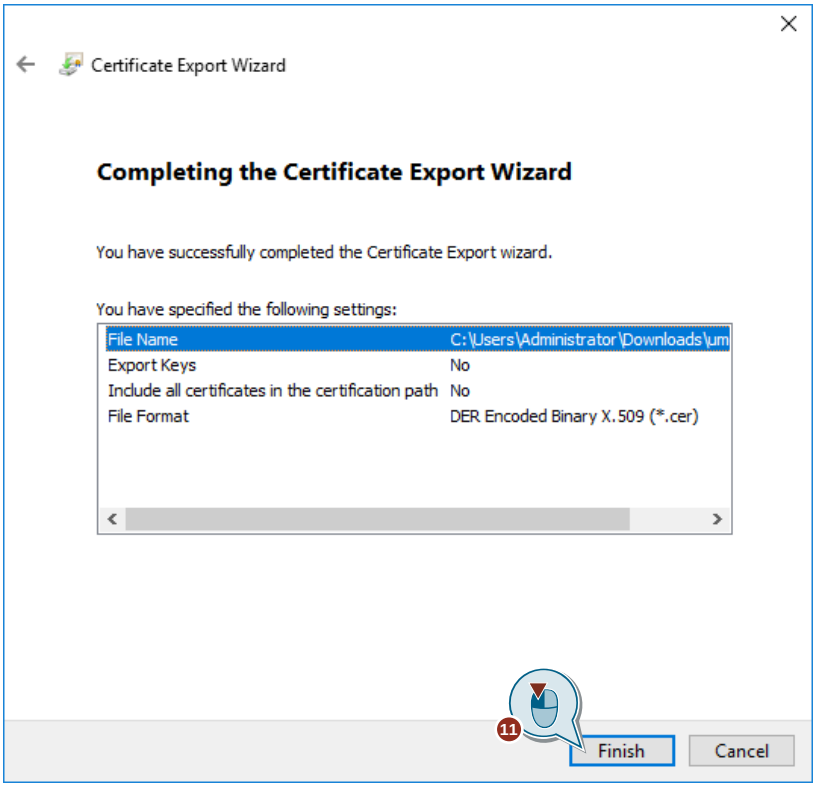
7. Select the export format "DER encoded binary X.509 (.CER)".
8. Click on "Next".



9. Enter the name of the file you wish to export.
10. Click on "Next".

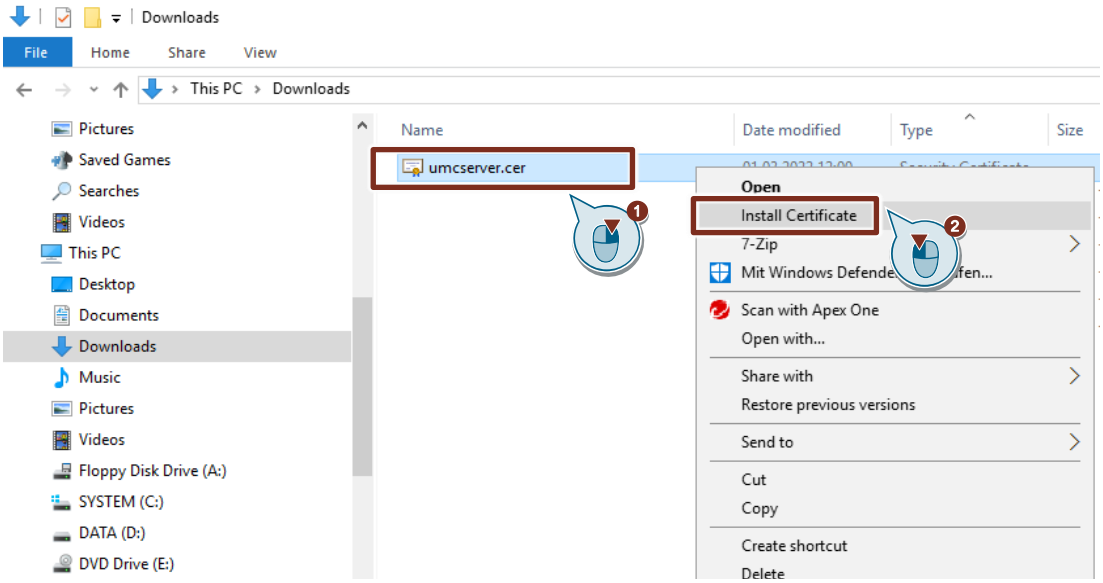


11. Click the "Finish" button to complete the certificate export.

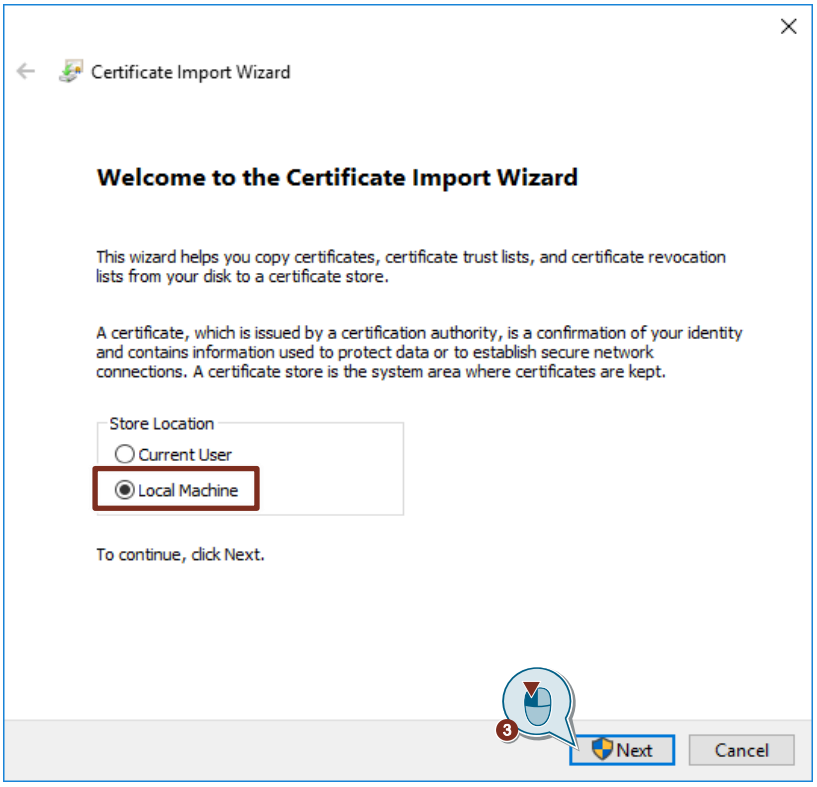


5.4.2 Install certificate on the UMC ring server PC

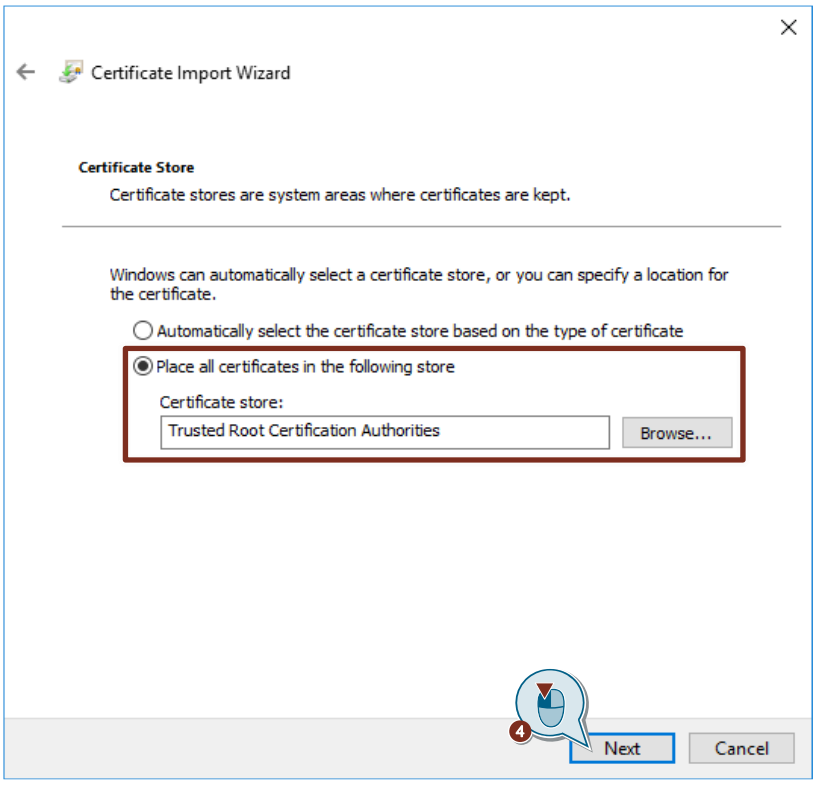
1. Select the exported file in Explorer and right-click the file.
   The context menu opens.
2. Select "Install Certificate" in the context menu.
   The "Certificate Import Wizard" will open.



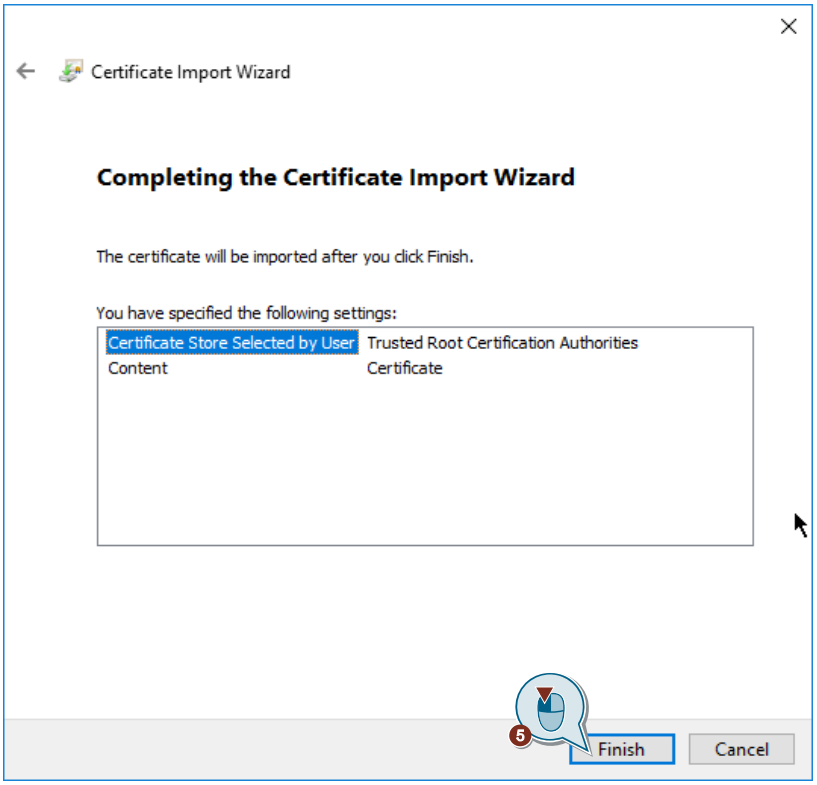
3. Select the save location as "Local Machine" and click "Next".



4. Select the "Trusted Root Certification Authorities" certificate store and click "Next".



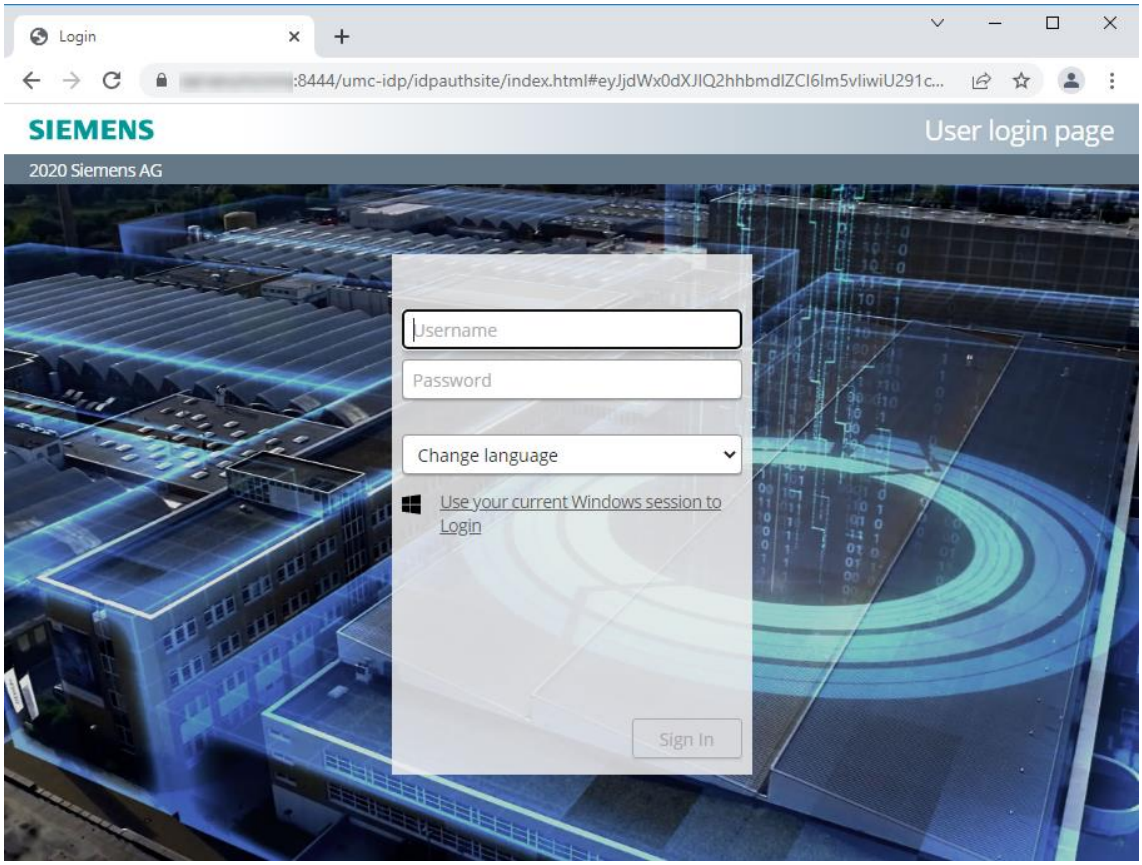
5. Click "Finish" to finish importing the certificate.



Result

The connection to the UMC WBM in the web browser is now secure.

Figure 5-3



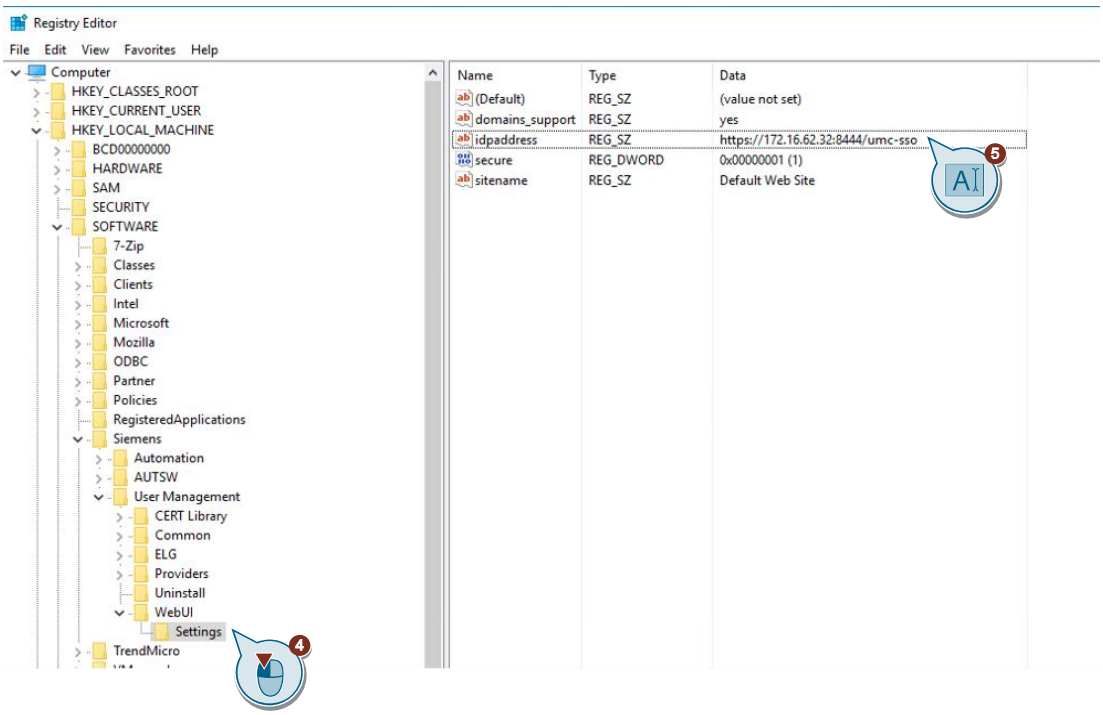
5.5 Single sign-on (SSO) to UMC via IP address instead of host name

Most settings are automatically set up by the installation routine. The following settings are necessary if you use SSO via the IP address to log in to UMC from SINEC NMS/SINEMA RC:

1. Open the "configuration.json" file in a text editor that you have run as an administrator.
   The "configuration.json" file is located in the path "C:\Siemens\UserManagement\Web\umc-sso\config".
2. Enter your IP address with the prefix "https://" for the "reverseProxy" and the port "8444" for the "reverseProxyPort".
   Then save and close the file.

```
{
    "private": {
        "UMCDllFolderPath": "C:/Program
Files/Siemens/UserManagement/bin",
        "useHttps": false,
        "httpsServerKey": "",
        "httpsServerCert": "",
        "configurationInterval": 60000,
        "idpListenerPort": 49133
    },
    "reverseProxy": "https://172.16.62.32",
    "reverseProxyPort": "8444",
    "override": false
}
```

3. Open the registry with <Win + R> and enter "regedit".
   The "Registry Editor" will open.
4. Navigate to the registry key "HKEY_LOCAL_MACHINE\SOFTWARE\Siemens\User Management\WebUI\Settings\".
5. For the parameter "idpaddress", enter the IP address in place of the host name.

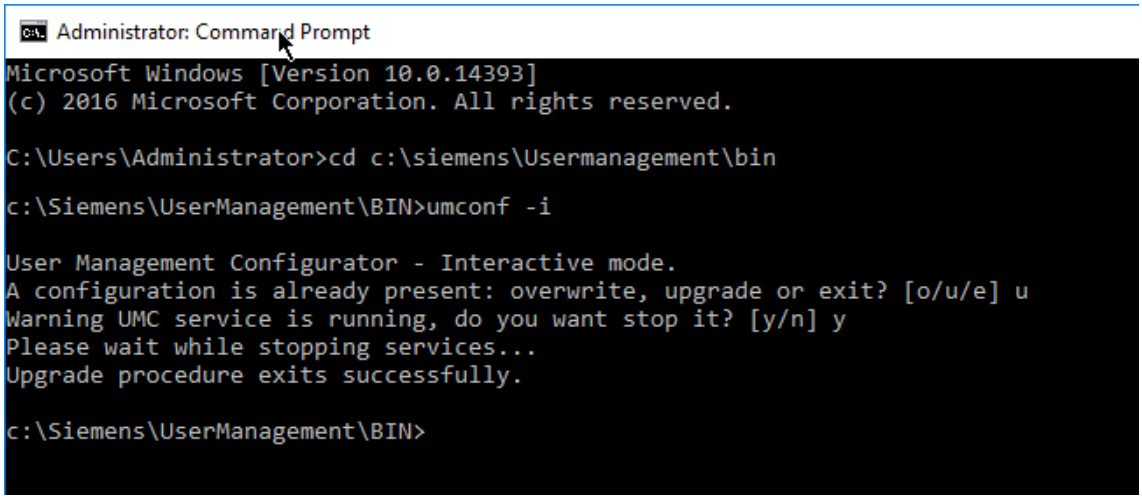


5.6 Changing the PC name

UMC V2.7 has the web SSO screen which can be accessed for UMC via the PC name. The following steps must be carried out so that this link stays current when the PC name is changed:

1. Open the console on your UMC server PC as an administrator.
2. Use the following command to navigate to the UMC installation folder:
   `cd C:\Siemens\UserManagement\BIN`
3. Enter the following command to run the program "umconf.exe" in interactive mode:
   `umconf -i`
4. Update the configuration by entering "u".
5. Enter "y" to stop the UM service "UMCService".

Figure 5-4



The configuration has been updated successfully.

5.7 Downgrading a server to an agent

By default, a UMC is set up as a UMC ring server after installation. To downgrade a ring server to a UMC agent, enter the necessary commands through the console. Refer to chapter 5.8 for the necessary commands.

5.8 Connecting application to the UMC ring server

TIA Portal and WinCC Unified are connected to the UMC ring server of SINEMA NMS / SINEC RC via the console.

Connect TIA Portal to UMC ring server of SINEC NMS / SINEMA RC

1. Open the console on your TIA Portal PC as an administrator.
2. Change the directory with the following command:
   `cd C:\Program Files\SIEMENS\Automation\UserManagement\BIN`
3. Delete the existing configuration with the command below.
   `umconf -D -f`
4. Bind your installation as a UMC agent to the UMC ring server using the following command.
   `umconf -a -f -c [UMC ring server PC name]`
5. Enable secure communication with the following command. Replace "User" and "Password" with the login credentials of a UMC user with "UM_ADMIN" permissions, for example those of UMC administrators.
   `umx -x [User] [Password] -AP -setakp`

TIA Portal is now connected to your existing UMC ring server. Close the console.

Note

Alternatively, it is possible to use the "TIA Administrator" tool to connect TIA Portal to the UMC ring server.

After TIA Portal has been connected to the UMC ring server using the "TIA Administrator" tool, restart the PC or service "UMC secure Communication" to declare the PC as a UMC agent.

Connect WinCC Unified PC to UMC ring server of SINEC NMS / SINEMA RC

Start the Command Prompt (CMD) as admin for the WinCC Unified PC.

1. Open the console on your TIA Portal PC as Administrator.
2. Change the directory with the following command:
   `cd C:\Program Files\SIEMENS\Automation\UserManagement\BIN`
3. Use the following command to delete the existing configuration.
   `umconf -D -f`
4. Bind your installation as a UMC server to the UMC ring server with the following command.
   `umconf -j -f -m 0 -c [UMC ring server PC name]`
5. Enable secure communication with the following command. Replace "User" and "Password" with the login credentials of a UMC user with "UM_ADMIN" permissions, for example those of UMC administrators.
6. Enable desktop single sign-on for WinCC Unified Panels.
   `umconf -dsso enable -f`

WinCC Unified is now connected to your existing UMC ring server. Close the console.

5.9 Password policies in UMC

UMC offers you the ability to adapt your password policies to fit your own company policies.

Figure 5-5

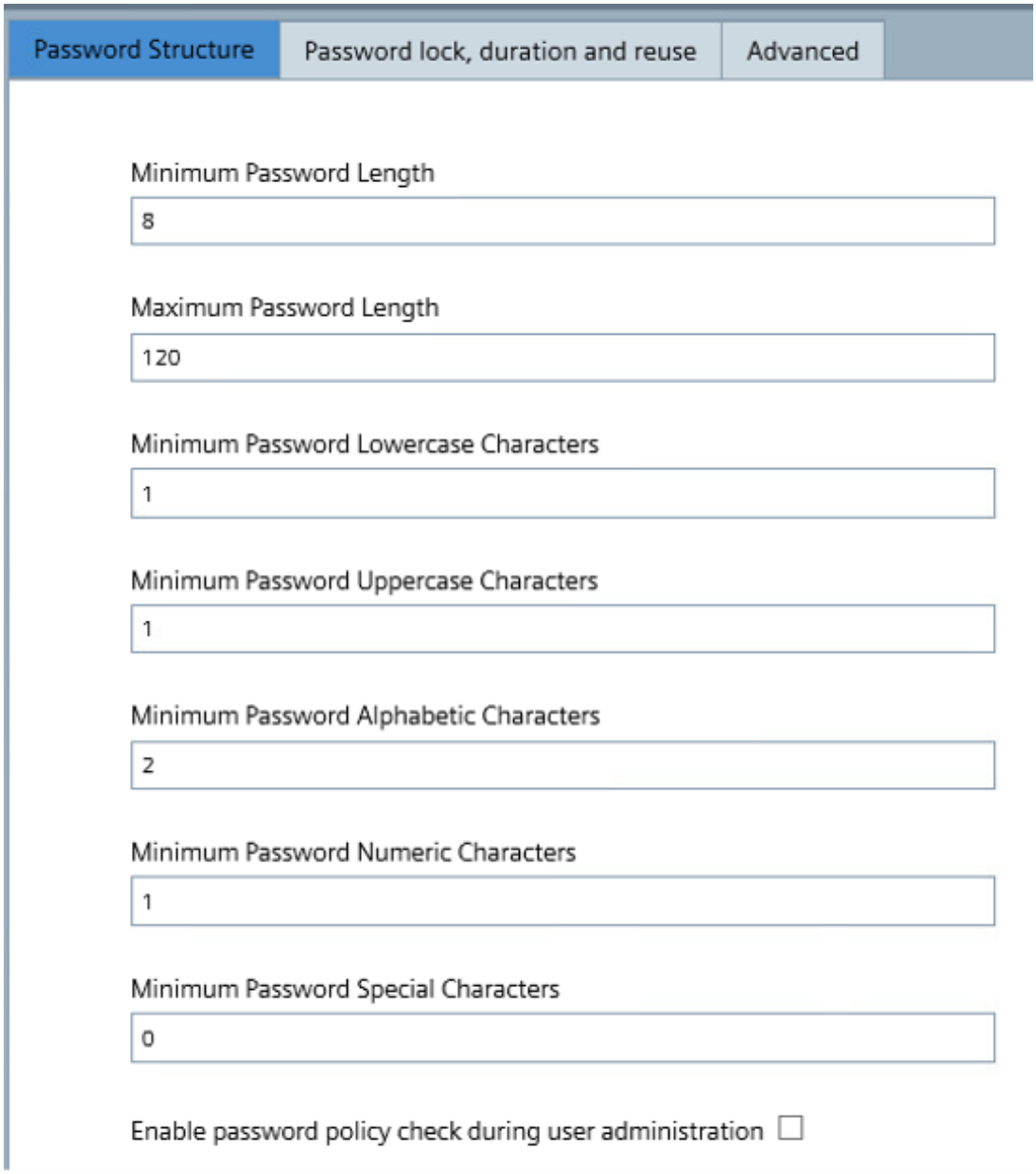
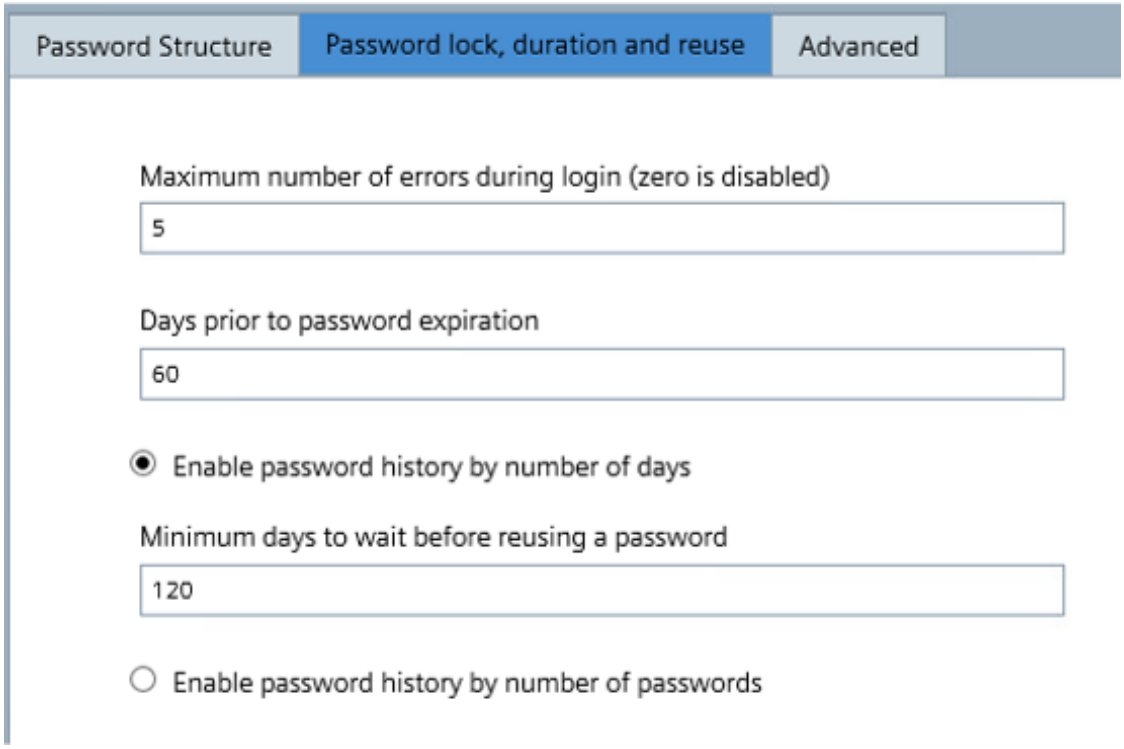


Figure 5-6



Note

The password policies apply to users created in UMC. The password policies do not apply to users managed through the Microsoft Active Directory.

5.10 Troubleshooting

5.10.1 Error when running "UMConf.exe"

If the "UMConf.exe" cannot be executed or is aborted during execution, uninstall UMC.

Note The "UMC_InstallationManual" chapter 7 "How to Uninstall UMC" describes how to uninstall UMC.

After you have successfully uninstalled UMC, reinstall it (see chapter 3.1).

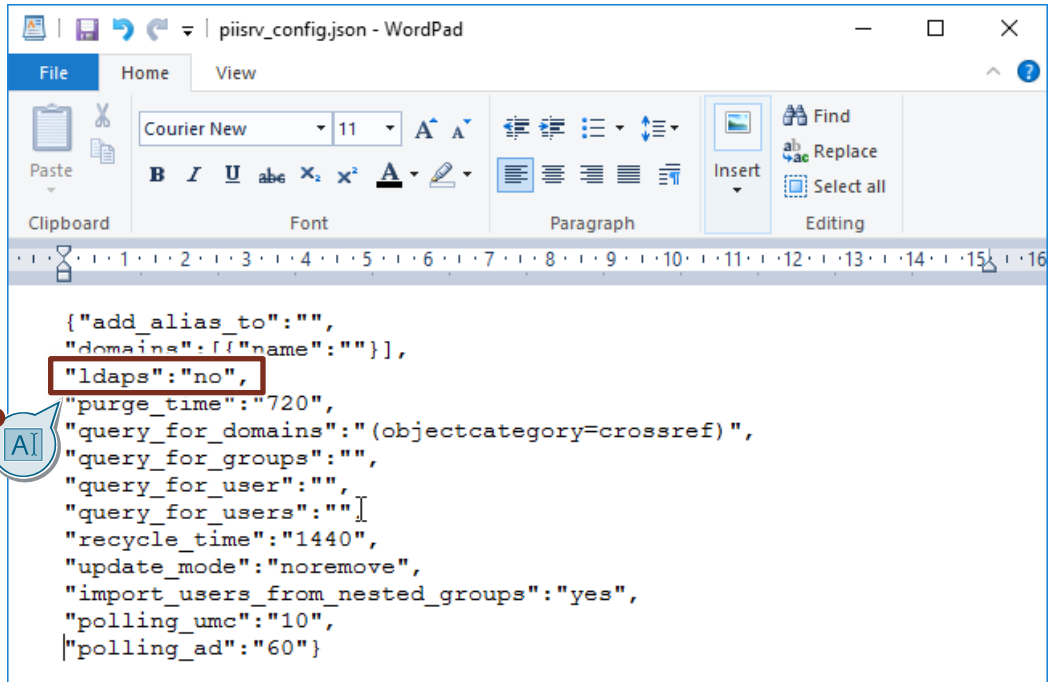
5.10.2 Domain group appears in UMC as "Undefined"

Configure UMC provisioning (AD communication) in LDAP mode

In accordance with the Microsoft update, the default configuration of the UMC provisioning (AD communication) in UMC 2.9 SP3 is configured in LDAPS mode by default.

If the AD is configured in LDAP mode, the communication between AD and UMC ring server does not work and the domain group appears in UMC as "Undefined". Proceed according to the instructions below to modify the configuration of the UMC provisioning in UMC.

1. Open the file "piisrv_config.json" in a text editor that you have run as an administrator. The file "piisrv_config.json" is located in the path "C:\ProgramData\Siemens\UserManagement\Conf".
2. Set the "ldaps" parameter to "no" to configure the UMC provisioning service (AD communication) in UMC in LDAP mode (Lightweight Directory Access Protocol).



Note If the "ldaps" parameter is not present, create it. If the "ldaps" parameter is not present, the default value is "yes".

3. Save the file "piisrv_config.json" and restart the UM service "UPService".
4. If you have several UMC servers or UMC ring servers in operation, repeat the procedure there.

Note

In the "UMC_InstallationManual", in chapter 9 "Appendix", you will find a description of the "piisrv_config.json" file with all possible parameters and values.

Allow ports for AD communication in the firewall

AD communication uses the following ports:

- port 3269 to receive users for groups
- port 636 to receive users

Allow the ports in the Microsoft AD server firewall:

5.10.3 Members of domain groups are not imported into UMC

1. Open the file "piisrv_config.json" in a text editor that you have run as an administrator. The file "piisrv_config.json" is located in the path "C:\ProgramData\Siemens\UserManagement\Conf".
2. Set the parameter "import_users_from_nested_groups" to "yes". This will search for all users in sub-groups of groups to import the users into UMC and assign them to the higher-level group.

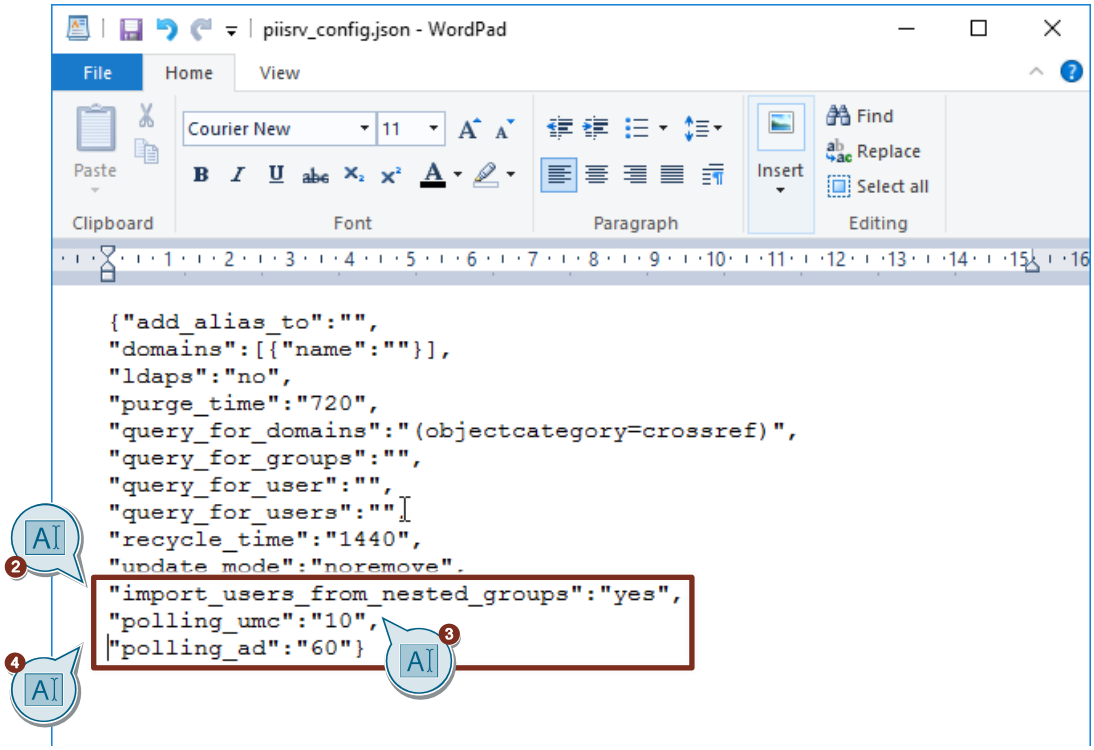
Note If the parameter "import_users_from_nested_groups" does not yet exist, create it. If the parameter "import_users_from_nested_groups" does not exist, the default value is "no".

3. By default, the UMC users are synchronized with each other every 60 seconds. Adjust the parameter "polling_umc" to the desired time span in seconds, e. g. 10 seconds. If the parameter does not yet exist, create it.
4. Data synchronization of the login data and users between the Microsoft Active Directory and the UMC ring server takes place every 600 seconds by default. Adjust the parameter "polling_ad" to the desired time span in seconds, e. g. 60 seconds. If the parameter does not yet exist, create it.

Note Only modify the parameters "polling_umc" and "polling_ad" if absolutely necessary.

5. Save the file "piisrv_config.json" and restart the UM service "UPService".
6. If you have several UMC servers or UMC ring servers in operation, repeat the procedure there.

Figure 5-7



Note

In the "UMC_InstallationManual", in chapter 9 "Appendix", you will find a description of the "piisrv_config.json" file with all possible parameters and values.

6 Appendix

6.1 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

6.2 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

6.3 Links and literature

Table 6-1

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
\3\	FAQ "How does User Management Component (UMC) work with SINEC NMS?" https://support.industry.siemens.com/cs/ww/en/view/109780332

6.4 Change documentation

Table 6-2

Version	Date	Change
V1.0	10/2020	First edition
V2.0	02/2021	Added chapter 3.2.3 and chapter 4.
V2.1	10/2021	Update for UMC V2.9.3 and WinCC Unified
V2.2	04/2022	Additions to chapter 3.2.3 and chapter 5