User Administration in WinCC (TIA Portal)

WinCC V13 SP1 (Basic/Comfort/Advanced),
Basic Panel, Comfort Panel,
WinCC Runtime Advanced V13 SP1

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

Siemens Industry Online Support

Warranty and Liability

Note

The Application Examples are not binding and do not claim to be complete regarding the circuits shown, equipping and any eventuality. The Application Examples do not represent customer-specific solutions. They are only intended to provide support for typical applications. You are responsible for ensuring that the described products are used correctly. These Application Examples do not relieve you of the responsibility to use safe practices in application, installation, operation and maintenance. When using these Application Examples, you recognize that we cannot be made liable for any damage/claims beyond the liability clause described. We reserve the right to make changes to these Application Examples at any time without prior notice.
If there are any deviations between the recommendations provided in these Application Examples and other Siemens publications − e.g. Catalogs − the contents of the other documents have priority.

We do not accept any liability for the information contained in this document.
Any claims against us – based on whatever legal reason – resulting from the use of the examples, information, programs, engineering and performance data etc., described in this Application Example shall be excluded. Such an exclusion shall not apply in the case of mandatory liability, e.g. under the German Product Liability Act ("Produkthaftungsgesetz"), in case of intent, gross negligence, or injury of life, body or health, guarantee for the quality of a product, fraudulent concealment of a deficiency or breach of a condition which goes to the root of the contract ("wesentliche Vertragspflichten"). The damages for a breach of a substantial contractual obligation are, however, limited to the foreseeable damage, typical for the type of contract, except in the event of intent or gross negligence or injury to life, body or health. The above provisions do not imply a change of the burden of proof to your detriment.
Any form of duplication or distribution of these Application Examples or excerpts hereof is prohibited without the expressed consent of the Siemens AG.

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 only form one element of such a concept.
Customer is responsible to prevent unauthorized access to its plants, systems, machines and networks. Systems, machines and components should only be connected to the enterprise network or the internet if and to the extent necessary and with appropriate security measures (e.g. use of firewalls and network segmentation) in place.
Additionally, Siemens' guidance on appropriate security measures should be taken into account. For more information about industrial security, please visit http://www.siemens.com/industrialsecurity.

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends to apply product updates as soon as available and to always use the latest product versions. Use of product versions that are no longer supported, and failure to apply latest updates may increase customer's exposure to cyber threats.
To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed under http://www.siemens.com/industrialsecurity.

Table of Contents

1 Task

1.1 Overview

Introduction

Automation facilities are highly accurate and available systems that play a major role in a company's manufacturing processes. Moreover, the increasing communication within a facility and across multiple facilities makes the overall system more complex. To be able to monitor and operate these facilities accordingly, the processes are visualized through HMI operator panels.

If the facility is operated by unauthorized staff, production can be impaired as a result. What is more, unauthorized persons can directly manipulate the facilities or steal know-how.

To prevent this, all facilities have to be protected against unauthorized access. WinCC (TIA Portal) allows you to implement this feature using the integrated user administration and thus increase the security of the facility.

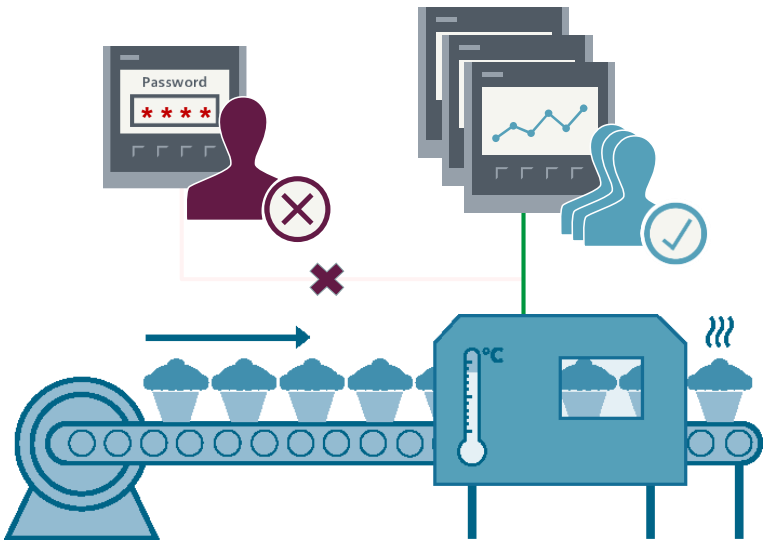
1.2 Requirements

The following illustration gives a brief overview of the requirements for the automation task.

It has to assure that

- authorized staff members can log in.
- multiple staff members can be logged in simultaneously (bigger facilities).
- staff members can access functions and data depending on their authorizations.
- unauthorized persons are denied access to the facility and the data.

Figure 1-1



2 Solution

2.1 Overview

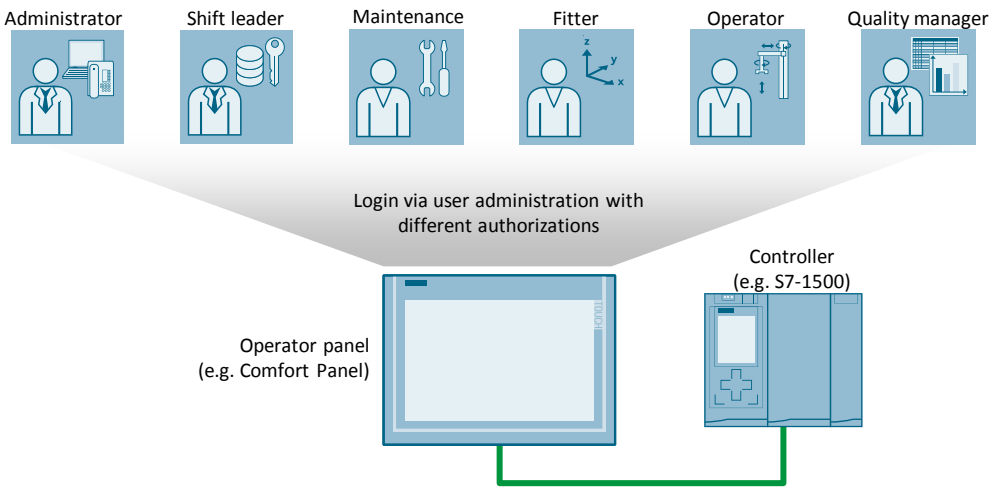
Core topics of this application

In this application example, you will learn:

- basic information on users, user groups and authorizations,
- how to increase the security of the facility by means of an appropriate user administration,
- the difference between local and central user administration,
- which configuration steps are necessary to successfully implement a user administration.

Schematic layout

Figure 2-1



Advantage

The information provided on user administration provides the following benefits:

- time and cost savings thanks to a detailed step-by-step instruction,
- overview of the possible user administration concepts,
- help determining when a specific type of user administration is reasonable.

Delimitation

This application does not describe the basic programming of an HMI in the TIA Portal and user management on Windows operating systems.

Required knowledge

Users are assumed to have basic knowledge of WinCC (TIA Portal) configuration and basic information on user management on Windows operating systems.

2.2 Hardware and software components

2.2.1 Validity

This application is valid for

- WinCC (TIA Portal) V13 SP1

2.2.2 Components used

The following components were used to create the application:

Hardware components

Table 2-1

Component	Qty	Article number	Note
SIMATIC CPU 1513-1 PN	1	6ES7513-1AL01-0AB0	Not relevant for user administration in WinCC (TIA Portal).
Memory card 24 MB	2	6ES7954-8FL02-0AA0	
SIMATIC HMI KTP700 Basic	1	6VA123-2GB03-0AX0	Alternatively, you can use other Basic Panels (requires a device exchange).
SIMATIC HMI TP1200 Comfort	1	6AV2124-0MC01-0AX0	Alternatively, you can use other Comfort or Mobile Panels (device exchange necessary).
Industrial PC SIMATIC IPC 547E	1	6AG4104-3….-….	This IPC is an example; other IPCs can be used, too.

Software components

Table 2-2

Component	Qty	Article number	Note
STEP 7 Professional V13 SP1 Upd 8	1	6ES7822-1A.03-….	
WinCC Advanced V13 SP1 Upd 8	1	6AV2102-0AA3-0A.5	
WinCC Runtime Advanced V13 SP1 Upd 8	1	6AV2104-0.A03-0A.0	
SIMATIC Logon V1.5 SP3 Upd 3	1	6ES7658-7B…-….	
Windows 7 Professional	1	Microsoft	

3 Basics

3.1 User administration (general)

Objective

The user administration aims to set up access protection for data and functions within the Runtime to protect the applications against unauthorized operation.

Example project

Besides facility operation only, there are several other application cases that have to be operated by different users.
Example:

- An administrator can have access to the user administration. But the administrator must not be allowed to change the product's recipe data.
- A quality manager is authorized to monitor the facility parameters, but he must not operate the facility.

The use cases of the respective end customer are usually not determined before on-site commissioning. The user administration in WinCC (TIA Portal) including users, user groups and their authorization helps you implement the selected cases taking the most straightforward approach.

3.2 Users, user groups and authorizations

3.2.1 Users

General

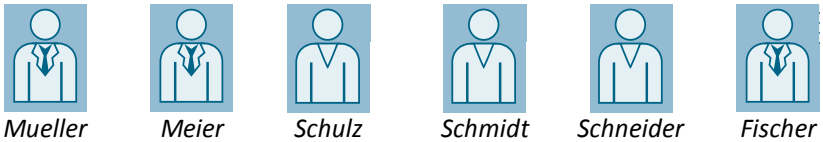
The users in WinCC (TIA Portal) are the basis of the user administration. As a first step, a "user" has to be created in the user administration. To do so, the name and password of the user are stored in the user administration. The user "Admin" is already defined by default in WinCC (TIA Portal).

The following section will use an example to illustrate the principle of user administration. Chapter 4 later describes the configuration based on this example scenario.

Example project

A company has several production facilities and employees. The employees Mueller, Meier, Schulz, Schmidt, Schneider and Fischer are responsible for "production facility A" in the company.

Figure 3-1



3.2.2 User groups

General

To assign an authorization to a user, that user must be a member of a user group. By default, the user groups "administrator group" and "user" are defined by default in WinCC (TIA Portal).

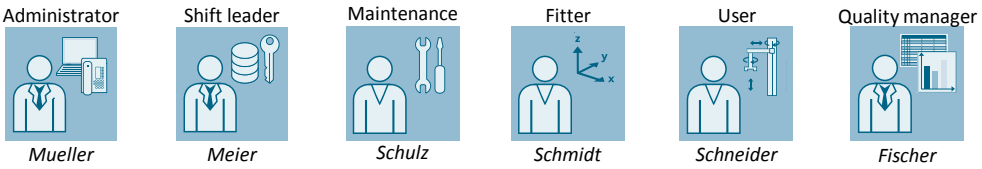
In addition to the predefined user groups, it is possible to create and edit other groups, e.g. the group "Production facility A", "Maintenance", "Fitter" etc.

Each user has to be assigned to a user group and can be a member of one group only.

Example project (user groups)

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

Figure 3-2



According to the employees' responsibilities, the associated user groups (administrator, shift supervisor, maintenance, fitter, user, quality manager) are now created in WinCC (TIA Portal) and the employees are assigned to the groups.

3.2.3 Authorizations

General

In WinCC (TIA Portal), authorizations serve the purpose of defining the access rights of the user groups. Based on these authorizations, you can select the individual access rights at a later stage. Three authorizations ("user management", "monitor" and "operate") are already defined by default in the system. They can be renamed during configuration, but not deleted. Moreover, you can create additional authorizations.

After all authorizations have been created, you can assign the corresponding authorization to each user group. A group can have several authorizations at the same time.

Example (authorizations)

In this example scenario, three more authorizations (maintenance, recipes change, and parameter change) are defined in addition to the default authorizations.

In the next step, the authorizations from chapter 3.2.2 are assigned to the user groups according to the following table.

Table 3-1

	Authorizations					
User groups	**User administration**	**Monitor**	**Operate**	**Service**	**Recipes change**	**Parameter change**
Administrator	X					
Shift leader		X	X		X	X
Maintenance			X	X		
Fitter			X		X	X
Operator		X	X			
Quality manager		X				

The user administration has thus been set up completely and forms the basis of access protection later on.

Note Creating a user administration does not mean that data and functions are already protected against unauthorized access. Access protection only becomes active when assigned to objects.

Chapter 4.2 details how to create a user, user group and authorizations in the TIA Portal.

3.2.4 Performance characteristics depending on the operator panel

The following overview shows the maximum number of users, user groups and authorizations that can be configured.

Table 3-2

	Basic Panel	Comfort/Mobile Panel	WinCC Runtime Advanced
Users	50	50	100
User groups	50	50	50
Authorizations	32	32	32

3.3 Functions in the Runtime

After you have created the user administration with different user groups and authorizations, they can be assigned to objects (e.g. a button) and enhance facility protection.

3.3.1 Access protection

To set up access protection for security-relevant functions and data of a facility, this must be accounted for already when creating the project. Use the properties of the corresponding control to enter the corresponding authorization under "Properties > Security > Security in Runtime". You thereby restrict operation of the security-relevant functions to the respective user groups.

Note Changing or expanding the access protection in the Runtime is no longer possible.

Operation in the Runtime

If the functions (e.g. a button) are activated in the Runtime, a login dialog will pop up and prompt the operator to authenticate with user name and password.

The system checks these entries against the data in the user administration and operation is permitted if they are found to match. If the authentication has failed, operation will not be possible. A message opens reading "Invalid password or user name. Login failed."

Protecting projects and operating systems

The principle described above now yields various security concepts for operator panels, projects and entire facilities. Protecting the projects and operating systems is crucial in this context.

As a rule, shutting down the Runtime should be access protected. Thus, unauthorized operators are denied access to the operator panel's operating system.

Note

Access protection does not prevent operating errors. You have to make sure that only qualified and authorized staff constructs, starts and maintains facilities and machines.

For more information, see the application example Panel Security Guidelines.

Chapter Configuring access protection gives a step-by-step instruction on how to configure access protection for functions.

3.3.2 Login and logout using system functions

You have successfully protected all security-relevant functions and data in your project against unauthorized access. Now you want to see during facility operation who is currently logged in to change users if necessary.

The system functions "Login"/ "Logout"

To generally log a user in or out, e.g. before and after a shift, you can use the "Login" and "Logout" system functions. The user name and password are read via one tag respectively and checked against the stored user data of the user administration and the user is logged in or out.

Note

Alternatively, you can use the additional system function "ShowLogonDialog". This function opens a separate login window where the user can enter user name and password.

The corresponding configuration of the system functions "Login" and "Logout" is described in chapter 4.3.2.

3.3.3 Other system functions

Description

Subsequently, we will outline the function of the other system functions in connection with the user administration. For more detailed descriptions, see the system manual of WinCC Advanced V13 SP1, chapter System Functions.

ExportImportUserAdministration

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

GetUserName

Writes the user name of the user logged in at the operator panel into the specified tag.

GetGroupNumber

Reads the group number of the user currently logged in at the operator panel and writes it to the specified tag.

GetPassword

Writes the password of the user logged in at the operator panel into the specified tag.

Note Make sure that passwords are not publicly visible to prevent misuse of data.

ShowLogonDialog

Opens a dialog at the operator panel in which the user can log in at the operator panel.

Overview of the system functions

Table 3-3

	Basic Panel	Comfort / Mobile Panel	WinCC Runtime Advanced
Logout	X	X	X
Login	X	X	X
ExportImportUserAdministration	--	X	X
GetUserName	X	X	X
GetGroupNumber	X	X	X
GetPassword	X	X	X
ShowLogonDialog	X	X	X

3.3.4 User login with RFID card reader

In addition to the standard login via the login dialog, the user can also log in using an RFID card reader. The application example User Login on operator panels with RFID CardReader provides a detailed description of the hardware configuration and configuration steps required to this end.

3.3.5 User administration via user display

Objective

To adjust the user administration during facility operation in an easy and flexible manner, the "user display" control offers a selection of the key functions required during operation of the facility.

Depending on the user group affiliation, you can enter different settings in the user display.

Figure 3-3

User	Password	Group	Logoff time
Admin	********	Administrator group	10
Maintenance Engineer	********	Service	20
PLC User	********	Unauthorized	5
User	********	Users	5

Administrators

All users groups with the authorization "user administration" (default setting for the "administrator group") can hence

- add and delete users
- release blocked users
- edit user names and passwords (to be documented in writing were applicable)
- edit group affiliations
- adjust logout times.

Other user groups

The user display allows all other user groups that do not have the authorization "user administration" to

- edit their own passwords.
- edit the logout time.
- see all members of the same user group.

Chapter 4.3.3 describes how to configure a user display and adjust the user administration in the Runtime.

3.4 Local user administration concept

Differentiation

Depending on the size and complexity of the facility, there are different user administration concepts. We distinguish between:

- local user administration and
- central user administration (see chapter 3.5).

3.4 Local user administration concept

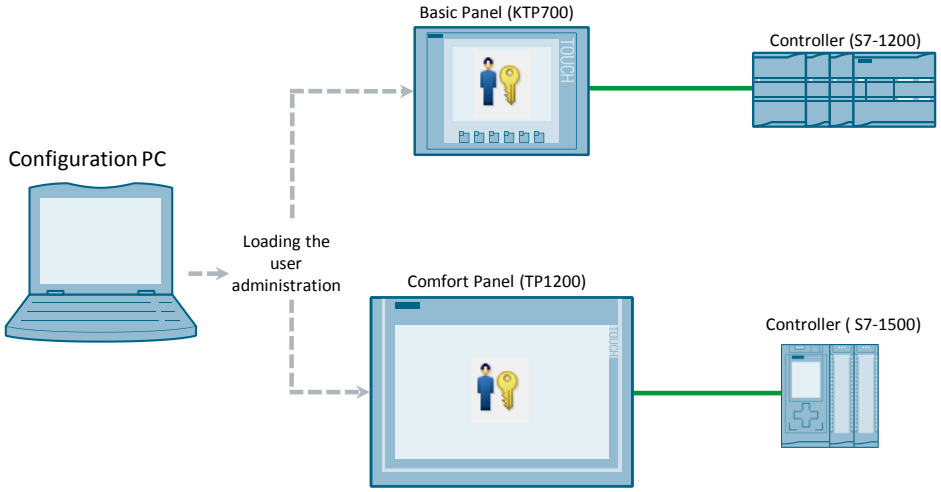
Application

The local user administration concept is suitable for smaller and less complex automation projects comprising a low number of operator panels. Here, the user administration is configured in the TIA Portal and subsequently transferred to the operator panel.

When a user logs in at the operator panel, the access data are checked against the user administration of the operator panel. After successful authentication, the user is logged in.

Principle

Figure 3-4



Advantages

- Easy configuration in the TIA Portal
- User administration configurable for all operator panels and Runtime Advanced
- Individual user administration for each operator panel possible
- Transferring users, groups and authorizations between operator panels via Drag&Drop.

Disadvantages

- Complex if multiple operator panels are involved – multiple configurations
- Variety of access data – different access data possible for different subsystems
- Complex adding users

3.5 Central user administration (SIMATIC Logon)

General

The WinCC (TIA Portal) option package SIMATIC Logon is designed for the central user administration and comprises five software modules.

1. **SIMATIC Logon Service**

   SIMATIC Logon Service is the central access protection for SIMATIC applications and facility sections.

2. **SIMATIC Logon Role Administration**

   The SIMATIC Logon Role Administration allows you to manage the roles of an application and assign them to Windows groups including the assignment of authorizations.

3. **SIMATIC Logon Eventlog Viewer**

   SIMATIC Logon Eventlog Viewer is a component that records and displays events for an application.

4. **SIMATIC Electronic Signature**

   Electronic Signature allows creating electronic signatures for status transitions in the process and for process interventions.

5. **SIMATIC Logon Development Kit**

   The Development Kit is designed for programmers who want to integrate SIMATIC Logon into a customer application.

Access protection

Access protection with SIMATIC Logon can be implemented using the two software components "SIMATIC Logon Service" and "SIMATIC Logon Role Administration". As this is directly related to the user administration, these two sub-packages will be described in more detail in the next two subsections.

Further information

For more information on the individual software components, see the SIMATIC Logon configuration manual, chapter SIMATIC Logon.

3.5.1 Access protection with SIMATIC Logon Service

Objective

SIMATIC Logon Service enables a central and facility-wide user administration building on the Windows operating system of a logon server.

Functioning

The user data are stored and managed on a central logon server via the user management of the Windows operating system.

The user groups and authorizations are still configured in the user administration of WinCC (TIA Portal). Additionally, you create user groups with the same name on the logon server in the user administration. Because the names are identical, the configured authorization is assigned to each user group in the Runtime.

You only have to create the users on the logon server and not in WinCC (TIA Portal), because they will be applied dynamically by the server during login.

The user can now edit his password at the operator panel and the password will be applied directly by the logon server if the Windows user is authorized accordingly.

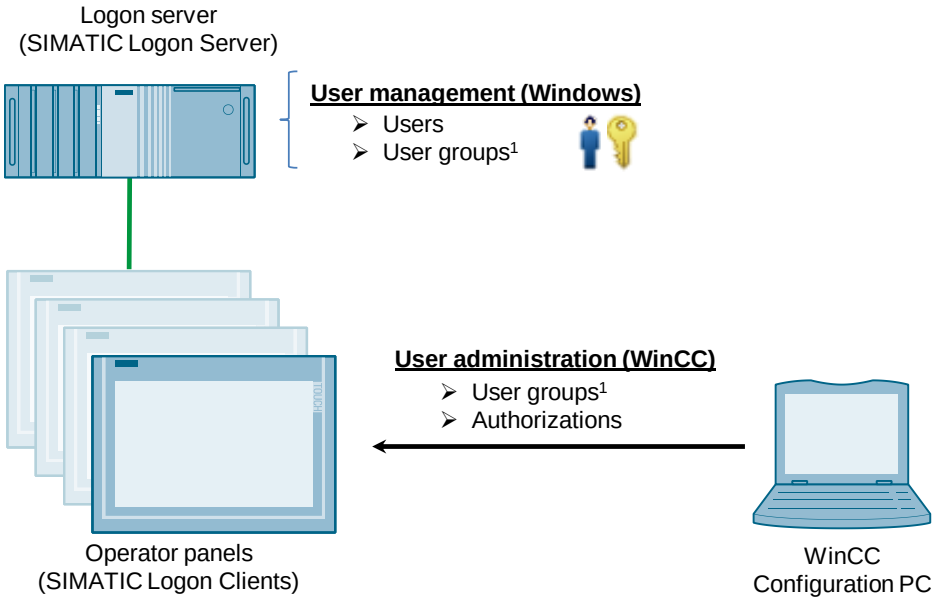
For an exact description of how to configure SIMATIC Logon as the central user administration, see chapter 4.3.3.

Prerequisite

- SIMATIC Logon is installed and configured at the logon server.
- Each operator panel has its own SIMATIC Logon license that is stored centrally on the logon server.

Schematic layout

Figure 3-5



[1] User groups must be named identically

Application

SIMATIC Logon is the preferred solution for more complex automation projects and larger facilities comprising multiple operator panels.

Advantages

- User data are created and managed via the Windows operating system.
- All access data are managed centrally.
- Users can be added easily later on.
- Quick facility-wide adjustment of authorizations, groups and users
- Uniform facility-wide access data

Disadvantages

- The user administration of Basic Panels is not possible via SIMATIC Logon.
- Additional hardware (e.g. for the SIMATIC Logon server)
- User groups in WinCC (TIA Portal) and Windows user groups must be identical.

- Separate SIMATIC Logon licenses are required.
- No login possible when the connection is down.

3.5.2 License protection via SIMATIC Logon Role Administration

Description

The SIMATIC Logon Role Administration allows you to manage roles. A role in this context is the authorization of a group/user within an application to execute a certain action (e.g. transfer licenses).

The authorizations do not concern the WinCC (TIA Portal) project but more general functions of applications, for example access control of users to the "Automation License Manager" (ALM).

The SIMATIC Logon Role Administration thus allows developing a simple concept to protect licenses in the SIMATIC environment.

Example FAQ

The FAQ How do you store licenses on a server and protect them from unauthorized access? describes how to use the Automation License Manager in connection with the SIMATIC Logon Role Administration.

Traceability

As an additional option, all login and logout attempts, user authentication actions and password changes are recorded in the supplied software component SIMATIC Logon Eventlog Viewer. It allows tracing login times and users to a certain extent.

3.6 SIMATIC WinCC Audit (TIA Portal)

Description

SIMATIC WinCC Audit (TIA Portal) is an optional package for WinCC (TIA Portal). In interaction with the WinCC user administration, it helps improve the quality requirement of manufacturing processes. Based on the requirements of the "Good Manufacturing Practice" (GMP) you have to use to

- identify and authenticate users before working on the facility
- comment, document and electronically sign operator actions required in the production process
- centrally archive all operator actions requiring verification.

This enables the actions, the time and the operator who executed a function to be tracked consistently.

Application

Fields of application for GMP-conforming configuration are found primarily in the following industries:

- Pharmaceutical and medical industry
- Food and beverage industry
- Cosmetics industry
- Mechanical engineering companies for the above mentioned sectors.

Further information

For more detailed information about the SIMATIC WinCC Audit (TIA Portal) optional package, see the WinCC Advanced manual, chapter WinCC Audit.

4 Configuration and Settings

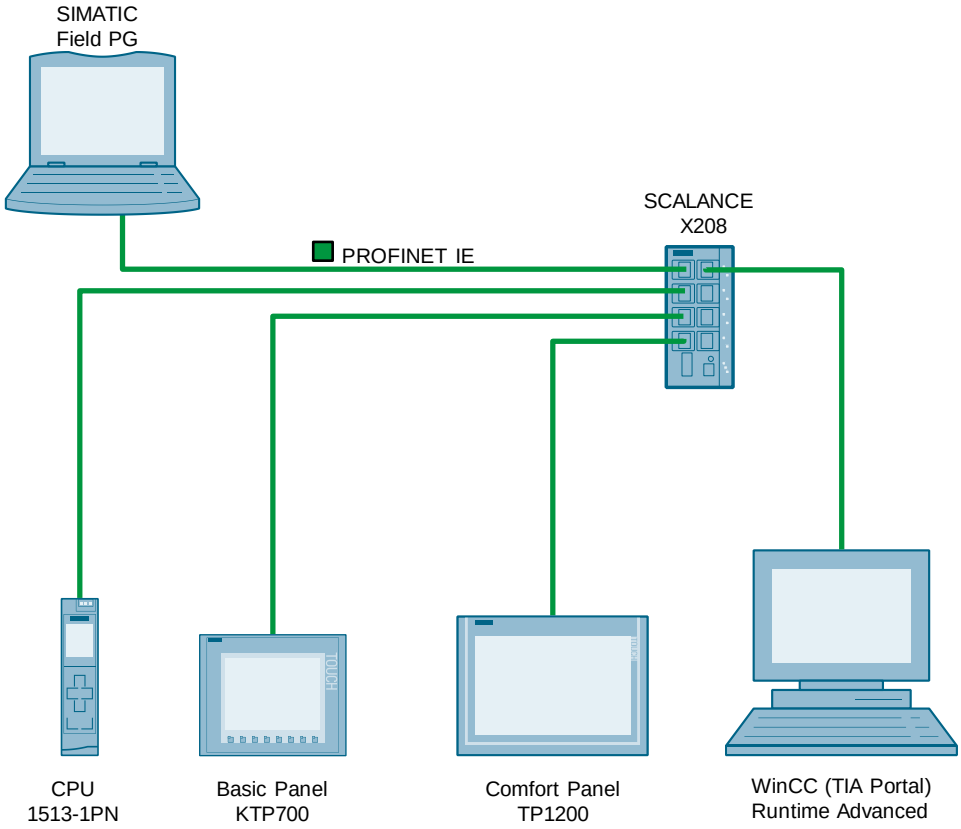
This chapter details which configurations and settings are necessary in order to implement a user administration in WinCC (TIA Portal).

4.1 Hardware configuration

4.1.1 Local user administration

The following illustration shows the basic hardware configuration of the application example with local user administration.

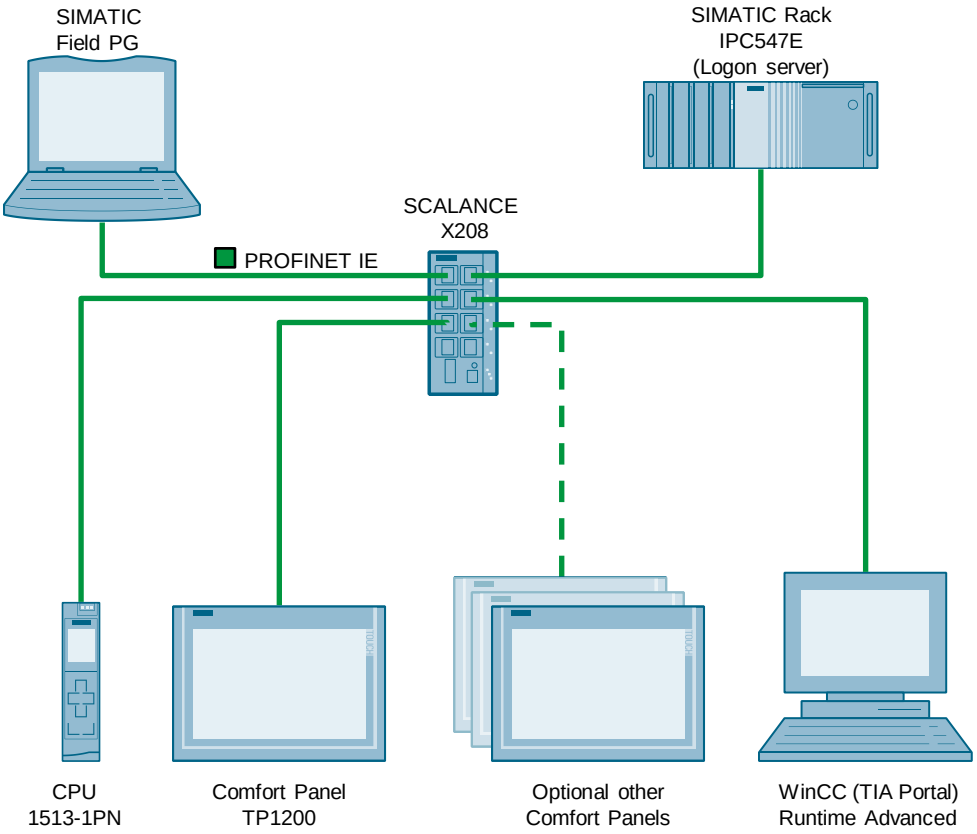
Figure 4-1



4.1.2 Central user administration with SIMATIC Logon

The following illustration shows the structure of the application example in connection with the central user administration using SIMATIC Logon.

Figure 4-2



4.2 Configuring users, user groups and authorizations

To configure the user administration with practical relevance, the application example is implemented based on the principles described in chapter 3.

The following table summarizes again all users, user groups and authorizations which are important for the following steps.

Note

We recommend creating an overview of which users, user groups and authorizations are necessary before creating a user administration. The following table is merely one way to present this in a clearly structured way.

Optionally, a column could be added to this table which contains the passwords of the individual users. When doing so, you have to make sure that the sensitive data are accessible to authorized staff only.

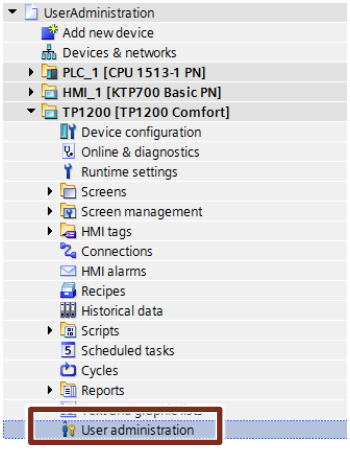
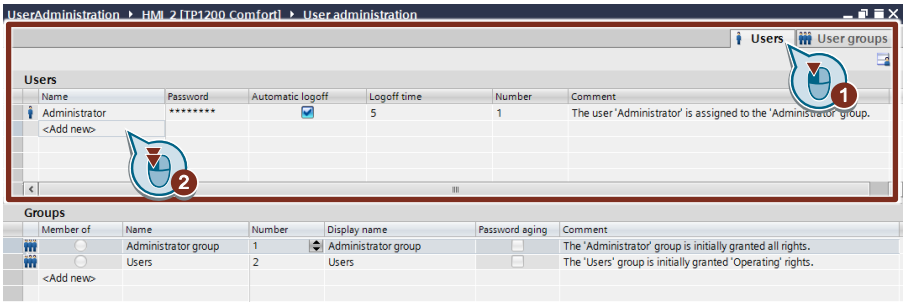
Table 4-1

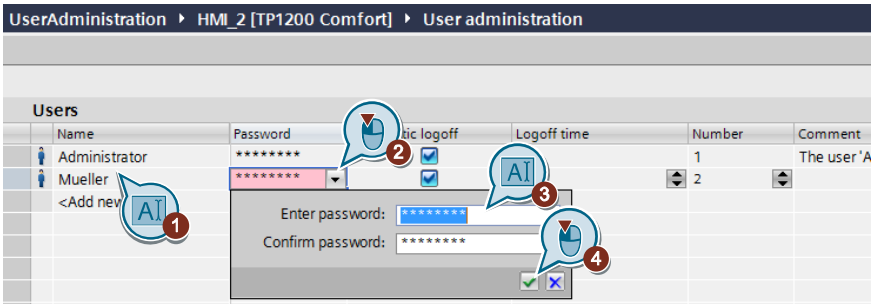
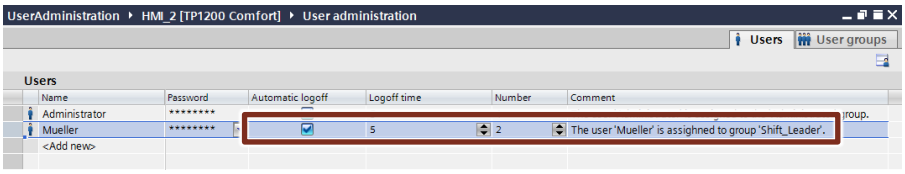
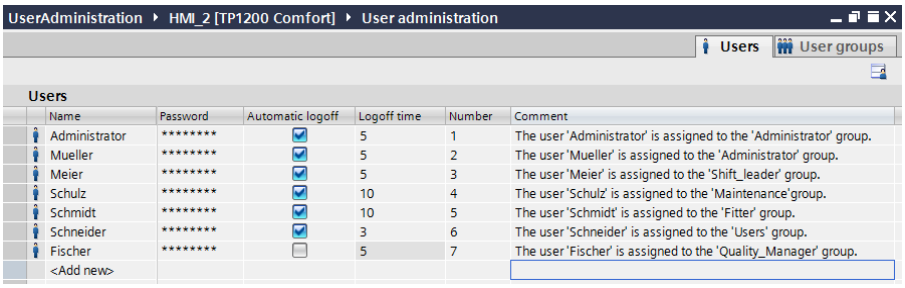
User							Authorizations					
Mueller	Meier	Schulz	Schmidt	Schneider	Fischer	User groups	User administration	Monitor	Operate	Service	Recipes change	Parameter change
X						**Administrator**	X					
	X					**Shift leader**		X	X		X	X
		X				**Maintenance**			X	X		
			X			**Fitter**			X		X	X
				X		**User**		X	X			
					X	**Quality manager**		X				

4.2.1 Configuring users

The following table shows which configuration and setting steps are necessary for a new user.

Table 4-2

No.	Action
1.	Open the WinCC (TIA Portal) configuration via the project navigation. Next double-click "User administration". 
2.	Select the "Users" (1) tab and double-click "Add new" (2) in the "Users" table.  A new user is created automatically with default user data.

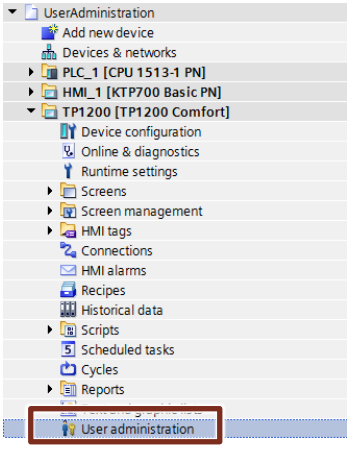
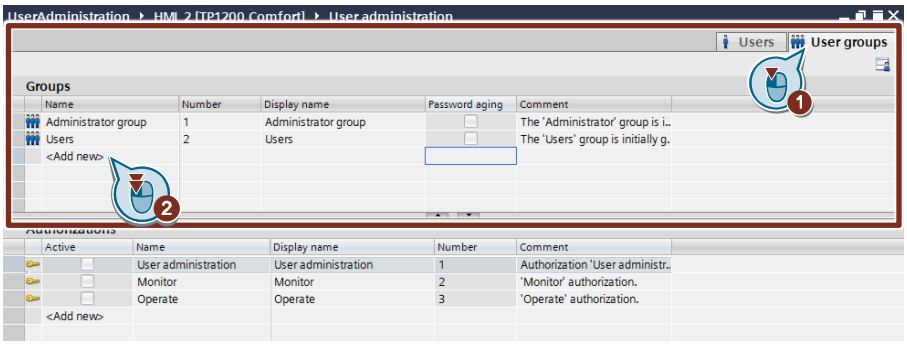
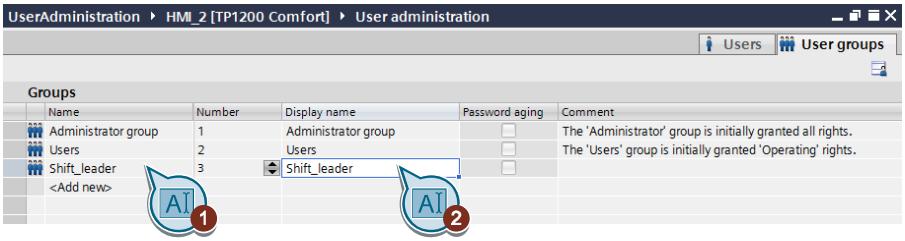
No.	Action
3.	• Rename the new user according to Table 4-1 (1). • Change the password of the user. Confirm the password change (3). • Confirm your entry with the green checkmark (4). 
4.	**Optional:** You can change the user's default settings of the parameters "Automatic logoff", "Logoff time", "Number" and "Comment". In this example, all default settings of the user data were retained. 
5.	Add all other users and adjust their user data. 
6.	Save your project.
7.	The configuration of users in WinCC has been completed.

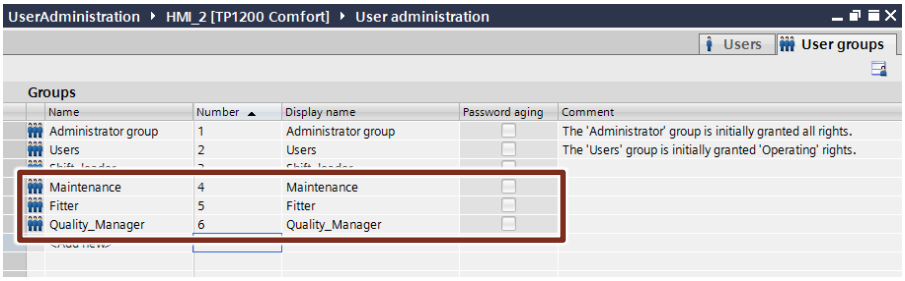
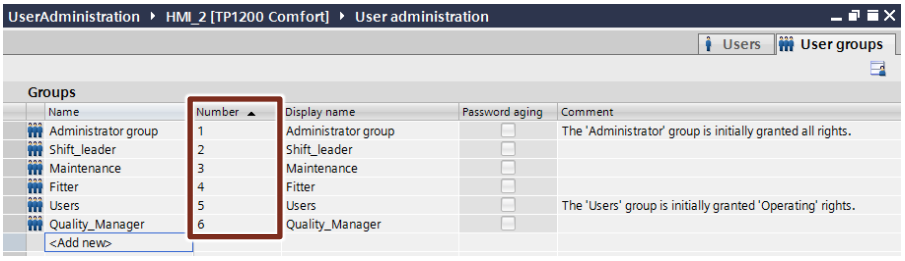
4.2.2 Configuring and assigning user groups

Creating user groups

The following table shows which configuration and setting steps are required to create user groups.

Table 4-3

No.	Action
1.	Open the WinCC (TIA Portal) configuration via the project navigation. Next double-click "User administration". 
2.	• Select the "User groups" tab (1). • Double-click "Add new" (2) in the "Group" table to create a new user group.  A new user group is created automatically. **Note** The user groups "Administrator group" and "Users" are already configured by default and can be renamed but not deleted.
3.	Change the name (1) and the display name (2) of the new user group to "Shift leader". 

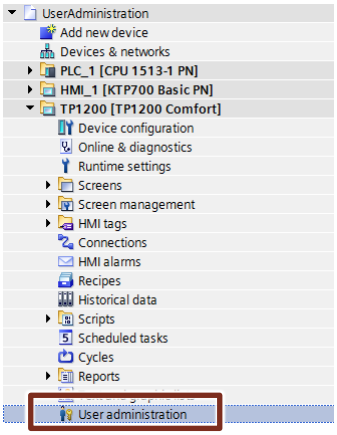
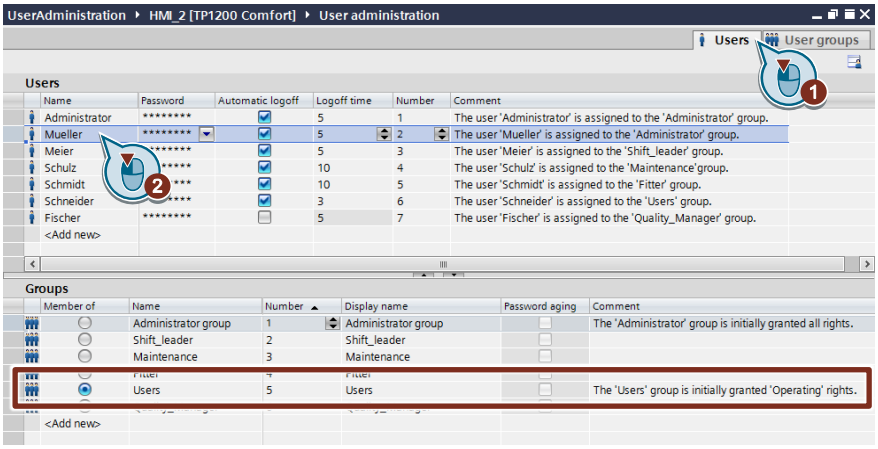
No.	Action
4.	• Create three more user groups as described in step 2 and 3. • Rename the groups to "Maintenance", "Fitter" and "Quality manager".  **Note** The "Password aging" radio button is not available by default. To activate it, you have to enable password aging in the Runtime settings of the operator panel. For more detailed descriptions, see chapter 4.2.4 "Optional: Adjusting the Runtime settings".
5.	**Optional:** By changing the user group number, you can resort the individual user groups. 
6.	Save your project.
7.	You have successfully completed the creation of user groups.

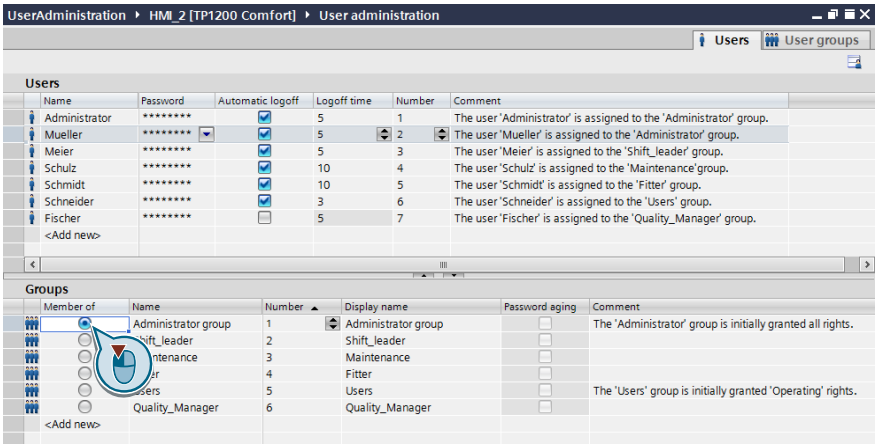
Assigning user groups

The following table shows you which configuration and setting steps are necessary to assign user groups.

To assign user groups, users and user groups must already have been created in your project.

Table 4-4

No.	Action
1.	Open the WinCC (TIA Portal) configuration via the project navigation. Next double-click "User administration". 
2.	Select the user "Mueller" (2) in the "Users" tab (1).  In the "Groups" table, you can see the current user group to which the user "Mueller" is assigned. **Note** All newly created users are assigned to the "Users" group by default.

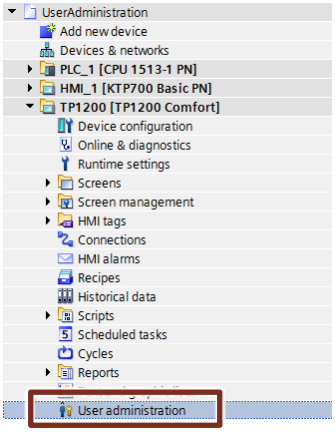
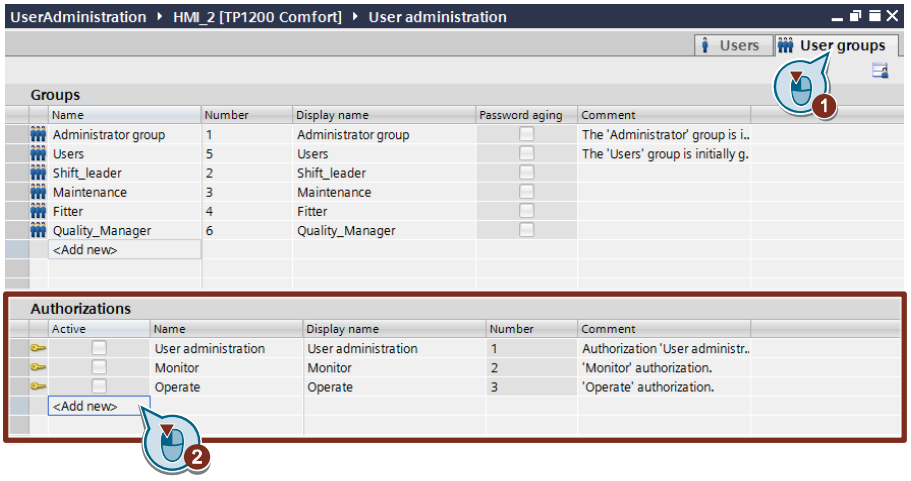
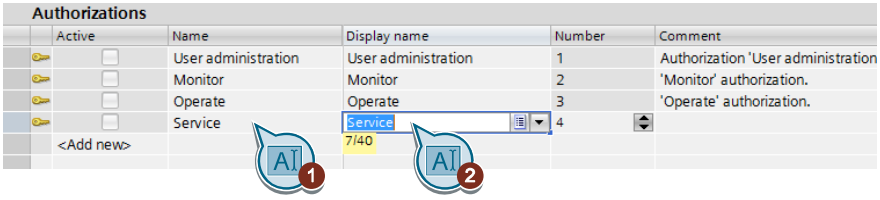
No.	Action
3.	Select the radio button of the "Administrator group" to assign the user Mueller to this group.  **Note** The users can only be a member of one user group at a time.
4.	Continue by selecting more users ("Meier", "Schmidt", "Schulz", "Schneider" and "Fischer") one after the other and assign them to the corresponding user group, see Table 4-1.
5.	Save your project.
6.	You have successfully assigned the members to the user groups.

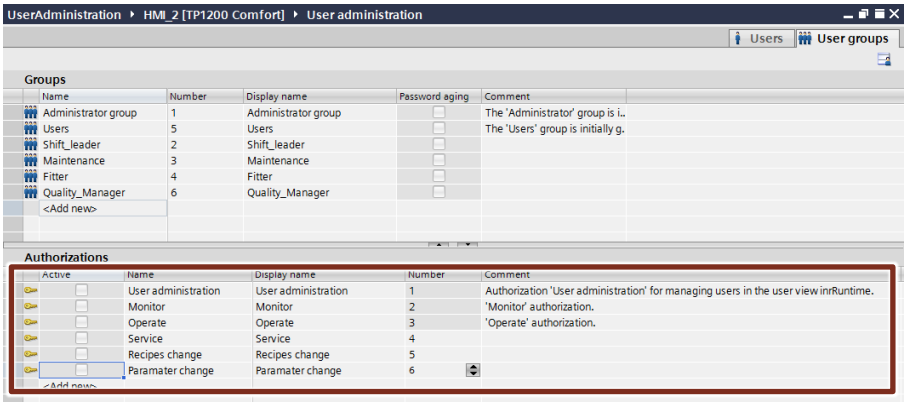
4.2.3 Configuring and assigning authorizations

Creating authorizations

The following table shows you how to create authorizations for user groups.

Table 4-5

No.	Action
1.	Open the WinCC (TIA Portal) configuration via the project navigation. Next double-click "User administration". 
2.	• Select the "User groups" tab (1). • Double-click "Add new" (2) in the "Authorizations" table to create a new authorization.  The new authorization "Authorization_1" is created automatically. **Note** The authorizations "User administration", "Monitor" and "Operate" exist by default. They can be renamed but not deleted.
3.	Change the name (1) and the display name (2) of the new authorization to "Service". 

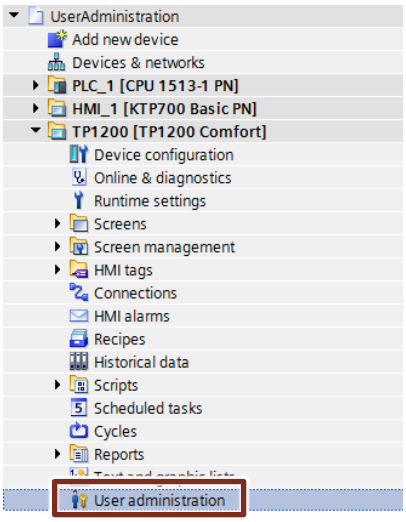
No.	Action
4.	Create two more authorizations and name them "Recipes change" and "Parameter change". 
5.	All authorizations for the example project have thus been created and the authorizations configured.

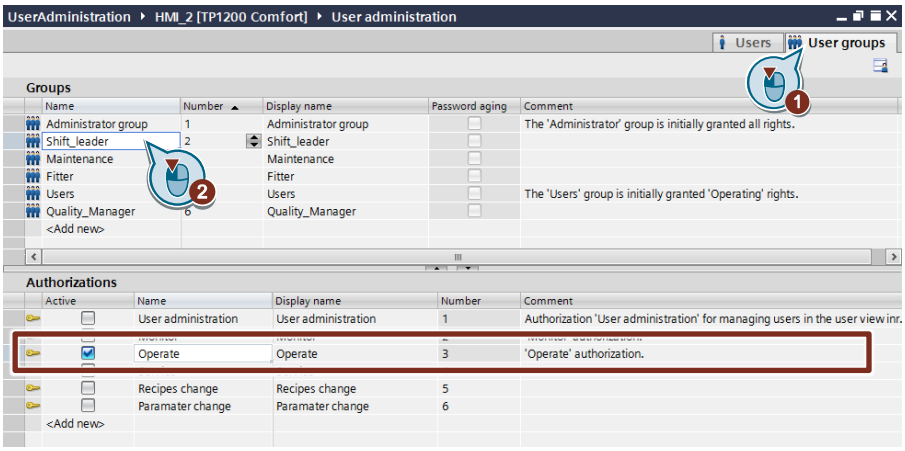
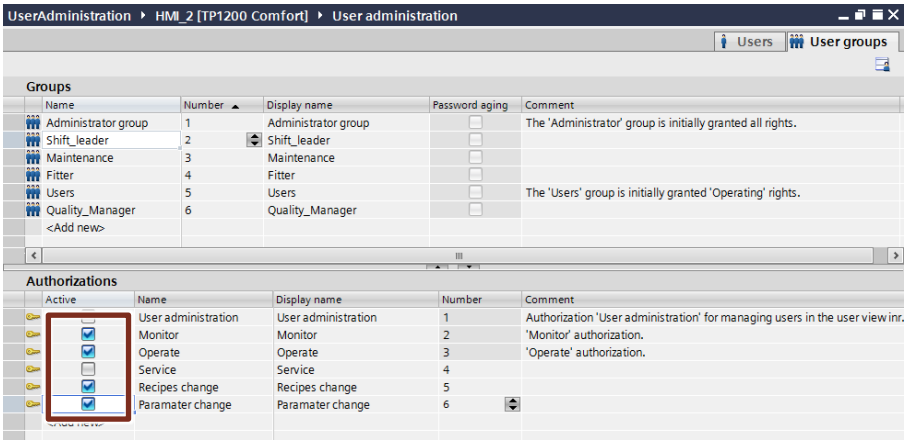
Assigning authorizations

The following table shows you how to assign authorizations to a user group.

To assign authorizations, user groups and authorizations must already have been created.

Table 4-6

No.	Action
1.	Open the WinCC (TIA Portal) configuration via the project navigation. Next double-click "User administration". 

No.	Action
2.	Select the "Shift_leader" group (2) in the "User groups" tab (1).  In the "Authorizations" table, you can see the currently assigned authorization "Operate". **Note** All newly created user groups have the "Operate" authorization assigned to them by default.
3.	Assign the following authorizations to the "Shift_leader" user group. • Monitor • Recipes change • Parameter change  **Note** Click the radio button again to disable the authorization.
4.	Next click the other user groups successively and assign them the corresponding authorizations, see Table 4-1.
5.	Save your project.
6.	You have successfully configured the user administration.

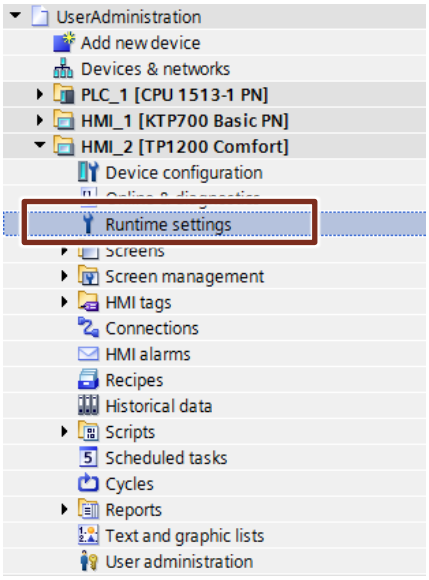
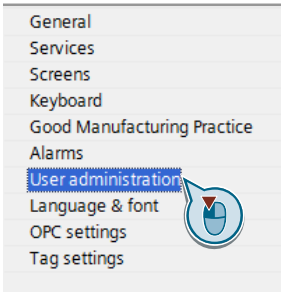
Note By default, the "User administration" authorization is the first authorization number. User groups with this authorization can manage all other users in the Runtime via the user display.

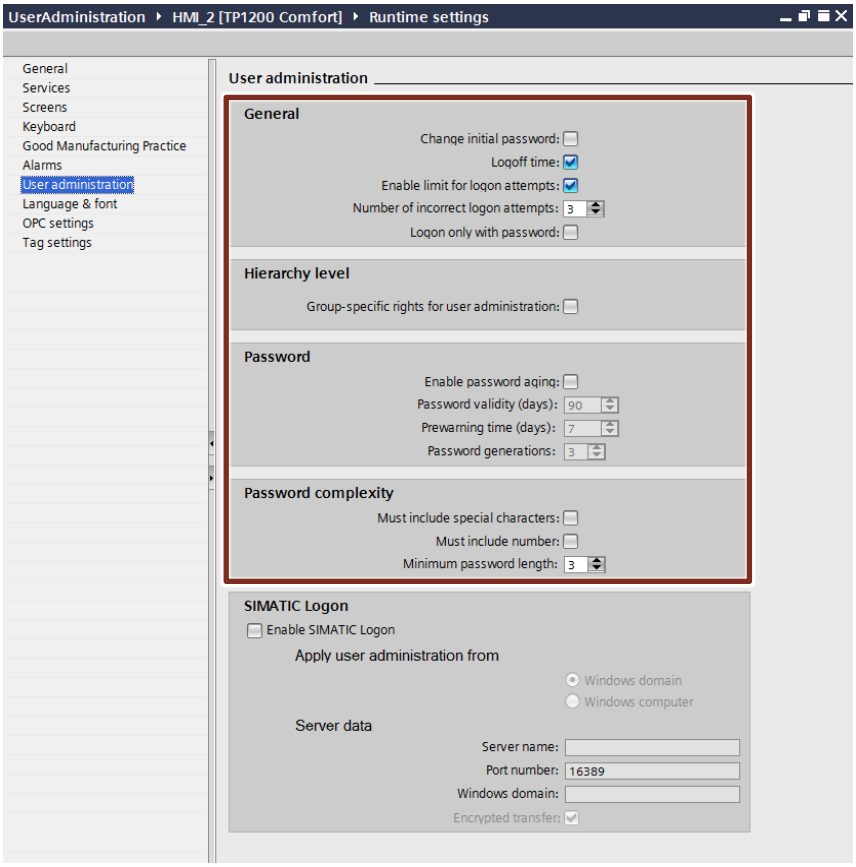
4.2.4 Optional: Adjusting the Runtime settings

Note The selection of the options in the Runtime settings depends on the respective operator panel.

The following table describes which setting options are available for the user administration under the Runtime settings of the respective operator panel.

Table 4-7

No.	Action
1.	Open the WinCC (TIA Portal) configuration via the project navigation. Next double-click "Runtime settings". 
2.	Click the user administration in the area navigation. 

No.	Action
3.	The Runtime settings of the user administration open, providing various options to adjust e.g. the password complexity.  **Note** For detailed explanations on the individual options, see the WinCC Advanced manual, chapter User administration settings.

4.3 Configuring access protection and user display

This chapter shows how to set up access protection for a function (e.g. operate a button) and log in and out via system functions.

Moreover, an example is used to explain how to display the currently logged in user and configure or operate the user display.

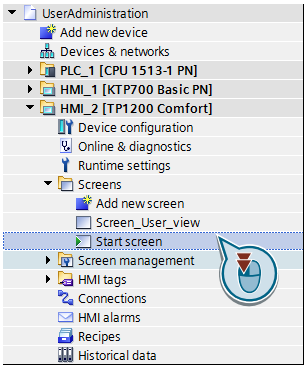
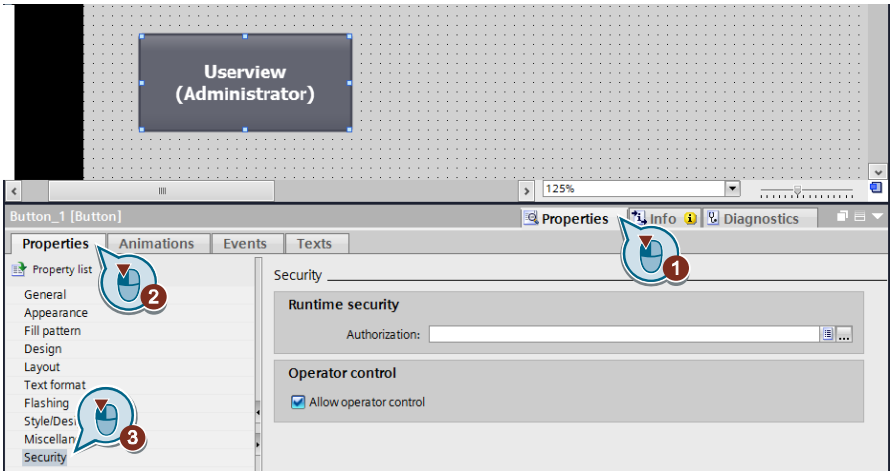
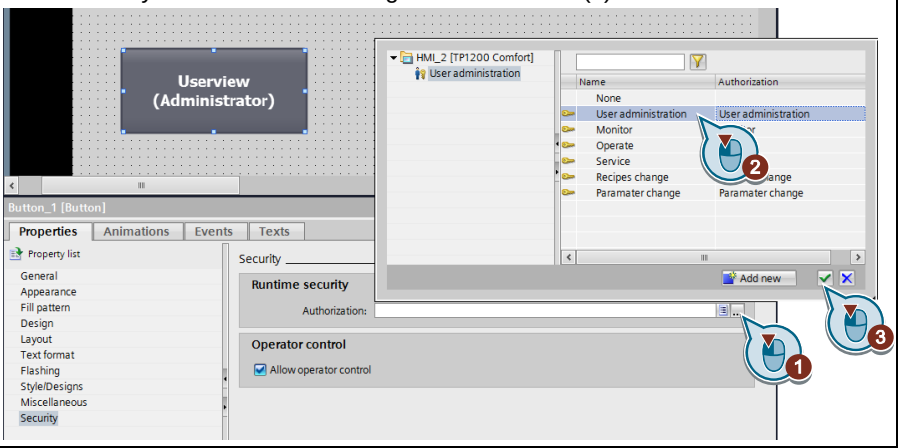
Prerequisite

- A project created with at least one operator panel
- Configured user administration with users, user groups and the corresponding authorizations

4.3.1 Configuring access protection

The following table describes how to set up access protection for the function of a button.

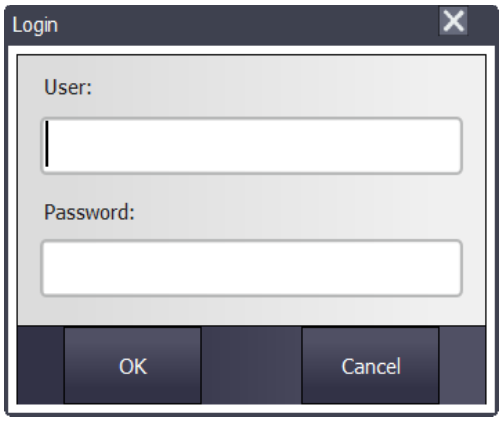
Table 4-8

No.	Action
1.	Open a screen, e.g. the start screen, and insert a button. 
2.	Select the option "Security" (3) in the "Properties" tab (2) of the button properties (1). 
3.	• Under "Runtime security", click the dropdown list box (1) and select the "User administration" authorization (2) in the context menu. • Confirm your selection with the green check mark (3). 
4.	Save your project and load it to your operator panel.

Behavior in the Runtime

When the button is operated in the Runtime, the login dialog opens prompting the user to log in unless the user is already logged in. If the user authentication has been successful, the configured system function, e.g. "ActivateScreen", is executed the next time the button is operated.

Figure 4-3



If the login has been incorrect or not authorized, the system message "Invalid password or user name. Login failed." will be displayed.

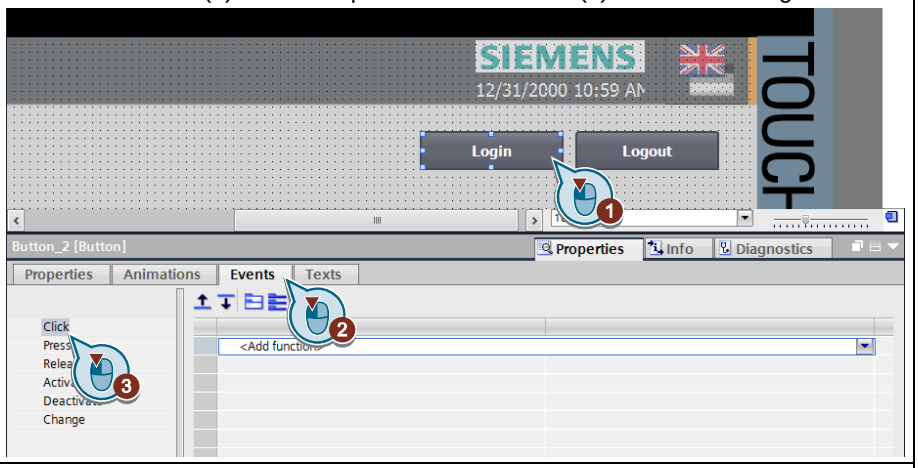
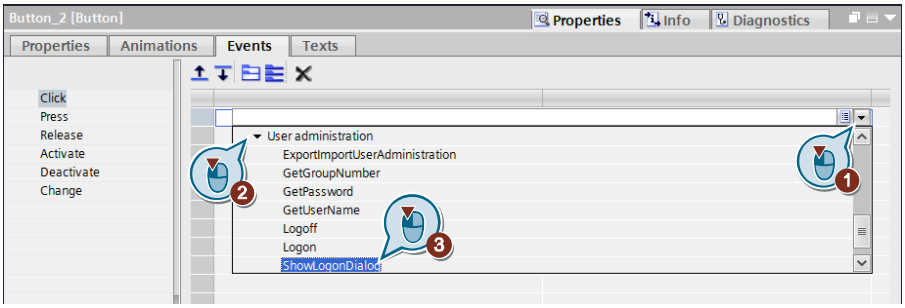
If a user without administrator rights operates the access-protected button, the user will be logged in but the function will not be executed. Instead the system will display a message stating that the user is not sufficiently authorized.

4.3.2 Logging in and out via system functions

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

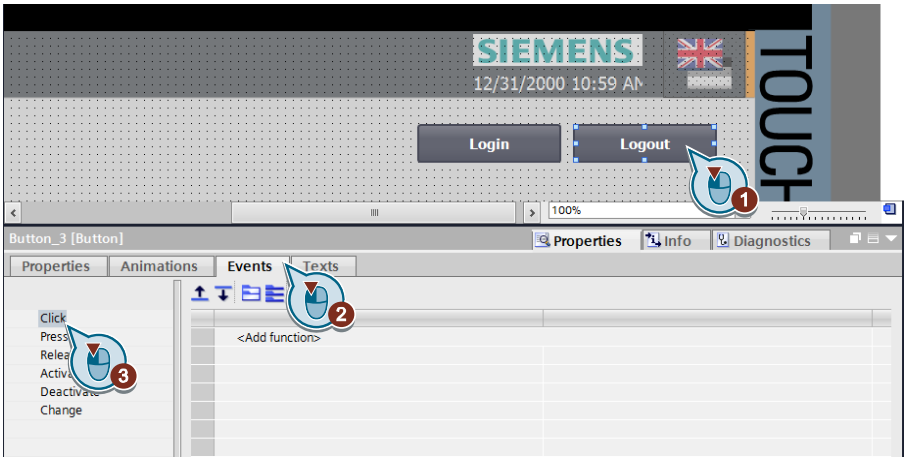
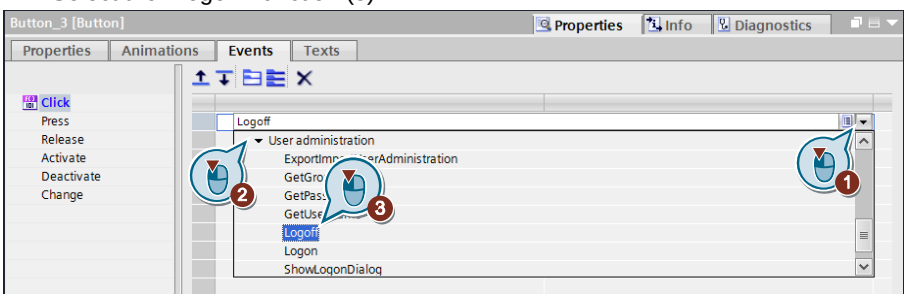
Login

Table 4-9

No.	Action
1.	Create two buttons in the configuration. Name these buttons "Login" and "Logout". 
2.	• Select the "Login" button (1). • Select "Click" (3) in the "Properties > Events" tab (2) in the area navigation. 
3.	• Open the dropdown list box (1) and navigate to "User administration" (2) in the context menu. • Select the "ShowLogonDialog" function (3).  The login dialog has thus been configured.

Log out

Table 4-10

No.	Action
1.	• Select the "Logout" button (1). • Click on "Click" (3) in the "Properties > Events" tab (2) in the area navigation. 
2.	• Open the dropdown list box (1) and navigate to "User administration" (2) in the context menu. • Select the "Logoff" function (3). 
3.	Save your project and load it to the operator panel.

Behavior in the Runtime

In the Runtime, you can confirm the "Login" button and the dialog shown in Figure 4-3 is displayed. The user can now authenticate again. An incorrect login attempt causes the system to display the message "Invalid password or user name".

Note If the login has been successful, there will be no feedback about the successful login on the operator panel by default. This function has to be configured additionally; see the following chapter Display of the currently logged in user.

When the "Logout" button is applied, the currently logged in user will be logged out. No feedback on the successful logout is displayed; this would have to be configured additionally if necessary.

4.3.3 Display of the currently logged in user

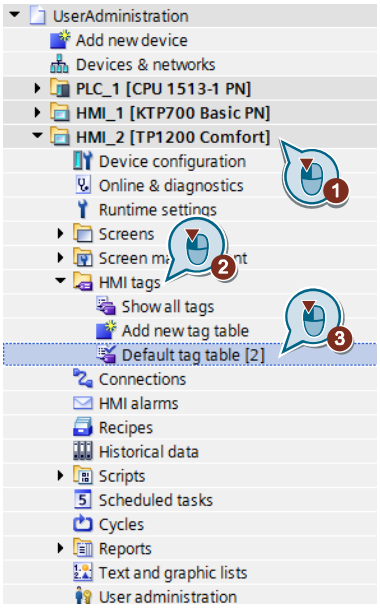
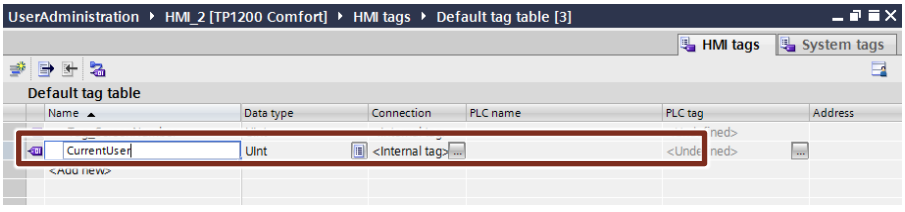
In order to obtain information from the operator panel as to whether a user was logged in or out successfully or which user is currently logged in, additional functions are necessary.

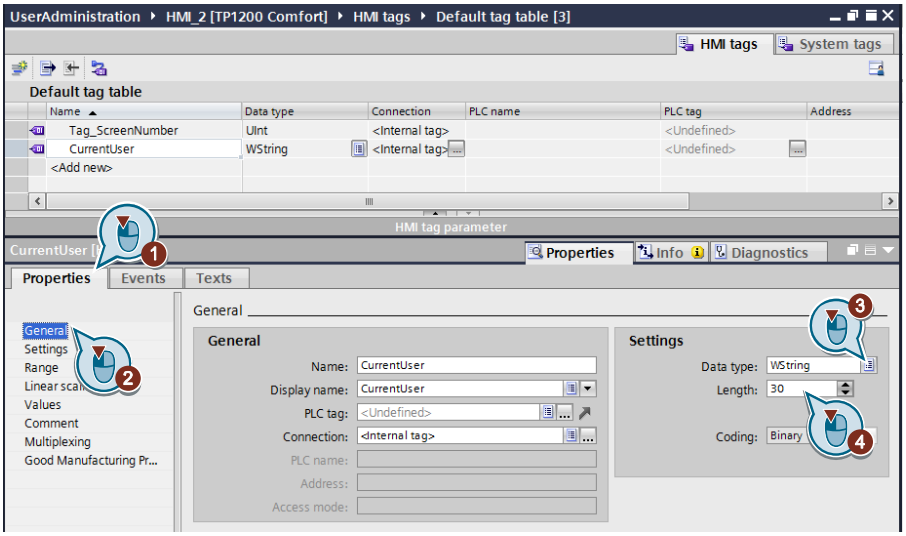
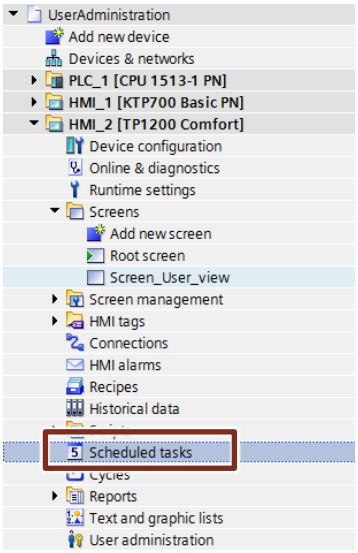
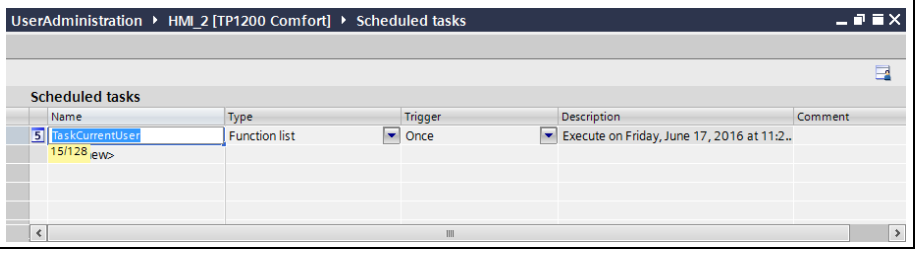
The following table describes how to configure this feature using an I/O field.

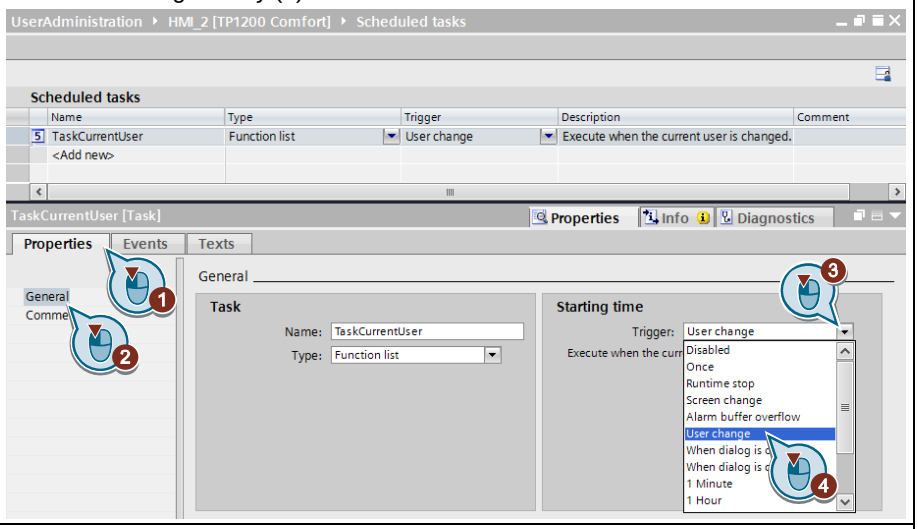
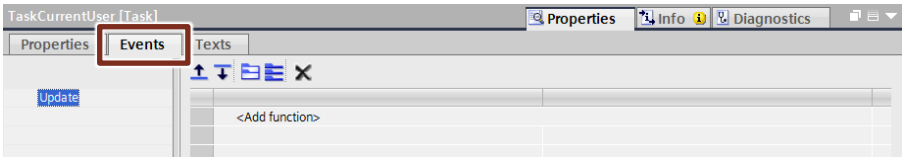
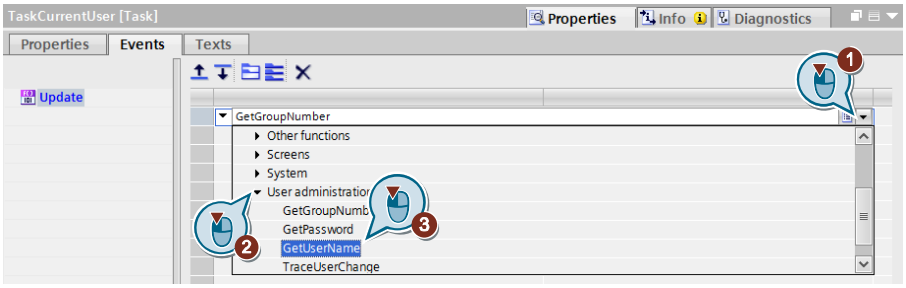
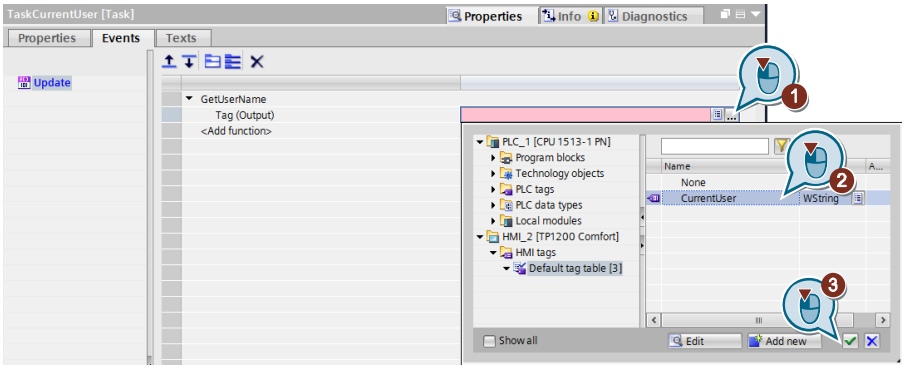
Prerequisite

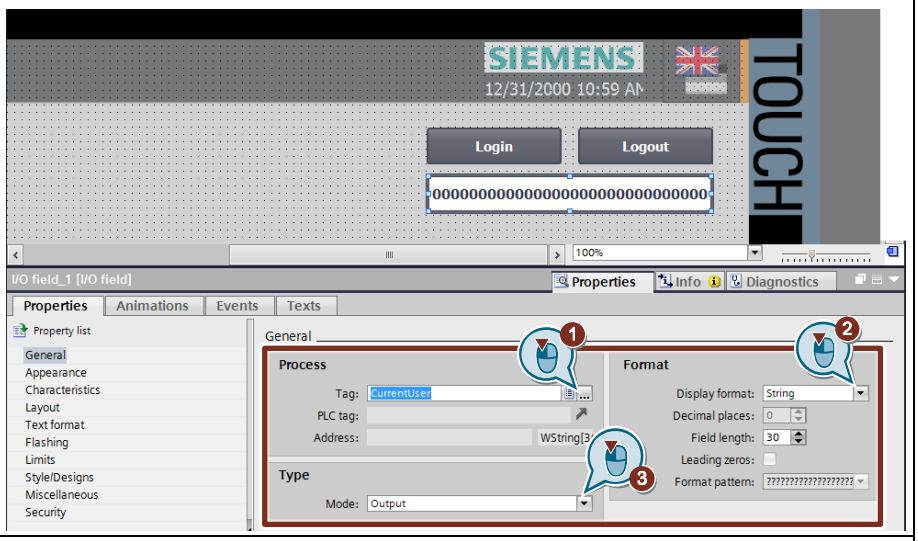
The login and logout of a user must already be configured for this purpose, for example as described in the two previous chapters.

Table 4-11

No.	Action
1.	Open the "Default tag table" (3) under "HMI tags" (2) in the project navigation of your HMI operator panel. 
2.	Create a new tag named "CurrentUser". 

No.	Action
3.	• Under "Properties" (1) open the "General" context menu (2). • Change the data type to "WString" (3). • Increase the character length to 30 (4). 
4.	Open "Scheduled tasks" in the project navigation. 
5.	• In the "Scheduled tasks" table, click "<Add new>" to create a new task. • Rename the task to "TaskCurrentUser". 

No.	Action
6.	• Open the properties (1) of the newly created task and select "General" (2) in the area navigation. • Under "Starting time > Trigger", open the dropdown list box (3) and select the "User change" entry (4). 
7.	Next open the "Events" of created task. 
8.	Open the dropdown list box (1) in the table and select the function "GetUserName" (3) under "System>User administration" (2). 
9.	• Select the context menu (1) in the system function under "Default tag table". • Select the "CurrentUser" tag (2). • Confirm the entry (3). 

No.	Action
10.	In the project navigation, switch to "Screens".
11.	Create an I/O field in your screen.
12.	Click the I/O field and select in "Properties > General": • the "CurrentUser" tag (1) • the "String" display format (2) under "Format" • the output mode under "Type". 
13.	Save the project and load it to your operator panel.

Behavior in the Runtime

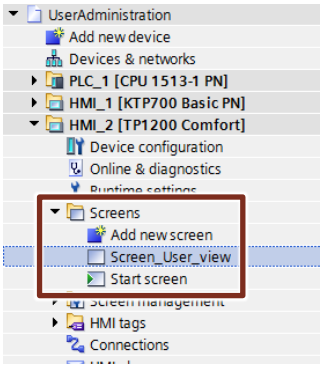
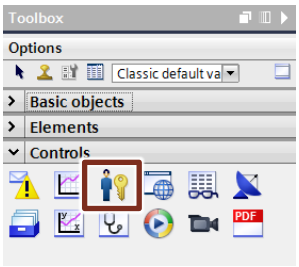
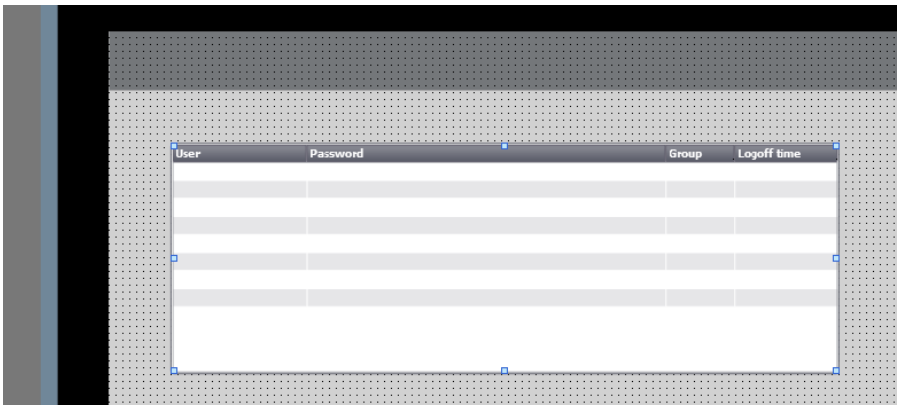
After successful login, the name of the currently logged in user appears in the I/O field.

Figure 4-4

If the user logs out again, the user name is removed from the I/O field.

4.3.4 User display and operation

Table 4-12

No.	Action
1.	In the project navigation, open the "Screen_User_view" screen under the HMI screens. 
2.	• Open the "Toolbox task card and expand the "Controls" tab. • Select the "User display" control. 
3.	• Drag&Drop the "User display" into the editable area of the "Screen_UserDisplay" screen. • Edit the size of the user display if necessary. 
4.	Save the project and load it to your operator panel.

Behavior in the Runtime

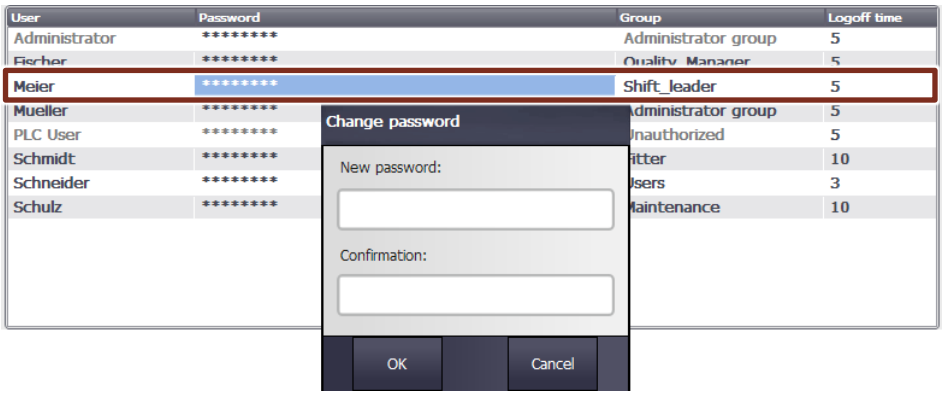
Within the Runtime, an administrator can log in and access the user display to change user data, unlock users and add or delete new users.

Note Users without administrator rights can also access the user display, but they will only see such users that are a member of the same user group.

1. Editing user data

In order to edit the user data of a user, select the row containing the user and the cell you want to edit. In this example, we want to change the password of the user Meier.

Figure 4-5

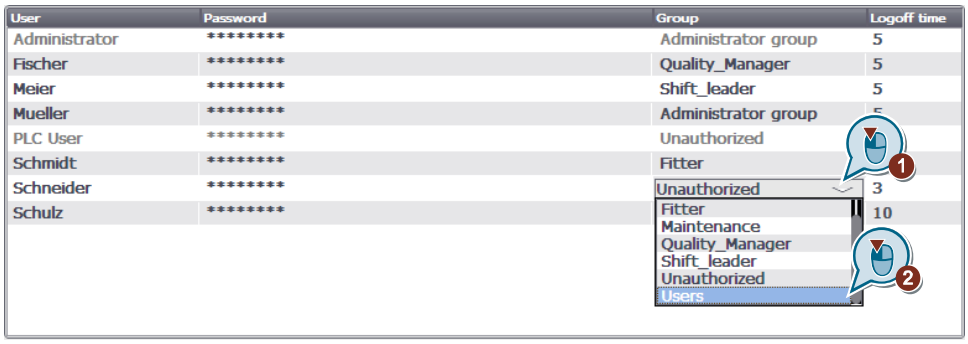


2. Unlocking users

If a user has tried to log in several times using the wrong password during facility operation and has exceeded the allowed number of login attempts, that user will be locked and assigned to the "Unauthorized" user group.

As an administrator you can unlock such users again via the user display. To do so, select the name of the locked user and assign him or her the original user group via the dropdown list box in the "Group" column. This action will unlock the user.

Figure 4-6

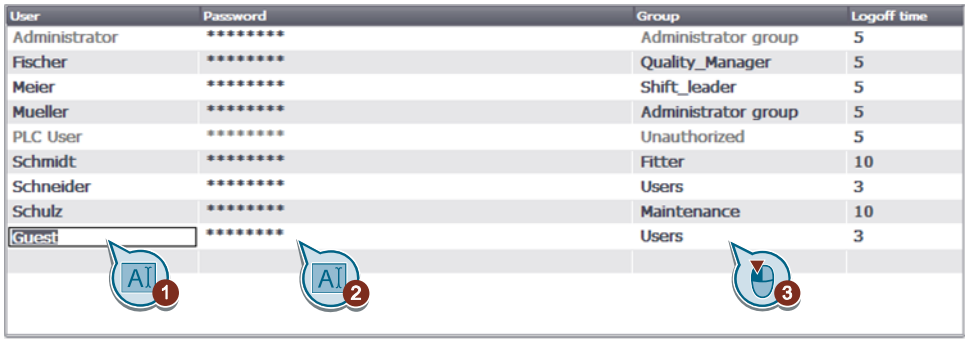


3. Adding and deleting users

As an administrator you can also add new users to or delete existing ones from the user administration via the user display in the Runtime.

To add a new user, click an empty row of the user display and assign a new name (1). Subsequently, you can assign a password (2) and a user group (3) to the new user. The procedure is analogous to the first case example "Editing user data".

Figure 4-7



To delete a user from the user administration, delete the user name in the "User" column and confirm with Enter.

4.4 Configuring SIMATIC Logon

This chapter gives a detailed step-by-step instruction on how to create a central user administration via SIMATIC Logon.

The users, user groups and authorizations of the previous chapter (see Table 4-1) will be used for this purpose.

Prerequisite

- SIMATIC Logon is installed.
- User groups and authorizations have already been created in WinCC (TIA Portal).

Hinweis If you want to log on to a remote SIMATIC Logon Server, you must open the port 16389 in the firewall configuration of the server.

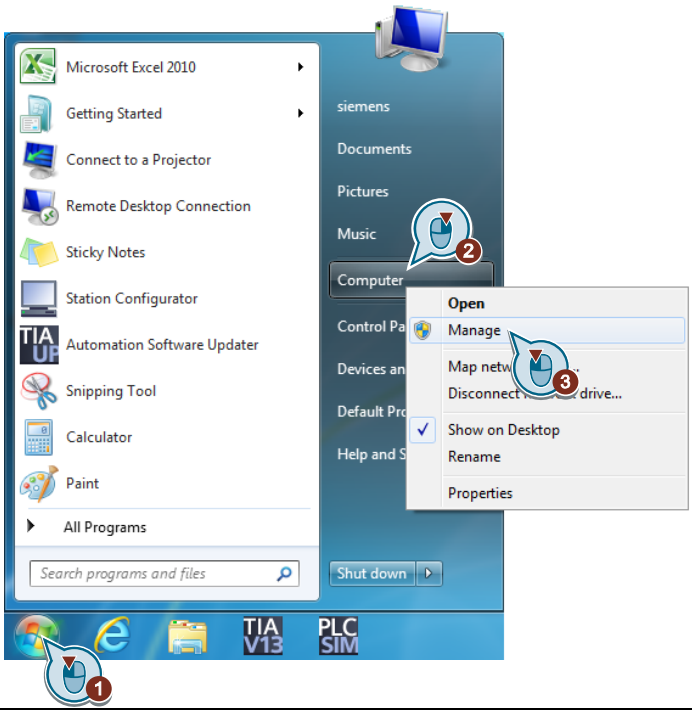
Instruction

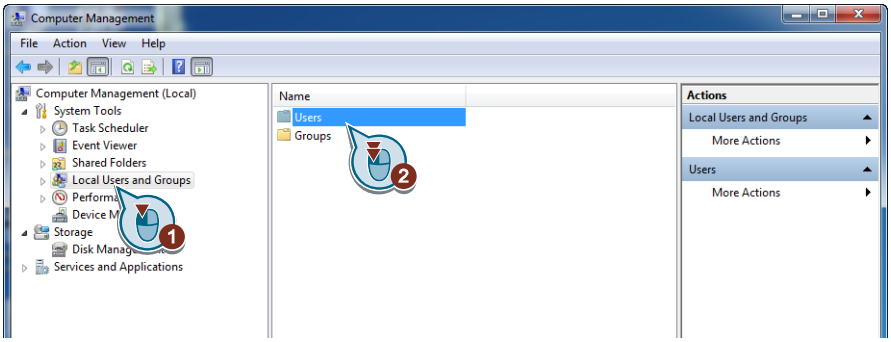
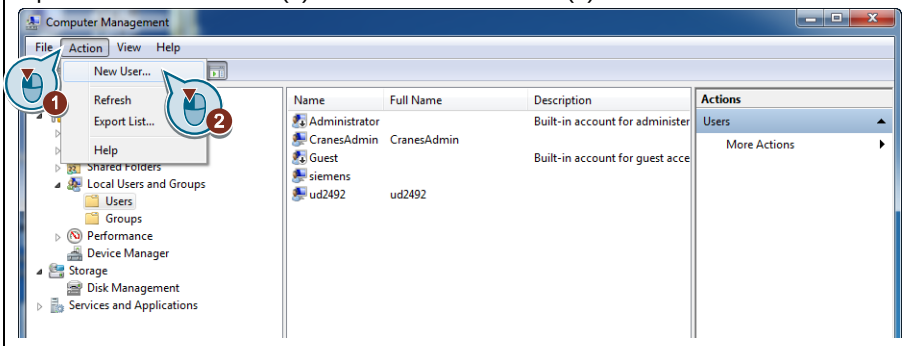
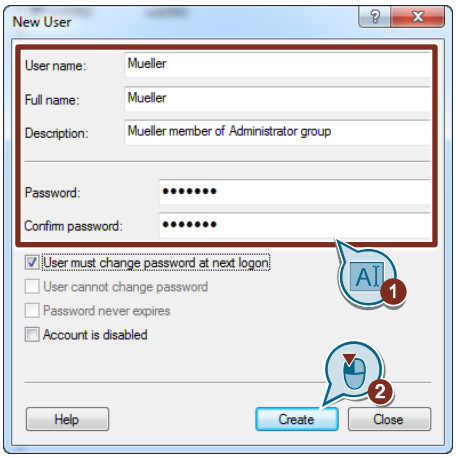
To create the central user administration with SIMATIC Logon, the following five steps are necessary:

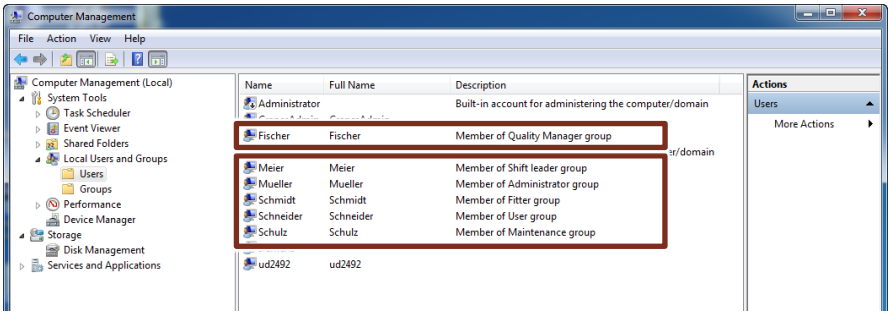
1. Creating the user in Windows user management
2. Creating user groups in Windows user management and assigning users to these user groups
3. Creating user groups in WinCC (TIA Portal)
4. Creating and assigning authorizations in WinCC
5. Activating SIMATIC Logon in WinCC (TIA Portal)

4.4.1 Creating the user in Windows user management

Table 4-13

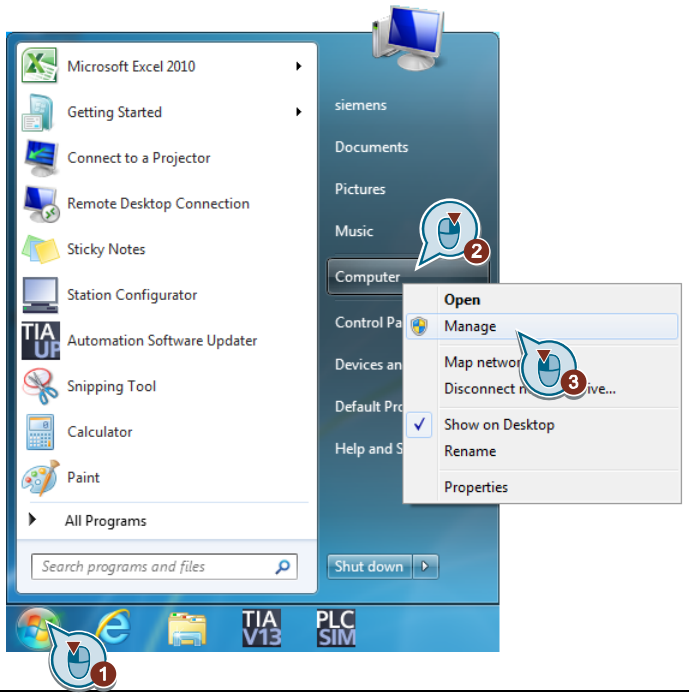
No.	Action
1.	Open the Windows Computer Management. 

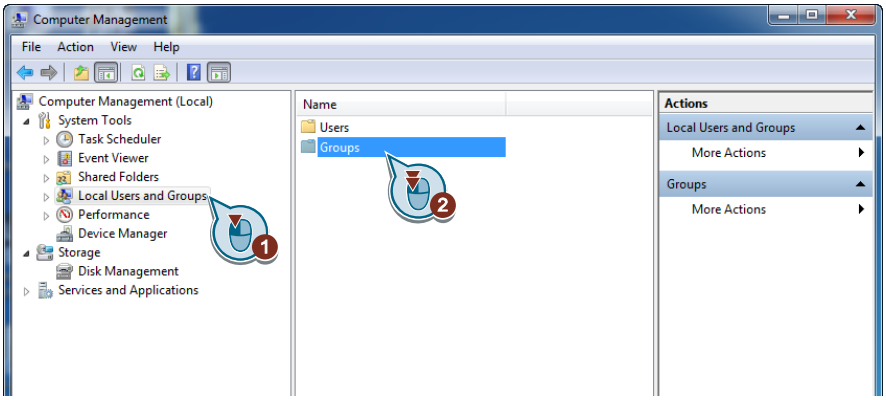
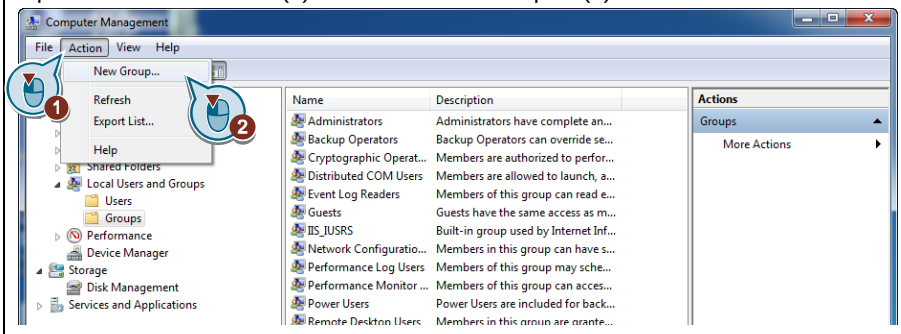
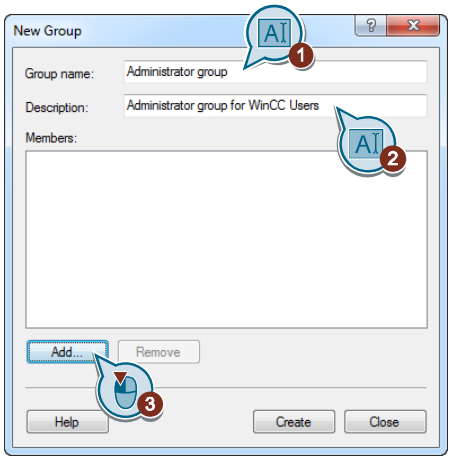
No.	Action
2.	• Select "Local Users and Groups" (1). • Next double-click "Users" (2) to open Windows user management.  An overview of all existing users opens.
3.	Open the "Action" menu (1) and click "New User..." (2).  The dialog for creating a new user opens.
4.	• Enter the user name, the full name, an optional description and the password of user "Mueller" (1). • Then click "Create" (2).  **Note** After clicking the "Create" button, the user is created in the background. To see the newly created user in the user administration, you have to close the "New User" dialog.

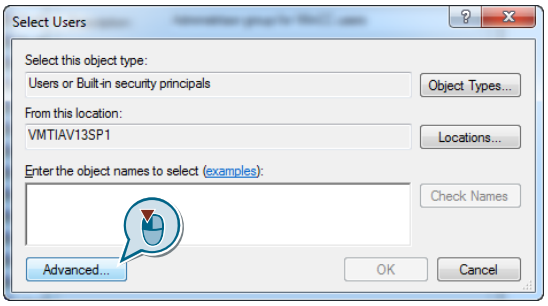
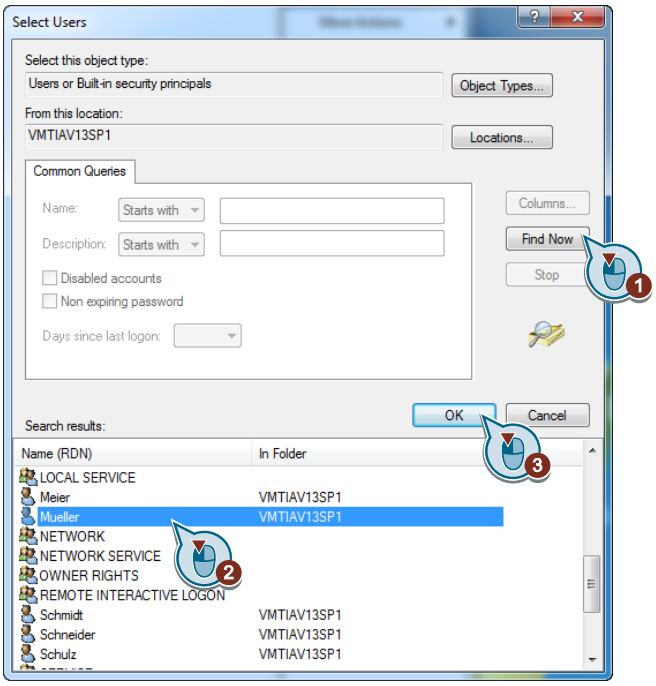
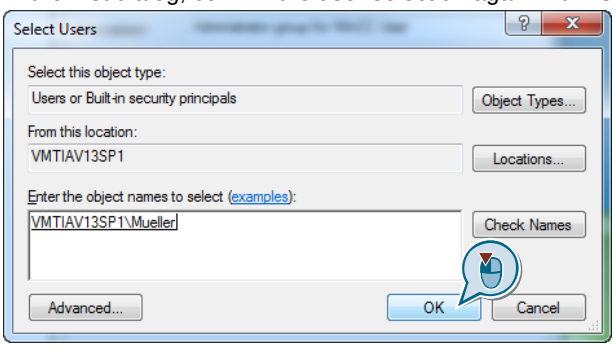
No.	Action
5.	Repeat step 3 and 4 to create the five other users (Meier, Schmidt, Schulz, Fischer and Schneider). 
6.	All users have been created.

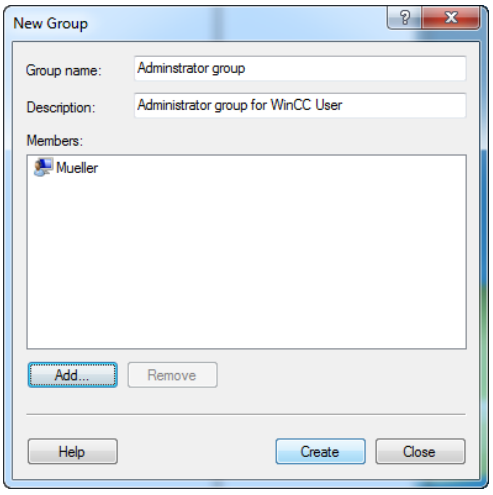
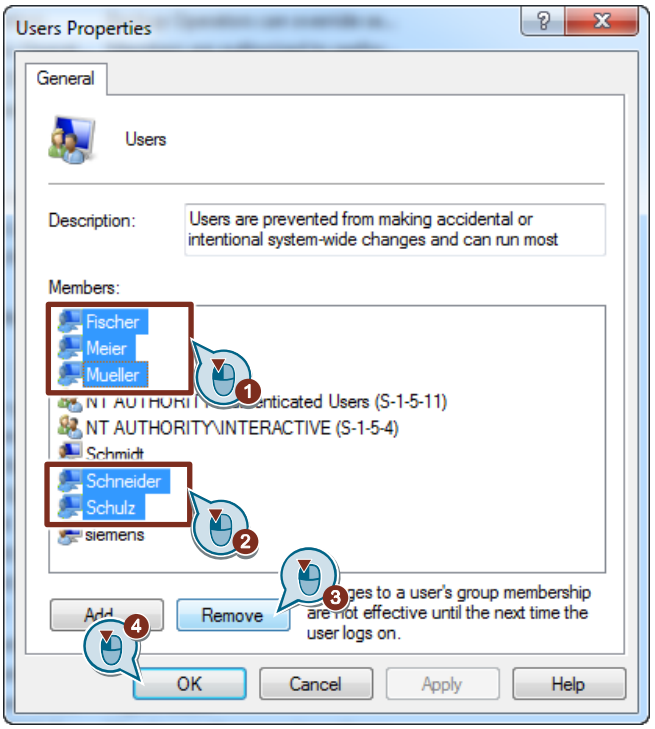
4.4.2 Creating user groups in Windows user management and assigning users to these user groups

Table 4-14

No.	Action
1.	Open the Windows Computer Management. 

No.	Action
2.	Click "Local Users and Groups" (1) and next click "Groups" (2). 
3.	Open the "Action" menu (1) and click "New Group..." (2).  The dialog for creating a new group opens.
4.	• Enter the name (1) and optionally a description (2) of the user group. • Next click "Add..." (3) below "Members".  **Note** When entering the group names, make sure that the user groups in Windows and in WinCC are named identically.
5.	A dialog for selecting the users opens.

No.	Action
6.	Click "Advanced..." to display the logged in users.  Another dialog opens in which you can select users.
7.	• Click "Find Now" (1) to list all users of the Windows user management. • Select the user "Mueller" (2) and confirm with "OK" (3).  The second dialog to select users closes.
8.	In the first dialog, confirm the user selection again with "OK".  The dialog closes.
9.	The selected user is entered as a member into the list of the administrator group.

No.	Action
10.	Click "Add..." to create the user group. 
11.	Create four more user groups (shift leader, maintenance, fitter, quality management) according to Table 4-1 and assign the corresponding users to the groups. **Note** The "Users" user group is created by default in Windows. All newly added users are automatically assigned to this group.
12.	• Open the user group "Users" and select the users Fischer, Meier, Mueller, Schneider and Schulz. (1)+(2) • Next click "Remove" (3) and confirm with "OK" (4).  **Note** If a user is assigned to multiple Windows groups, only one group may be created at the operator panel.
13.	Close the computer management.

Note At the logon server, a user can be a member of multiple user groups at the same time. At the operator panel, however, only one such user group is allowed to be known.
Otherwise, a message will be output in the Runtime at the operator panel stating that the user cannot explicitly be assigned to one user group. The login attempt fails.

4.4.3 Creating user groups in WinCC (TIA Portal)

How to configure user groups in WinCC (TIA Portal) is already detailed in this application example, see chapter Configuring and assigning user groups.

When using SIMATIC Logon, you do not necessarily have to assign users to the user groups in WinCC (TIA Portal).

ATTENTION **If the SIMATIC Logon server fails, it may no longer be possible to log in via SIMATIC Logon at the operator panel.**

To allow logging in at the operator panel in spite of this, we recommend assigning the administrator to the WinCC (TIA Portal) user groups also locally. If the logon server fails, the administrator can thus log in locally at the operator panel and create other users.

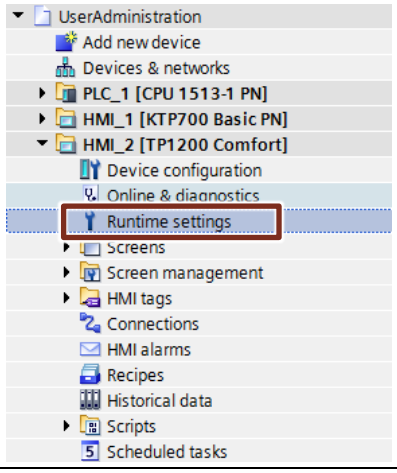
4.4.4 Creating and assigning authorizations in WinCC (TIA Portal)

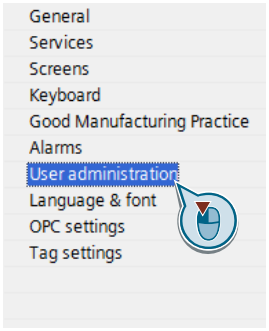
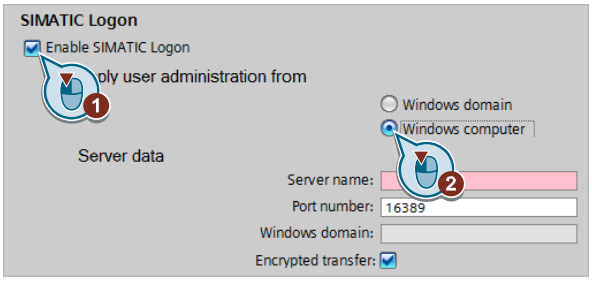
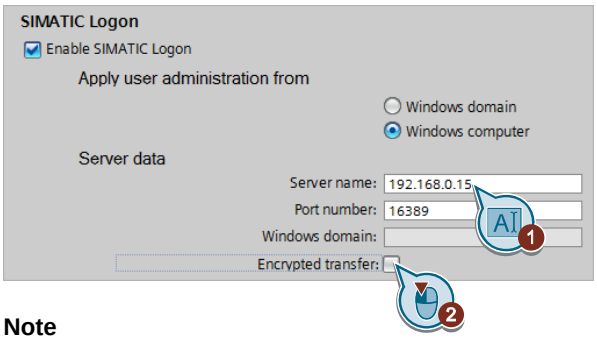
How to create and assign authorizations in WinCC (TIA Portal) is already detailed in this application example, see chapter Configuring and assigning authorizations.

4.4.5 Activating SIMATIC Logon in WinCC (TIA Portal)

To complete the user administration with SIMATIC Logon, you still need to activate it in WinCC (TIA Portal). The following table shows which steps are necessary to this end.

Table 4-15

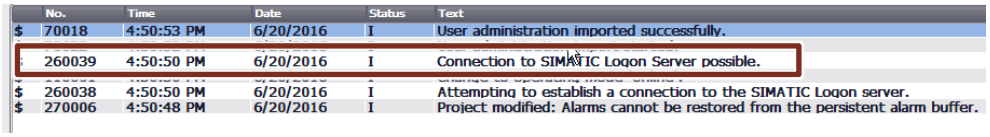
No.	Action
1.	In the TIA Portal, open the Runtime settings of the operator panel in which to activate SIMATIC Logon. 

No.	Action
2.	Select "User administration" in the area navigation. 
3.	• Activate the "Enable SIMATIC Logon" (1) radio button under the options listed under "User administration". • Next activate the "Windows computer" radio button. 
4.	• In the "Server name" field enter the IP address of the SIMATIC Logon computer (1). • Subsequently, disable the radio button "Encrypted transfer" to establish a simple unencrypted connection (2).  **Note** If you want to establish an encrypted connection between the operator panel and SIMATIC Logon, you need the corresponding certificates. For more information and a detailed instruction, see the FAQ How do you encrypt the connection between SIMATIC Logon and a Comfort Panel or a WinCC Runtime Advanced?.
5.	Save the project and load it to your operator panel.

4.4.6 Behavior in the Runtime

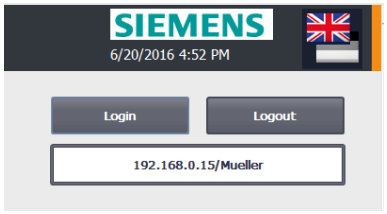
After the Runtime has started on the operator panel, the operator panel will try to first establish a connection to the logon server. Once this has been accomplished, the message text "Connection to SIMATIC Logon Server possible" is displayed.

Figure 4-8



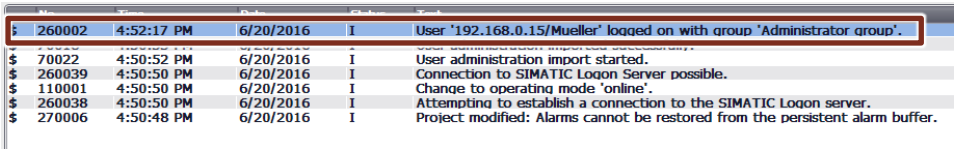
Next you can log in at the SIMATIC Logon Server using the Login button (see chapter Login and logout using system functions). Upon successful login, the display of the currently logged in user (see also chapter Display of the currently logged in user) will show the IP address of the logon server and the name of the logged in user.

Figure 4-9



Additionally, a message confirming the successful login is displayed in the message display.

Figure 4-10



5 Related Literature

Table 5-1

	Topic
\1\	Siemens Industry Online Support http://support.industry.siemens.com
\2\	Download page of the entry https://support.industry.siemens.com/cs/ww/en/view/109738532
\3\	Manual WinCC Advanced V13 SP1 https://support.industry.siemens.com/cs/ww/en/view/109091876
\4\	Manual SIMATIC Logon https://support.industry.siemens.com/cs/ww/en/view/34519648

6 History

Table 6-1

Version	Date	Modifications
V1.0	09/2016	First version
V1.1	06/2018	Add port release for SIMATIC Logon Server