

User Administration in WinCC Professional

SIMATIC WinCC Professional V16 /
SIMATIC Logon V1.6

https://support.industry.siemens.com/cs/ww/en/view/109738532

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.

© Siemens 2021 All rights reserved

Table of contents

Legal information **2**

1 Task **5**

1.1 Overview 5
1.2 Requirements 5

2 Solution **6**

2.1 Overview 6
2.2 Hardware and Software Components 7

3 Fundamentals **8**

3.1 User Administration (General) 8
3.2 Users, User Groups, and Permissions 8
3.2.1 User 8
3.2.2 User Groups 9
3.2.3 Permissions 9
3.2.4 Features Dependent on Operator Panels 10
3.3 Functions in Runtime 11
3.3.1 Access Protection 11
3.3.2 Login and Logout via System Functions 12
3.3.3 User Login with RFID Card Reader 12
3.3.4 User Administration via User Display 12
3.4 Central User Administration ("SIMATIC Logon") 14
3.4.1 Access Protection via a "SIMATIC Logon" Logon Server 15
3.4.2 Access Protection via Domain Controller 16

4 Local User Administration **17**

4.1 Configuration of Users, User Groups, and Permissions 18
4.1.1 User Configuration 19
4.1.2 Configuration and Assignment of User Groups 21
4.1.3 Configuration and Assignment of Permissions 25
4.1.4 Optional: Dynamic logon 29
4.2 Configuration of Access Protection and User Display 31
4.2.1 Configuration of Access Protection 31
4.2.2 Login and Logout with System Functions 32
4.2.3 Display of the Currently Logged-In User 34
4.2.4 User Display and Operation 35

5 Central User Administration with "SIMATIC Logon" **39**

5.1 Preparation for the Use of "SIMATIC Logon" 40
5.1.1 Creating User Groups in WinCC (TIA Portal) 41
5.1.2 Creating and Assigning Permissions in WinCC (TIA Portal) 41
5.1.3 Activate "SIMATIC Logon" in WinCC(TIA Portal) 41
5.2 "SIMATIC Logon" as Logon Server 43
5.2.1 Creating Users in Windows User Administration 45
5.2.2 Creating User Groups in Windows User Administration and Assigning Users 47
5.3 Windows Domain Controller as Logon Server 51
5.4 Traceability and Advanced Diagnostic Data 53
5.4.1 Traceability 53
5.4.2 Diagnostic Data 54

6 Appendix **57**

6.1 Service and support 57
6.2 Industry Mall 58
6.3 Links and literature 58

© Siemens AG 2021 All rights reserved

6.4 Change documentation 59

© Siemens AG 2021 All rights reserved

1 Task

1.1 Overview

Introduction

Automation systems are high-precision and high-availability systems that play an essential role in the production of a company. The increasing communication within a plant and across several plants also increases the complexity of the overall system. In order to be able to monitor and operate these systems accordingly, the processes are visualized via HMI Operator Panels.

If the system is operated by unauthorized personnel, production faults may occur. Furthermore, manipulations and theft of know-how by unauthorized persons can be carried out directly on the systems.

To avoid this, it is important to protect all equipment from unauthorized personnel. With WinCC (TIA Portal) you can implement this with the integrated user administration and thus increase plant safety.

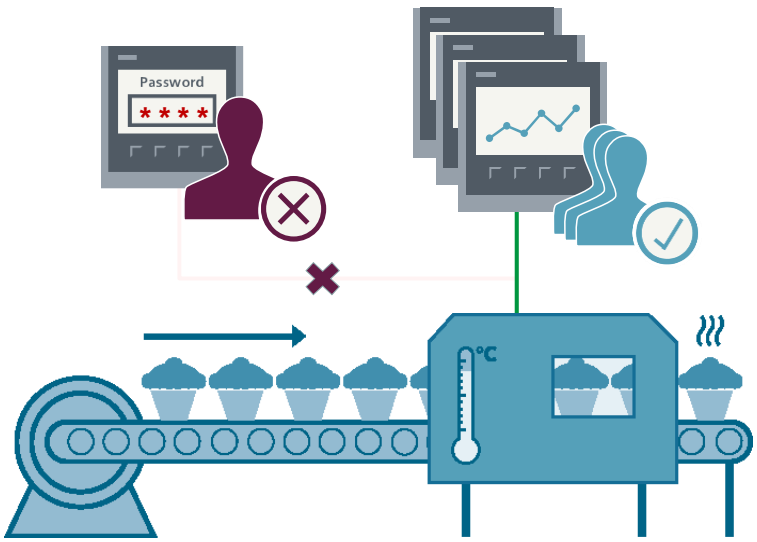
1.2 Requirements

The following figure gives you an overview of the requirements of the automation task.

Here it must be ensured that

- authorized employees can log in.
- several employees can be logged in at the same time (larger systems).
- Employees have access to the functions and data in accordance with their permissions.
- authorized employees are automatically logged out after a specified period of inactivity.
- unauthorized persons are denied access to the facility and data.

Figure 1-1



© Siemens AG 2021 All rights reserved

2 Solution

2.1 Overview

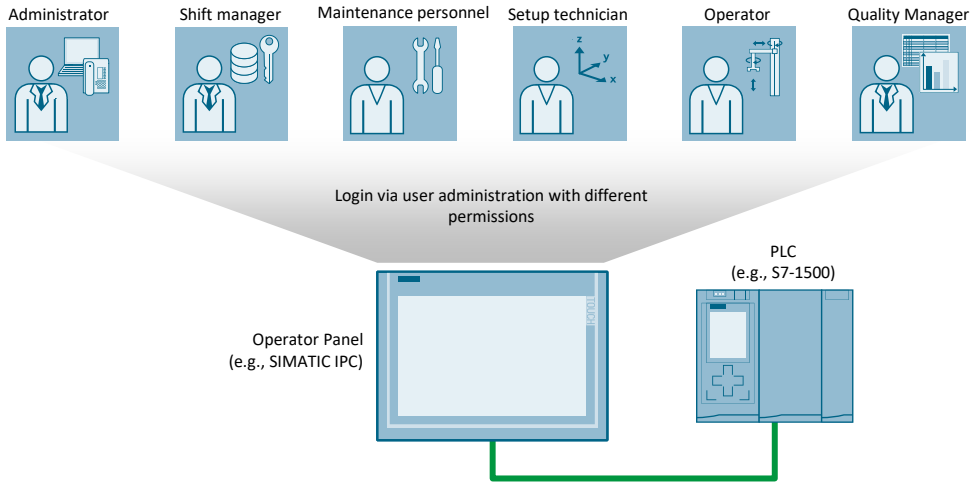
Core contents of the application

In this application example you will learn:

- Basic information about users, user groups, and permissions.
- How you can improve your plant safety with appropriate user administration.
- The difference between local user administration with WinCC Professional and central user administration with WinCC Professional in conjunction with "SIMATIC Logon".
- Which configuration steps are necessary to successfully implement a user administration.

Diagram

Figure 2-1



Advantage

The user administration content described here has the following advantages:

- Save time and money with detailed step-by-step instructions.
- Overview of the possible user administration concepts.
- Selection aids, which type of user administration makes sense when.

Delimitation

This application does not contain a description of the basic programming of an HMI in TIA Portal or the user administration under Windows operating systems.

Required knowledge

Basic knowledge of the configuration of WinCC (TIA Portal) as well as basic information on user administration under Windows operating systems is required.

© Siemens AG 2021 All rights reserved

2.2 Hardware and Software Components

The application has been created with the following components:

Software components

Table 2-1

Components	Qty.	Article number	Note
WinCC Engineering V16	1	6AV2103-0..06-..	
WinCC Runtime Professional V16	1	6AV2105-....6-0	
SIMATIC LogonV1.6	1	6ES7658-7BX61-0YA0	
Windows 10 LTSB	1		Microsoft

© Siemens AG 2021 All rights reserved

3 Fundamentals

3.1 User Administration (General)

Goal

The goal of user administration is to have access protection to data and functions within Runtime and thus to protect the applications from unauthorized operators.

Sample project

In addition to pure plant operation, there are a number of other applications in which users have to perform different tasks on the plant.
Example:

- An administrator can have access to the user administration. However, they must not be able to change the recipe data of the product.
- A quality manager can monitor the system values, but is not allowed to operate the system.

How the individual application cases will look at the respective end customer is usually not determined until the commissioning on site. The user administration in WinCC Professional with users, user groups, and their permissions helps you to realize the selected cases.

3.2 Users, User Groups, and Permissions

3.2.1 User

General

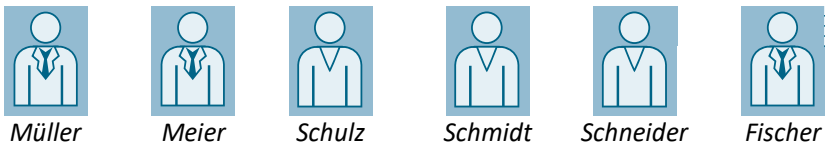
The users in WinCC (TIA Portal) represent the basis of user administration. The first step is to create a "user" in the user administration. The name and password of the user are stored in the user administration. The user "Admin" is predefined in WinCC (TIA Portal).

For better illustration, the functionality of the user administration is explained below using an example. Section 4 describes the configuration based on this scenario example.

Sample project

A company has several production facilities and employees. In the company, the employees Müller, Meier, Schulz, Schmidt, Schneider and Fischer are responsible for "Production Facility A".

Figure 3-1



Note In central user administration with "SIMATIC Logon", the users are part of the respective Windows User Administrator, instead of being created in WinCC (TIA Portal).

© Siemens AG 2021 All rights reserved

3.2.2 User Groups

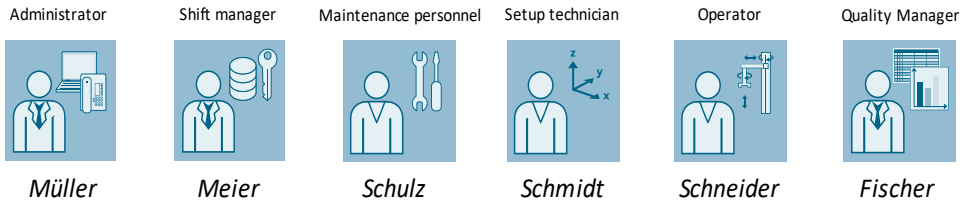
General

- For a user to be assigned a permission, it must belong to a user group. By default in WinCC (TIA Portal) the user groups "Administrator group" and "Users" are predefined.
- In addition to the predefined user groups, other groups can also be created and edited, e.g. the groups "Production facility A", "Maintenance employee", "Setup technician", etc.
- Each user is assigned to exactly one user group.

Sample project (user groups)

In user administration, the six employees (Müller, Meier, Schulz, Schmidt, Schneider and Fischer) are created as users. Each of these employees has different areas of responsibility, as shown in the figure below.

Figure 3-2



According to the responsibilities of the employees, the corresponding user groups (administrator, shift leader, maintenance technician, setup technician, user, quality manager) are now created in WinCC (TIA Portal) and the employees are then assigned to the groups.

3.2.3 Permissions

General

- Permissions are used in WinCC (TIA Portal) to define the access permissions of user groups.
- The permissions allow or deny the users of the respective user groups various operating options within Runtime.
- Various permissions ("User administration", "Monitor", and "Operate") have been created in the system. These can be renamed during configuration, but not deleted. You can also create additional permissions.
- Once all permissions have been created, you can assign the appropriate permissions to each user group. A group can have several permissions at the same time.
- With local user administration in WinCC, users can also have permissions assigned or revoked directly.

Note If "SIMATIC Logon" is used for central user administration, only user groups are created in WinCC. As a result, you can only assign permissions to user groups, not to individual users.

© Siemens AG 2021 All rights reserved

Example (Permissions)

In the example scenario, three additional permissions (maintenance, changing recipes, changing parameters) are defined in addition to the predefined permissions.

In the next step, the permissions are assigned to the individual user groups according to the following table:

Table 3-1

	Permissions					
User Groups	**User management**	**Monitoring**	**Operating**	**Service**	**Change recipes**	**Changing parameters**
Administrator	X					
Shift manager		X	X		X	X
Maintenance personnel			X	X		
Setup technician			X		X	X
Operator		X	X			
Quality Manager		X				

The user administration is thus completely created and forms the basis for later access protection.

Note The creation of a user administration does not mean that the data and functions are protected against unauthorized access. The access protection only becomes effective in connection with the assignment to the objects.

Creating users, user groups, and permissions in WinCC (TIA Portal) is described in detail in Section 4.

3.2.4 Features Dependent on Operator Panels

You can create a maximum of 200 users in Runtime Professional.

For more information about user administration in the TIA Portal, see the following link:

https://support.industry.siemens.com/cs/ww/en/view/109773506/126103583499

© Siemens AG 2021 All rights reserved

3.3 Functions in Runtime

After you have created the user administration with different user groups and permissions, you can assign the permissions to control elements (e.g., a button). This makes it possible to increase system safety.

3.3.1 Access Protection

In order to set up access protection for security-relevant functions and data in a plant, this must be taken into account when the project is created. Via the properties of the respective Control, you can enter the respective permission under "Properties > Security > Security in Runtime". They thus restrict the operation of the safety-relevant functions to the respective user groups.

Note Within the WinCC Runtime, you can no longer change or extend the access protection.

Runtime operation

If the objects (e.g. a button) are pressed in Runtime, a login dialog appears and the user is prompted to authorize himself with his username and password.

These entries are compared by the system with the data in the user administration and, if they match, the operation is permitted. If the authorization is incorrect, no operation is possible. A message "Invalid password or username. Login failed." appears in the message display.

Project and operating system protection

According to this principle described above, a wide variety of safety concepts can now be developed for Operator Panels, projects and complete systems. The protection of projects and operating systems plays an important role here.

In principle, the termination of Runtime should be provided with access protection. Unauthorized operators are therefore not granted access to the operating system of the Operator Panel.

Note Access protection does not protect against operating errors. You yourself must ensure that only suitably trained and authorized personnel construct, commission, operate and maintain plants and machines.

Configuring access protection for functions is described in a step-by-step guide in Section 4.2.

© Siemens AG 2021 All rights reserved

3.3.2 Login and Logout via System Functions

You have provided and protected all security-relevant functions and data in your project with access protection. Now you want to see who is currently logged in during plant operation in order to change the user if necessary.

System functions "Log in"/"Log out"

To generally log a user on and off, for example before and after a shift, you can use the system function "ShowLogon Dialog". A login window is opened in which the user can enter his username and password.

When the login button is pressed, these values are read in and compared with the user administration data. If these match, the user is logged in. The user can log out again via the logout button.

The corresponding configuration of the system function "ShowLogon Dialog" is described in Section 4.2.2.

Another useful system function for user administration in WinCC Runtime Professional is the "ExportImportUser Administration" function.

This exports the user administration of the project into the specified file or imports it from the file into the project.

More information about the system functions of the user administration in WinCC Runtime Professional can be found under the following link:

https://support.industry.siemens.com/cs/ww/en/view/109773506/111031158795

3.3.3 User Login with RFID Card Reader

In addition to the conventional login via the login dialog, there is also the option of logging in using an RFID card reader. More information on this topic can be found via the following link:

https://support.industry.siemens.com/cs/ww/en/view/109779685

3.3.4 User Administration via User Display

Goal

The "User View" Control offers a selection of the most important functions required during plant operation so that user administration can be adapted quickly and easily during plant operation.

Depending on the user group you belong to, you can make different settings in the user display.

Figure 3-3

User	Password	Group	Logoff time
Fischer	******	Quality_Manager	After 5 minutes of inactivity
Schneider	******	Schift_leader	No
Schmidt	******	Fitter	After 5 minutes of inactivity
Schulz	******	Maintance	After 5 minutes of inactivity
Meier	******	Schift_leader	After 5 minutes of inactivity
Müller	******	Administrator group	After 5 minutes of inactivity
Administrator	******	Administrator group	After 5 minutes of inactivity

© Siemens AG 2021 All rights reserved

Administrators

All user groups with the permission "User administration" (preset for the "Administrator group") can now:

- Add and delete users
- edit all usernames and passwords (document in writing if necessary)
- Change group memberships
- adjust all logout times

Further user groups

All other user groups that do not have the "User administration" permission have the option in the user display:

- change your password
- edit your own logout time

The configuration of the user display and the user administration in Runtime can be found in Section 4.2.4.

CAUTION	**Unintentional overwriting of existing user settings**
	Changes made by the User Administrator in Runtime are not persistently applied in CS. When loading the ES to the OS, the changed settings on the OS are overwritten. When using the import function of the User Administrator, note the following: • Entered user passwords are retained during reimport. • All other configuration changes are overwritten during reimport.

© Siemens AG 2021 All rights reserved

3.4 Central User Administration ("SIMATIC Logon")

For more complex automation projects and systems with several Operator Panels, a central user administration with "SIMATIC Logon" is the ideal solution.

Goal

- "SIMATIC Logon" Service" enables a central and plant-wide user administration, based on the Windows User Administrator of a logon server.
- It is also possible to access the user administration of a Domain Controller directly and to use its user structure (Active Directory) for the permissions management of your automation system.
- With "SIMATIC Logon" you can bundle the user administration of several local (Panels) and central systems (WinCC Servers).

Traceability

As an additional option, all logon and logoff attempts, user authentications, and password changes are recorded in the supplied software component "SIMATIC Logon" Eventlog Viewer. This allows logon times and important operator entries to be traced back.

Advantages

- User data is created and managed via Windows operating system
- Central administration of all access data
- Simple subsequent addition of a user
- Quickly customize plant-wide permissions, groups, and users
- Uniform, plant-wide access data (synchronization of user data)

Disadvantages

- Individual assignment of permissions for individual users is not possible in WinCC (TIA Portal), therefore, each user is assigned the permissions of their respective group

Access protection

Access protection with "SIMATIC Logon" is provided for the Operator Panels with the "SIMATIC Logon Service" software component.

Additional information

Additional information about the individual software components of "SIMATIC Logon" may be found in the Configuration Manual in Section
https://support.industry.siemens.com/cs/ww/en/view/109748663/82820955787

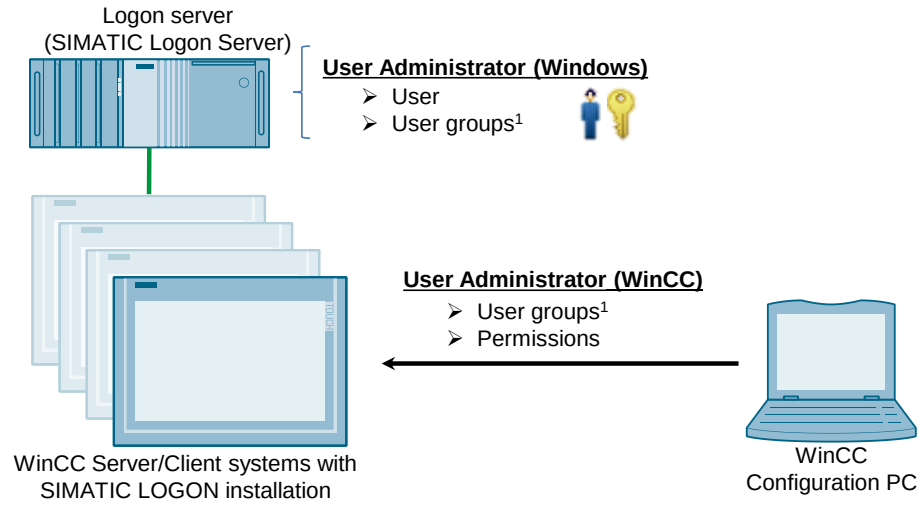
and in the manual "SIMATIC STEP 7 Basic/Professional V16 and SIMATIC WinCC V16"
https://support.industry.siemens.com/cs/ww/en/view/109773506/111031158795.

© Siemens AG 2021 All rights reserved

3.4.1 Access Protection via a "SIMATIC Logon" Logon Server

Principle Logon Server

Figure 3-4



[1] Names must be identical.

Functionality of the Logon Server

- The user data is created and managed on a central logon server via the user administration of the Windows operating system.
- The user groups and permissions are still configured in the WinCC user administration.
- In addition, you create user groups with the same names on the logon server in the user administration. The configured permission is assigned to each user group in Runtime because the names are identical.
- You only have to create the users on the SIMATIC logon server. These are dynamically transferred from the logon server during the logon process in WinCC.
- The user can now change his/her password on the Operator Panel, and this is handled directly by the logon server if the Windows user has the corresponding permission.
- A detailed description of configuring "SIMATIC Logon" as the central user administration may be found in Section 5.

Logon Server Requirements

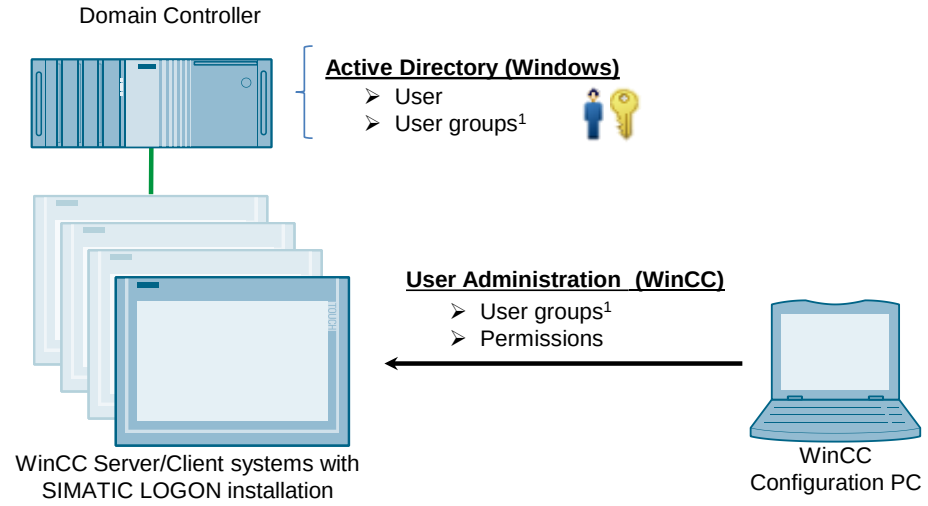
- "SIMATIC Logon" is installed and configured on the logon server.
- A licensed version of "SIMATIC Logon" is installed on each Operator Panel. For WinCC Professional, the required license is part of the scope of delivery.
- The logon server has been made known to the Operator Panel via the "SIMATIC LOGON" configuration.

© Siemens AG 2021 All rights reserved

3.4.2 Access Protection via Domain Controller

Principle Domain Controller

Figure 3-5



1 Names must be identical.

Functionality Domain Controller

- The user data is created and managed on a central Domain Controller via the Active Directory of the Windows operating system.
- The user groups and permissions are still configured in the WinCC user administration.
- In addition, you create user groups with the same name on the Domain Controller in the Active Directory. The configured permission is assigned to each user group in Runtime because the names are identical.
- You only need to create the users on the Domain Controller. These are dynamically adopted by the Domain Controller during the login process in WinCC.
- The user can now change their password on the Operator Panel, and this is adopted directly by the Domain Controller if the Windows user has the corresponding permission.
- A detailed description of configuring "SIMATIC Logon" as the central user administration may be found in Section 5.

Domain Controller Requirements

- A licensed version of "SIMATIC Logon" is installed on each Operator Panel. For WinCC Professional, the required license is part of the scope of delivery.
- The Domain Controller has been recognized by the Operator Panels via "SIMATIC LOGON" configuration.
- The users of the domain have been granted the following permissions for authenticated users:
  - "Read"
  - "Change password"

© Siemens AG 2021 All rights reserved

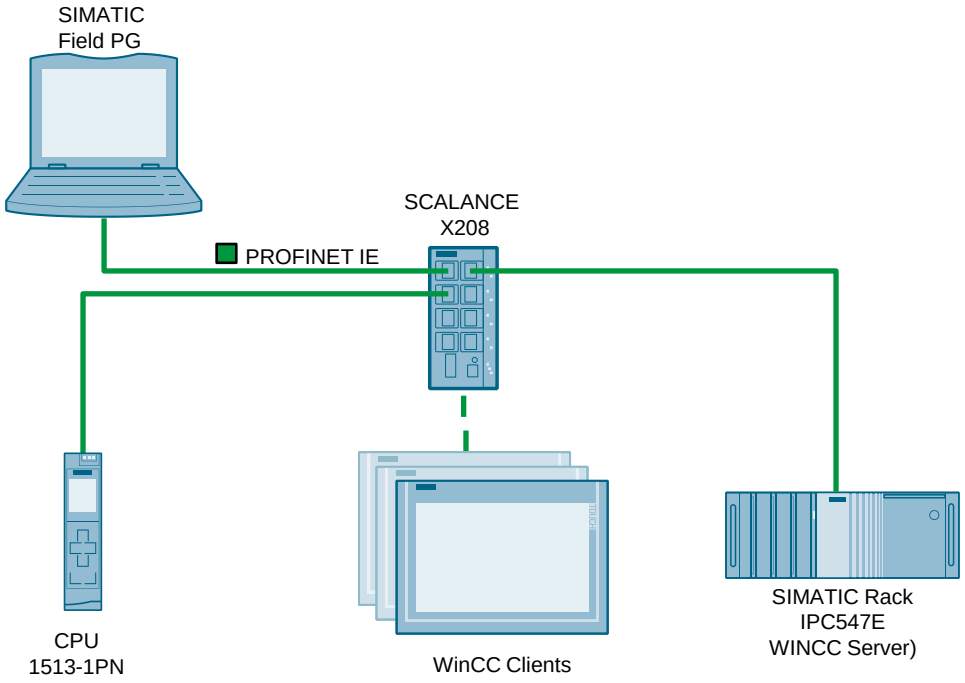
4 Local User Administration

This Section describes the process of configuring the local user administration in WinCC (TIA Portal).

Local User Administration with a WinCC Server

The following figure shows the structure of the application example in connection with the local user administration on a WinCC Server.

Figure 4-1



© Siemens AG 2021 All rights reserved

4.1 Configuration of Users, User Groups, and Permissions

In order to configure the user administration project in a practical manner, the Application Example from the fundamentals in Section 3 is implemented.

The following table shows a summary of all users, user groups, and permissions that are relevant for the following steps.

Note

Before creating the user administration, obtain an overview of the necessary users, user groups, and permissions. The following table is one way of making this clear.

Optionally an extension of this table with a further column for the passwords of the individual operators is conceivable. However, you must ensure that sensitive data is only accessible to authorized personnel.

Table 4-1

User							Permissions					
Müller	**Meier**	**Schulz**	**Schmidt**	**Schneider**	**Fischer**	**User groups**	**User management**	**Monitoring**	**Operating**	**Service**	**Change recipes**	**Changing parameters**
X						**Administrator**	X					
	X					**Shift manager**		X	X		X	X
		X				**Maintenance personnel**			X	X		
			X			**Setup technician**			X		X	X
				X		**User**		X	X			
					X	**Quality Manager**		X				

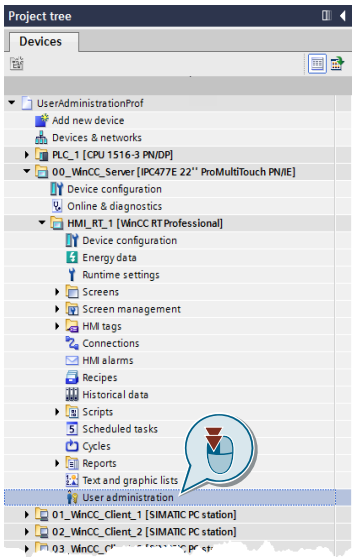
© Siemens AG 2021 All rights reserved

4.1.1 User Configuration

The following instructions show you which configuration and configuration steps are necessary for a new user.

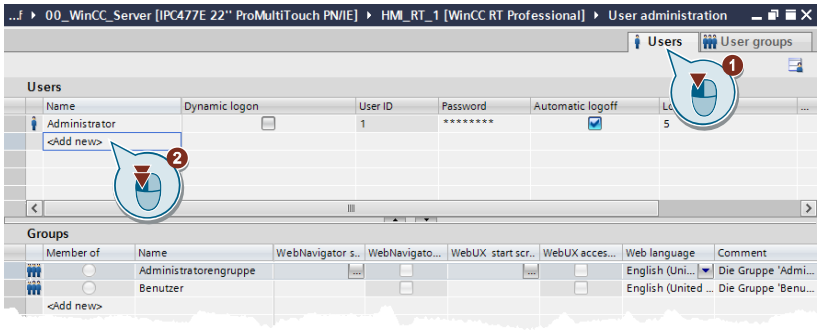
1. Open the WinCC Server configuration via the project navigation. Then double-click on "User administration" to open it.

   Figure 4-2



2. In the work area, select the Users tab (1) and double-click Add new in the Users table (2). A new user with preset user data is automatically created.

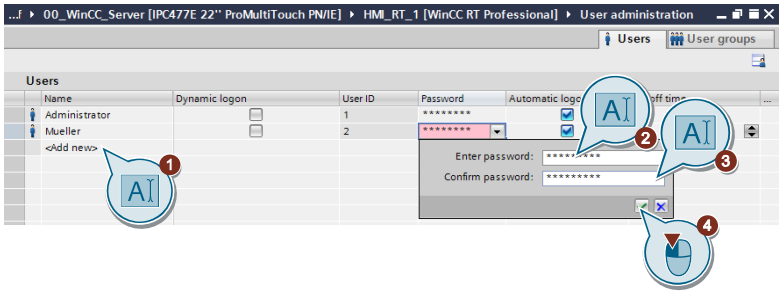
   Figure 4-3



© Siemens AG 2021 All rights reserved

3. Rename the new user according to the Table 4-1 (1). Change the password of the user. To confirm the password, enter it again (3). Confirm the entry with the green checkmarks (4).

Figure 4-4

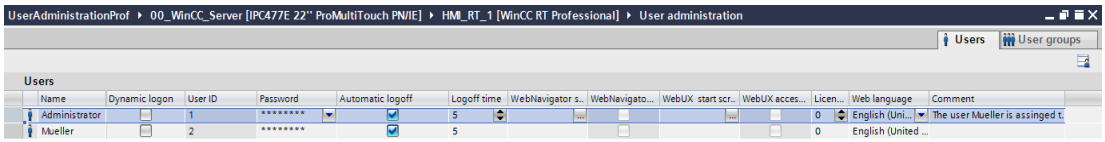


4. Optional:

   You can activate and adjust the preset parameters "Automatic logout", "Logout time", "Number", "Comment" and the settings of the user's web applications ("WebNavigator" and "WebUX") as required.

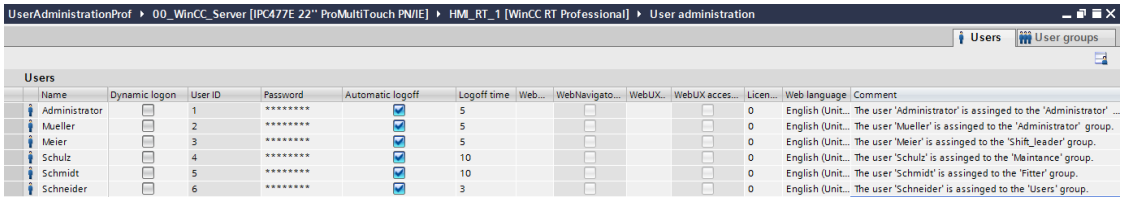
   In this example, all preset user data is left.

Figure 4-5



5. Add all other users and adjust their properties.

Figure 4-6



6. Save your project.

Result

The configuration of the users for your WinCC Server/client system is completed.

© Siemens AG 2021 All rights reserved

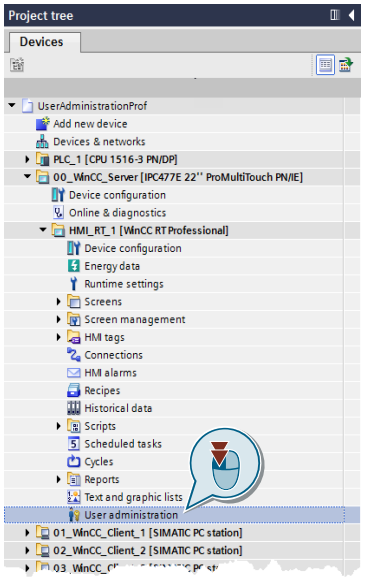
4.1.2 Configuration and Assignment of User Groups

Creating User Groups

The following instructions show you which configuration and configuration steps must be carried out in order to create user groups.

1. Open the WinCC Server configuration via the project navigation. Then double-click on "User administration" to open it.

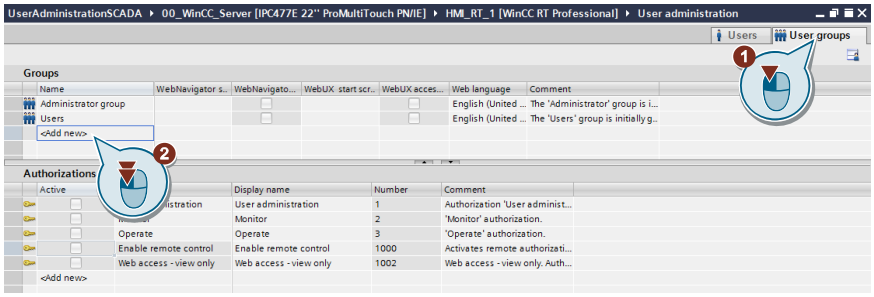
   Figure 4-7



2. In the work area, select the "User groups" tab (1). In the Groups table, double-click Add new (2) to create a new user group.

Note The user groups "Administrators Group" and "Users" are preconfigured and can only be renamed, but not deleted.

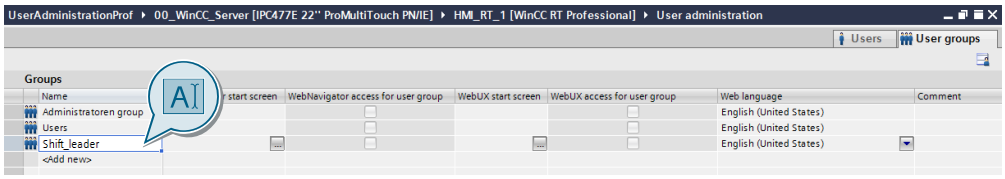
Figure 4-8



© Siemens AG 2021 All rights reserved

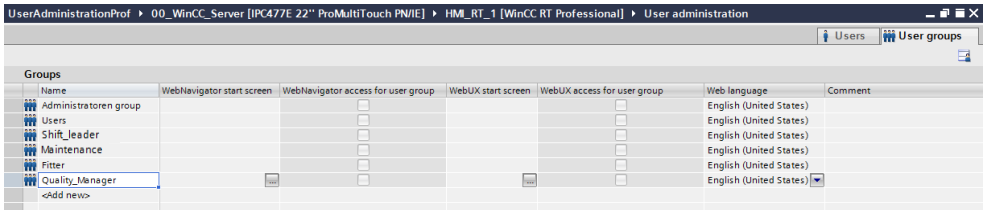
3. Change the name of the newly created user group to "Shift Supervisor".

Figure 4-9



4. Create three additional user groups as described in steps 2 and 3. Rename the groups to "Maintenance technician", "Setup technician", and "Quality manager".

Figure 4-10



5. Save your project.

Result

The creation of the user groups is hereby completed.

© Siemens AG 2021 All rights reserved

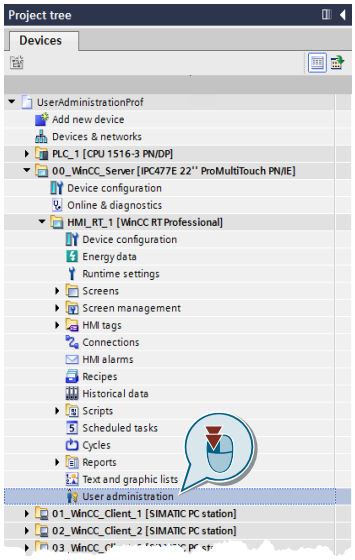
Assigning user groups

The following instructions show you which configuration and configuration steps you must carry out in order to assign user groups.

The requirement for assigning user groups is that you have already created users and user groups in your project.

1. Open the WinCC Server configuration via the "Project tree". Then double-click on "User administration" to open it.

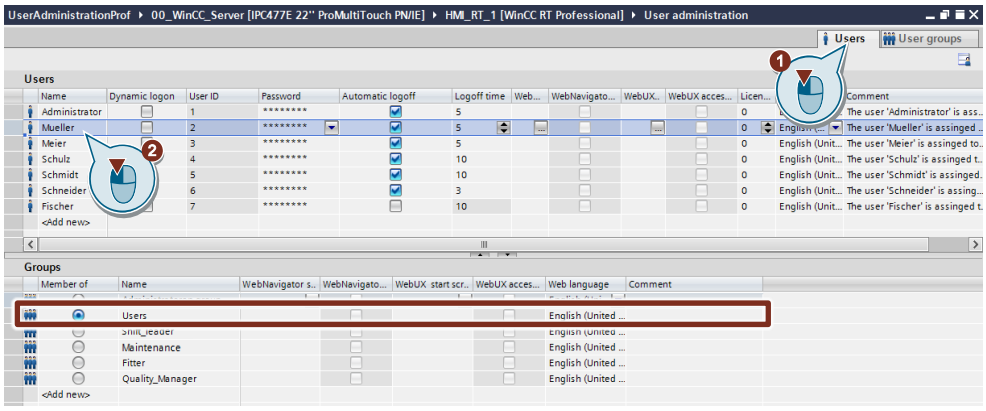
Figure 4-11



2. On the Users tab (1), select the Mueller user (2). In the "Group" table, you can see the current user group to which the "Miller" user is assigned.

Note All newly created users are assigned to the "Users" group by default.

Figure 4-12

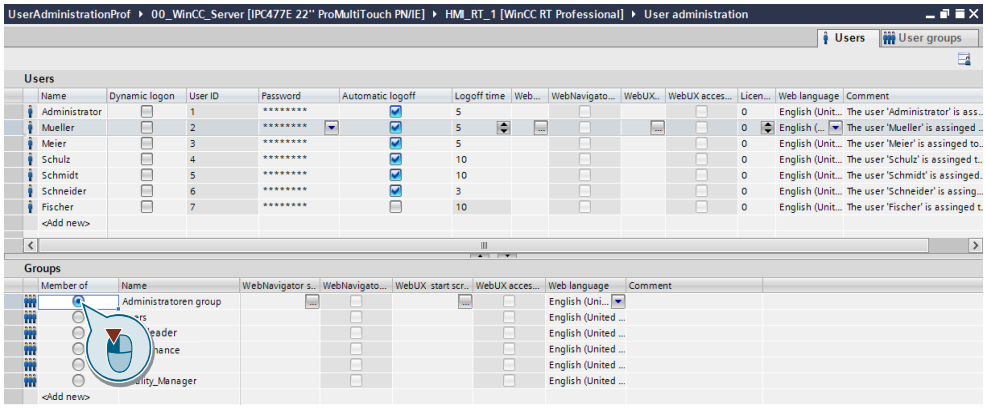


© Siemens AG 2021 All rights reserved

3. Enable the "Administrators Group" checkbox to assign the Müller user to this group.

Note Users can only ever be members of one user group.

Figure 4-13



4. Then select the other users ("Meier", "Schmidt", "Schulz", "Schneider" and "Fischer") one after the other and also assign the intended user groups to them, see Table 4-1.
5. Save your project.

Result

The assignment of the members to the user groups is hereby completed.

© Siemens AG 2021 All rights reserved

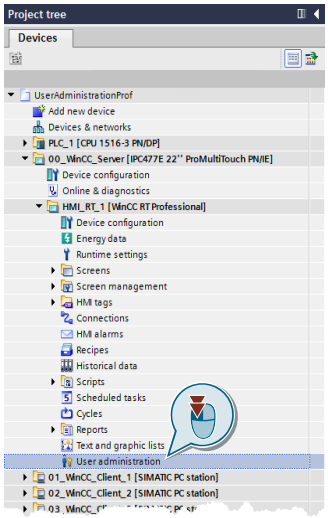
4.1.3 Configuration and Assignment of Permissions

Creating permissions

The following instructions show you how to create permissions for user groups.

1. Open the WinCC Server configuration via the project navigation. Then double-click on "User administration" to open it.

Figure 4-14

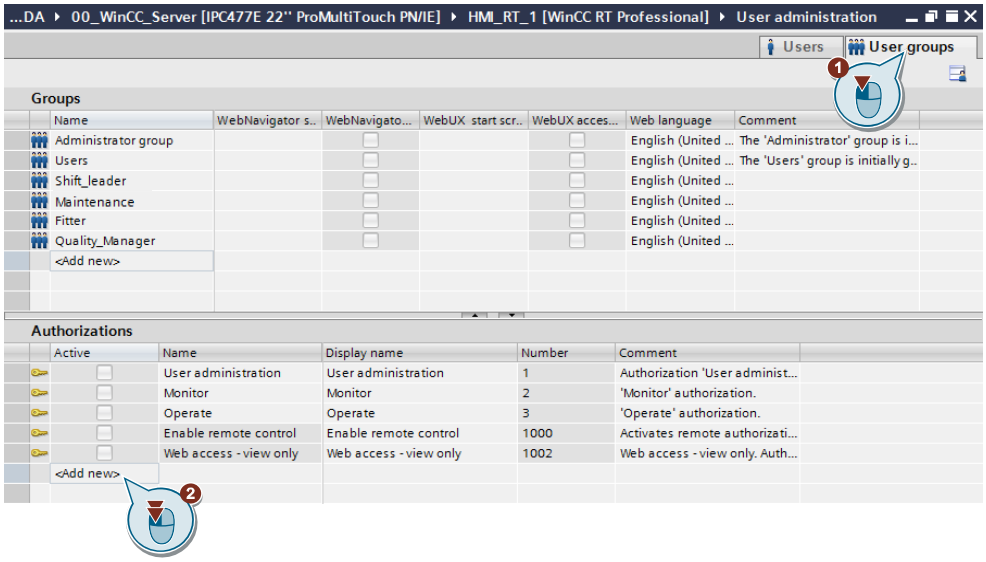


2. In the work area, select the "User groups" tab (1). In the "Authorizations" table, double-click (2) on "Add new" to create a new permission.

   A new permission "Authorization_1" is created automatically.

Note The "User administration", "Monitoring", and "Operating" permissions have already been assigned. They can be renamed but not deleted.

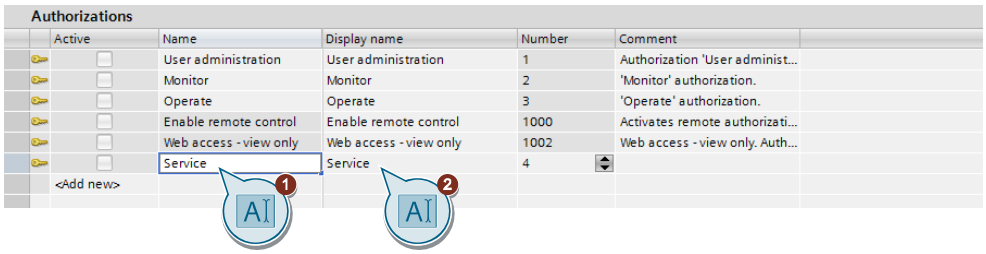
Figure 4-15



© Siemens AG 2021 All rights reserved

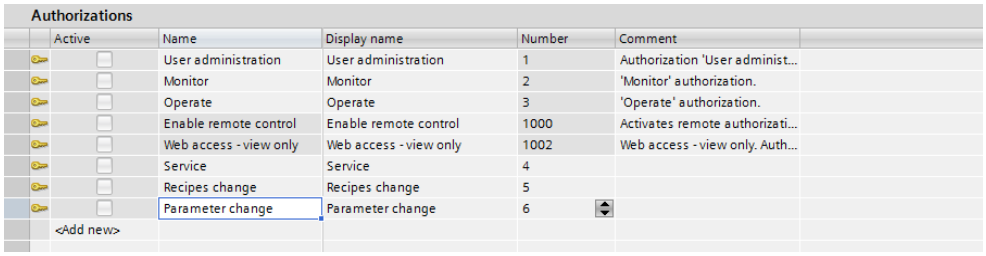
3. Change the "Name" (1) and "Display name" (2) of the new permission set to "Service".

Figure 4-16



4. Create two more permissions and name them "Change recipes" and "Change parameters".

Figure 4-17



Result

All permissions for the sample project are, therefore, created and the configuration of the permissions is completed.

© Siemens AG 2021 All rights reserved

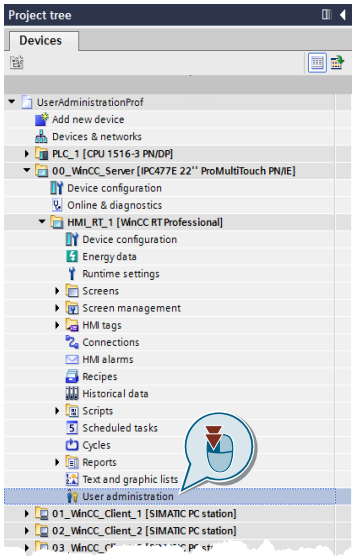
Assigning permissions

The following instructions show you how to assign permissions to a user group.

The requirement for assigning permissions is that user groups and permissions have already been created.

1. Open the WinCC Server configuration via the project navigation. Then double-click on "User administration" to open it.

Figure 4-18

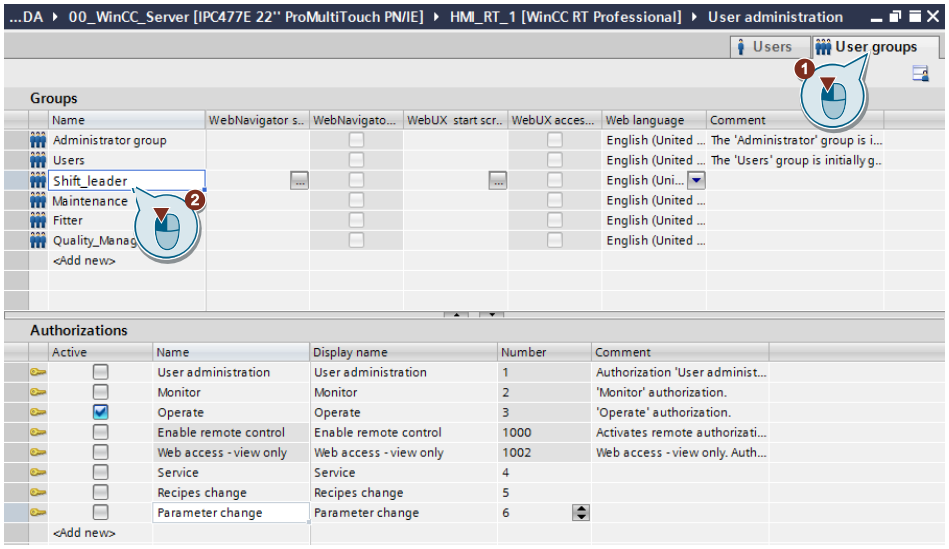


2. On the "User groups" tab (1), select the "Shift supervisor" group (2).

   In the table "Authorizations", you can see the currently assigned permission "Operate".

Note All newly created user groups are assigned the "Operate" permission by default.

Figure 4-19

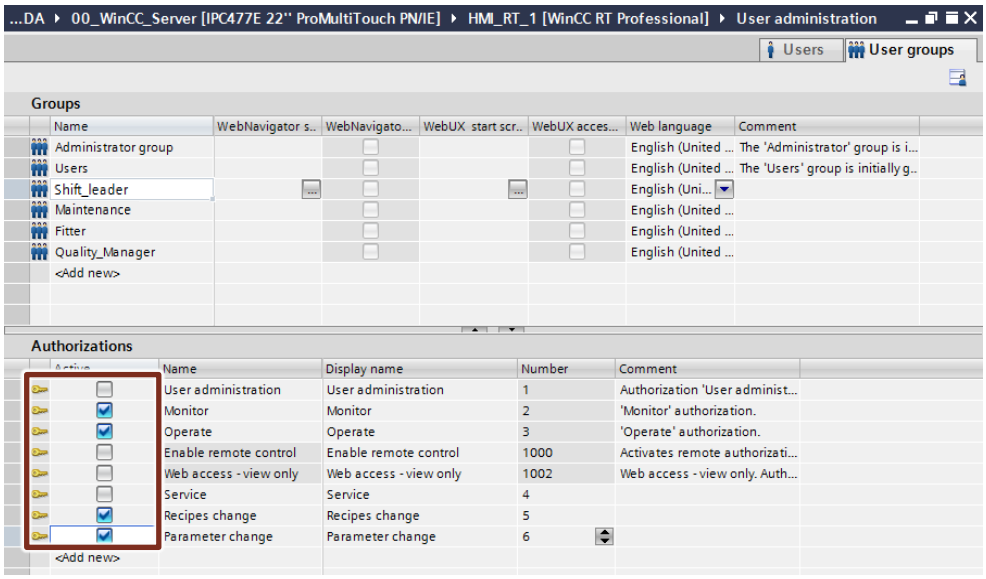


© Siemens AG 2021 All rights reserved

3. Assign the following permissions to the Shift Supervisor user group by clicking the checkboxes next to the labels:
   - Monitoring
   - Change recipes
   - Changing parameters

Note Enabling the checkbox again deactivates the permission again.

Figure 4-20



Note The "User Administration" permission is the first permission number by default. User groups with this permission can manage all users in Runtime via the "User Control".

4. Then, select the other user groups one after the other and assign them the corresponding permissions, see Table 4-1.
5. Save your project.

Result

The configuration of the user administration is now complete.

© Siemens AG 2021 All rights reserved

4.1.4 Optional: Dynamic logon

In WinCC TIA Portal it is possible to activate "Dynamic Login".

This login procedure is used to automatically log a user in by setting a system variable on the Operator Panel.

For example, you could create a user with dynamic login for your maintenance personnel. The corresponding system variable could be set by a key switch for which only the responsible maintenance personnel have the keys.

The maintenance staff can thus log on quickly when the system arrives, perform their tasks and log off automatically by deactivating the key switch.

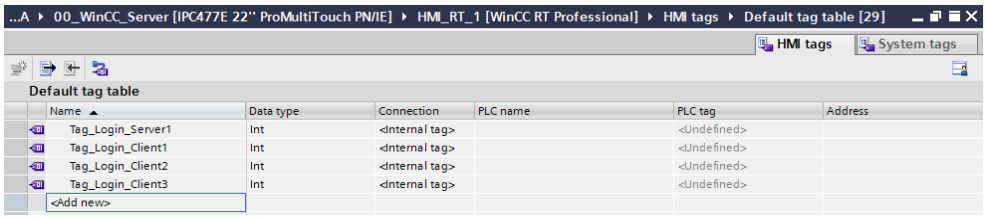
To configure the "Dynamic Logon" of your system, carry out the following configuration steps.

Note Make sure that the "Dynamic Logon" can only be configured for the individual devices if the HMI and Ethernet connections have been set up correctly.

1. Create an internal tag of type "Integer" for each Operator Panel in the tag management of your server.

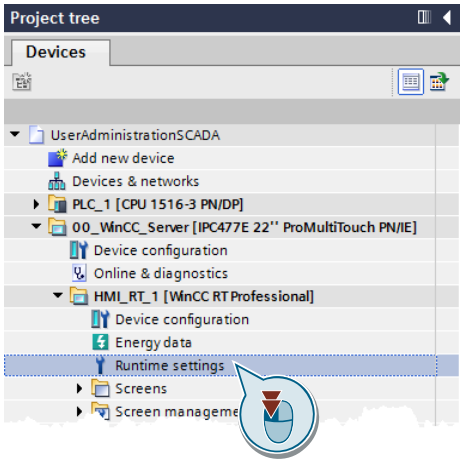
Note The tags used must be binary coded and have at least 8 characters.

Figure 4-21



2. Open the "Runtime settings" of your WinCC Server via the project navigation.

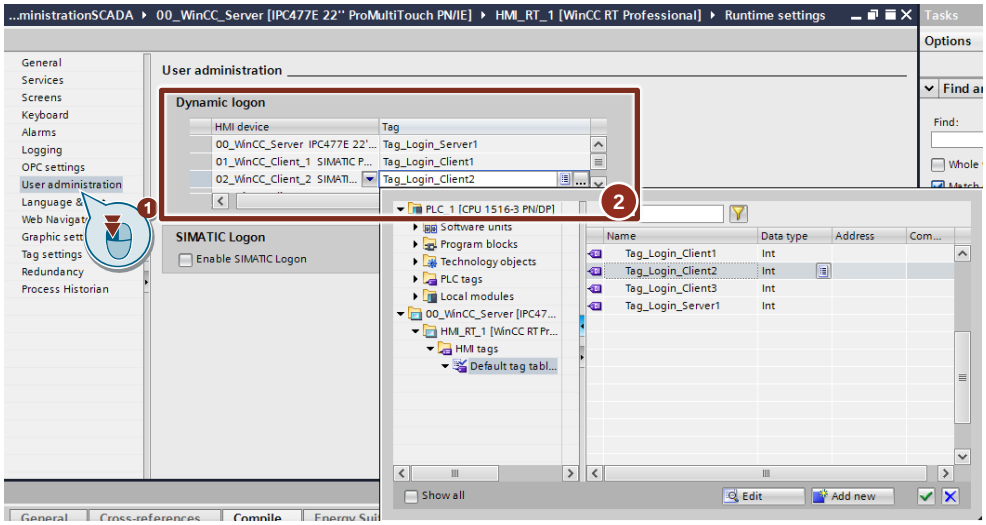
Figure 4-22



© Siemens AG 2021 All rights reserved

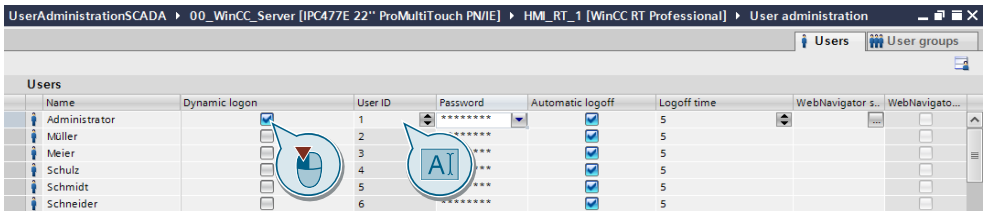
3. Click on "User administration" in the area navigation (1). In the field "Dynamic Logon" in the first column "HMI device", assign the devices that you want to enable for dynamic login. In the "Tag" column, select the variables that you have created for the individual devices (2).

Figure 4-23



4. You must then activate the users for dynamic login and give them a specific "User ID".
   Open the user configuration under "User administration > Users". Enable the checkbox for dynamic logon for the user (1). The "User ID" is used to identify the user. If necessary, you can also change these.

Figure 4-24



The user is automatically logged into the corresponding device if one of the tags that you assigned to the HMI Operator Panels in step 3 corresponds to the value of the user ID of the user. You then have to set and reset these with an event. A key switch, for example, is recommended for this purpose.

Note

The user remains logged in as long as the tag for the "Dynamic Logon" of the Operator Panel has the value of his "User ID". If the value 0 is assigned to the tag, no user is logged on to the device.

Result

The configuration of the dynamic login is complete.

© Siemens AG 2021 All rights reserved

4.2 Configuration of Access Protection and User Display

This section shows how to create access protection for a function (e.g. operating a button) and how operators can log in and log out using system functions.

In addition, an example will explain how to display the currently logged in user and how to configure or operate the user display.

Requirement

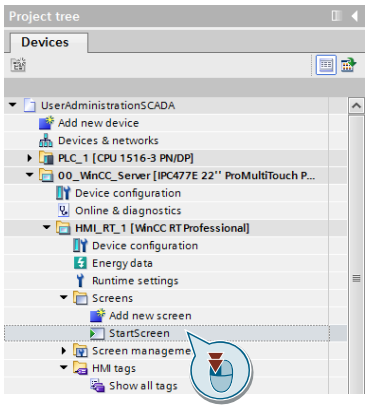
- Created TIA Portal project with at least one configured Operator Panel
- Configured user administration with users, user groups and corresponding permissions

4.2.1 Configuration of Access Protection

The following table describes how to provide the function of a button with access protection.

1. Open a screen, e.g., the Start Screen, and insert a button from the toolbox.

Figure 4-25

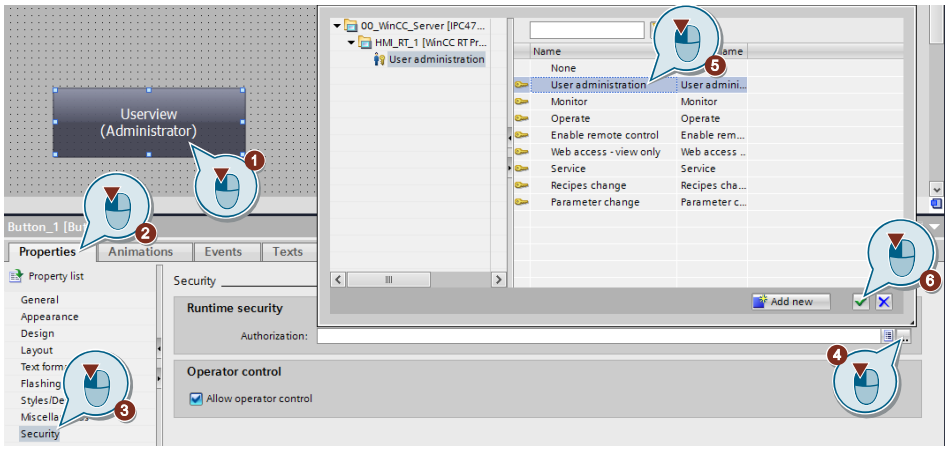


© Siemens AG 2021 All rights reserved

2. Select the button by clicking on it (1). In the "Properties" tab (2), open the "Security" item (3) by clicking it.
   Under "Runtime security", click the extension field (4). Select the "User administration" permission (5) from the context menu.

   Confirm your selection with the green check mark (6).

Figure 4-26



3. Save your project and transfer it to the Operator Panel.

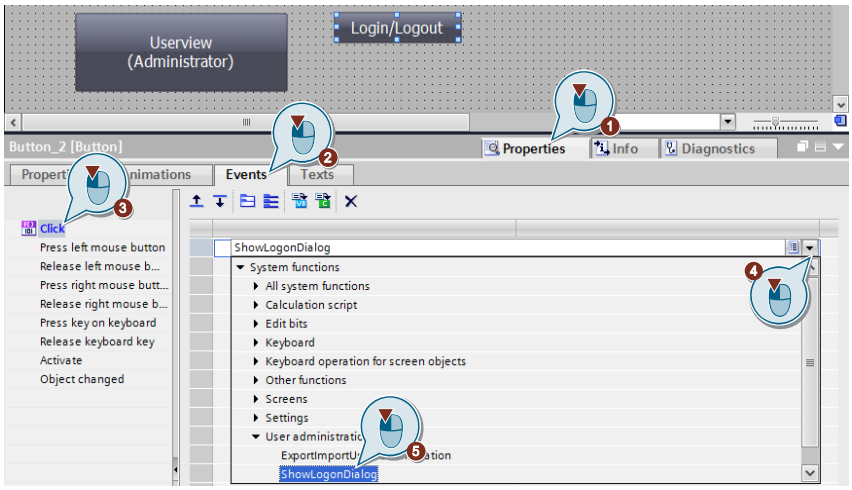
4.2.2 Login and Logout with System Functions

The following section describes how to log in and out centrally using the system functions "ShowLogonDialog" and "Logout".

In order to log on/off a user to the Operator Panel, you need a button that displays the logon window.
Create another button for this. In the "Properties" (1), open the "Events" tab (2). Select the event "Click" (3) and assign the function "ShowLogonDialog" (5) from the predefined functions in the drop-down list (4).

The logon dialog is therefore completely configured.

Figure 4-27



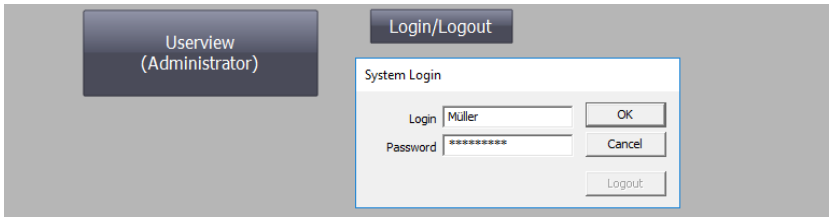
© Siemens AG 2021 All rights reserved

Behavior in Runtime

In Runtime, press the "Login/Logout" button to open the login dialog. The user can authorize himself in this dialog. An incorrect login results in a system message with the following message: "Invalid password or username. Login failed." appears in the message display.

Note If the login is successful, there is no response indicating this on the Operator Panel by default. This must also be configured, see the following section 4.2.3.

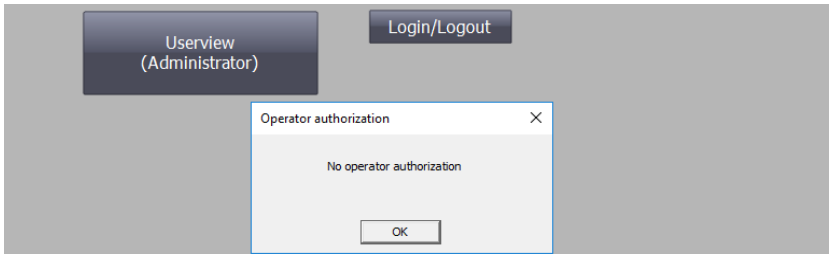
Figure 4-28



If the user is logged in, he can press the button and execute the function behind it.

If a user without sufficient permissions presses the access protected button, the function is not executed. Instead, the following system message appears: "No operator authorization".

Figure 4-29

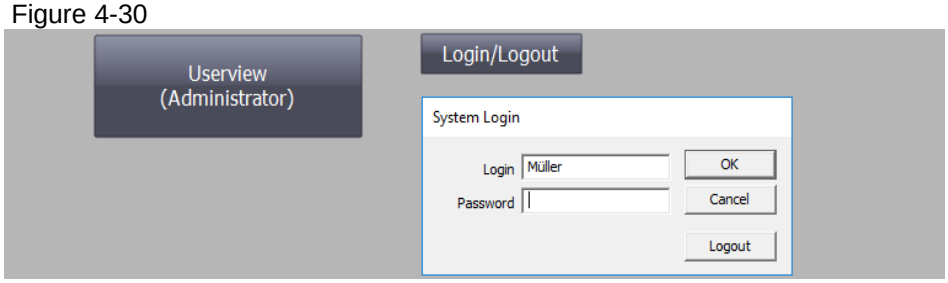


To log off the system again, the user clicks the "Login/Logout" button again. If an authorized user is logged in, the input fields "Username" and "Password" are grayed out. The previously grayed out button "Logout" is now clearly displayed.

The user can now log out by clicking on the "Logout" button. The device is now free again for a new login of a user.

Note Only one user can be logged into Runtime at a time. If another user is logged in, the previously logged in user is automatically logged out.

Figure 4-30



© Siemens AG 2021 All rights reserved

4.2.3 Display of the Currently Logged-In User

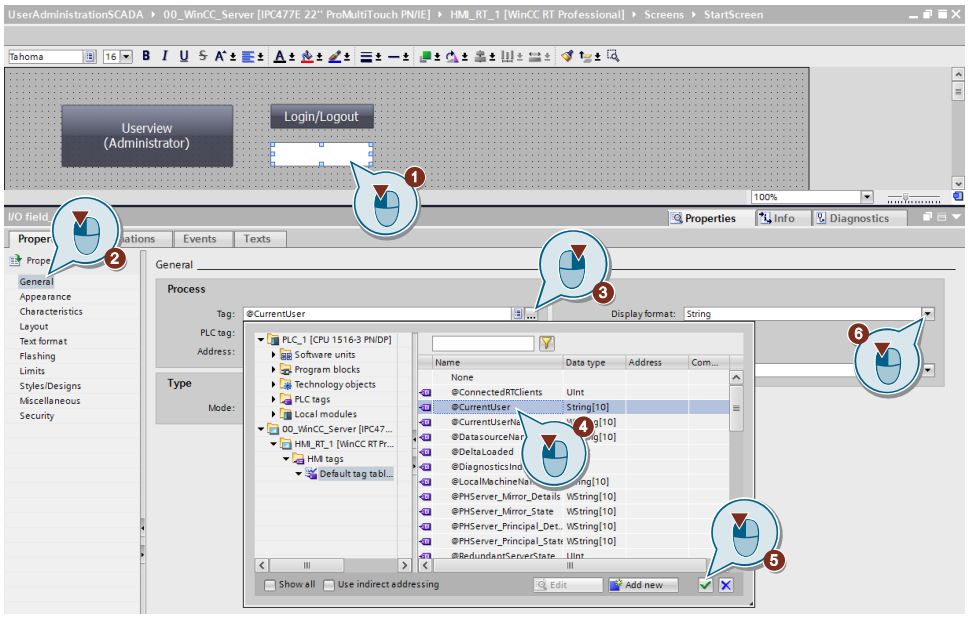
Further configuration steps are required in order to receive a response from the Operator Panel in Runtime as to whether a user has been successfully logged on or logged off or which user is currently logged on.

The following table describes how you can configure this using an I/O field.

Requirement

As a requirement, the login and logout of a user must already be configured, as described in Section 3.3.2.

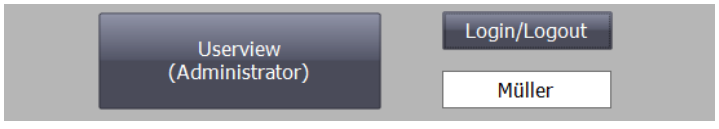
1. Open your created image with the name "StartScreen" and insert a new "I/O field".
2. Select the field (1). Switch to "Properties > General" (2).
   Open the drop-down list of the property "Variable" ("Tag") (3) and select the variable "@CurrentUser".
   Confirm your selection with the green check mark (5).
   Change the "Display format" to the data type "String" (6).
   Figure 4-31



Behavior in Runtime

After successful login, the name of the currently logged in user appears in the "I/O Field".

Figure 4-32



If the user logs off again, the username is removed from the "I/O field".

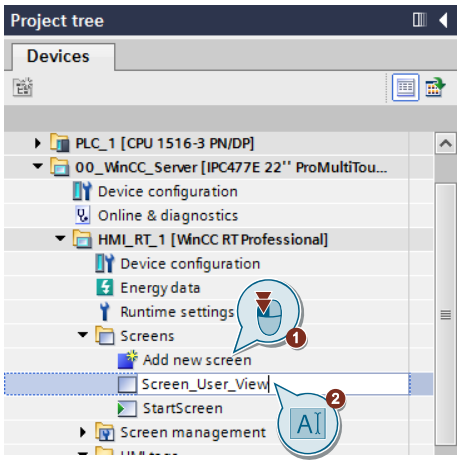
© Siemens AG 2021 All rights reserved

4.2.4 User Display and Operation

This section shows you how to use the "User view". This Control gives you an overview of the users existing in the project, as well as the possibility to administer them. For more information, see the "Behavior in Runtime" sub-section of this section.

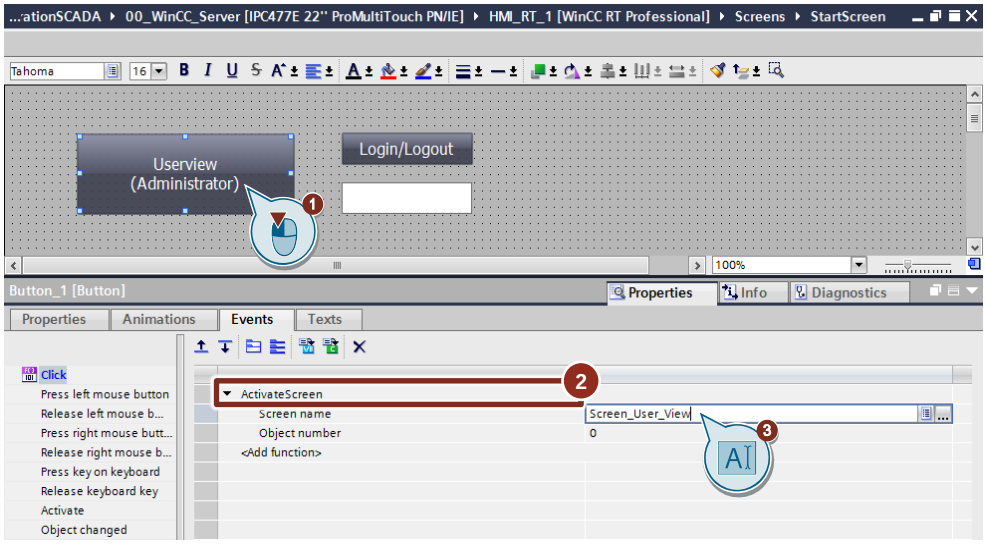
1. Double-click the "Add new screen" button to create a new HMI image (1) and rename it to "Screen_User_View" (2).

Figure 4-33



2. Open the Start Screen.
   Select the button "Userview (Administrator)" (1).
   Add the function "ActivateScreen" to the settings of the button under "Properties > Events > Click" (2). Enter the name of the inserted image "Screen_User_View" (3) in the parameter "Image name" ("Screen name").

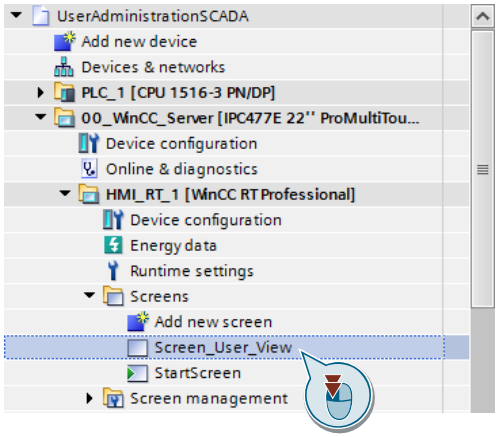
Figure 4-34



© Siemens AG 2021 All rights reserved

3. Open the image "Screen_User_View" with a double click.

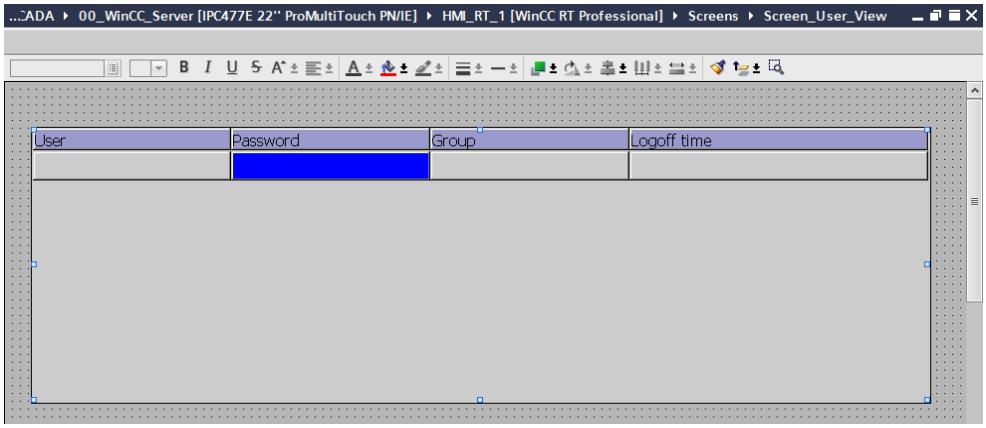
Figure 4-35



4. Open the task card "Toolbox" and expand the Controls palette.

   Select the "User view" Control and drag and drop it into the image. Adjust the format and size if necessary.

Figure 4-36



5. Save the project and transfer it to the Operator Panel.

© Siemens AG 2021 All rights reserved

Behavior in Runtime

Within Runtime, an administrator can log on and access the user display. As an administrator, you see all users created in the project. You can change the associated user data and add or delete new users.

Note Users without administrator rights can also access the user display, but they only see themselves in the user display. You can double-click on your entry to open a window in which you can set your password and logout time.

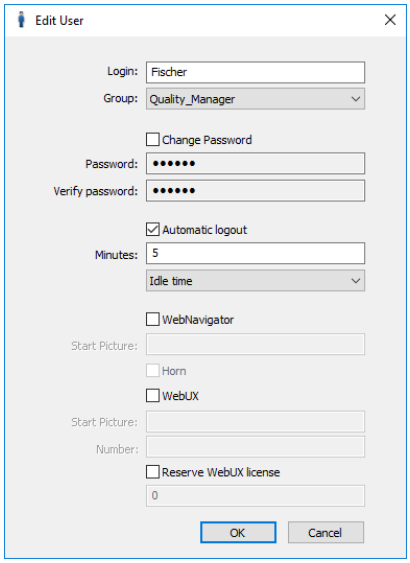
Figure 4-37

User	Password	Group	Logoff time
Fischer	******	Quality_Manager	After 5 minutes of inactivity
Schneider	******	Schift_leader	No
Schmidt	******	Fitter	After 5 minutes of inactivity
Schulz	******	Maintance	After 5 minutes of inactivity
Meier	******	Schift_leader	After 5 minutes of inactivity
Müller	******	Administrator group	After 5 minutes of inactivity
Administrator	******	Administrator group	After 5 minutes of inactivity

6. Change user data

In the user display, the administrator can change a user's data. A double click the user in the user display opens the Configuration window with the respective data. The editable data and permissions are the same as those you have when creating the project.

Figure 4-38



© Siemens AG 2021 All rights reserved

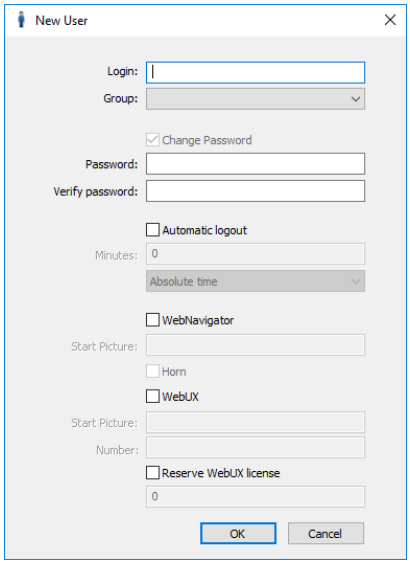
7. Add/Delete User

As an administrator, you can add or remove new users to the user administration using the user display in Runtime.

To add a new user, double-click an empty row in the user display. A Configuration window opens automatically, in which you can create the new user with password, logon name and access permissions.

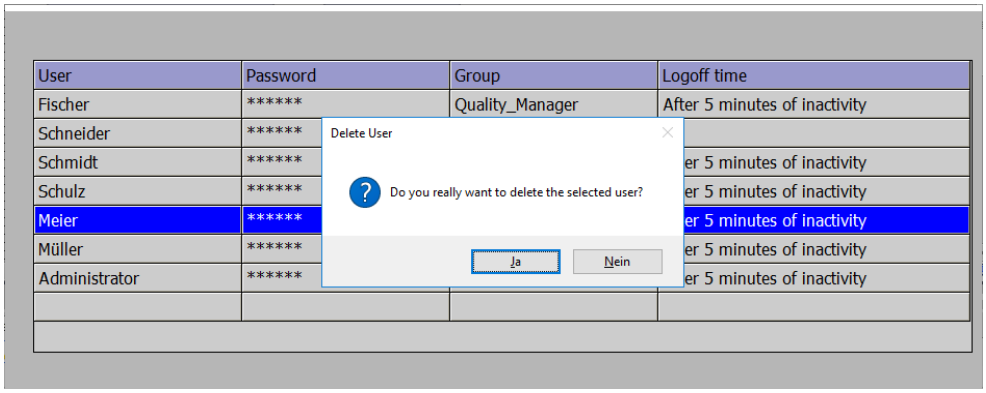
After you have created the user, you see his or her entry in the user display.

Figure 4-39



To delete a user from the user administration, select the user by clicking on the entry in the user display and press the <Del> key. You must then confirm the removal of the user in a dialog box

Figure 4-40



© Siemens AG 2021 All rights reserved

5 Central User Administration with "SIMATIC Logon"

This section describes how to configure the central user administration with "SIMATIC Logon" and how to use it in WinCC Professional.

"Simatic Logon" can be set up

- locally, or via a separate logon server, or
- for one domain

.

Logon server

Setup is identical whether on the local computer or as a separate logon server (see Section 5.2). In both cases, the respective users and user groups must be created in the Windows User Administrator. In addition, the installation of "SIMATIC Logon" is required on the local computer or logon server.

Domain Controller

It is not necessary to set up or install "SIMATIC Logon" on a Domain Controller. The respective users and user groups are managed by the system administrator in the "Active Directory" of the domain.

You can find further information on this in Section 5.3.

© Siemens AG 2021 All rights reserved

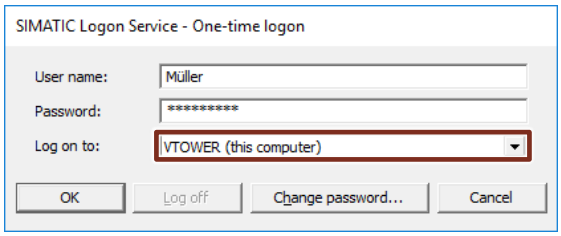
Functionalities with "SIMATIC Logon"

- The logon server of "SIMATIC Logon" or a Domain Controller can be used for user administration across projects. This saves time when configuring widely distributed systems.
- The login data is synchronized. When an owner changes their password on a machine, it is also changed on the logon server or Domain Controller.
- You can quickly create new users, assign permissions, or delete old users via the logon server or Domain Controller.
- From this point on, the functions for creating, deleting, and editing users must be carried out via the "Computer Administration > Users and Groups" or, in the case of a Domain Controller, in the "Active Directory".
- A log file is created, which records every login and logout in WinCC. This log can be accessed via the path "Desktop > SIMATIC Logon > SIMATIC Logon Eventlog Viewer".

Behavior in Runtime

- Within Runtime, the user can log on with the Windows logon data created.
- The user is automatically assigned to the WinCC group, which has the same name as the Windows group to which he belongs. They, therefore, also receive all permissions of the WinCC user group.
- When logging in with the "SIMATIC Logon" login window, you must also select the logon server or the Domain Controller.

Figure 5-1



5.1 Preparation for the Use of "SIMATIC Logon"

Note

In this example the default settings of "SIMATIC Logon" are used.

- To configure the settings of "SIMATIC Logon", you must be a member of the Windows group "Logon_Administrator".
- You must also be a member of the Windows Administrators or Power Users group.
- Via the path "Windows Desktop > SIMATIC Logon > SIMATIC Logon configure" you reach the configuration menu with the help of your login data.

Requirement

The configuration steps for local user administration (see Section 4) have been implemented.

Note

The users created in WinCC are not required by "SIMATIC Logon" and, therefore, do not have to be configured.

Procedure

The following steps are necessary to create the central user logon with "SIMATIC Logon":

1. Install "SIMATIC Logon" on each Operator Panel.
2. Create and assign permissions in WinCC (TIA Portal).
3. Create user groups in WinCC (TIA Portal).
4. Activate "SIMATIC Logon" in WinCC (TIA Portal).
5. Make the logon server or the Domain Controller known to the Operator Panels via "SIMATIC LOGON" configuration.

© Siemens AG 2021 All rights reserved

5.1.1 Creating User Groups in WinCC (TIA Portal)

Configuring user groups in WinCC (TIA Portal) is described in detail in this application example, see Section 4.1.2.

5.1.2 Creating and Assigning Permissions in WinCC (TIA Portal)

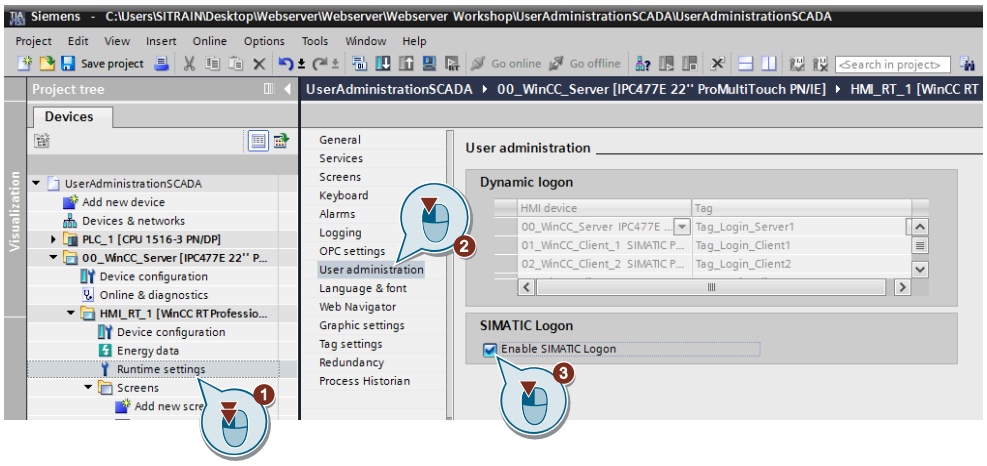
Creating and assigning permissions in WinCC (TIA Portal) is described in detail in this application example, see Section 4.1.3.

5.1.3 Activate "SIMATIC Logon" in WinCC(TIA Portal)

To complete the user administration with "SIMATIC Logon", you have to activate it in WinCC (TIA Portal). The following instructions will show you which steps are necessary.

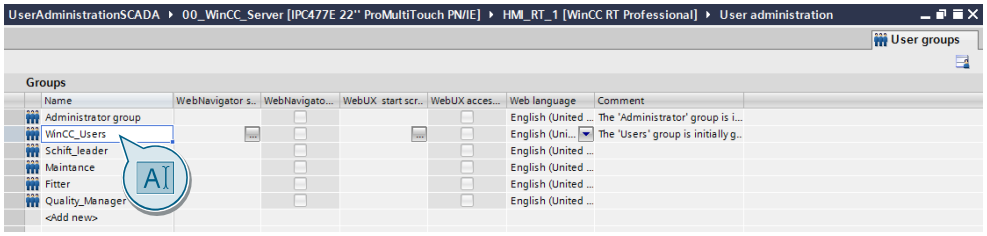
1. Open the "Runtime settings" of the WinCC Server with a double click (1). In the "Runtime settings", switch to the "User administration" options (2). Enable the checkbox "Enable SIMATIC Logon" (3).

Figure -2



2. In the "User administration" of WinCC (TIA Portal), rename the user group "Users" to "WinCC_Users".

Figure 5-3



Result

You have successfully activated "SIMATIC Logon" and adapted the groups in WinCC (TIA Portal) to those of Windows.

© Siemens AG 2021 All rights reserved

Note

Enabling "SIMATIC Logon" has the following effects on your project:

- The dynamic logon is deactivated.
- The "User" option in the "User administration" is hidden.
- The WinCC login window is replaced by that of "SIMATIC Logon".
- The "User view" Control loses the functionality for editing individual users. The corresponding symbols are grayed out.

© Siemens AG 2021 All rights reserved

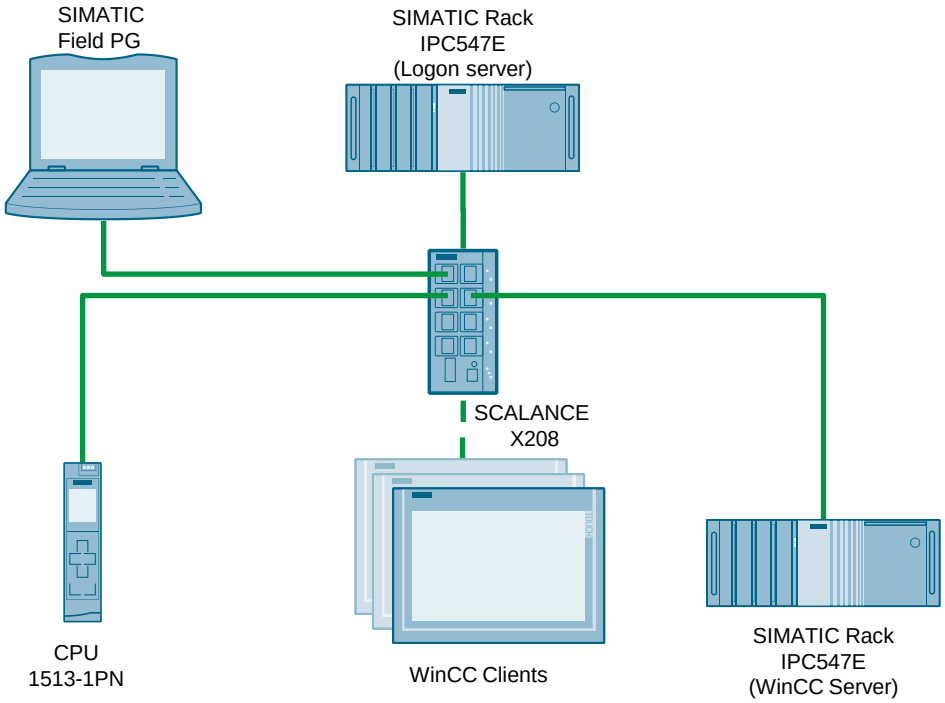
5.2 "SIMATIC Logon" as Logon Server

This Section shows you how to configure a "SIMATIC Logon" logon server and use it for user administration in WinCC (TIA Portal).

Central user administration with a logon server

The following figure shows the structure of the application example in connection with the central user administration with a logon server.

Figure 5-4



Note The WinCC Server and the logon server can also be set up together on a PC system.

© Siemens AG 2021 All rights reserved

CAUTION	**If the "SIMATIC Logon" logon server fails, it may no longer be possible to log into the Operator Panels via "SIMATIC Logon".** To enable logging into the Operator Panels nevertheless, proceed as follows: • In the "General" tab of the "Configure SIMATIC Logon" dialog box, you can activate and change the "Default User". • In contrast to all other users, the "Default group" and the "Default user" cannot be listed in the Windows User Administrator. The "Default User" is a member of the "DefaultGroup" and "Emergency_Operator" roles and continues to enable operation of the system in the event of a failure of the "SIMATIC Logon" logon server.

Requirement

The preparations for the use of "SIMATIC Logon" (see Section 5.1) have been implemented.

Procedure

The following steps are necessary to create the central user logon with "SIMATIC Logon":

1. Creating Users in Windows User Administration.
2. Creating User Groups in Windows User Administration and Assigning Users.

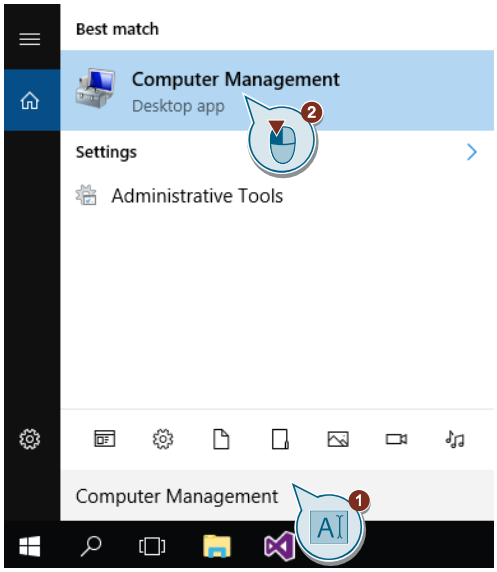
© Siemens AG 2021 All rights reserved

5.2.1 Creating Users in Windows User Administration

Carry out the following configuration steps on the system that is to act as the logon server.

1. Open the Windows Search and enter the term "Computer Management" in the search box (1). Click the Computer Management entry to open it (2).

Figure 5-5

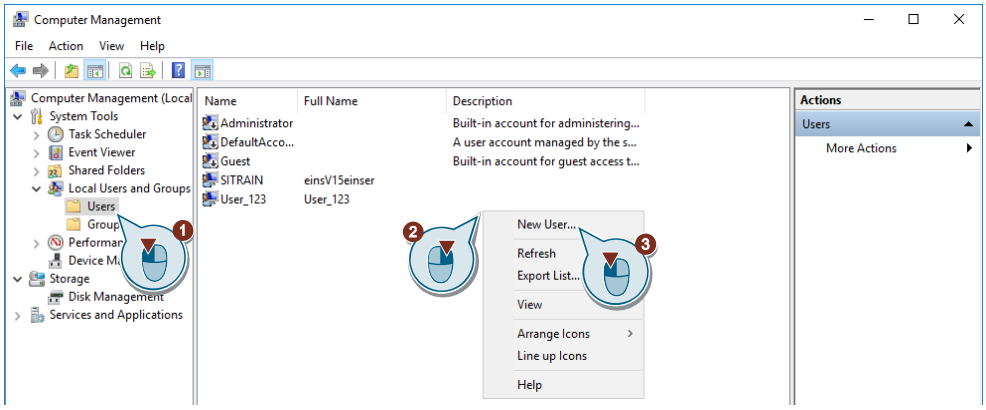


2. Expand the list "Local Users and Groups" with one click and select the folder "Users" (1).

   In the middle area of the Management Console you can see the currently created users.

   Right-click on an empty space in the middle area of the Management Console (2) and click on "New User..." in the context menu (3).

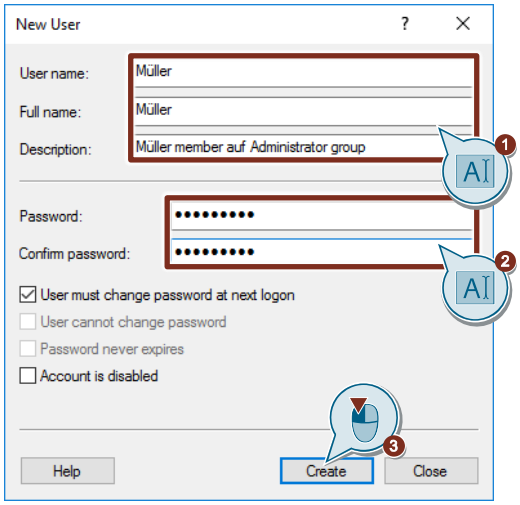
Figure 5-6



© Siemens AG 2021 All rights reserved

3. A window for creating a new user opens. Enter the login name, the name and a description of the user (1). Enter a password for the user and confirm this (2). Finish creating the user by clicking on the "Create" button (3).

Figure 5-7



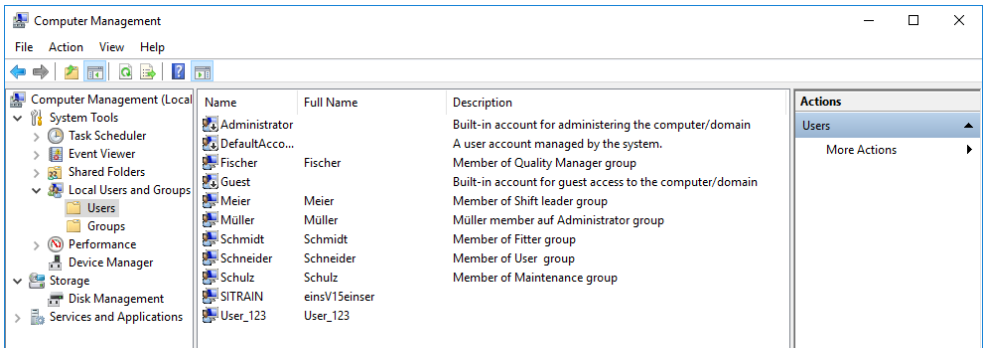
Note After pressing the "Create" button, the user is created in the background. To see the newly created user in the user administration, you must close the "New user" dialog.

4. Repeat steps 3 and 4 to create the five other users (Meier, Schmidt, Schulz, Fischer, Schneider).

Result

You have successfully created all users on the Windows computer.

Figure 5-8

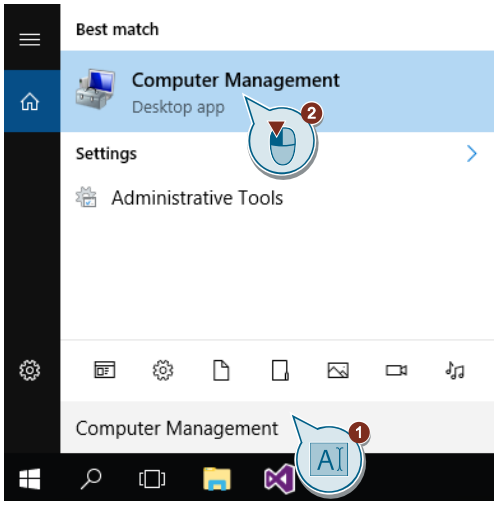


© Siemens AG 2021 All rights reserved

5.2.2 Creating User Groups in Windows User Administration and Assigning Users

1. Open the Windows search and enter the term "Computer Management" in the search field (1). Click the Computer Management entry to open it (2).

Figure 5-9

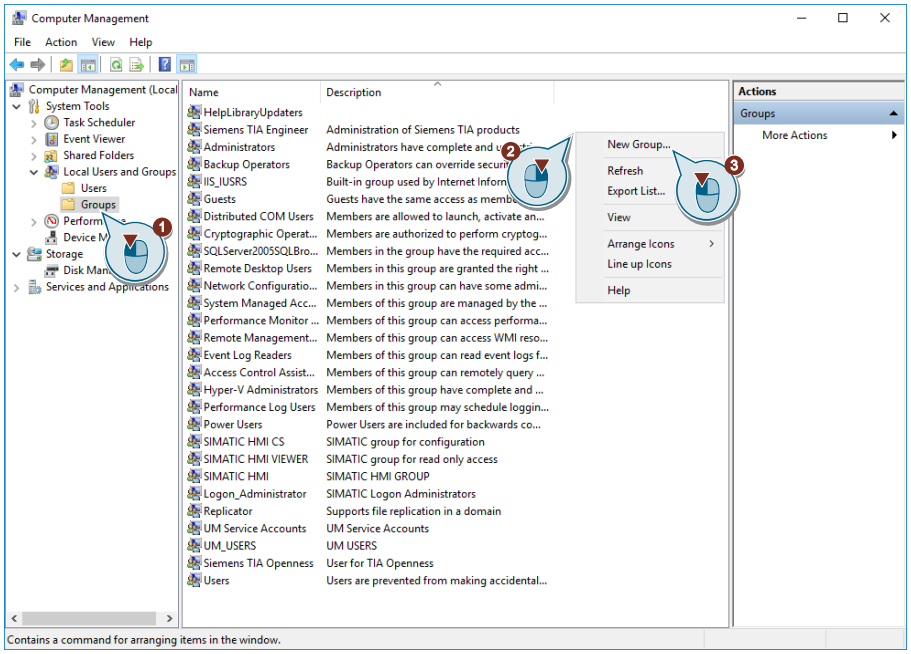


2. Click to expand the "Local Users and Groups" list and select the "Groups" folder (1).

   In the middle area of the Management Console, you can see the groups that are currently created.

   Right-click on an empty space in the middle area of the Management Console (2) and click on "New Group..." in the context menu (3).

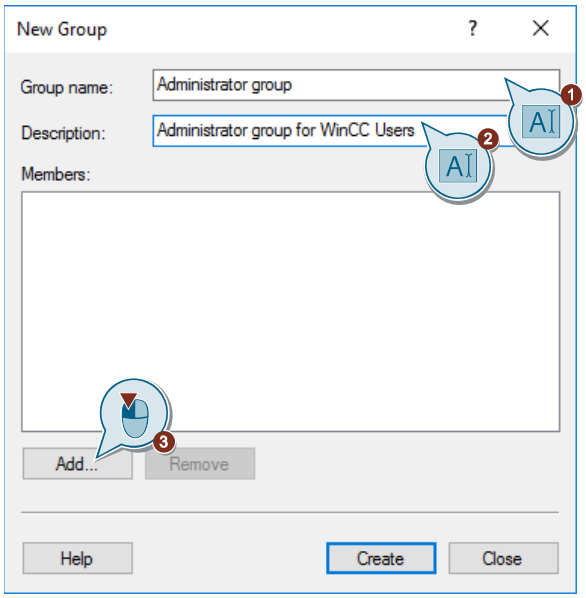
Figure 5-10



© Siemens AG 2021 All rights reserved

3. Enter the name (1) and, if necessary, the description (2) of the user group. Then click on "Add..." under "Members" (3).

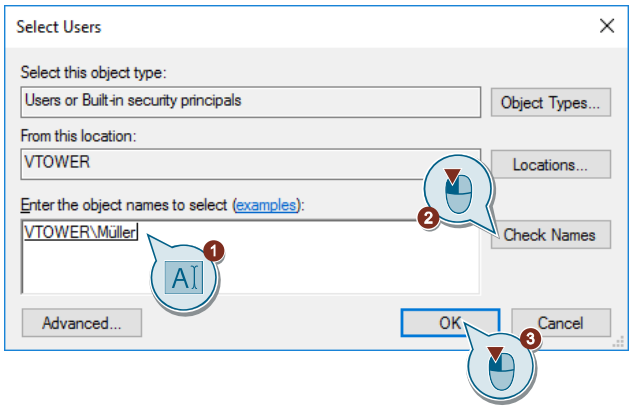
Figure 5-11



Note Make sure that the names of the group names are identical between the user groups in Windows and the user groups in WinCC. The default groups provided by Windows always have the English name.

4. Enter the names of the users you want to assign to the group (1). Then click on the "Check Names" button (2). If the names are entered correctly, they are displayed with the corresponding host name and underlined after the check. When you have finished selecting users, click on the "OK" button (3).

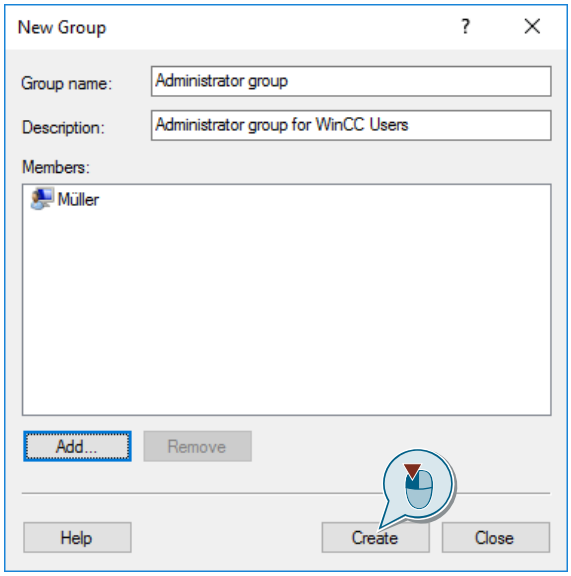
Figure 5-12



© Siemens AG 2021 All rights reserved

5. In the Create window, click the Create button.

Figure 5-13



6. Create five additional user groups (shift supervisor, maintenance, setup technician, quality management, WinCC_Users) according to Table 4-1 and assign the respective users to the groups.

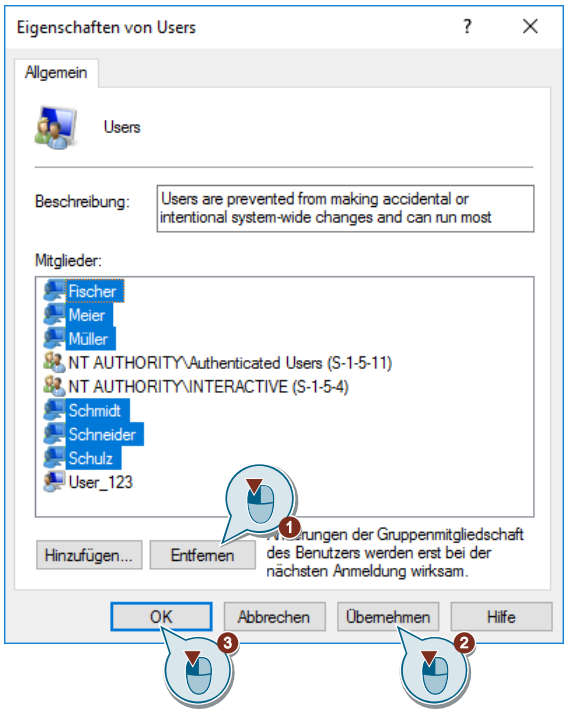
CAUTION	**Prevent Windows users from operating the system**
	The "User" user group is created by default in Windows. All newly created Windows users are automatically assigned to this group. In WinCC, each user may only be assigned to one group. For this reason, the users who are to belong to another WinCC group must be removed from it. If you also use the Windows group "Users" in the WinCC user administration, all Windows users have the option of logging on to WinCC and operating your automation system and causing damage if necessary. It is recommended to remove all WinCC users from the Windows Users group and to create a standard Windows user with a login for all WinCC users. In the WinCC user administration you should rename the group "Users" to "WinCC_Users" and create a separate group with the same name in Windows. You can then assign all "Operators" to this group. This ensures separation between Windows and WinCC users and only authorized personnel can operate the system.

© Siemens AG 2021 All rights reserved

7. Open the user group "Users" and select the users Fischer, Meier, Mueller, Schneider, Schmidt and Schulz.
   Then click on "Remove" (1) and confirm with the buttons "Apply" (2) and "OK" (3).

Note Users who do not belong to the Windows Users group or the Administrators group can no longer log on to Windows. It is recommended that you configure a general user with auto-login function for logging into Windows.

Figure 5-14



Note A user can be a member of several user groups on the logon server at the same time. In the WinCC project, however, it may only be known to one of these user groups.
Otherwise, a message is displayed on the Operator Panel in Runtime that the user cannot be explicitly assigned to a user group. The logon process fails.

Users who are not members of the Windows Users or Administrators groups can no longer log into Windows with their login data.

Result

You have successfully created all user groups for WinCC in Windows and assigned the corresponding users.

© Siemens AG 2021 All rights reserved

5.3 Windows Domain Controller as Logon Server

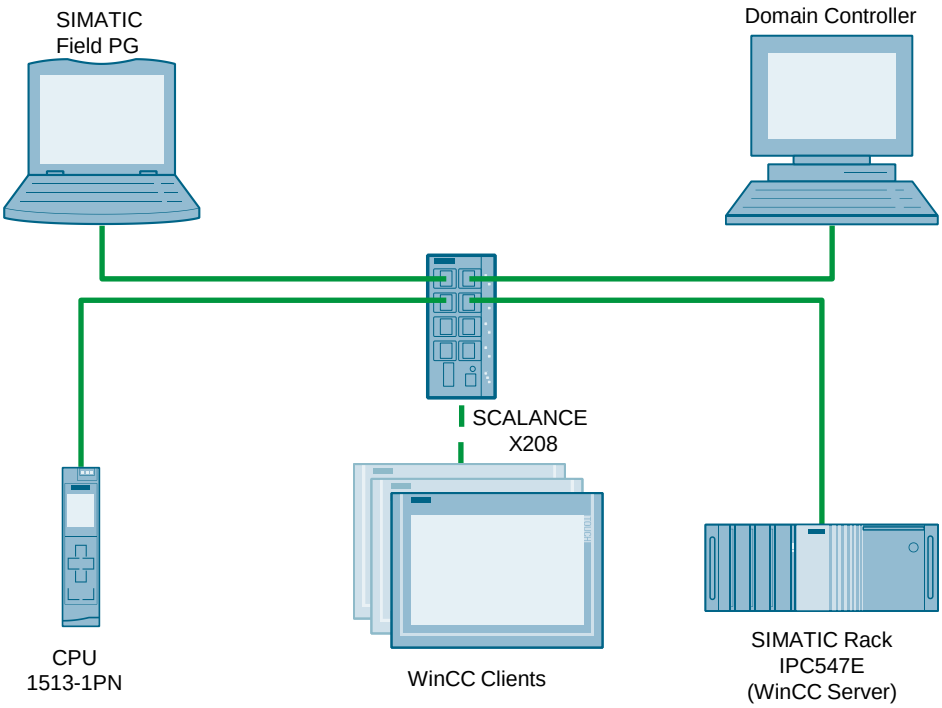
This Section shows you how to configure "SIMATIC Logon" in connection with a Domain Controller and how to use it for user administration in WinCC (TIA Portal).

Note For more information about operating WinCC in a domain environment, see the following entry: https://support.industry.siemens.com/cs/ww/en/view/78346833

Central User Administration with a Domain Controller

The following figure shows the structure of the application example in connection with the central user administration and a Domain Controller.

Figure 5-15



© Siemens AG 2021 All rights reserved

CAUTION	**If the Domain Controller fails, it may no longer be possible to log into the Operator Panel via "SIMATIC Logon".** To enable logging into the Operator Panels nevertheless, proceed as follows: • In the "General" tab of the "Configure SIMATIC Logon" dialog box, you can activate and change the "Default User". • In contrast to all other users, the "Default group" and the "Default user" cannot be listed in the Windows User Administrator. The "Default User" is a member of the roles "DefaultGroup" and "Emergency_Operator" and allows the system to continue to be operated if the Domain Controller fails.

Requirement

The preparations for the use of "SIMATIC Logon" (see Section 5.1) have been implemented.

Procedure

The following steps are necessary to create the central user logon with "SIMATIC Logon":

1. Create a domain group.
2. Create domain users and assign them to a domain group.
3. Assign the following authenticated user permissions to the users of the domain:
   - "Read"
   - "Change password"

Note	The installation and operation of WinCC in a Microsoft domain environment is described in this application example: https://support.industry.siemens.com/cs/ww/en/view/78346833 Creating a domain group is described in Section 2.8 of the included manual. Creating domain users and assigning them to a domain group is described in Section 2.9 of the included manual.

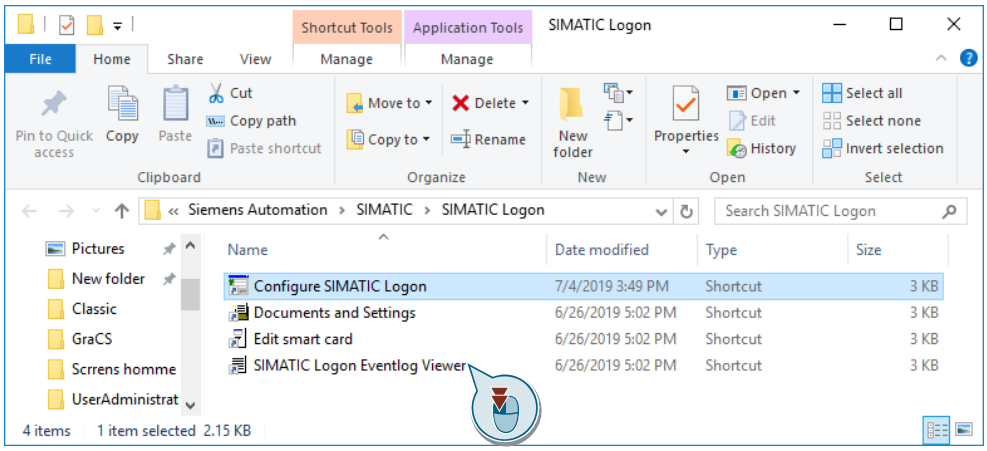
© Siemens AG 2021 All rights reserved

5.4 Traceability and Advanced Diagnostic Data

5.4.1 Traceability

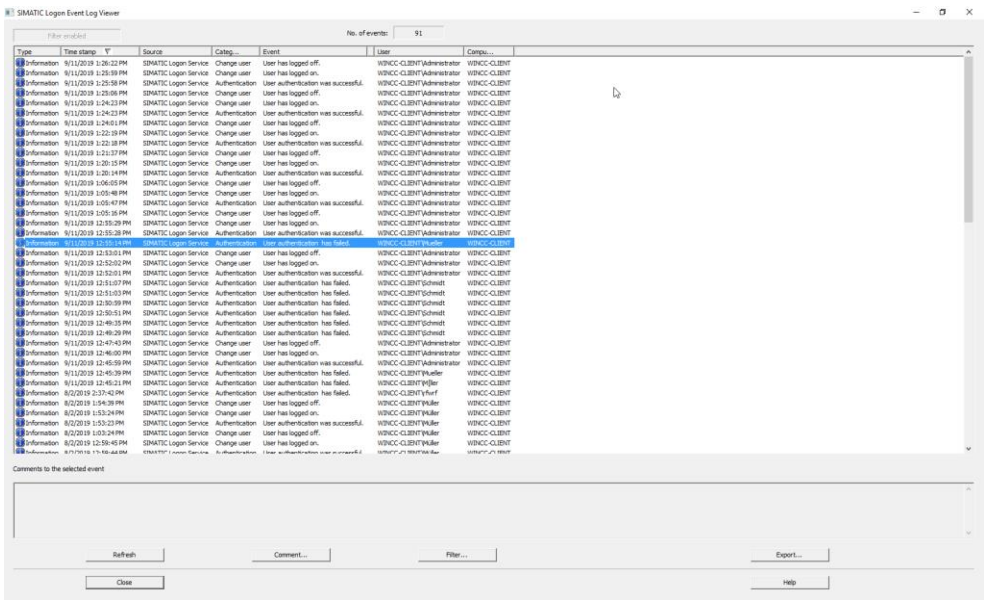
As an additional option, all logon and logoff attempts, user authentications and password changes are recorded in the supplied software component ""SIMATIC Logon" Eventlog Viewer". This allows logon times and important operator entries to be traced back.

Figure 5-16



The following figure shows an example of an event log in the "SIMATIC Logon Eventlog Viewer".

Figure 5-17



© Siemens AG 2021 All rights reserved

5.4.2 Diagnostic Data

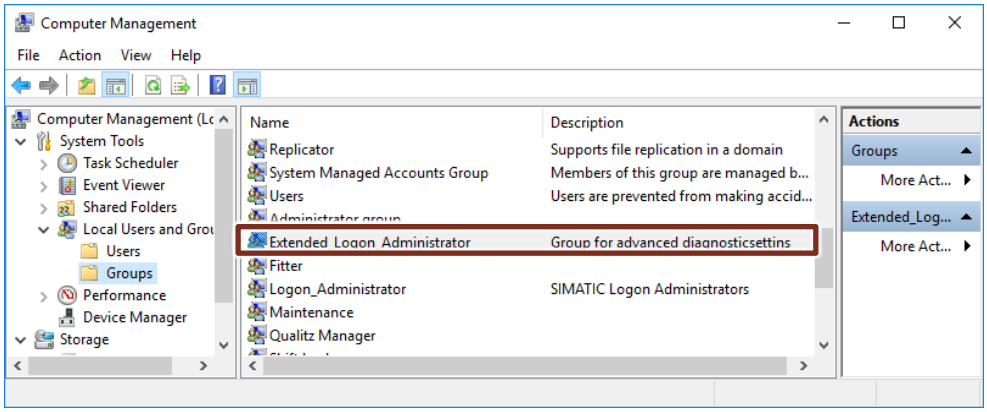
It is possible to activate extended diagnostic data in the SIMATIC logon configuration. These can help to detect problems in case of complications when logging in via SIMATIC Logon (e.g. long login times).

To activate this diagnostic data, follow the instructions below.

1. In Computer Management, create a new Windows user group called "Extended_Logon_Administrator". You can read about how to create a user group in Windows in Section 5.2.2.

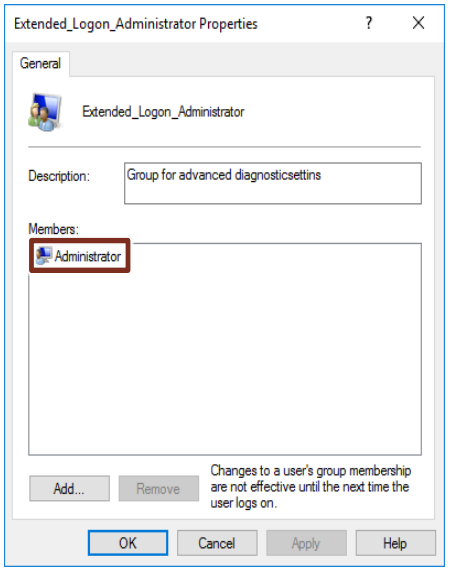
Note Make sure that the name "Extended_Logon_Administrator" of the user group is spelled correctly, otherwise the desired diagnostic functions will not be available.

Figure 5-18



2. Add a Windows user to the user group who you want to have access to the SIMATIC Logon diagnostic data settings. You can also find out how to assign a user to a group in Windows in Section 5.2.2.

Figure 5-19



© Siemens AG 2021 All rights reserved

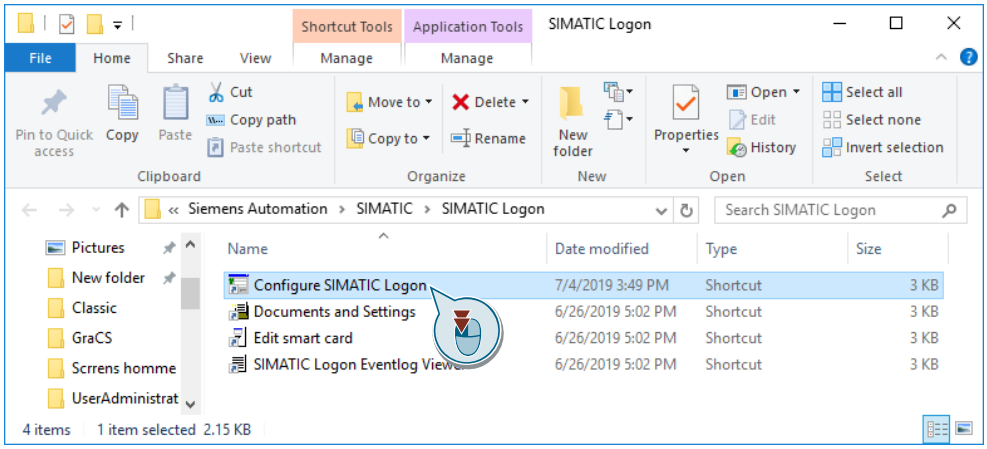
3. Open the configuration of SIMATIC Logon with a double click on the desktop icon "Simatic Logon"

Figure 5-20



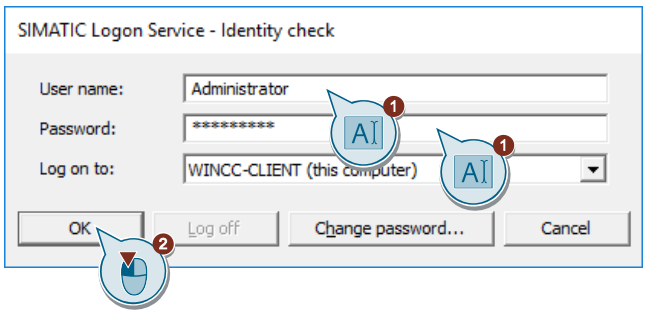
4. The directory with the shortcuts to the SIMATIC Logon Tools is opened. Open the SIMATIC Logon Configuration with a double click on the shortcut "Configure SIMATIC Logon".

Figure 5-21



5. You will be prompted to identify yourself in a login dialog that appears. Enter the login data of the user you have assigned to the Windows group "Extended_Logon Administrator" (1) and confirm with the "OK" button (2).

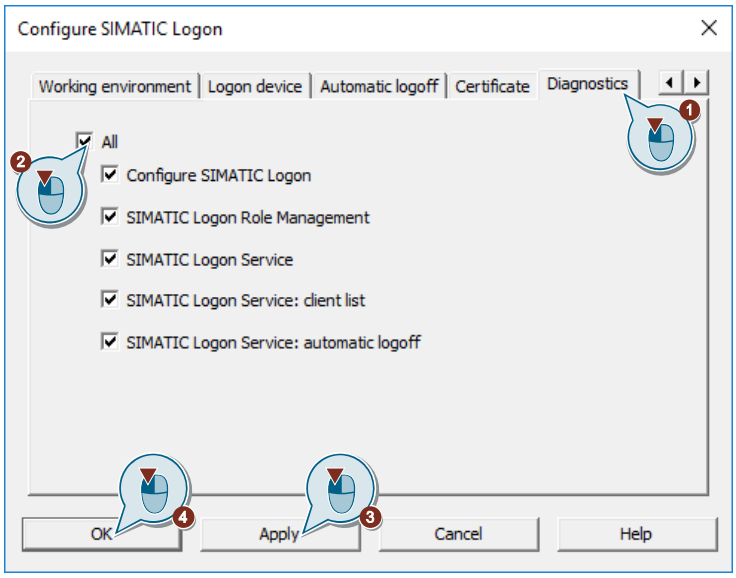
Figure 5-22



© Siemens AG 2021 All rights reserved

6. Due to the settings, a new tab called "Diagnostics" has become visible in the configuration tool of SIMATIC Logon. Select this tab with one click (1) and mark the diagnostic data you want to record (2). Confirm your selection by clicking on the "Apply" button. Close the configuration tool by clicking on the "OK" button (4).

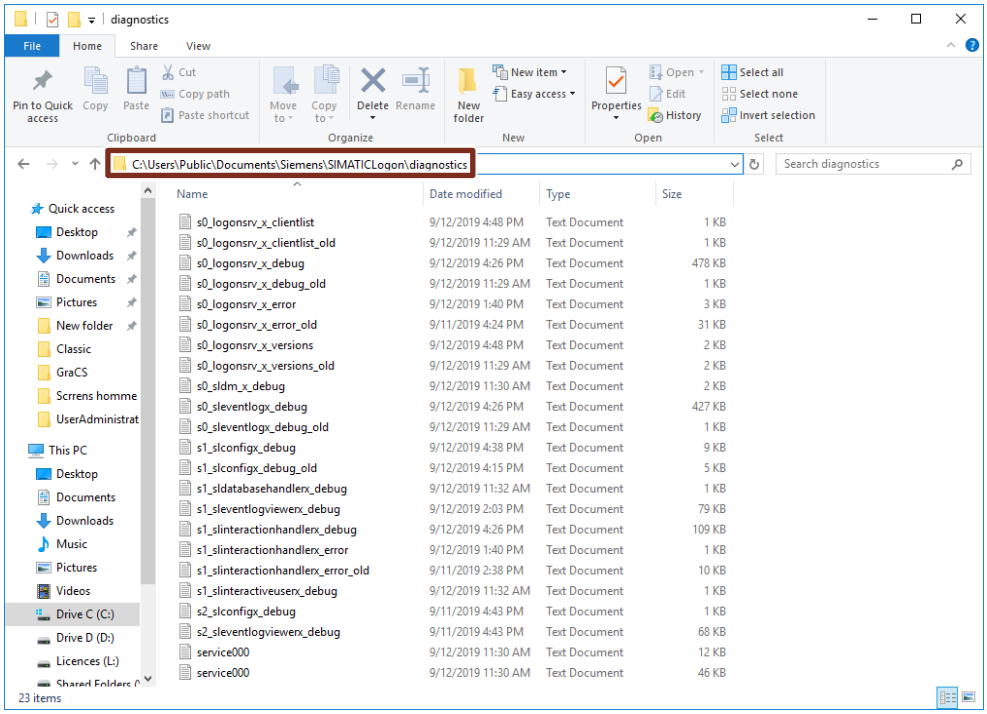
Figure 5-23



Result

You have successfully activated the extended diagnostic data. These can be viewed via the path "C: > Users > Public > Documents > Siemens > SIMATIC Logon > diagnostics".

Figure 5-24



© Siemens AG 2021 All rights reserved

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.

Note

You will learn about the products used in this application example in the courses:

- SITRAIN course: SIMATIC WinCC Professional, SCADA in the TIA Portal (Article ID: 109758618)

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

© Siemens AG 2021 All rights reserved

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 entry page of the application example https://support.industry.siemens.com/cs/ww/en/view/109738532
\3\	Manual: SIMATIC STEP 7 Basic/Professional V16 and SIMATIC WinCC V16 Using the User Administrator https://support.industry.siemens.com/cs/ww/en/view/109773506/126103583499
\4\	Manual: SIMATIC STEP 7 Basic/Professional V16 and SIMATIC WinCC V16 Central user administration with SIMATIC Logon https://support.industry.siemens.com/cs/ww/en/view/109773506/119618863115
\5\	Manual: "SIMATIC Logon" https://support.industry.siemens.com/cs/ww/en/view/109748663/82820955787
\6\	Delivery release PM-LOGON V1.7 https://support.industry.siemens.com/cs/ww/en/view/109779685
\7\	Application example: Installation and operation of WinCC in a Microsoft domain environment https://support.industry.siemens.com/cs/ww/en/view/78346833

© Siemens AG 2021 All rights reserved

6.4 Change documentation

Table 6-2

Version	Date	Modifications
V1.0	07/2019	First version
V1.1	03/2021	Revision regarding SIAMTIC logon in the domain

© Siemens AG 2021 All rights reserved