

The background image shows a man in a light blue shirt looking at a tablet. Overlaid on the image are various digital graphics: a '24/7' icon with a circular arrow, a 'NEWS' icon with a person silhouette, a 'Home' icon, and a network diagram with three nodes. The overall theme is industrial digitalization.

SIEMENS

Ingenuity for life

Connecting WinCC Unified to User Management Component (UMC)

WinCC Unified / 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

Legal information	2
1 Introduction	4
1.1 Overview	4
1.2 Functional description	5
2 Engineering	7
2.1 Hardware setup	7
Requirements	7
2.2 Adjusting settings in the UMC	8
2.3 Configuring the engineering PC with WinCC Unified (TIA Portal)	11
2.3.1 Connecting the engineering PC to the UMC domain	11
Example 12	
2.3.2 Importing the UMC user groups into TIA Portal	15
2.3.3 Adjusting the runtime settings	17
2.3.4 Server ID	19
2.4 Configuring the WinCC Unified PC station	22
2.5 Configuring the Unified Comfort Panel	25
3 Operation	27
3.1 Logging in to the WinCC Unified PC station with a UMC user	27
3.2 Logging in to the Unified Comfort Panel with a UMC user	29
4 Useful information	31
4.1 Installing UMC certificate in WinCC Unified PC station	31
4.2 Adding PC station to the UMC whitelist	40
4.3 Single-station system	43
4.4 UMC service disabled	45
5 Appendix	46
5.1 Service and support	46
5.2 Industry Mall	47
5.3 Links and literature	47
5.4 Change documentation	47

1 Introduction

1.1 Overview

Efficient user administration is an essential part of every security concept. The User Management Component (UMC) user administration enables system-wide central maintenance of users with optional integration of 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 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).

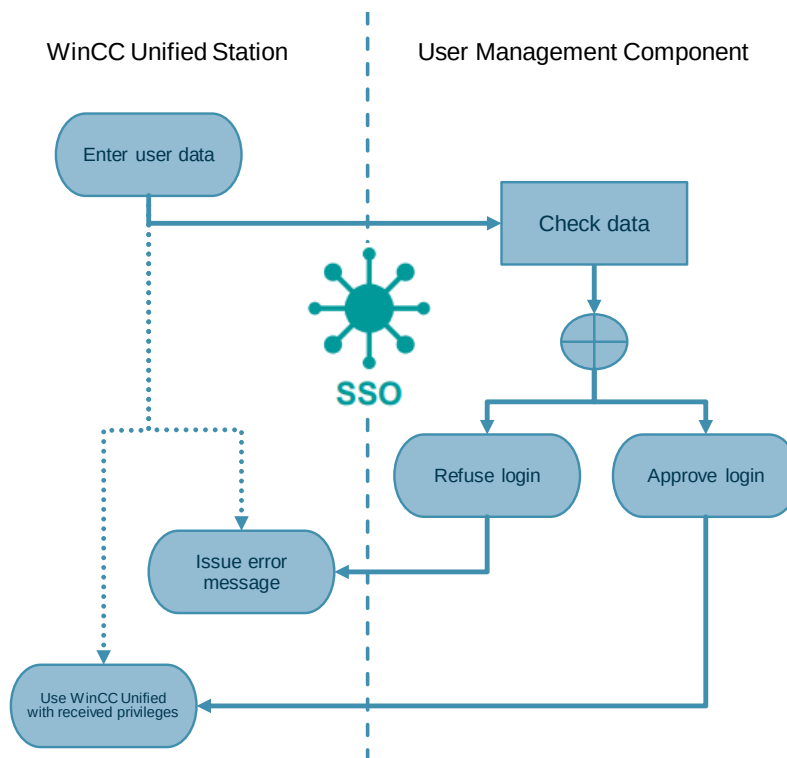
You can import central users and user groups into various applications or use them as temporary users.

This document builds upon the "UMC base document" under the same Item-ID. The "UMC base document" describes the installation and setup of UMC. In this document you will learn how to connect a WinCC Unified PC station or a Unified Comfort Panel to UMC and log in with a UMC user or a user from the Microsoft Active Directory.

1.2 Functional description

The UMC server receives the login requests of the connected applications and checks the credentials that the central user enters. The application then receives a response as to whether the login data are correct, and the login is approved.

Figure 1-1



NOTE

Mixing central and local users is not possible.

Multiple simultaneous sessions per user are possible.

WinCC Unified uses the Single Sign-On (SSO) mechanism for authentication with the UMC server. The Single Sign-On (SSO) login is divided internally into the following components:

- Web Single Sign-On (web SSO)
- Desktop Single Sign-On (desktop SSO)

Due to the web client technology (every client is a web browser), the logon for the WinCC Unified PC station is accomplished via web SSO. For web SSO, the authentication always takes place at the identity provider responsible.

The identity provider is a central access system which users can log on to.

In the context of UMC, the UMC ring server or the UMC server can provide this service as an identity provider, although only one identity provider per UMC domain is permitted to exist.

On the Unified Comfort Panel, due to the panel technology, the user logs on via desktop SSO on the corresponding UMC server. The authentication via desktop SSO can occur on any UMC server type.

NOTE

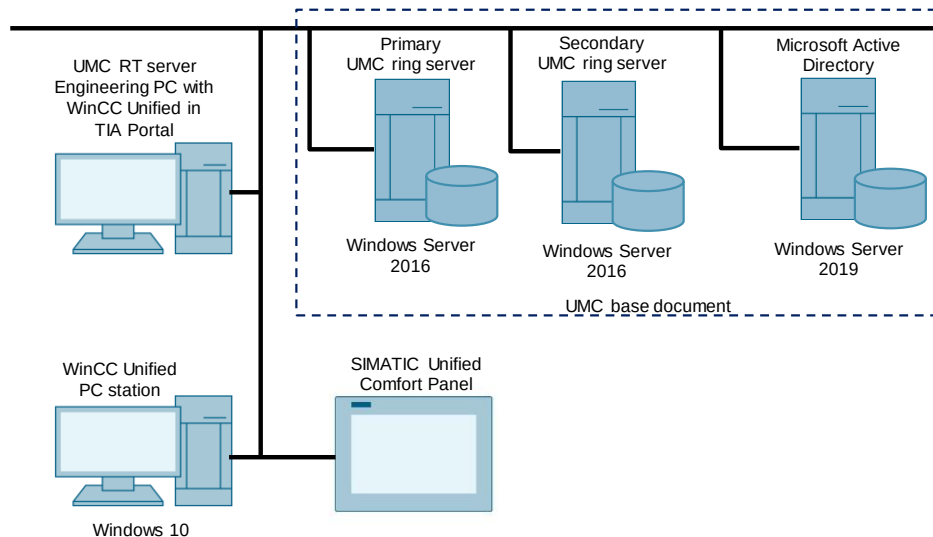
If the user logs on via the web client of the Unified Comfort Panel, then the web SSO mechanism will be used.

2 Engineering

2.1 Hardware setup

The following figure shows the structure of the application example.

Figure 2-1



In this application example, the engineering PC with TIA Portal and WinCC Unified will be added to the existing UMC domain as a UMC RT server. This gives the user the ability to authenticate via the engineering PC either for the WinCC Unified PC station or for the Unified Comfort Panel.

The user can register the WinCC Unified PC station and the Unified Comfort Panel for authentication either on the UMC RT server or on the UMC ring server.

Requirements

This application example builds upon the "UMC base document". Ensure that UMC and (optionally) the Microsoft Active Directory are set up accordingly.

Users and groups

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

Table 2-1

User	Groups
AdminUMC	Administrator (UMC)
MYCORP\John.Doe	Administrator for WinCC Unified, domain user
MaxMuster	Operator for WinCC Unified, UMC user

2.2 Adjusting settings in the UMC

To use a UMC user in WinCC Unified, the user must be a member of a group that is created or imported in UMC, and which is linked with a role in WinCC Unified Engineering.

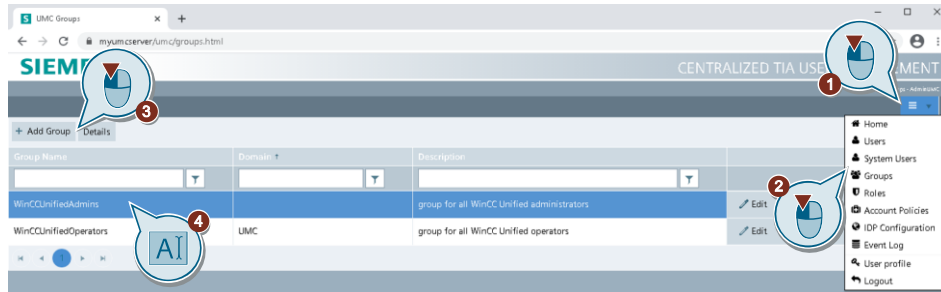
Open UMC Web Based Management (WBM)

1. Open any web browser on the primary UMC ring server. In the web browser, enter one of the following URLs:
 - <https://localhost:<Port>/UMC>
 - <https://<IP address>:<Port>/UMC>
2. Log in with a UMC administrator.



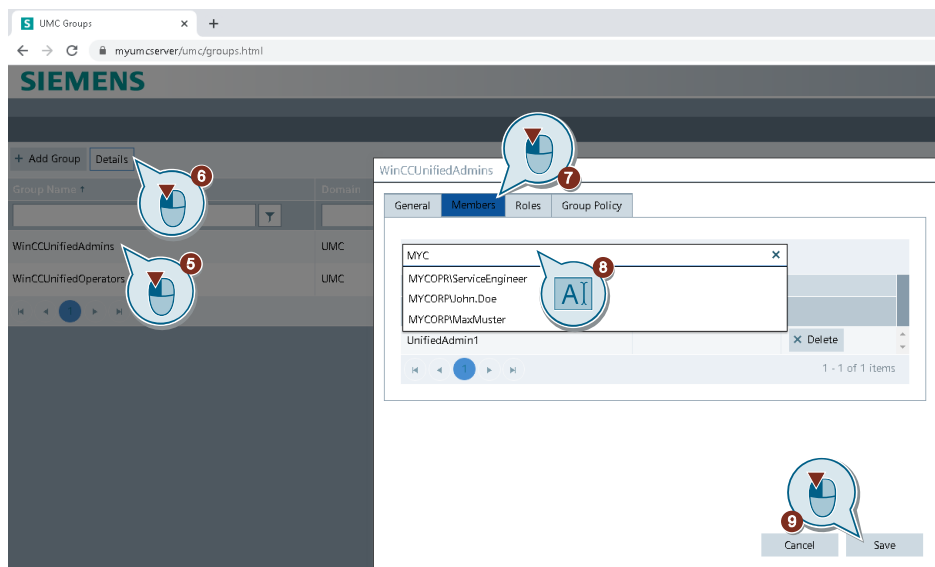
Create a group in UMC

1. Click the menu icon.
2. Open the "Groups" menu.
3. Click "Add Group" to create a new group.
4. Enter a group name, such as "WinCCUnifiedAdmins", and an optional description.



Note To retroactively modify the description of a group, select the desired group and click "Edit".

5. Select the newly created group.
6. Click "Details".
The Details view opens.
7. Open the "Members" tab.
8. Enter the users that need administrative access to the WinCC Unified runtime or Unified Comfort Panel.
9. Save your entries.



10. If you need additional WinCC Unified users who should not receive administrative access (e. g. WinCC Unified operators), then create additional groups and add the desired members to them. You will assign the Unified roles to the respective imported user groups later in TIA Portal. Remember that you will need to activate the users by activating the corresponding checkbox when creating the users.

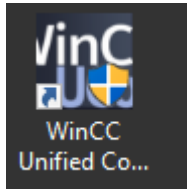
The modifications in the UMC ring server are complete.

2.3 Configuring the engineering PC with WinCC Unified (TIA Portal)

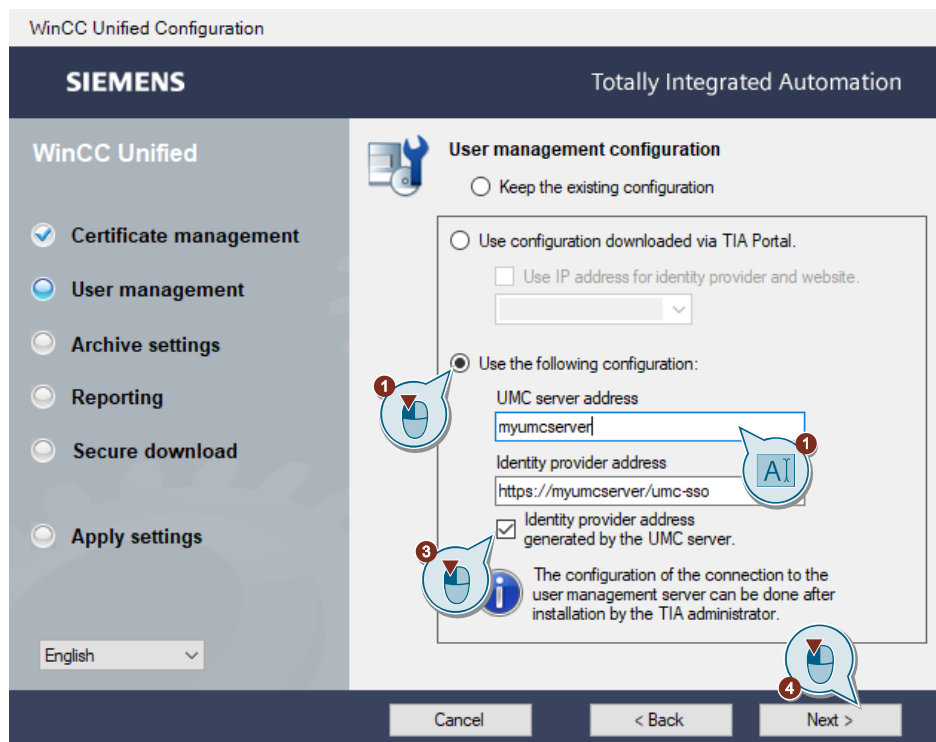
2.3.1 Connecting the engineering PC to the UMC domain

Linking WinCC Unified Engineering in TIA Portal to the UMC ring server is possible with the console. Proceed according to the instructions below:

1. Start the WinCC Unified Configurator on the PC where TIA Portal and WinCC Unified are installed.



2. In the "User Management" category, select the option "Use the following configuration".
3. Enter the PC name of the UMC ring server.
4. Activate the checkbox "Identity provider address generated by the UMC server".
5. Click on "Next".



Note

If TIA Portal is installed on the engineering PC, it will be necessary to select the option "Use the following configuration" so that you can import the UMC users and user groups into TIA Portal from the UMC domain.

If you select the option "Use configuration downloaded via TIA Portal", it will not be possible to import users or user groups from the UMC domain for WinCC Unified projects with centralized user management.

Note

If the option "Use the following configuration" is selected with TIA Portal on the engineering PC, you will only be able to locally simulate WinCC Unified projects with the central user management.

WinCC Unified projects with local user management cannot be simulated.

6. Continue the rest of the configuration steps in the WinCC Unified Configuration Tool and then close the Configurator.
7. Run the console on your TIA Portal PC as an administrator.
8. Change the directory using the following command:
`cd C:\Program Files\SIEMENS\Automation\UserManagement\BIN`
9. Delete the existing configuration using the following command:
`umconf -D -f`
10. Link your installation as UMC server to the UMC ring server.
`umconf -j -f -m [ServerType] -c [UMC Ring Server PC Name] -u [use name having the UM_Join function right] -p [password of user] -v -fp [fingerprint of your UMC domain]`

Note

Server types:

0: UMC server

1: UMC ring server

2: UMC RT server

Note

Use the following command to get the thumbprint of your UMC domain:

`umconf -fingerprint`

Example

```
umconf -j -f -m 2 -c myumcserver -u AdminUMC -p Simatic123! -v -fp
335C1321E110841144B8BBA2DC1054FC580FCE6
```

Note

For detailed information, for example on configuration or downgrading as an agent, refer to the manual "UMC 2.9.3 UMC CONF User Manual" or the "UMC base document".

11. Enable secure communication. You need a user with administrative permissions on the UMC ring server.
`umx -x [UMC admin username] [UMC admin password] -AP -setakp`
12. Close the console.

The engineering PC with WinCC Unified (TIA Portal) is now connected to your existing UMC ring server.

Note

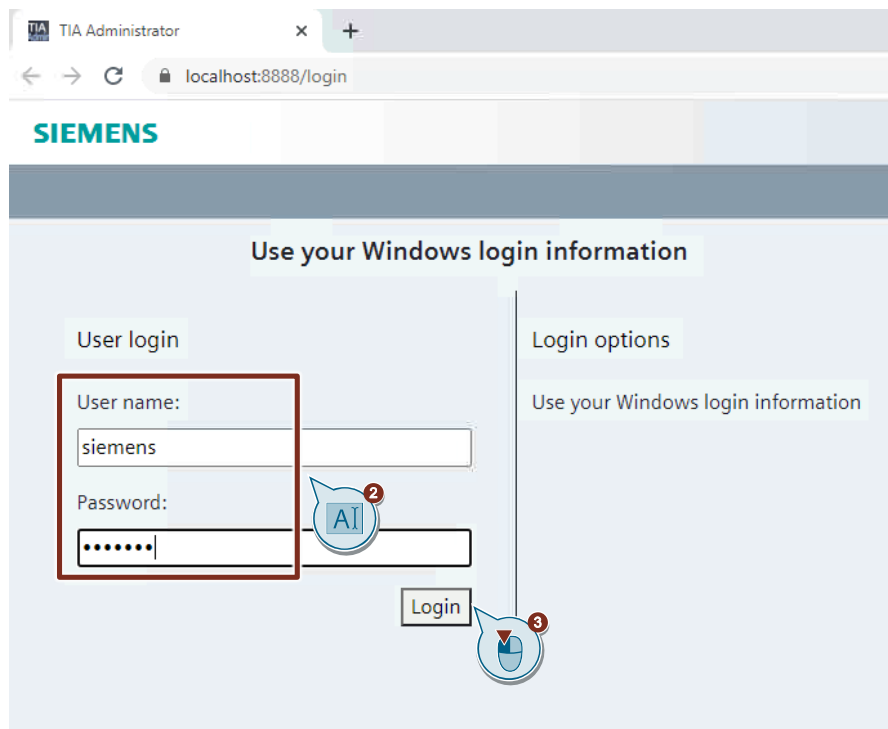
Alternatively, linking the engineering PC as UMC server with the UMC domain can be accomplished with the TIA Administrator Tools.

Alternative

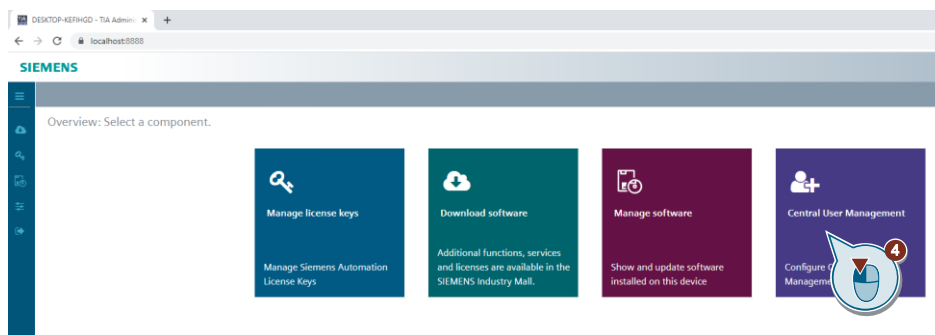
Alternatively, linking the engineering PC as UMC server with the UMC domain can be accomplished with the TIA Administrator Tools.

Proceed according to the instructions below:

1. Start the TIA Administrator Tool.
2. Enter the username and password of a local Windows user.
3. Click the "Login" button.



4. Select the "Central User Management" component



5. Select the "Agent" or "Server" mode.
6. Specify the server address, e. g. enter the name of the UMC ring server (domain server).
7. Click the "Validate" button.

8. Click the "Approve" button to acknowledge the server ID.

9. Enter the username and password of an UMC user (UMC user with UMC_Join privilege).
10. Click the "Connect" button.

The engineering PC has been successfully added as a UMC server.

Note

The TIA Administrator Tool always creates a UMC RT server.

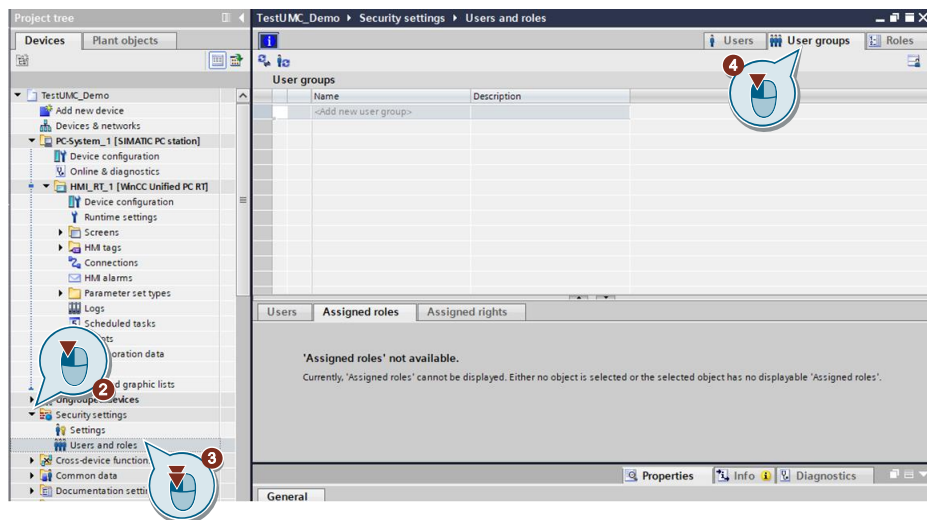
2.3.2 Importing the UMC user groups into TIA Portal

The WinCC Unified-specific privileges for accessing WinCC Unified are assigned with the user groups.

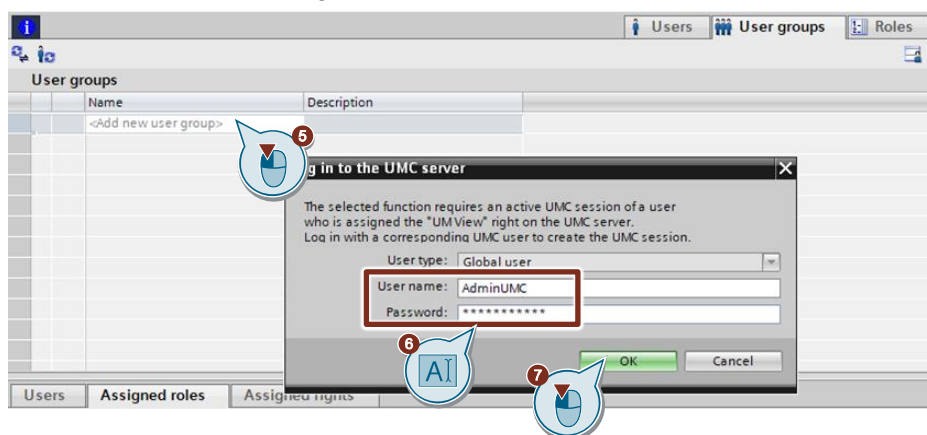
The user groups have been created in the central user administration (UMC) and are linked in TIA Portal with the corresponding WinCC Unified role.

Import the UMC user groups as follows:

1. Start TIA Portal and create a project with a WinCC Unified PC station or a Unified Comfort Panel.
2. Navigate to "Security settings" in the project tree.
3. Double-click on "Users and roles".
4. Open the "User groups" tab in the workspace area.



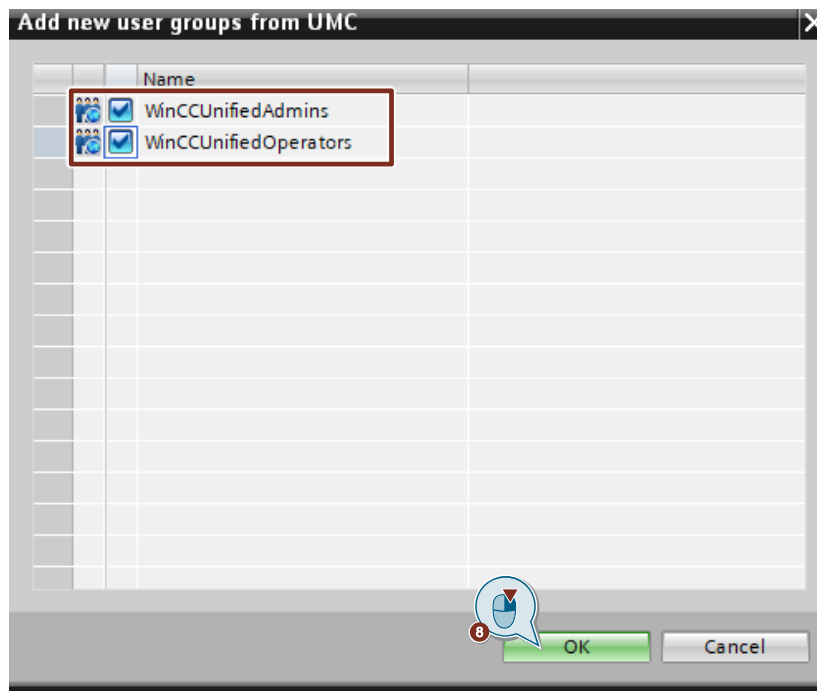
5. Add a new user group.
6. Enter the username and password of a user who has the UMC privilege "UM View".
7. Click the "OK" button to log on to the UMC server.



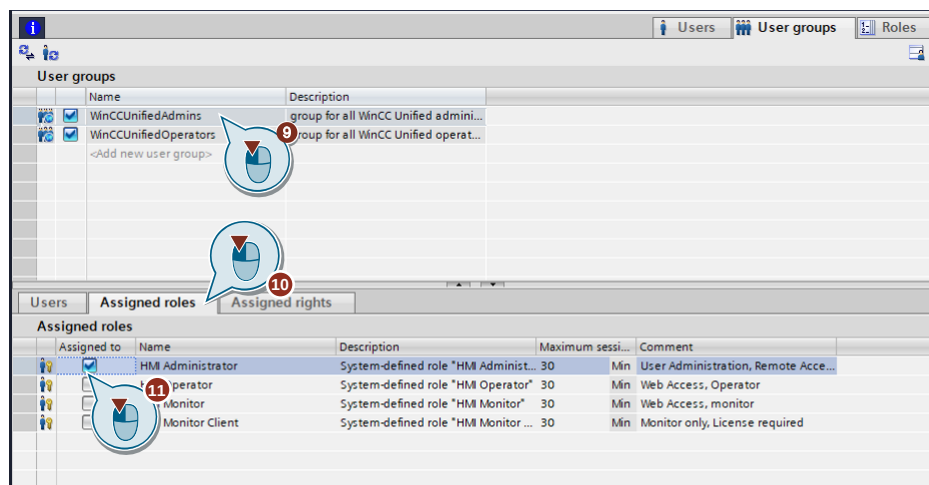
Note

For detailed information on the UMC privileges, refer to the manual "UMC Web UI User Manual", chapter 1.5.

8. Select the UMC user groups.



9. Select the user group to link it with a WinCC Unified role or an HMI role.
 10. Open the "Assigned roles" tab.
 11. Activate the WinCC Unified role or the HMI role to be assigned to the user group.



Note WinCC Unified privileges for individual screen elements are linked with the role beforehand.

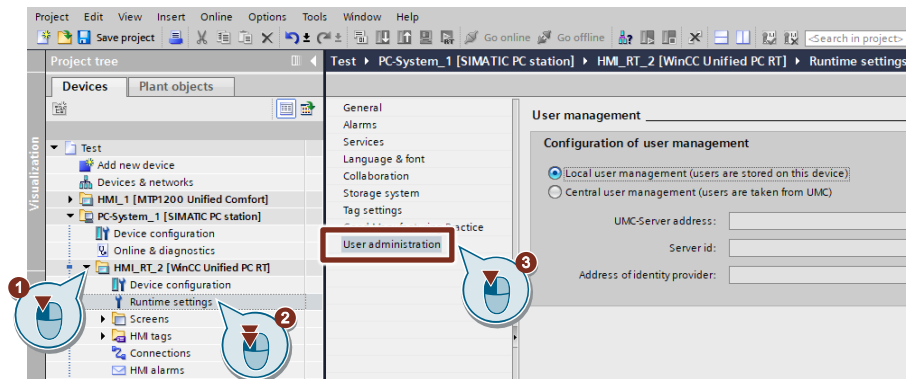
12. Repeat the step for all necessary user groups.

2.3.3 Adjusting the runtime settings

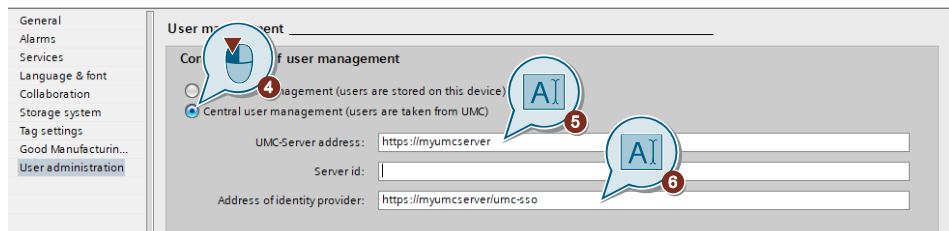
In the WinCC Unified project, use the runtime settings for the WinCC Unified PC station and the Unified Comfort Panel to select whether the local or central user management will be used.

Make the following settings in the "Runtime settings" of the WinCC Unified PC station and Unified Comfort Panel.

1. Navigate to the device folder of the WinCC Unified PC station or Unified Comfort Panel in the project tree.
2. Double-click on "Runtime settings".
3. Navigate to the "User administration" category.



4. Enable the central user administration.
5. Enter the address of the UMC server (desktop SSO).
6. Enter the address of the identity provider (web SSO).



Note

In a distributed UMC domain with UMC ring server and multiple UMC servers or UMC RT servers, you can decide which server of the UMC domains should be used for user authentication of the WinCC Unified PC station or Unified Comfort Panel.

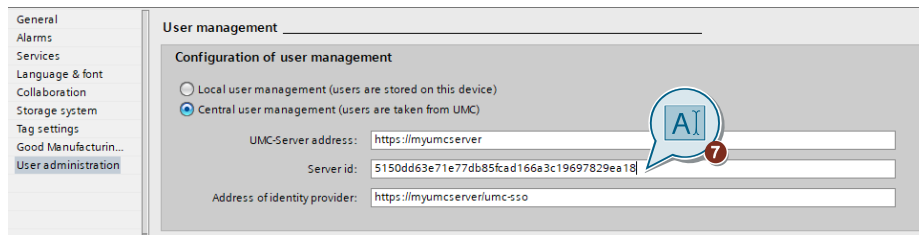
Use the following parameters to specify the authentication site via desktop SSO (desktop single sign-on) for the Unified Comfort Panel.

- Address of the UMC server
- Server ID

The UMC server can also be reached via a static IP address if no name resolution is configured.

You will use the address of the central identity provider to specify the authentication site via web SSO (web single sign-on) for the WinCC Unified PC station.

7. Enter the server ID ("Server id").



The screenshot shows the 'User management' configuration window. On the left is a sidebar with menu items: General, Alarms, Services, Language & font, Collaboration, Storage system, Tag settings, Good Manufacturin..., and User administration (which is highlighted). The main area is titled 'User management' and contains a 'Configuration of user management' section. This section has two radio buttons: 'Local user management (users are stored on this device)' and 'Central user management (users are taken from UMC)'. The 'Central user management' option is selected. Below the radio buttons are three text input fields: 'UMC-Server address' with the value 'https://myumcserver', 'Server id' with the value '5150dd63e71e77db85fcad166a3c19697829ea18', and 'Address of identity provider' with the value 'https://myumcserver/umc-ss'. A blue callout bubble with a red circle containing the number '7' points to the 'Server id' field.

Note

The server ID is the thumbprint from the web certificate used by the web server on which the UMC server or UMC ring server is installed (see chapter [2.3.4](#)).

The configuration of the WinCC Unified project is complete. Load the configuration to the WinCC Unified PC station or the Unified Comfort Panel.

2.3.4 Server ID

The WinCC Unified PC station or the Unified Comfort Panel communicate via an encrypted https connection with the UMC server to check the authentication.

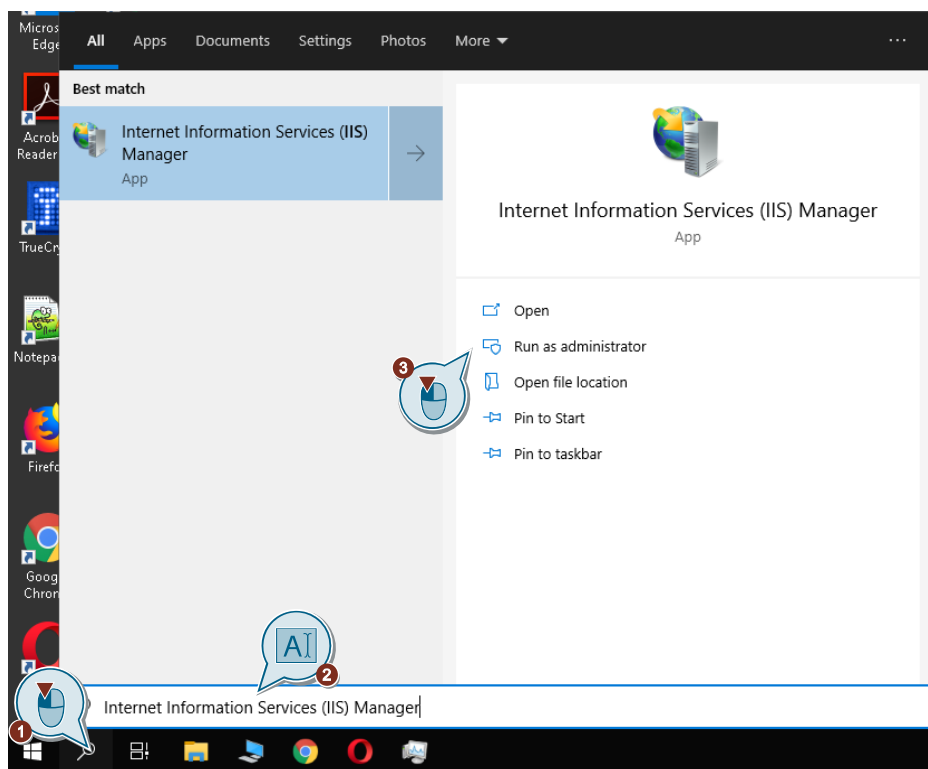
The server ID is the thumbprint of the web certificate (https) on which the UMC server is installed.

Note

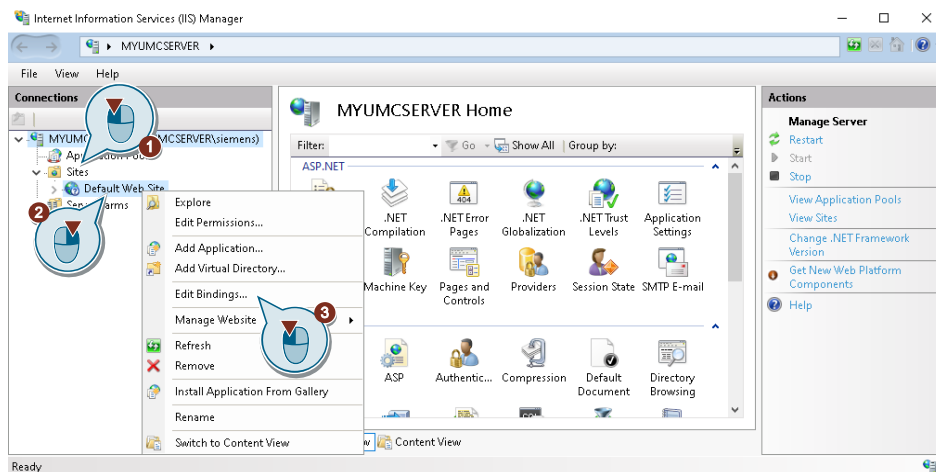
In a distributed UMC domain with UMC ring server and multiple UMC servers and UMC RT servers, you can decide which server of the UMC domains should be used for user authentication of the WinCC Unified PC station and Unified Comfort Panel.

Find the server ID and the thumbprint of the web certificate by following the instructions below:

1. Open the Internet Information Services (IIS) Manager on the PC that the WinCC Unified PC station or Unified Comfort Panel needs to connect to for authentication.



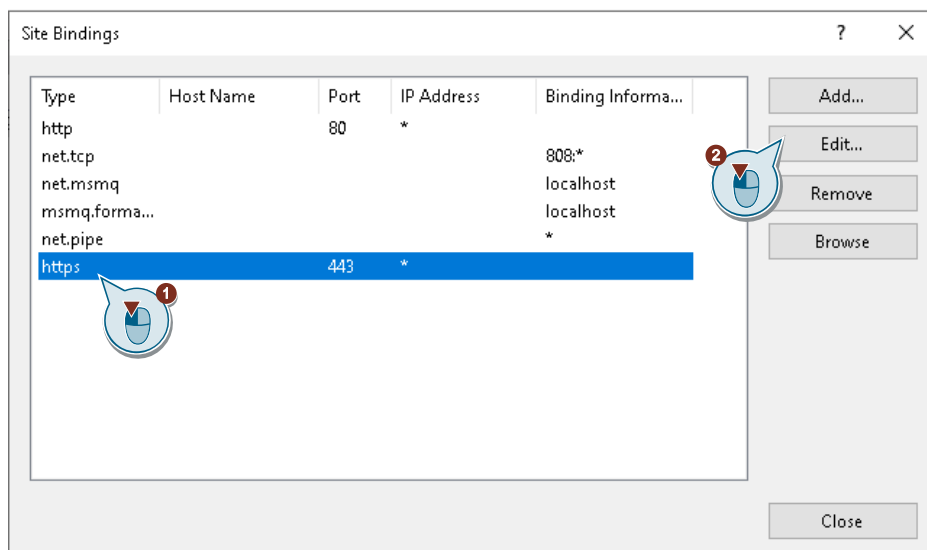
2. Edit the bindings for the default website in the IIS.



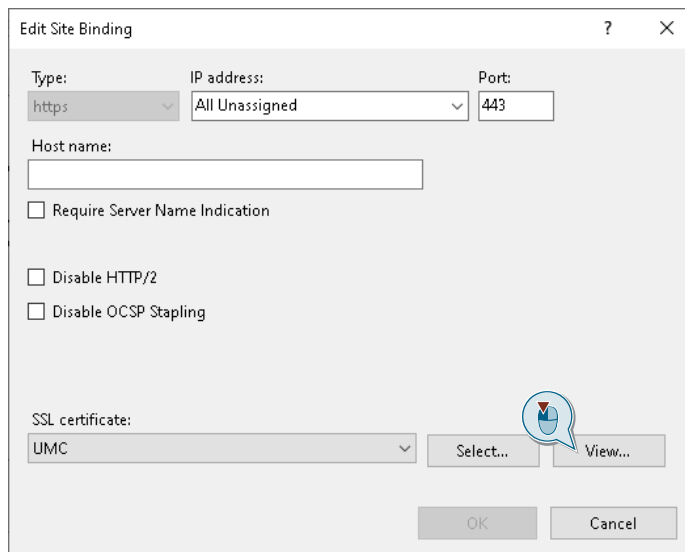
Note

If WinCC Unified is already installed on the same PC (single-station system), select the website "WinCC Unified SCADA" as the website.

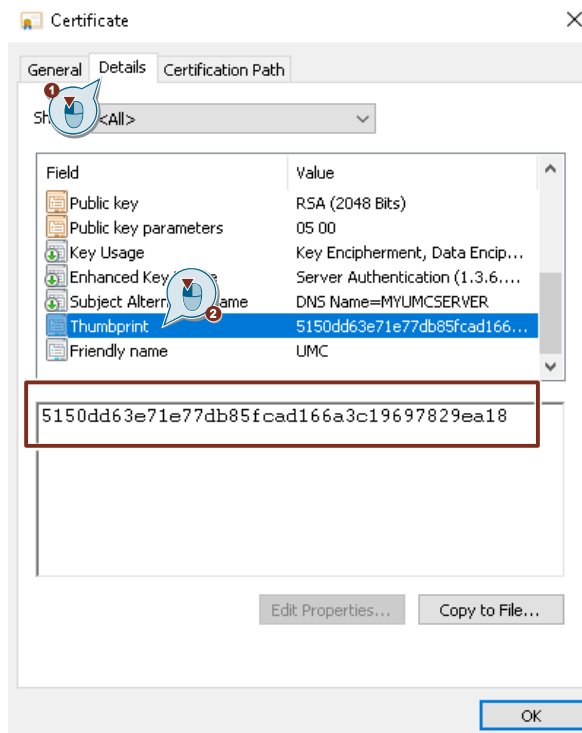
3. Edit the binding for the type "https".



4. Open the stored SSL certificate.



5. Open the details of the SSL certificate and select the "Thumbprint" attribute.



6. Copy the thumbprint of the certificate and paste the thumbprint to the "Runtime settings" of the WinCC Unified PC station.

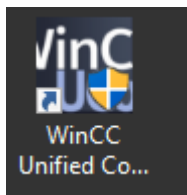
2.4 Configuring the WinCC Unified PC station

The WinCC Unified PC station logs on to the UMC server via the single sign-on (SSO) mechanism for identity verification. The UMC server receives the logon request from the WinCC Unified runtime and checks the data entered by the user. The application then receives a response as to whether the login data are correct, and the WinCC Unified runtime is approved.

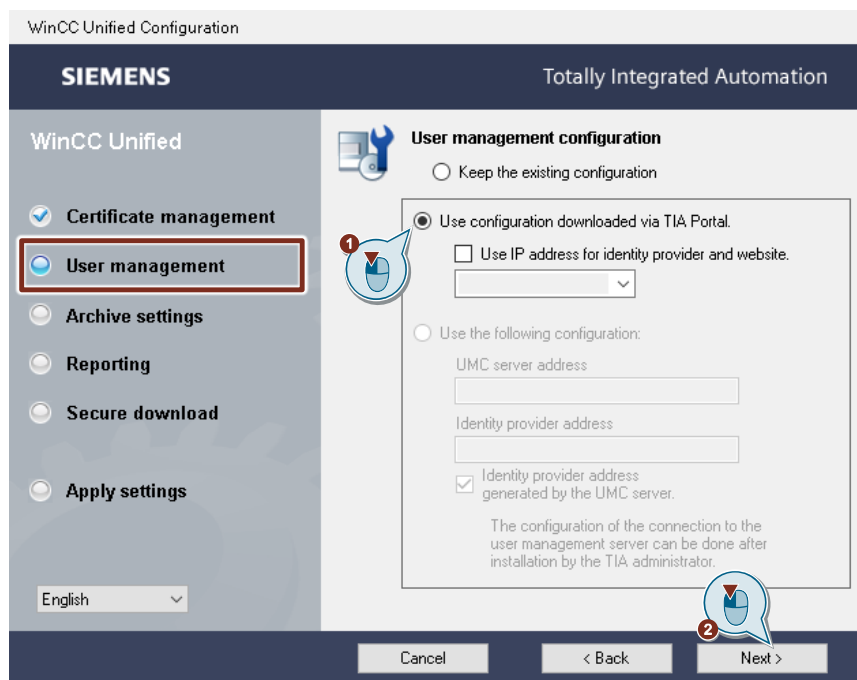
You do **not** need a separate UMC installation on the WinCC Unified PC station.

Configure the WinCC Unified PC station according to the instructions below.

1. Start the WinCC Unified Configuration Tool on the PC station.



2. In the "User Management" category, select the option "Use configuration downloaded via TIA Portal".

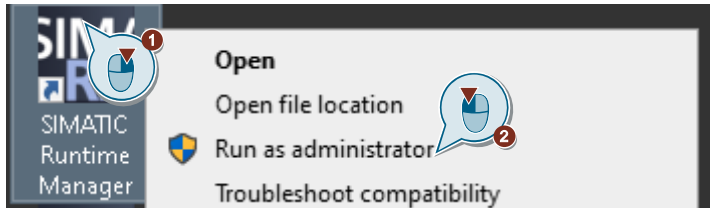


Note

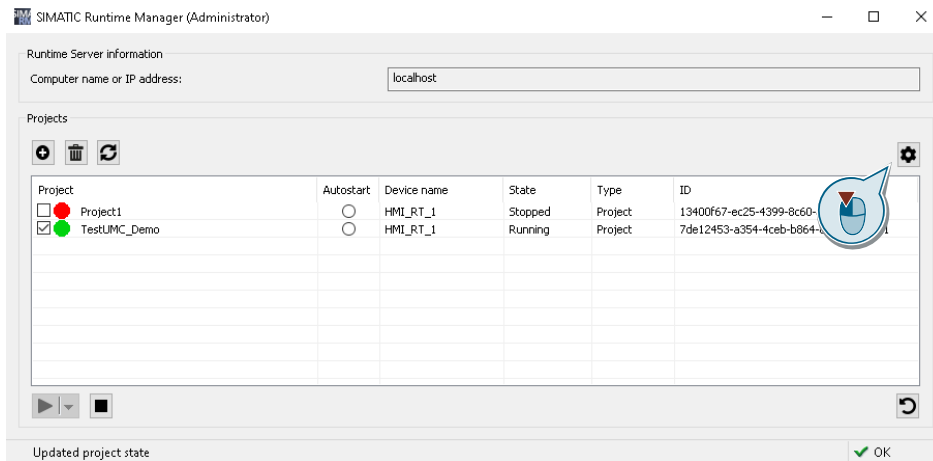
The address of the UMC server and of the identity provider will be downloaded from the TIA Portal project.

If the UMC server cannot be reached under the PC name (name resolution, e. g. per DNS), it is possible to add the static IP address of the UMC server.

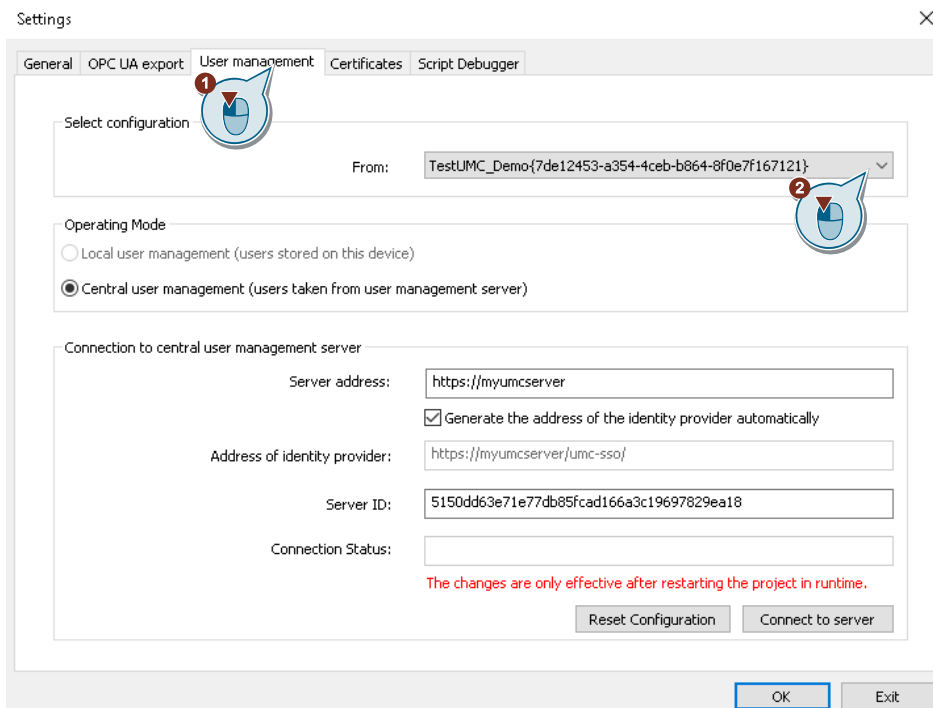
3. Continue the rest of the configuration steps and apply the settings from the WinCC Unified Configuration Tool.
4. If you have not yet downloaded the WinCC Unified PC station configuration from the engineering PC to the WinCC Unified runtime, then start the download via TIA Portal. To apply the configurations from the project to the WinCC Unified runtime, it is necessary to uncheck the corresponding checkbox for the user administration in the download dialog.
5. On the WinCC Unified PC station, start the SIMATIC Runtime Manager as an administrator.



6. Open the SIMATIC Runtime Manager settings.



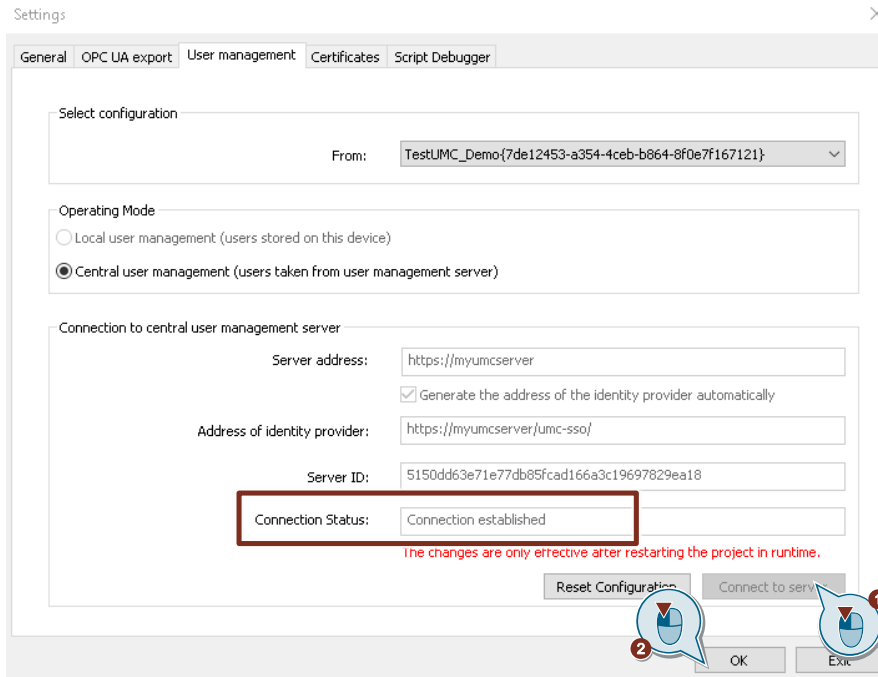
7. Switch to the "User Management" tab and select the project that you loaded before as a configuration.



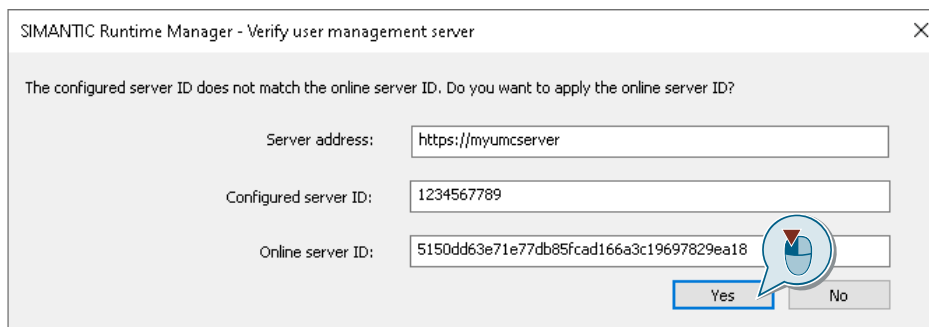
NOTE

The SIMATIC Runtime Manager will show your configured settings for the user administration that you configured in the TIA Portal "Runtime settings" (see chapter [2.3.3](#)).

8. Test the connection to the UMC server once and confirm with "OK".



9. If the configured server ID does not match the online server ID, the following dialog will appear.

**CAUTION**

For security reasons, check the online server ID against the actual server ID (certificate thumbprint, see chapter [2.3.4](#)) before you apply the online server ID.

10. Close the settings and restart the WinCC Unified runtime.
11. Close the SIMATIC Runtime Manager.
12. The configuration of the WinCC Unified PC station is complete.

2.5 Configuring the Unified Comfort Panel

The Unified Comfort Panel logs on to the UMC server via the single sign-on (SSO) mechanism for identity verification. The UMC server receives the logon request from the Unified Comfort Panel and checks the data entered by the user. The application then receives a response as to whether the login data are correct.

You can configure the central user management via the Control Panel on the Unified Comfort Panel.

Requirements

The configuration has been successfully loaded to the panel as described in chapter [2.3](#).

Proceed as follows for the configuration on the Unified Comfort Panel.

1. Open the Control Panel on the Unified Comfort Panel.
2. Open the "UMAC settings" in the "Security" category.



3. Check the configuration of the central user management and verify the connection to the UMC server.

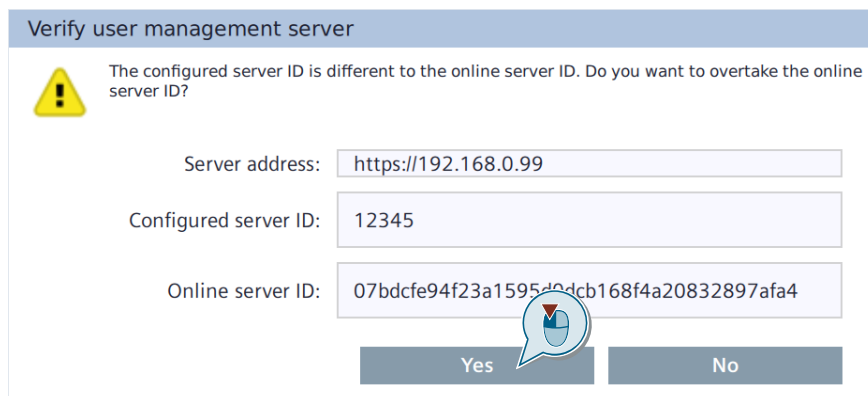


Note

The setting for whether to use the local or central user management is defined in the TIA Portal project in the "Runtime settings" for the Unified Comfort Panel.

In this dialog, you can still modify the settings pertaining to the central user management if necessary.

4. If the configured server ID does not match the online server ID, then the following dialog will appear.



CAUTION

For security reasons, check the online server ID against the actual server ID (certificate thumbprint, see chapter [2.3.4](#)) before you apply the online server ID.

This completes the configuration of the Unified Comfort Panel.

3 Operation

3.1 Logging in to the WinCC Unified PC station with a UMC user

Requirements

The engineering steps have been carried out successfully as described in chapter [2](#).

UMC users or users from the Windows Active Directory have already been created in the UMC domain or imported to it (see "UMC base document", chapter 4).

Procedure

1. Open the WinCC Unified runtime in a web browser.

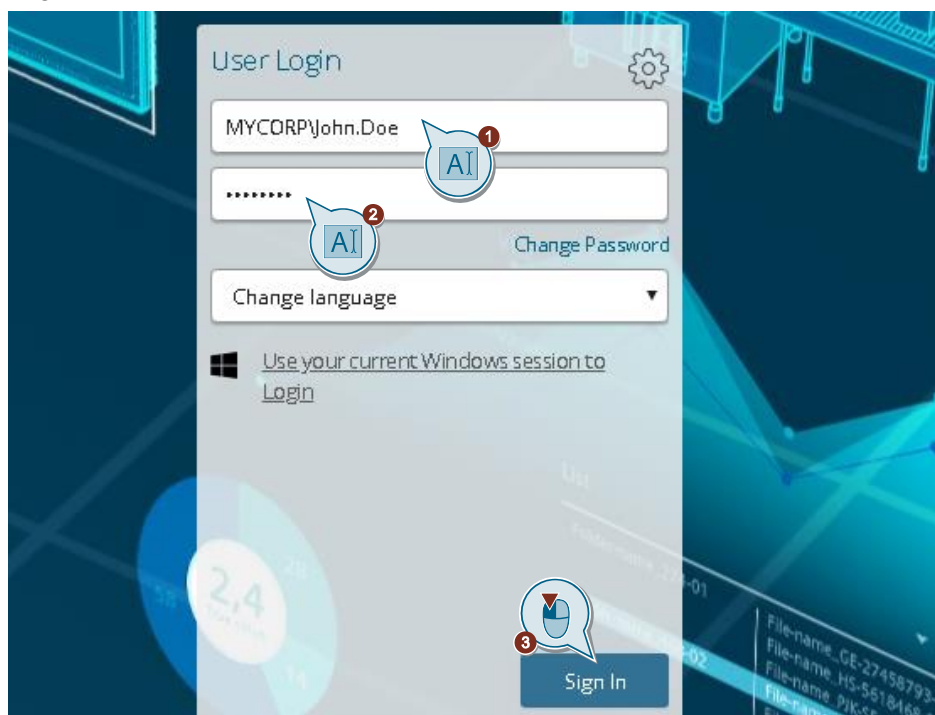


NOTE

When opening the WinCC Unified runtime, the error "SwacLogin is unavailable" may occur and the login dialog might not appear.

Proceed as described in chapter [4.1](#).

2. Log in with the UMC user or Windows domain user.

**Note**

If the error message "The validation of the parameter 'service' failed" appears during login, follow the steps described in chapter [4.2](#).

3.2 Logging in to the Unified Comfort Panel with a UMC user

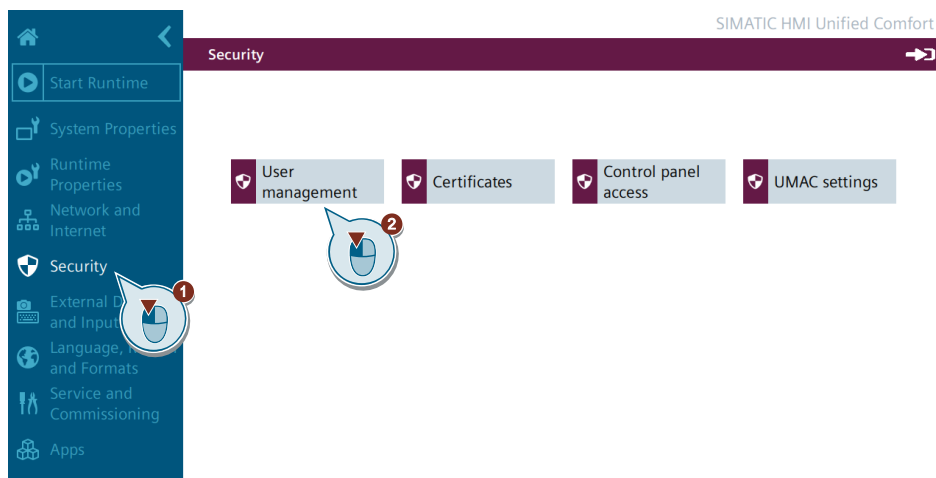
Requirements

The engineering steps have been carried out successfully as described in the previous chapter.

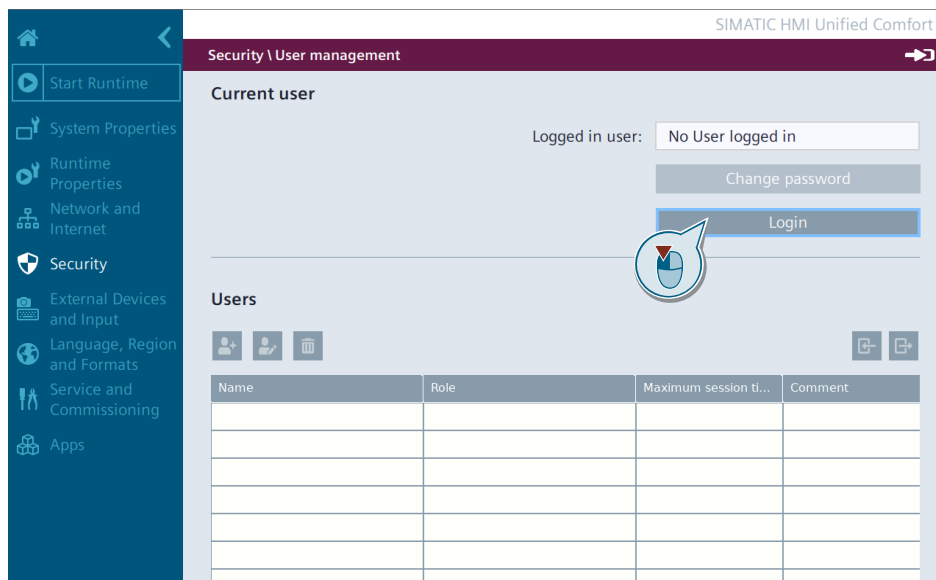
UMC users or users from the Windows Active Directory have already been created in the UMC domain or imported to it (see "UMC base document", chapter 4).

Procedure

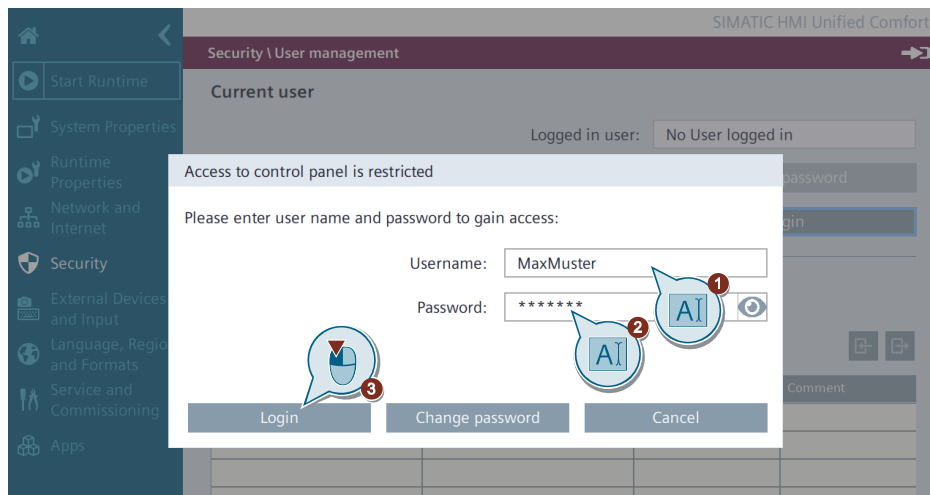
1. Open the Control Panel on the Unified Comfort Panel and open the "User management" in the "Security" category.



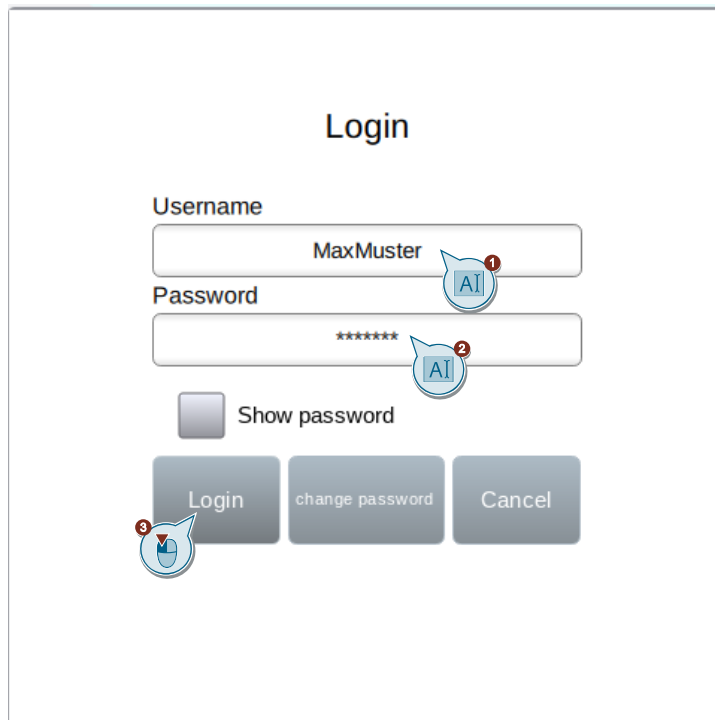
2. Click "Login" to open the login dialog.



- Log in with your UMC user or the user from the Windows Active Directory.



- In the Panel runtime, you can log in via the following dialog once you click on a screen object that you do not have permissions for.



4 Useful information

4.1 Installing UMC certificate in WinCC Unified PC station

Once a project is fully downloaded to a WinCC Unified PC station, you may see the following error when opening the WinCC Unified homepage:

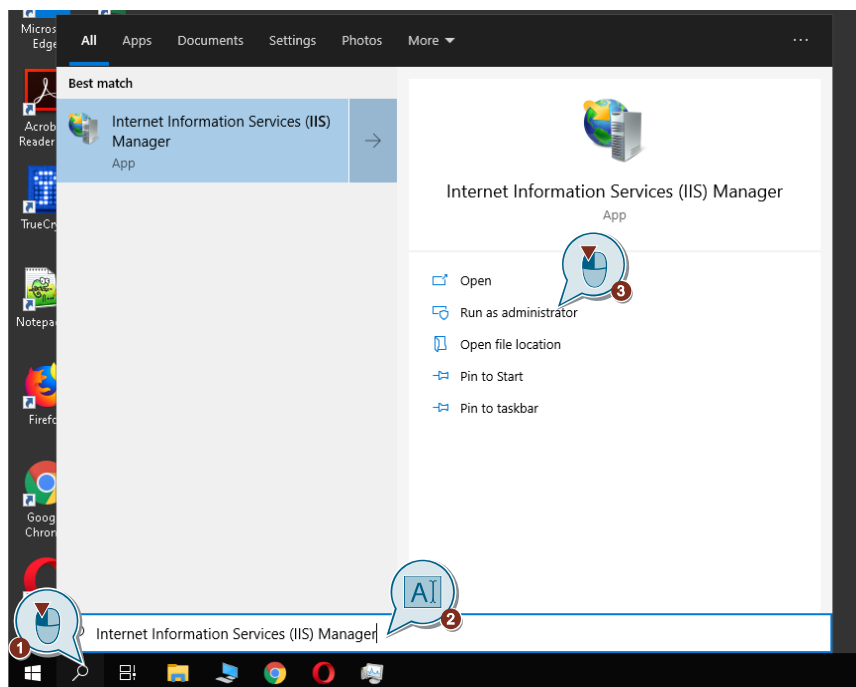
Figure 4-1



Due to an invalid certificate, the UMC server cannot be reached for authentication.

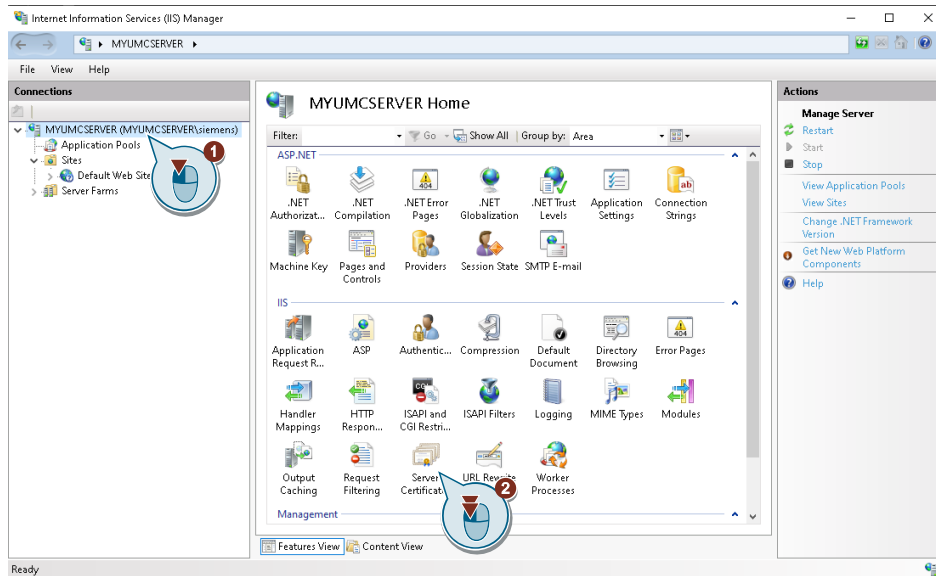
Proceed as follows to export the UMC web certificate and install it on the WinCC Unified PC station:

1. Open the Internet Information Services (IIS) Manager on the PC where the UMC server is installed for authentication.

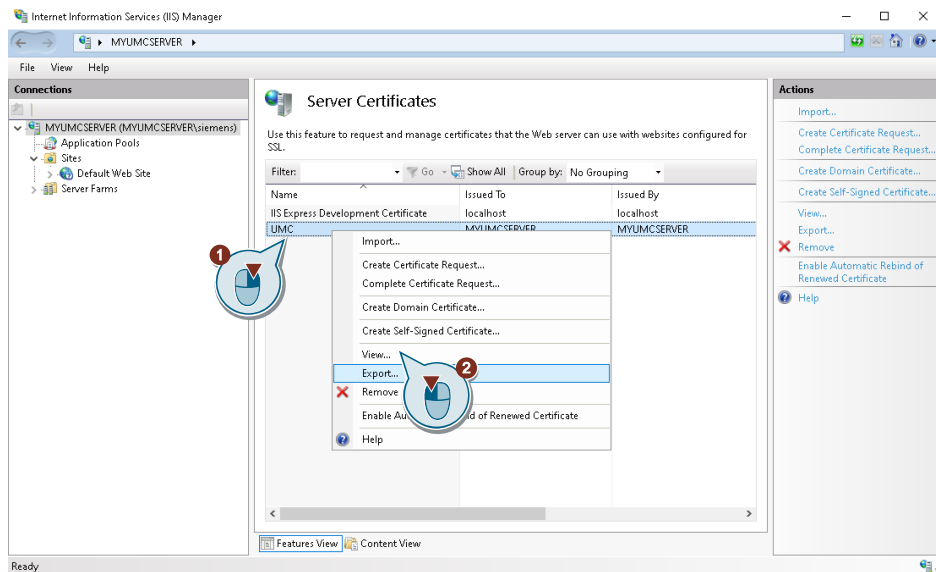


4 Useful information

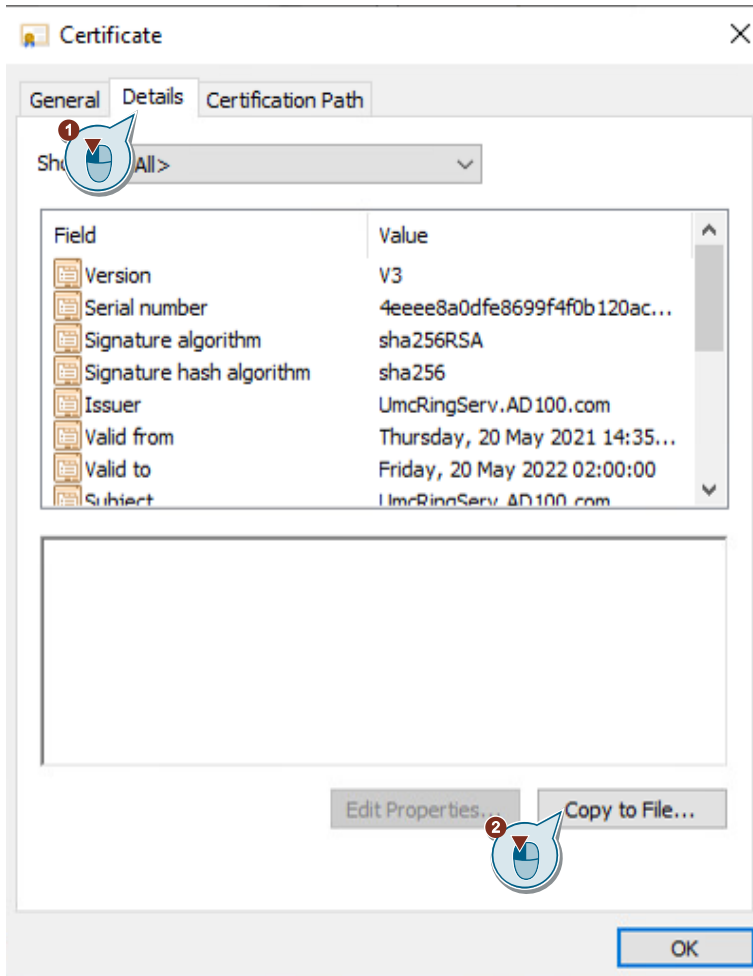
2. Open the server certificates in the IIS.



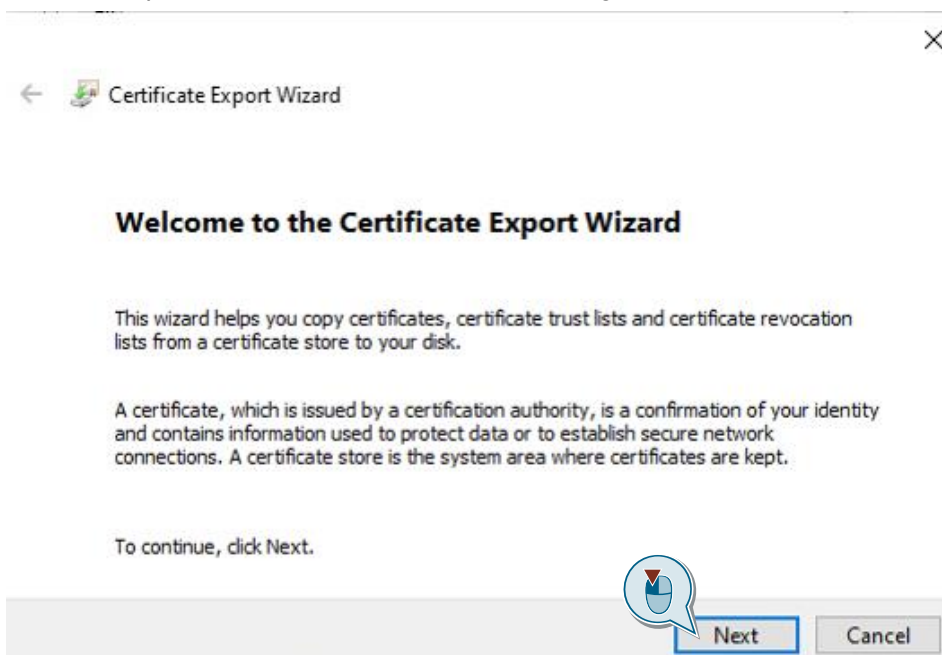
3. Right-click on the web certificate for UMC. The context menu opens. Select "View" in the context menu. The "Certificate" dialog will open.



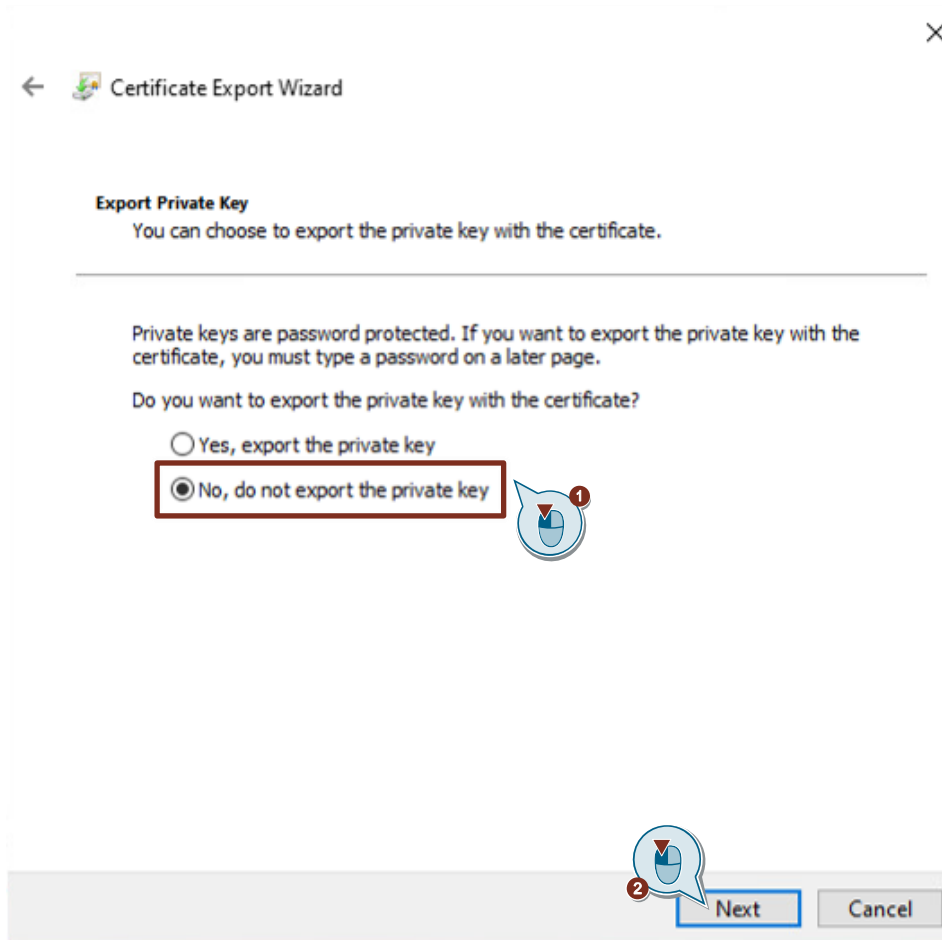
4. Open the "Details" tab and save the certificate as a file.



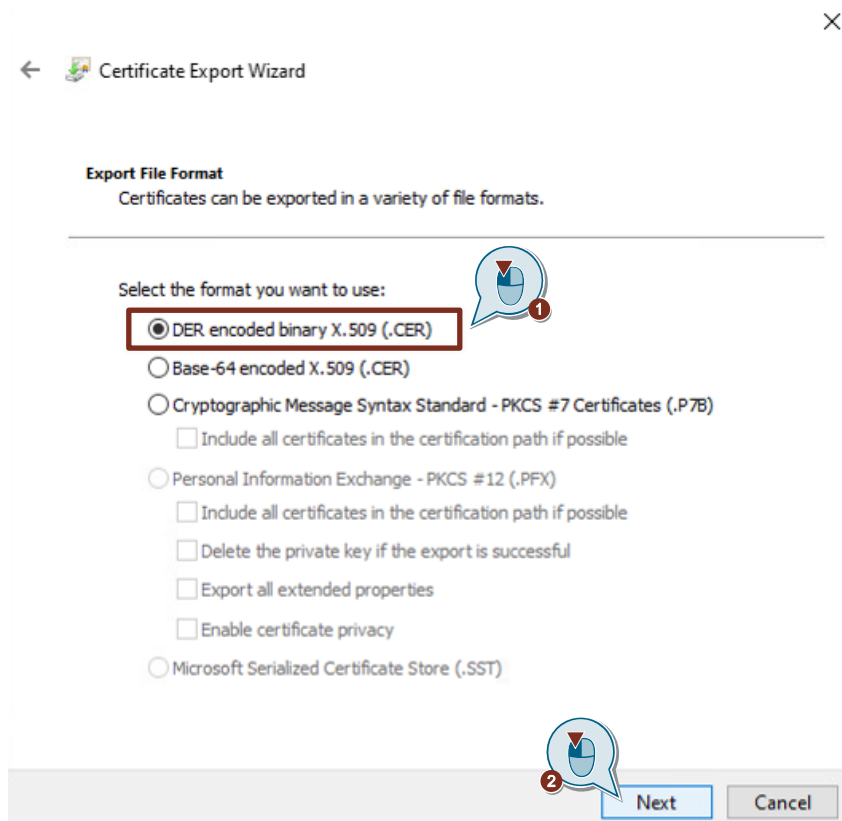
5. Start the Export Wizard and make additional settings.



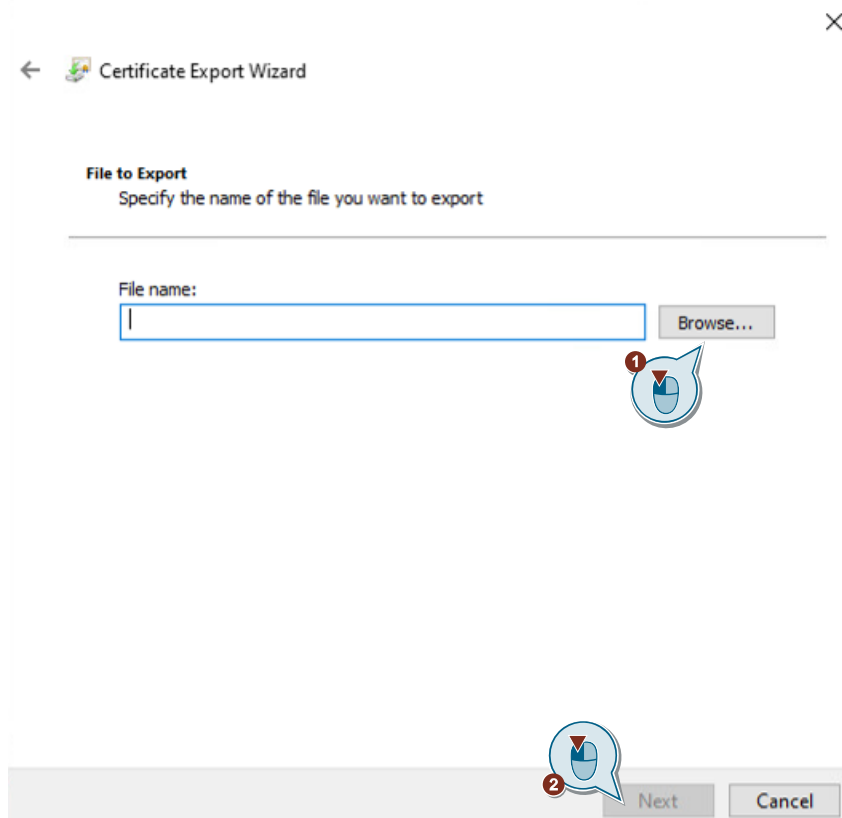
6. Export the certificate without the private key.



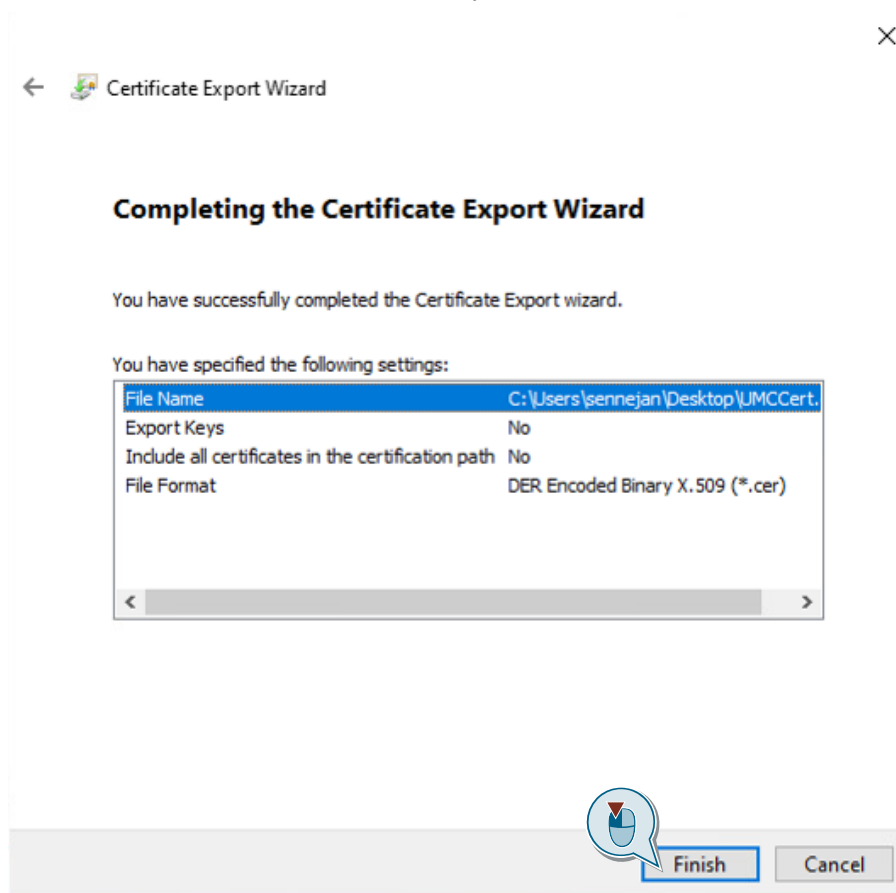
7. Select the format "DER encoded binary X.509 (.CER)".



8. Specify the export directory.

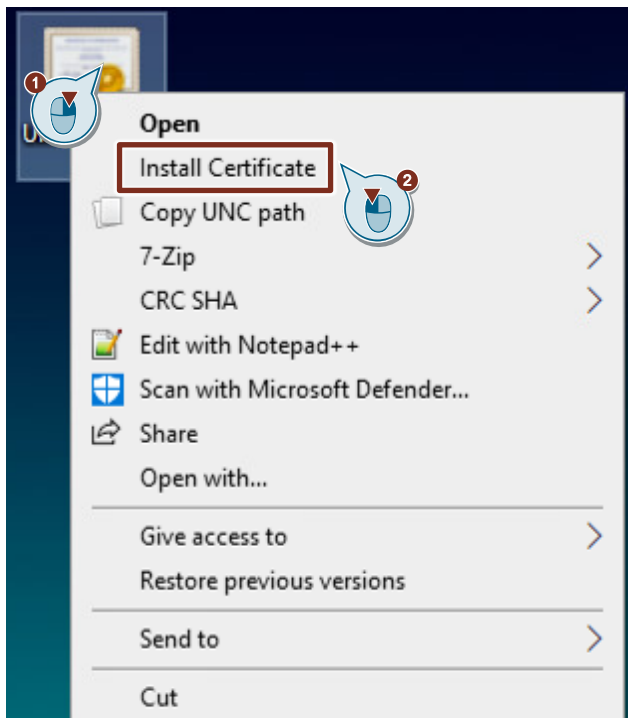


9. Click the "Finish" button to close the Export Wizard.

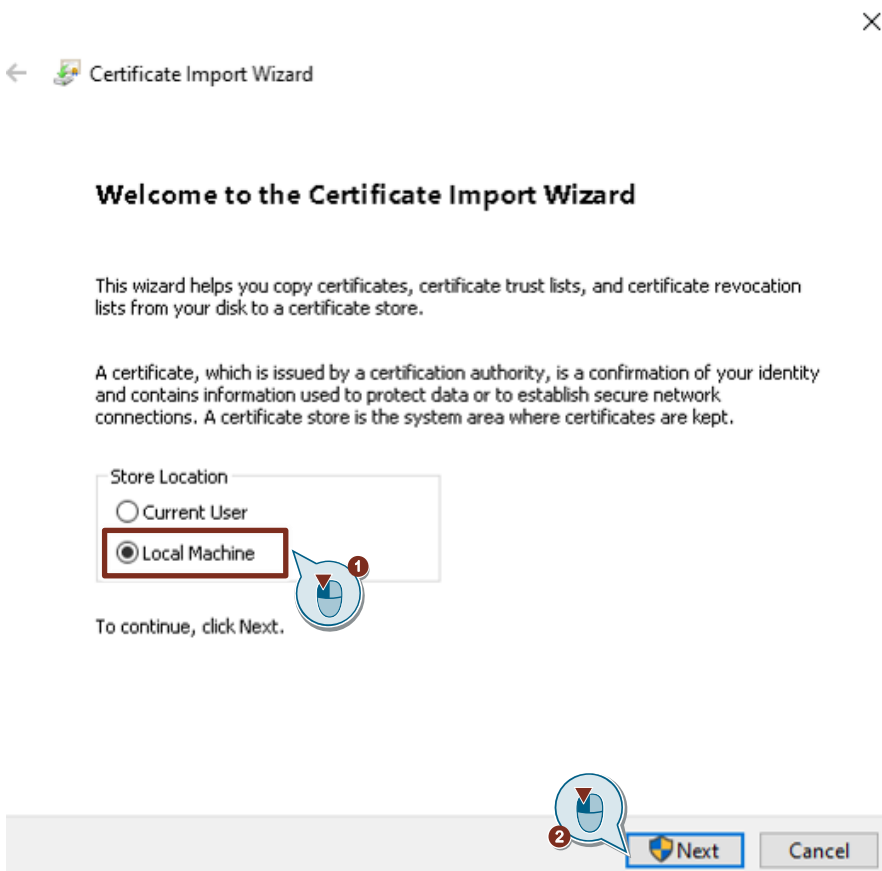


10. Copy the certificate to the WinCC Unified PC station.

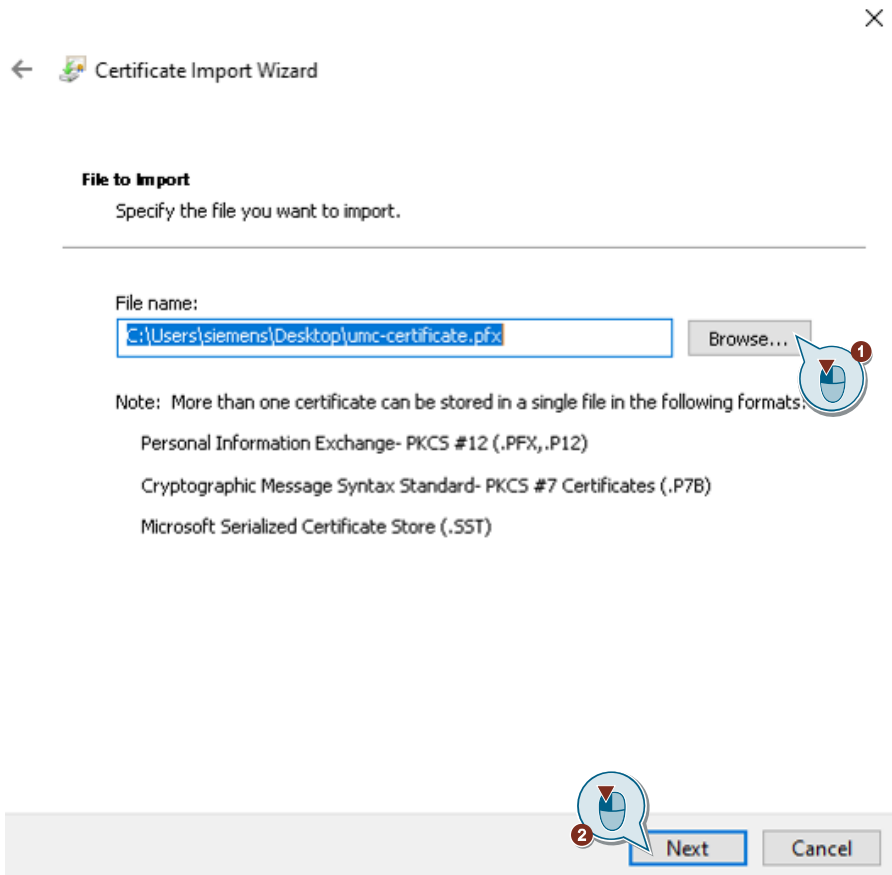
11. Install the certificate on the WinCC Unified PC station.



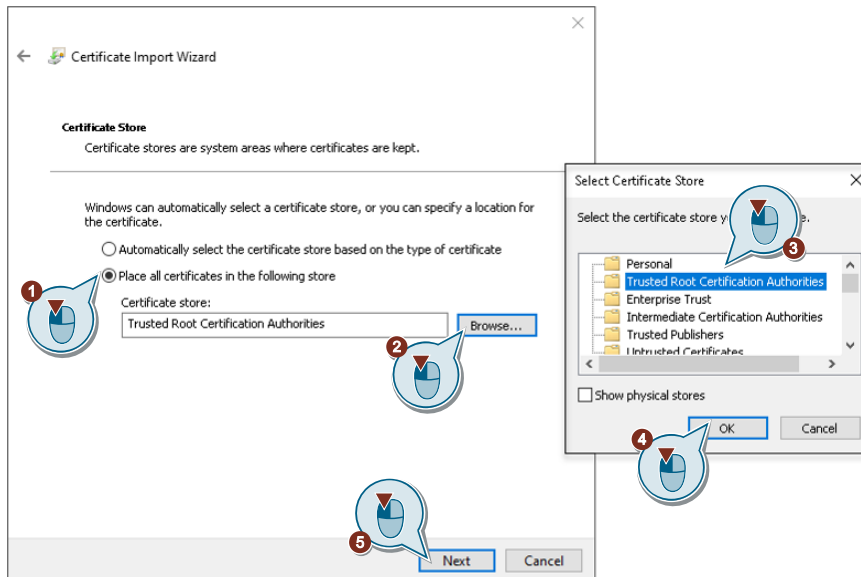
12. The Windows Certificate Import Wizard will guide you through the installation. Select the local machine as the save location.



13. If it is not already selected, select the certificate, and click the "Next" button.



14. Select "Trusted Root Certification Authorities" as certificate store.



15. Click the "Finish" button to close the Windows Certificate Import Wizard.

✕

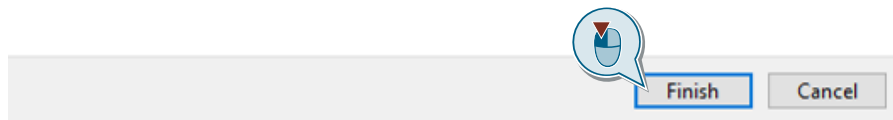
←  Certificate Import Wizard

Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

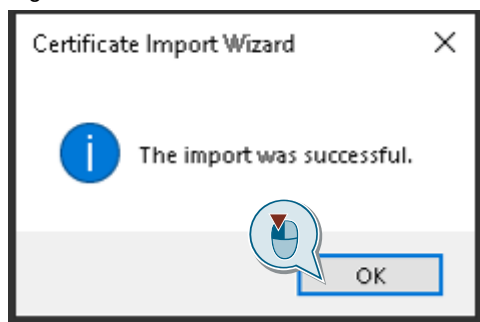
You have specified the following settings:

Certificate Store Selected by User	Trusted Root Certification Authorities
Content	PFX
File Name	C:\Users\siemens\Desktop\umc-certificate.pfx



The certificate has been successfully installed.

Figure 4-2



Note

If the error message still appears, run the WinCC Unified Configuration Tool again and make sure the user management is correctly configured.

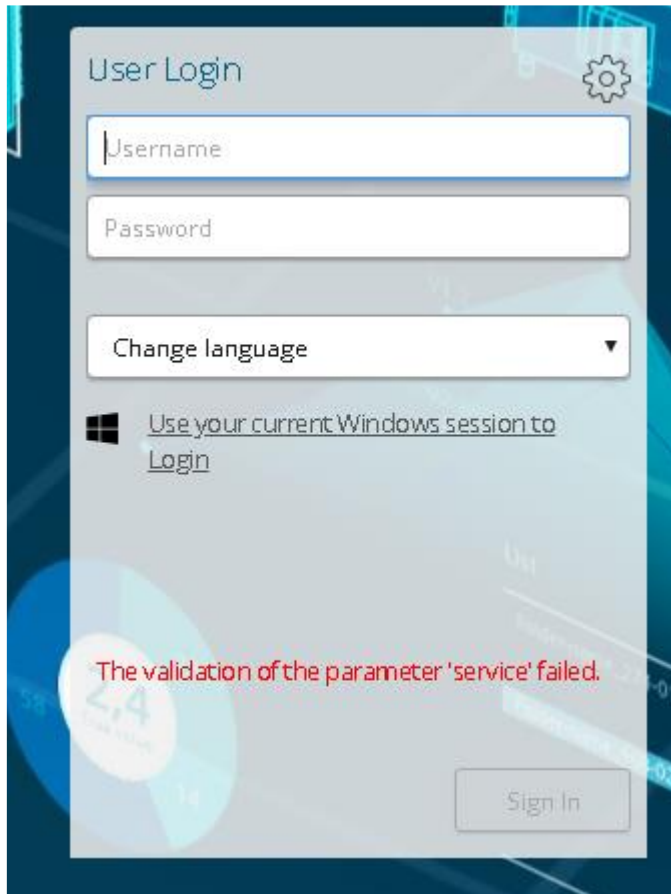
When the error message appears, you can press the <F12> key in the browser to open the "Console" pane and identify the error.

Errors like "ERR_CERT_AUTHORITY_INVALID" or "ERR_NAME_NOT_RESOLVED" can be remedied with the steps listed above.

4.2 Adding PC station to the UMC whitelist

If you see the following error message when logging in to the WinCC Unified runtime, the WinCC Unified runtime has not yet been added to the UMC whitelist.

Figure 4-3

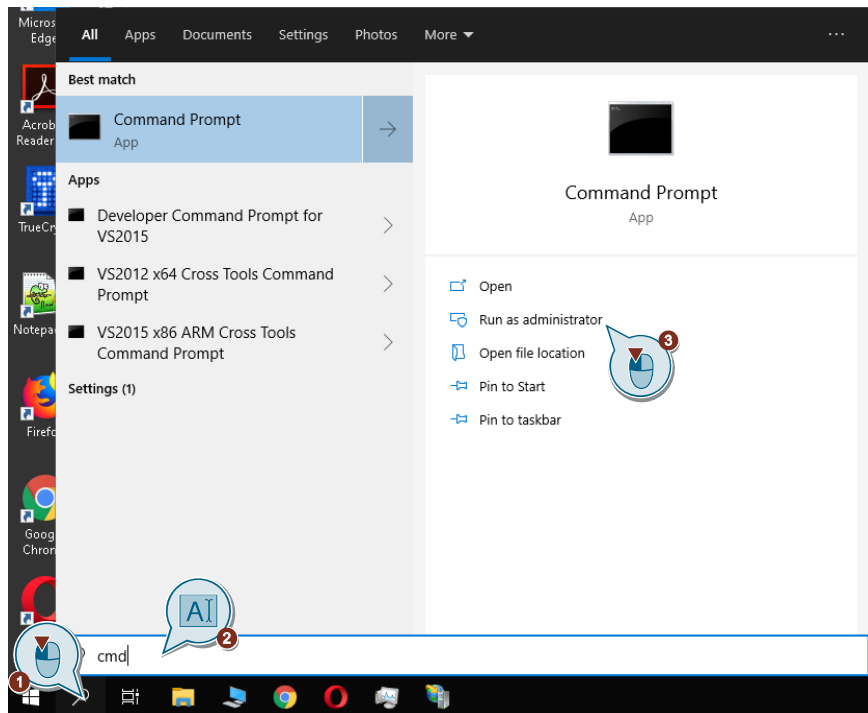


Proceed as follows to add the WinCC Unified PC station to the UMC whitelist.

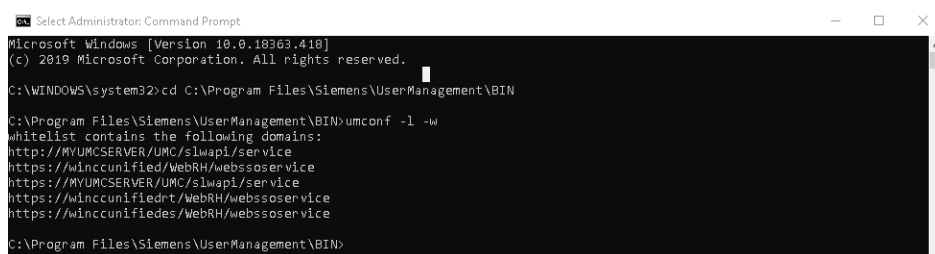
Note If the first login is made with the UMC administrator, then the host name will be automatically added to the UMC whitelist.

Note If a login to the Unified Comfort Panel is made via the web client, it will likewise be necessary to add the Unified Comfort Panel to the UMC whitelist with a static IP address.

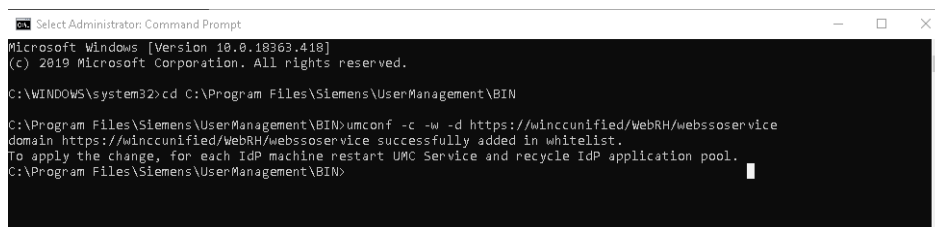
1. Run the "Command Prompt" as an administrator on the UMC ring server.



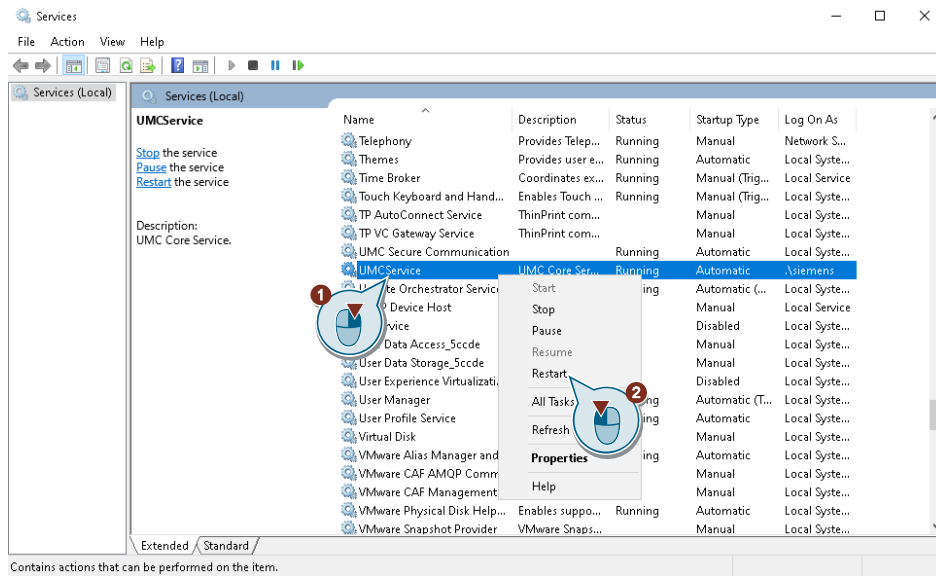
2. Change the directory using the following command:
`cd C:\Program Files\Siemens\UserManagement\BIN`
3. The following command will present you with all whitelist entries:
`umconf -l -w`



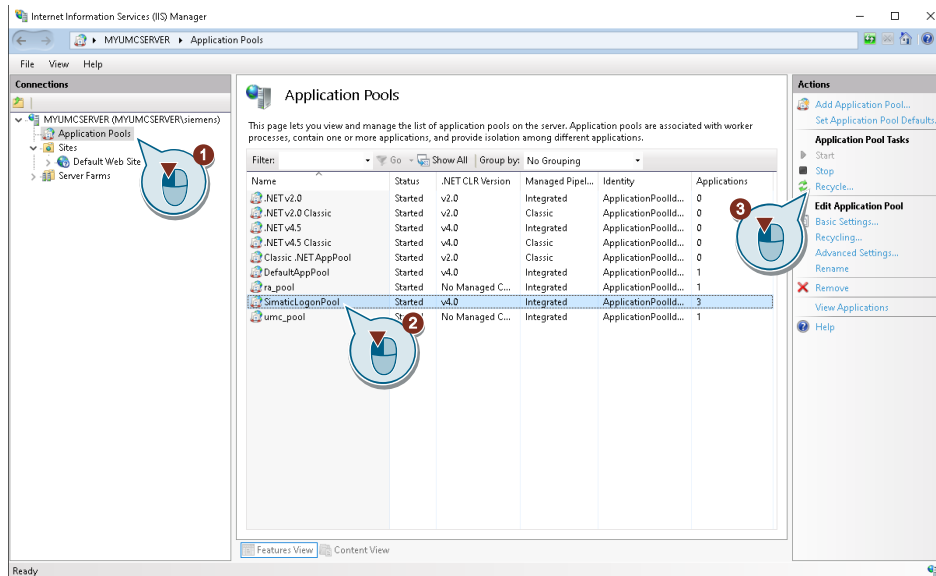
4. The entry "https://hostname/WebRH/webssoservice" is required for the WinCC Unified runtime login.
5. You can add the PC name of your WinCC Unified PC station to the UMC whitelist with the following command:
`umconf -c -w -d https://hostname/WebRH/webssoservice`



- Restart the UMC service on the PC that is acting as the identity verification location for WinCC Unified.



- On the PC acting as the identity verification location for WinCC Unified, open the IIS and recycle the Application Pool for the identity provider.

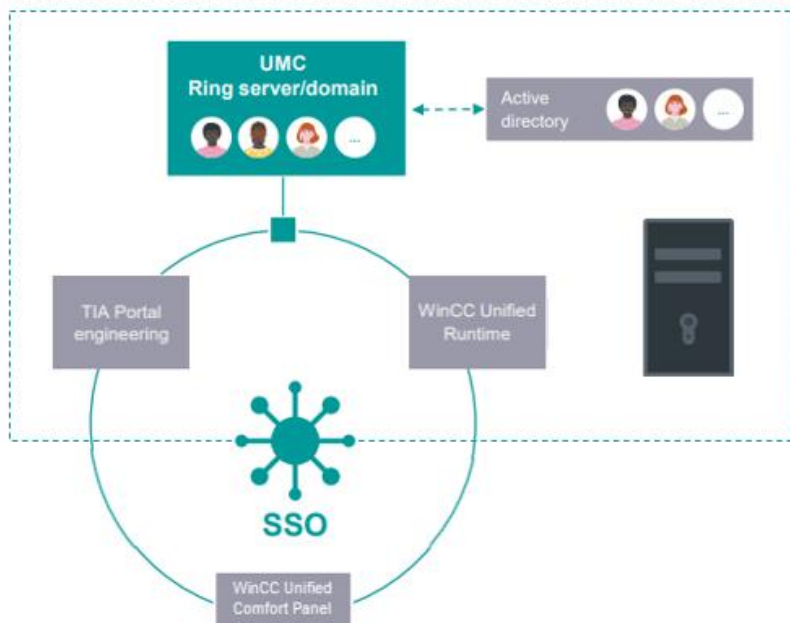


The entry has been successfully added to the UMC whitelist.

4.3 Single-station system

The following Figure shows the structure that is relevant for this section.

Figure 4-4



If the WinCC Unified runtime is installed with the UMC ring server on one PC, then a few things should be borne in mind.

- IIS is no longer set up on the single-station system per the "UMC base document", as WinCC Unified already configures IIS via the WinCC Unified Configuration Tool.
- The website "WinCC Unified SCADA" in IIS is used for the UMC tasks. It is necessary to run the Batch file "IdP_WebUi_Configurator.bat" with an additional parameter.

Requirements

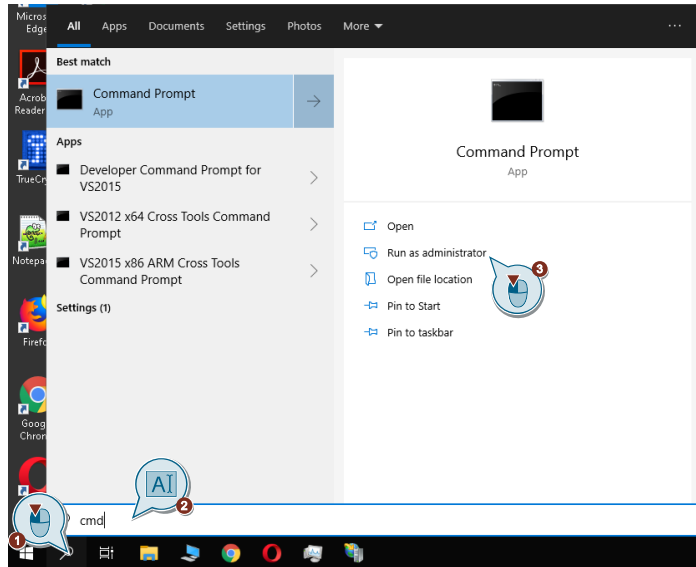
The UMC ring server is configured on the single-station system with WinCC Unified per the "UMC base document" (see "UMC base document", chapter 3.2.2).

The "UMC base document" describes the following configuration steps:

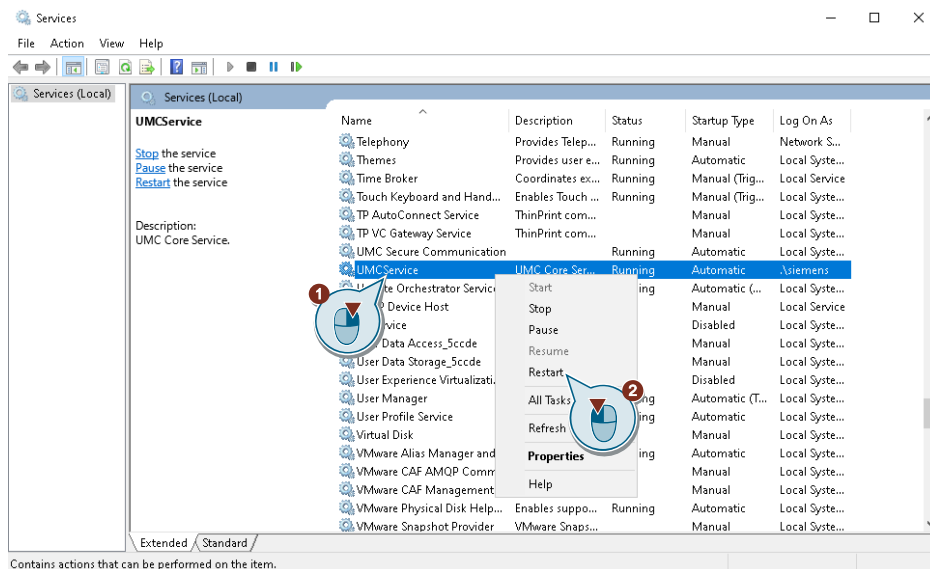
- Setting up the UMC ring server
- Creating the web interface for the UMC ring server identity provider with the Batch file "IdP_WebUi_Configurator.bat"

Procedure

1. Run the "Command Prompt" as an administrator on the single-station system.



2. Change the directory with the following command:
`C:\Program Files\Siemens\UserManagement\BIN`
3. Create the web interface for the identity provider with the parameter "WinCC Unified SCADA".
`IdP_WebUI_configurator.bat "WinCC Unified SCADA"`
4. Open the "Services" and restart the service called "UMCService".



5. The settings are complete. Continue with the configurations on the single-station system according to chapter 2.3. Not all steps from chapter 2.3 are necessary for the configuration of the single-station system.

4.4 UMC service disabled

When running the "umconf" command in the "Command Prompt", the following error message may appear:

```
C:\Program Files\Siemens\Automation\UserManagement\BIN>umconf

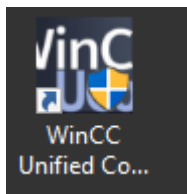
User Management Configurator - Interactive mode.
A configuration is already present: overwrite, upgrade or exit? [o/u/e] o
UM domain name: UMDomain

Error: SCM::StartService error after StartService
Error while creating domain. Cannot start services.

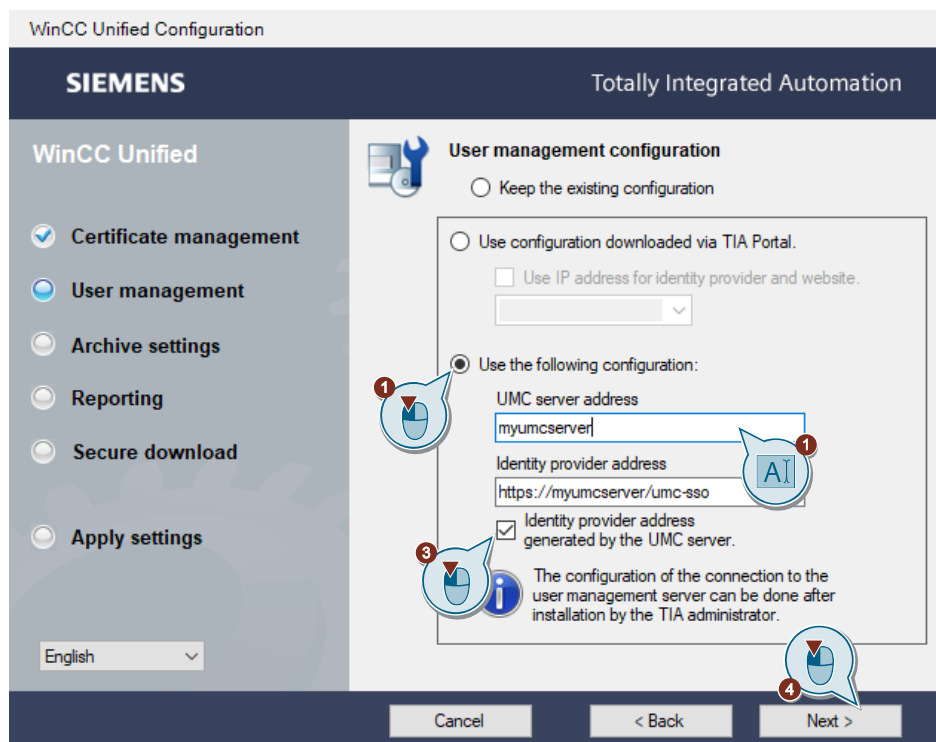
C:\Program Files\Siemens\Automation\UserManagement\BIN>
```

Proceed as follows to start the necessary UMC services:

1. Start the WinCC Unified Configuration Tool.



2. In the "User Management" category, select the option "Use the following configuration" and specify the PC name of the UMC ring server.



3. Continue the rest of the configuration steps in the WinCC Unified Configuration Tool and then close the Configurator.
4. Run the "umconf" command again in the "Command Prompt".

5 Appendix

5.1 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

5.2 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

5.3 Links and literature

Table 5-1

No.	Subject
\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

5.4 Change documentation

Table 5-2

Version	Date	Change
V1.0	10/2021	First version