

SIEMENS

SIMATIC

SIMATIC Logon V1.6

Configuration Manual

Security information

1

Conditions for secure
operation of SIMATIC Logon

2

User management and
electronic signatures

3

Hardware and Software
Requirements

4

Scope of delivery

5

Installation

6

SIMATIC Logon

7

Legal information

Warning notice system

This manual contains notices you have to observe in order to ensure your personal safety, as well as to prevent damage to property. The notices referring to your personal safety are highlighted in the manual by a safety alert symbol, notices referring only to property damage have no safety alert symbol. These notices shown below are graded according to the degree of danger.

 DANGER
indicates that death or severe personal injury will result if proper precautions are not taken.
 WARNING
indicates that death or severe personal injury may result if proper precautions are not taken.
 CAUTION
indicates that minor personal injury can result if proper precautions are not taken.
NOTICE
indicates that property damage can result if proper precautions are not taken.

If more than one degree of danger is present, the warning notice representing the highest degree of danger will be used. A notice warning of injury to persons with a safety alert symbol may also include a warning relating to property damage.

Qualified Personnel

The product/system described in this documentation may be operated only by **personnel qualified** for the specific task in accordance with the relevant documentation, in particular its warning notices and safety instructions. Qualified personnel are those who, based on their training and experience, are capable of identifying risks and avoiding potential hazards when working with these products/systems.

Proper use of Siemens products

Note the following:

 WARNING
Siemens products may only be used for the applications described in the catalog and in the relevant technical documentation. If products and components from other manufacturers are used, these must be recommended or approved by Siemens. Proper transport, storage, installation, assembly, commissioning, operation and maintenance are required to ensure that the products operate safely and without any problems. The permissible ambient conditions must be complied with. The information in the relevant documentation must be observed.

Trademarks

All names identified by ® are registered trademarks of Siemens AG. The remaining trademarks in this publication may be trademarks whose use by third parties for their own purposes could violate the rights of the owner.

Disclaimer of Liability

We have reviewed the contents of this publication to ensure consistency with the hardware and software described. Since variance cannot be precluded entirely, we cannot guarantee full consistency. However, the information in this publication is reviewed regularly and any necessary corrections are included in subsequent editions.

Table of contents

1	Security information.....	5
2	Conditions for secure operation of SIMATIC Logon.....	7
3	User management and electronic signatures.....	9
4	Hardware and Software Requirements.....	11
5	Scope of delivery.....	13
6	Installation.....	15
6.1	Overview of the installation tasks.....	15
6.2	How to Install SIMATIC Logon.....	16
6.3	How to make the required settings in the operating system.....	17
6.4	Retaining functionality if the SIMATIC Logon server fails.....	19
6.5	How to remove SIMATIC Logon.....	20
7	SIMATIC Logon.....	21
7.1	What is SIMATIC Logon?.....	21
7.2	Logon process via the SIMATIC Logon service.....	23
7.3	Overview of the required configuration tasks.....	25
7.4	SIMATIC Logon Service.....	26
7.4.1	What is the SIMATIC Logon Service?.....	26
7.4.2	Configuring SIMATIC Logon.....	26
7.4.2.1	How to Begin Configuration of SIMATIC Logon.....	26
7.4.2.2	The "Configure SIMATIC Logon" dialog box.....	27
7.4.2.3	How to make general settings ("General" tab).....	28
7.4.2.4	How to configure the working environment of SIMATIC Logon ("Working Environment" tab).....	30
7.4.2.5	How to configure the logon device ("Logon Device" tab).....	32
7.4.2.6	How to configure automatic logoff ("Automatic Logoff" tab).....	33
7.4.2.7	How to configure the certificate for the "SIMATIC Logon Remote Access" service ("Certificate" tab).....	34
7.4.2.8	How to add a user.....	36
7.4.2.9	How to remove a user.....	36
7.4.3	Logging on with SIMATIC Logon.....	37
7.4.3.1	Logging on with SIMATIC Logon Service.....	37
7.4.3.2	Logon via the logon dialog box (keyboard).....	38
7.4.3.3	Logon via a smart card reader.....	38
7.4.3.4	Logging on via another device.....	42
7.4.3.5	Logon via a screen keyboard.....	42
7.5	SIMATIC Logon Role Management.....	43
7.5.1	What is the SIMATIC Logon Role Management?.....	43
7.5.2	Structure of SIMATIC Logon Role Management.....	44

7.5.3	Assigning permissions for applications.....	46
7.5.3.1	Overview of the configuration tasks.....	46
7.5.3.2	How to create a role.....	46
7.5.3.3	How to configure a role.....	47
7.5.3.4	How to assign a role to groups and users.....	48
7.5.3.5	How to assign function rights to a role.....	49
7.5.3.6	How to assign Logon Stations to a role.....	49
7.5.3.7	How to assign Phases to a role.....	50
7.5.3.8	How to assign Security Areas to groups and users or to Logon Stations.....	50
7.5.3.9	How to delete a role.....	51
7.5.3.10	How to change the properties of a role.....	51
7.5.3.11	How to export role management data.....	52
7.5.3.12	How to assign groups and users to another computer.....	53
7.5.3.13	How to change the project password.....	53
7.5.3.14	Key combinations.....	54
7.5.3.15	Folder icons of the SIMATIC Logon Role Management.....	55
7.5.4	Calling dialog boxes from the shortcut menu.....	55
7.5.4.1	Working with shortcut menus.....	55
7.5.4.2	"New Role" shortcut menu.....	55
7.5.4.3	"Edit" shortcut menu.....	56
7.5.4.4	"Properties" shortcut menu.....	56
7.5.4.5	"Delete" shortcut menu.....	56
7.5.5	The toolbar and menu bar of SIMATIC Logon Role Management.....	56
7.5.5.1	Toolbar.....	56
7.5.5.2	Menu bar of SIMATIC Logon Role Management.....	57
7.5.5.3	File menu.....	58
7.5.5.4	Edit menu.....	58
7.5.5.5	Help menu.....	59
7.6	SIMATIC Logon Event Log.....	60
7.6.1	What is the SIMATIC Event Log Viewer?.....	60
7.6.2	The "SIMATIC Logon Event Log Viewer" dialog box.....	60
7.6.3	The "SIMATIC Logon Event Log Viewer - Filter Events" dialog box.....	61
7.6.4	How to Track Logons and Logoffs with the SIMATIC Logon Event Log Viewer.....	62
7.7	SIMATIC Electronic Signature.....	64
7.7.1	What is SIMATIC Electronic Signature?.....	64
7.7.2	Rules for Electronic Signatures.....	65
7.7.3	Signing operations.....	65
7.7.3.1	The "SIMATIC Electronic Signature: Acquire Signatures" dialog box.....	65
7.7.3.2	How to sign actions and state changes.....	66
7.8	SIMATIC Logon Development Kit.....	68
7.8.1	What is the SIMATIC Logon Development Kit?.....	68
Index		69

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>.

Conditions for secure operation of SIMATIC Logon

SIMATIC Logon must be operated as part of a holistic security concept. In general, the recommendations from the Siemens Industrial Security (<https://www.siemens.com/industrialsecurity>) websites apply.

In the PCS 7 & WinCC environment, the recommendations from the PCS7 & WinCC Security concept (<https://www.industry.siemens.com/topics/global/de/industrial-security/support/seiten/whitepaper.aspx>) apply. These include, among other things, a defense in depth, distribution into security cells, user management, access control as well as the use of antivirus solutions and firewalls.

In particular, SIMATIC Logon must only be used in trusted networks. SIMATIC Logon clients must be operated in the same trust zone as the SIMATIC Logon server. Direct access from external networks (e.g. the Internet) is not supported and must be prevented.

User management and electronic signatures

Introduction

In plants monitored and controlled by process control systems, there are special requirements relating to access to functions and plant areas.

Important requirements

The following requirements are important for the validation of plants:

- User management for assigning access rights to avoid unauthorized or unwanted access to the plant
- Creation and archiving of verification of important or critical actions

Implementation

In plants in which SIMATIC components are used, validation of the plant is possible with the following components:

Component	Area of application	Described in section
SIMATIC Logon	Assignment of user-specific rights	SIMATIC Logon (Page 21)
SIMATIC Electronic Signature	Querying and archiving the required verifications	SIMATIC Electronic Signature (Page 64)

FDA 21 CFR Part 11

SIMATIC Logon and SIMATIC Electronic Signature simplify the validation of plants in conformity to FDA 21 CFR Part 11. These globally recognized guidelines and requirements were formulated by the U.S. FDA (Food and Drug Administration).

Hardware and Software Requirements

Hardware requirements

You can find the latest hardware requirements in the readme file. You can open this from the Start menu:

Siemens Automation > Documentation > Readmes > Language > SL – Readme

Software requirements

You can find the latest software requirements in the readme file. You can open this from the Start menu:

Siemens Automation > Documentation > Readmes > Language > SL – Readme

Scope of delivery

Scope of delivery

The *SIMATIC Logon* software package consists of the following software components:

Software component	Area of application	Described in section
SIMATIC Logon Service	Central access protection for SIMATIC applications and plant areas	SIMATIC Logon Service (Page 26)
SIMATIC Logon Role Management	Role management for applications and their assignment to Windows groups including assignment of permissions	SIMATIC Logon Role Management (Page 43)
SIMATIC Logon Event Log Viewer	The SIMATIC Logon Event Log Viewer is a component that takes on the task of recording and displaying events for an application.	SIMATIC Logon Event Log Viewer (Page 60)
SIMATIC Electronic Signature	Creation of electronic signatures for state changes in the process and for accessing the process	SIMATIC Electronic Signature (Page 64)
SIMATIC Logon Development Kit	The Development Kit is intended for programmers who wish to integrate SIMATIC Logon in a customer application.	SIMATIC Logon Development Kit (Page 68)

Note

SIMATIC Logon requires a license.

See also

The "SIMATIC Logon Event Log Viewer" dialog box (Page 60)

Installation

6.1 Overview of the installation tasks

Overview of the installation tasks

Installing *SIMATIC Logon* involves the following tasks:

- Installing SIMATIC Logon (Page 16)
- Making the required settings in the operating system

Central logon computer for user authentication

If you use a central logon computer for user authentication, refer to the notes in the following section:

- Retaining functionality if the SIMATIC Logon logon computer fails (Page 19)

Removal

If you want to remove *SIMATIC Logon*, refer to the procedure in the following section:

- How to remove SIMATIC Logon (Page 20)

Software update

You run a software update just like a new installation. Ignore the message that there is a version of *SIMATIC Logon* already installed.

6.2 How to Install SIMATIC Logon

Introduction

SIMATIC Logon is installed with a setup program.

The following components are installed with the setup:

- **SIMATIC Logon Service**
- SIMATIC Logon Role management
- **SIMATIC Logon Event Log**
- **SIMATIC Electronic Signature**

Requirements

- You are logged on with **administrator rights** on the computer on which you want to install *SIMATIC Logon*.
- The Windows Explorer is open.
- All other programs have been shut down.

Procedure

You can find a description in the corresponding document accompanying the installation medium or *SIMATIC Logon* is installed with the setup of a product (with *SIMATIC PCS 7*, for example).

6.3 How to make the required settings in the operating system

Introduction

This section is intended for Windows administrators.

Requirements

- You are familiar with the administration of the Windows operating system.
- You are logged on as a member of the "Administrators" group in Windows.

Rules for the Windows "Logon_Administrator" group

- To configure SIMATIC Logon, a new Windows group called "Logon_Administrator" is required.
- All users who are members of the Windows group of "Logon_Administrators" are authorized to access the logon dialog box "Configure SIMATIC Logon".
- You should only assign users to the "Logon_Administrator" Windows group. If you assign a subgroup to the "Logon_Administrator" Windows group, its members will be prevented from accessing the "Configure SIMATIC Logon" dialog box. It is not possible to authenticate any members of a subgroup.

Users in a Windows domain

Note

SIMATIC Logon users must be direct members of a Windows group. The users may **not** belong to a subgroup of a Windows group.

Procedure

1. Enter all SIMATIC Logon users in the Windows user management.
Set the following items in order to enable the display of the full name of a logged on user in SIMATIC Logon:
 - Enter the full name of this user in the Windows user management.
2. Prepare for the configuration of SIMATIC Logon: Set up the "Logon_Administrator" group in Windows.
 - Background: Configure SIMATIC Logon in the "Configure SIMATIC Logon" dialog box (see the section "How to configure SIMATIC Logon (Page 26)"). The "Logon_Administrator" group must be set up in Windows user management in order to enable access to this dialog box.

Note

You can set up the "Logon_Administrator" group on the following media:

- On the local station
 - On a domain which can be accessed at the local station
-

3. Enter the user in the "Logon_Administrator" group. Assign all users who are going to work with the "Configure SIMATIC Logon" dialog box to the "Logon_Administrator" group.

6.4 Retaining functionality if the SIMATIC Logon server fails

Retaining functionality in case of failure

If you work with a logon computer for the SIMATIC Logon Service or with a domain, we recommend you take the following steps to guard against failure of this computer:

- Set up all required Windows groups and Windows users on the local computer.
- If the logon computer fails, you can select the local computer for logging on from the "Log on to" drop-down box of the logon dialog box.
- If the logon computer fails during the logon procedure, the logon procedure is automatically performed on the local computer. The failure and repeated authentication is recorded in the SIMATIC Logon event log.

6.5 How to remove SIMATIC Logon

Requirement

You are logged on with administrator rights on the computer on which you want to remove SIMATIC Logon.

Procedure

1. From the Start menu of Windows, select the menu command **Start > Settings > Control Panel**.
The "Control Panel" dialog box opens.
2. Double-click on "Add or Remove Programs" in the detailed view.
3. Select the "SIMATIC Logon" entry.
4. Click the "Remove" button.
5. When you are asked if you really want to remove SIMATIC Logon, click "Yes".
The dialog box for removing programs opens and removal begins.

Result

The selected component is removed.

Note

You should report any errors that occur during the removal of the program to the administrator responsible or to the service hotline.

SIMATIC Logon

7.1 What is SIMATIC Logon?

Components of SIMATIC Logon

With SIMATIC Logon, you can assign authorizations for SIMATIC applications and plant areas. The following software components belong to SIMATIC Logon:

Software component	Area of application	Described in section
SIMATIC Logon Service	Central access protection for SIMATIC applications and plant areas	SIMATIC Logon Service (Page 26)
SIMATIC Logon Role Management	Administration of application policies and their assignment to Windows groups, including the assignment of permissions.	SIMATIC Logon Role Management (Page 43)
SIMATIC Logon Eventlog Viewer	SIMATIC Logon Eventlog Viewer is a component which handles the logging and visualization of event for an application.	SIMATIC Logon Eventlog Viewer (Page 60)
SIMATIC Electronic Signature	Used to create electronic signatures for status transitions and user intervention in the process	SIMATIC Electronic Signature (Page 64)
SIMATIC Logon Development Kit	The Development Kit is designed for use by programmers who want to integrate SIMATIC Logon in customer applications.	SIMATIC Logon Development Kit (Page 68)

Start of SIMATIC Logon

The SIMATIC Logon dialog boxes are opened by the applications by means of application-specific calls. For information about the activation of application-specific calls of SIMATIC Logon, refer to the documentation of the corresponding application.

Application requirements

SIMATIC Logon components are only available to applications in which the SIMATIC Logon components have been integrated.

The description of the corresponding application shows whether or not any SIMATIC Logon components have been integrated.

Examples

The SIMATIC Logon components are integrated in the applications outlined below, for example:

- Automation License Manager
- WinCC
- SIMATIC BATCH
- STEP 7

Users in a Windows domain

Note

SIMATIC Logon users must be direct members of a Windows domain. These users may **not** be members of a subdomain of a Windows domain.

See also

The "SIMATIC Logon Event Log Viewer" dialog box (Page 60)

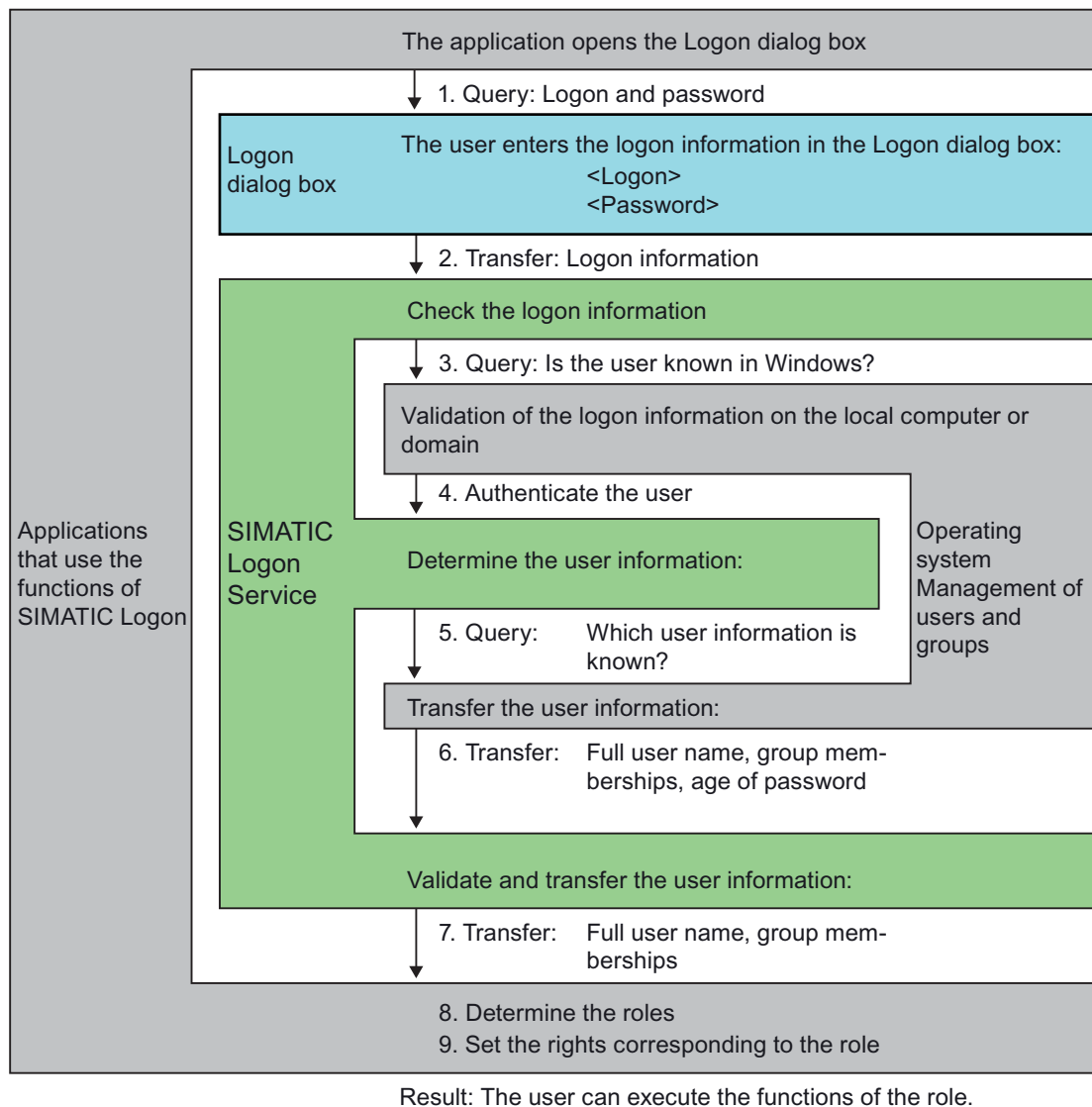
7.2 Logon process via the SIMATIC Logon service

Requirement

The logon routine was configured in SIMATIC Logon (for further information, refer to "Overview of necessary configuration tasks (Page 25)".

Logon process via the SIMATIC Logon service

The diagram below shows the automated process for user logon to an application with integrated SIMATIC Logon.



Result

The user data were registered in SIMATIC Logon. Other applications using SIMATIC Logon automatically receive these user data from SIMATIC Logon.

7.3 Overview of the required configuration tasks

Overview of the required configuration tasks

To log on using the SIMATIC Logon Service, the following configuration tasks are necessary:

Task	What?	Where?	Described in
1	Set up the "Logon_Administrator" group	Windows User Management	Online help of the operating system You can find the online help of the operating system with the keyword "Help and Support" .
2	Set up user accounts for SIMATIC Logon	Windows User Management	Online help of the operating system
3	Add the user accounts for SIMATIC Logon to the Windows groups	Windows User Management	Online help of the operating system
4	Configure the roles of the users	SIMATIC Logon Role Management	Section "Overview of the configuration tasks (Page 46)"
5	Configure SIMATIC Logon in the "Configure SIMATIC Logon" dialog box	"Configure SIMATIC Logon" dialog box	Section • "How to begin configuration of SIMATIC Logon (Page 26)" • "The "Configure SIMATIC Logon" dialog box (Page 27)"

7.4 SIMATIC Logon Service

7.4.1 What is the SIMATIC Logon Service?

SIMATIC Logon Service

SIMATIC Logon Service is the basis for SIMATIC Logon. The SIMATIC Logon Service implements access protection for applications (for example, SIMATIC BATCH or WinCC). The access protection is based on mechanisms of the Windows operating system.

The user logs on to and off from the application through the SIMATIC Logon Service.

Recording of events

SIMATIC Logon records the following events with the SIMATIC Logon Event Log Viewer:

- Successful logon
- Failed logon attempt
- Authentication of a user
- Logoff by user
- Automatic logoff
- Password change

The recorded events can be viewed using the SIMATIC Logon Event Log Viewer. For detailed instructions, refer to the section "How to Track Logons and Logoffs with the SIMATIC Logon Event Log Viewer (Page 62)".

Windows settings for the SIMATIC Logon Service

The section "How to make the required settings in the operating system (Page 17)" describes how to make the Windows settings.

7.4.2 Configuring SIMATIC Logon

7.4.2.1 How to Begin Configuration of SIMATIC Logon

Requirement

You are a member of the groups:

- "Administrators" or "Power users" Windows groups
- "Logon_Administrator" Windows group

Procedure

1. Select the menu command **Start > SIMATIC > SIMATIC Logon > Configure SIMATIC Logon**.
The "Configure SIMATIC Logon" logon dialog box opens.
2. Enter your logon data in the input fields of the Logon dialog box:

Input field	Meaning
User name	Input of the user name
Password	Input of the password
Log on to	Selection of the domain/the local computer

Result

The "Configure SIMATIC Logon (Page 27)" dialog box opens after successful logon.

Failure of the SIMATIC Logon computer

You can find more information about this in the section "Retaining functionality if the SIMATIC Logon server fails (Page 19)".

7.4.2.2 The "Configure SIMATIC Logon" dialog box

The "Configure SIMATIC Logon" dialog box

The "Configure SIMATIC Logon" dialog box has the following tabs:

Tab	Settings
General (Page 28)	• Select the display language • Activate the time display according to ISO 8601 • Activate a notice text that is displayed in the logon dialog box (keyboard) • Activation of the "Default User" function • Set a reminder for password change (reminder x days prior to expiration of password)
Working environment (Page 30)	Set from which computer the user data will be retrieved: • From this computer or from a "Windows domain" • From another computer (enter the name of the computer) • Activate accelerated user logon: only the global groups of domains (safety groups) and local computer groups are included.

Tab	Settings
Logon device (Page 32)	Setting which device will run the logon / authentication: • Keyboard • Smart card reader • Other devices • Enable the on-screen keyboard: – Windows on-screen keyboard ("osk.exe") – WinCC keyboard (CConScreenKeyboard) as of SIMATIC WinCC 7.3 and as of SIMATIC WinCC RT Prof. Edition V13 SP1 or later – Another on-screen keyboard, possibly with use of call parameters
Automatic logoff (Page 33)	Setting a waiting period for logoff of SIMATIC Logon.
Certificate (Page 34)	Settings for the "SIMATIC Logon Remote Access" service.

Automatic logoff

Note

The function "Automatic logoff" will become active after the next logon operation.

Log files

Errors are recorded in the log files for SIMATIC Logon. You can make these available to experts for analysis.

The Log files are available in the following folder:
 "...\\Siemens\\SimaticLogon\\diagnostics"

7.4.2.3 How to make general settings ("General" tab)

Introduction

You can make the following settings in the "General" tab of the "Configure SIMATIC Logon" dialog box:

- Display language for SIMATIC Logon
- Time display according to ISO 8601
- Activate and enter a notice text that is displayed in the logon dialog box (keyboard).
- Activate and change the "Default User"
- Password expiration reminder

Rules for creating users and groups

Note

In contrast to all other users, the "DefaultGroup" and the "Default User" **must not** be created in the Windows User Management. The "Default User" is a member of the "DefaultGroup" and "Emergency_Operator" roles. You determine the permissions of these roles in the respective applications.

Requirements

- The character set for the language in which you wish to work with SIMATIC Logon is available.
- You are a member of the groups:
 - "Administrators" or "Power users" Windows groups
 - "Logon_Administrator" Windows group

Procedure

1. Select the menu command **Start > SIMATIC > SIMATIC Logon > Configure SIMATIC Logon**. The "Configure SIMATIC Logon" logon dialog box opens.
2. Enter your logon data in the input fields of the Logon dialog box.
You can find more information about this in the section "How to Begin Configuration of SIMATIC Logon (Page 26)".
3. Select the display language from the "Language" drop-down list.
Languages available for installation:
 - German
 - English
 - French
 - Italian
 - Spanish
 - Japanese
 - Chinese
4. If you want to display the date and time in accordance to ISO 8601, activate the check box "Date / Time display according to ISO 8601". The time is then shown in the following format: CCYY-MM-DD hh:mm:ss ±hh:mm
The first part corresponds to Coordinated Universal Time (UTC), the difference to local time is given after the sign. CC: Century, YY: Year, MM: Month, DD: Day, hh: Hour, mm: Minute, ss: Seconds.
If this option is not selected, the data and time are shown in local time format.
5. If you want to display a notice text in the Logon dialog box (keyboard), select the check box "Show the following notice text at logon:" and enter the text you want to display in the text box.

6. If you want the "Default User" to always be logged on implicitly at system startup and at user logoff, activate the check box "Use the following data if the user is not explicitly logged on:".
If this check box is activated, you can enter or change the name of the group and the user. The length of the name must be at least 1 character.
7. If you have assigned passwords that are subject to a time limitation, enter a desired value in the input field "Days for reminder of password expiration".
Range for the setting: From 0 days (no reminder) to a maximum of 999 days
8. Click "Apply" or "OK".

Note

The changes take effect once the program is restarted.

7.4.2.4 How to configure the working environment of SIMATIC Logon ("Working Environment" tab)

Introduction

You can make the following settings in the "Working environment" tab of the "Configure SIMATIC Logon" dialog box:

- Set the computer from which the user data is to be acquired:
To enable access protection on a computer, SIMATIC Logon needs to know the location from which the user data should be acquired. The following settings are possible: Get user data from:
 - this computer or from a Windows domain
 - another computer (enter the name of the computer)
- Activate accelerated user logon: only the global groups of domains (safety groups) and local computer groups are included.

Obtaining user data from this computer or a Windows domain

When a domain server is available in the working environment, you can use SIMATIC Logon to take advantage of the group and user management features. Using the group and user management on the domain server once allows all PCs belonging to the domain access to the groups and users.

If the computer does not belong to a domain or no domain computer is available when the logon is performed, the local computer is automatically offered for the logon.

Note

It is not necessary to install SIMATIC Logon on the domain server.

Obtaining user data from another computer

If you want to get the user data from another computer, you need to specify the computer. Enter the corresponding name of the computer in the input field. You then only need to manage groups and users on this computer.

Note

SIMATIC Logon must be installed on the station which is to provide the user data.

Activate accelerated user logon:

If this option is selected, only the following groups are included at logon to SIMATIC Logon:

- Global groups of domains (safety groups) and
- Local computer groups

Otherwise SIMATIC Logon includes the following user groups on by default:

- Global groups of domains (safety groups)
- Local computer groups
- Local domain groups (safety groups)
- Local domain groups (distribution groups)
- Global domain groups (distribution groups)
- Universal domain groups (distribution groups)

Requirement

You are a member of the groups:

- "Administrators" or "Power users" Windows groups
- "Logon_Administrator" Windows group

Procedure

1. Select the menu command **Start > SIMATIC > SIMATIC Logon > Configure SIMATIC Logon**. The "Configure SIMATIC Logon" logon dialog box opens.
2. Enter your logon data in the input fields of the Logon dialog box.
You can find more information about this in the section "How to Begin Configuration of SIMATIC Logon (Page 26)".
3. Select the "Working environment" tab.

4. Make the following settings:
 - Activate the "from this computer or from a Windows domain" check box if SIMATIC Logon user data are to be provided from a domain or from a single-user station.
 - If SIMATIC Logon user data is to be provided by a Logon Station of the SIMATIC Logon group, activate the "from other computer" check box and enter the name of this station in the corresponding input field
Input of an IP address is not supported.
 - If you want to use accelerated user logon, select the checkbox "Include only global groups of domains (safety groups) and local groups of the computer".
5. Click "Apply" or "OK".

7.4.2.5 How to configure the logon device ("Logon Device" tab)

Introduction

You can make the following settings in the "Logon device" tab of the "Configure SIMATIC Logon" dialog box:

- To log on for an application for which access protection is activated, you can select one of the following possibilities:
 - Logon via the logon dialog box (keyboard)
 - Logon via a smart card reader
 - Logon via another device (for example, device that can identify fingerprints)
 - Logon via a screen keyboard

You can find additional information about logon devices in the section "Logging on with SIMATIC Logon Service (Page 37)".

- Enable the on-screen keyboard:
 - Windows on-screen keyboard ("osk.exe")
 - WinCC keyboard (CConScreenKeyboard) as of SIMATIC WinCC 7.3 and as of SIMATIC WinCC RT Prof. Edition V13 SP1 or later
 - Another on-screen keyboard, possibly with use of call parameters

Requirement

You are a member of the groups:

- "Administrators" or "Power users" Windows groups
- "Logon_Administrator" Windows group

Procedure

1. Select the menu command **Start > SIMATIC > SIMATIC Logon > Configure SIMATIC Logon**. The "Configure SIMATIC Logon" logon dialog box opens.
2. Enter your logon data in the input fields of the Logon dialog box.
You can find more information about this in the section "How to Begin Configuration of SIMATIC Logon (Page 26)".
3. Select the "Logon device" tab.
4. Make the following settings:
 - If you want to use the keyboard as the logon device, select the check box "Logon via keyboard".
 - If you want to use the chip card reader as the logon device, select the check box "Logon via chip card reader" and select the device from the drop-down list box.
 - If you want to use a device other than the keyboard or chip card reader as the logon device, select the check box "Logon via another device".
 - If you want to use the on-screen keyboard, select the checkbox "Use on-screen keyboard" and select the corresponding on-screen keyboard program. Default is the Windows on-screen keyboard ("osk.exe").
5. Click "Apply" or "OK".

Driver for "Logon via another device"

Note

The driver required for "Logon via another device" has to be supplied by the manufacturer. Ask your Siemens representative about available devices and their associated drivers.

7.4.2.6 How to configure automatic logoff ("Automatic Logoff" tab)

Introduction

You can activate and configure "Automatic logoff" for access management with SIMATIC Logon.

When "automatic logoff" is enabled and the mouse is not moved and no key is pressed for a certain time, the user is automatically logged off by the access management with SIMATIC Logon.

When the selected wait time has elapsed, a message is displayed informing you of the automatic logoff. The user can restart the wait time by moving the mouse or pressing any key. This avoids accidental logging off.

Note

A user can log off at any time without the wait time.

Logoff procedure and settings when the "Automatic logoff" check box is activated

If there was no activity on the computer during the wait time of "x" minutes, the logoff is started.

- A dialog box indicates that the user will be logged off after "y" seconds.
- The logoff procedure is completed after "x" minutes + "y" seconds.

Settings	from	to
Delay time "x" / in minutes	1	999
Time until automatic logoff "y" / in seconds	0	999

Requirement

You are a member of the groups:

- "Administrators" or "Power users" Windows groups
- "Logon_Administrator" Windows group

Procedure

1. Select the menu command **Start > SIMATIC > SIMATIC Logon > Configure SIMATIC Logon**. The "Configure SIMATIC Logon" logon dialog box opens.
2. Enter your logon information in the input boxes of the Logon dialog box.
You can find additional information about this in the section "How to begin configuration of SIMATIC Logon (Page 26)".
3. Open the "Automatic Logoff" tab.
4. Activate the "Automatic logoff" check box.
5. Enter the wait time before the notification of automatic logoff is displayed.
6. Enter the time for which the notification of automatic logoff should be displayed.
7. Click on the "Apply" button or the "OK" button.

7.4.2.7 How to configure the certificate for the "SIMATIC Logon Remote Access" service ("Certificate" tab)**Introduction**

You can use a secured connection with a "certificate" for access management with "SIMATIC Logon Remote Access". Without a "certificate" you can only use non-secured connections.

A secured connection is established with the help of Transport Layer Security (TLS) v1.2. With TLS 1.2 the entire communication between the server (SIMATIC Logon PC) and the client is encrypted.

You can use both self-signed certificates as well as certificates issued by a certification office.

Requirement

- You are a member of the groups:
 - "Administrators" Windows group
 - "Logon_Administrator" Windows group
- A certificate file in PEM format (.pem) and a private key must be stored on the SIMATIC Logon computer to establish a secured connection.
- Certificate and private key can be contained in one or two PEM files.
- The firewall rules are automatically created by SIMATIC Logon for Windows firewall. If you are using a different firewall, these rules must be managed by the administrator.

Procedure for configuring the encryption

1. Select the menu command **Start > SIMATIC > SIMATIC Logon > Configure SIMATIC Logon**. The "Configure SIMATIC Logon" logon dialog box opens.
2. Enter your logon data in the input fields of the Logon dialog box.
You can find more information about this in the section "How to Begin Configuration of SIMATIC Logon (Page 26)".
3. Select the "Certificate" tab.
4. Select the certificate file (.pem) and the private key which are stored on the server (SIMATIC Logon PC). If certificate and private key are present in one file, this is to be selected for both the "certificate" and "private key".
5. The certificate details are shown in the bottom area.
6. Select the "TLS-secured connection" and/or "Non-secured connection" check box.
 - If both options are set, both non-secured and secured connections are permitted.
 - If no option is set, the service will not accept any connections.
 - If the "TLS-secured connection" option is set, secured connections are accepted.
 - If the "Non-secured connection" option is set, only non-secured connections are accepted.
7. Click "Apply" and observe the displayed instructions (PC restart).

Procedure for deleting a certificate

1. Select the menu command **Start > SIMATIC > SIMATIC Logon > Configure SIMATIC Logon**. The "Configure SIMATIC Logon" logon dialog box opens.
2. Enter your logon data in the input fields of the Logon dialog box.
You can find more information about this in the section "How to Begin Configuration of SIMATIC Logon (Page 26)".
3. Select the "Certificate" tab.
4. The certificate details are shown in the bottom area.
5. Click "Delete certificate".
6. Click "Apply" and observe the displayed instructions.

Note

SIMATIC Logon provides no option to restore a deleted certificate. Make sure that you have a backup copy of the certificate before you delete it.

7.4.2.8 How to add a user

Procedure

1. Set up the user account in Windows.
2. Assign the user to the required Windows groups.
3. Use SIMATIC Logon Role Management (Page 43) to configure the permissions for SIMATIC applications and plant areas.

Additional information

- Online help of the operating system
You can open the online help of the operating system with the menu command **Start > Help and Support**.

7.4.2.9 How to remove a user

Procedure

1. Remove the user from an application using the SIMATIC Logon Role Management.
2. Remove the user from a group for a specific utility.
3. Remove the user from the Windows group.
4. Remove the user as a Windows user.

7.4.3 Logging on with SIMATIC Logon

7.4.3.1 Logging on with SIMATIC Logon Service

Types of logons

SIMATIC Logon Service distinguishes between two types of logons:

- **User identification:**
This checks if the user can be authenticated and if the user has permission for the respective application.
- **One-time logon:**
Following authentication, the user is logged on for all applications that support this logon method (Single sign on); the user is not required to logon multiple times or change the logon.

The user's logoff or change of logon may be rejected with this method because an application is in a state in which data can otherwise be lost.

The type of logon currently being used is shown in the title bar of the logon dialog box.

Logon options

To log on with an application for which access protection is activated, you can select one of the following options:

- Logon via the logon dialog box (keyboard) (Page 38)
- Logon via a smart card reader (Page 38)
- Logging on via another device (Page 42)

Actions during logoff

Independent of the logon device used, the following actions are performed when you log on:

- Authentication of the user
- Identification of the full user name
- Password age check (optional)
- Identification of the Windows groups to which the logged-on user belongs

Note

If a user can be authenticated, he or she is automatically assigned to the "Emergency_Operator" role. If an application supports this role, the user can perform actions according to the rights that have been set.

The "Emergency_operator" group does not need to be created in Windows User Management.

Configuration of the device for logging on with SIMATIC Logon

For information about configuring a device for logging on with SIMATIC Logon, refer to the section "How to configure the logon device ("Logon Device" tab) (Page 32)".

Calling the SIMATIC Logon Service

You start the SIMATIC Logon Service from the user interface of an application in which this service has been embedded. It cannot be started independently in Windows.

7.4.3.2 Logon via the logon dialog box (keyboard)

Opening the dialog box for logging on and off

The dialog box for logging on and off is started from the user interface of the application in which the service is embedded. It cannot be started independently in Windows.

Dialog box for logging on and off

The dialog box for logging on and off contains the following input boxes:

Input box	Meaning
User name	Enter the user name
Password	Enter the user password
Log on to	Select the domain / local computer

Dialog box for changing the password

From the dialog box for logging on and off, you can also open the dialog box for changing the password. The dialog box for changing the password contains the following input boxes:

Input box	Meaning
User name	Enter the user name
Log on to	Select the domain / local computer
Old password	Enter the password used up to now
New password	Enter the password to be used in the future
Password confirmation	Enter the password to be used in the future once more

7.4.3.3 Logon via a smart card reader

Introduction

SIMATIC Logon supports logons with a SIMATIC application via a smart card and smart card reader.

This section describes the requirements must be met and how to configure the smart card.

Note

Each user needs a smart card to use the smart card reader as the logon device.

Requirements for using smart card readers (connected to USB or COM port)

- The smart card reader meets the PC/SC specification.
- The smart card reader is connected according to the manufacturer instructions and the corresponding driver is installed.
- Select the smart card reader in "Configuring SIMATIC Logon" in the "Logon device" tab and activate the configuration with "OK" or "Apply".
- Microsoft Remote Desktop Protocol (RDP) is supported by SIMATIC Logon version 1.5.3 or higher:
 - Before establishing a remote desktop connection to a SIMATIC Logon PC, check whether the "Smartcards" option is selected in the options of the RDP under local resources.
 - Log on to the SIMATIC Logon PC via RDP.
 - Select the smart card reader in "Configuring SIMATIC Logon" in the "Logon device" tab and activate the configuration with "OK" or "Apply". This is not necessary if local and remote smart card readers with the same name are available and the smart card reader was already selected locally.
 - Before the RDP connection is terminated the configuration should be switched to keyboard unless local and remote smart card readers with the same name exist.

Rules

Note

SIMATIC Logon supports smart cards with operating systems listed in the Readme.

The data format on the smart card has changed as of SIMATIC Logon version 1.3. Smart cards that were created with previous versions cannot be used any longer and must therefore be rewritten.

The smart card must also be rewritten after a change of the Windows password. Otherwise the smart card contains the "old" password and the logon procedure is rejected.

The user authentication supported by SIMATIC Logon supports both the one-factor authentication security level (1-FA = owns the smart card) as well as the two-factor authentication security level (2-FA = owns the smart card and knows the PIN). If the card is lost at 1-FA, the card owner's Windows password must be changed.

A 2-FA is recommended. Only TCOS 3 smart cards are currently supported. If you only want 2-FA, you have to take appropriate measures so that no smart card with 1-FA is created and used.

Configuring smart cards

1. **Open the SIMATIC Logon link on the desktop > Edit Smart Card.**
The "SIMATIC Logon Service - Edit Smart Card" dialog box opens.
2. Enter the following data:
 - Logon PC
 - User name
 - Password
 - Password confirmation
3. To use 1-FA, clear the check mark at "Protect data with PIN". 2-FA is configured by default.
4. Insert the smart card in the smart card writer (reader).
5. Click the "Write data to smart card" button.
6. Enter the following data for 2-FA:

Note**Minimum number of characters for the PIN**

The PIN must consist of at least 8 characters and a maximum of 50 characters.

- PIN
 - Confirming the PIN
7. Click "OK".

The system checks the entered data. If the card is not a TCOS3 card, the error message "The inserted smart card is not supported for the current operation" is displayed. If authentication is successful, the system writes the data to the smart card.

Reading / checking smart card

If you use 1-FA, follow these steps:

1. **Open the SIMATIC Logon link on the desktop > Edit Smart Card.**
The "SIMATIC Logon Service - Edit Smart Card" dialog box opens.
2. Click the "Read data from smart card" button.

If the data on the smart card are OK, the logon PC and the user name are shown in the corresponding fields. The password is not displayed.

If you use 2-FA, follow these steps:

1. **Open the SIMATIC Logon link on the desktop > Edit Smart Card.**
The "SIMATIC Logon Service - Edit Smart Card" dialog box opens.
2. Click the "Read data from smart card" button.
The dialog box "Enter PIN" is opened.
3. Enter your PIN.

If the data on the smart card are OK and your PIN is correct, the logon PC and the user name are shown in the corresponding fields. The password is not displayed.

Deleting data

Follow these steps to delete data:

1. Read the data from your smart card.
2. Click the "Delete data from smart card" button.

Logon with smart card

If you use 1-FA, log on as follows:

1. Insert the smart card in the smart card reader.

You are now logged on in the system.

If you use 2-FA, log on as follows:

1. Insert the smart card in the smart card reader.
The dialog box "Enter PIN" is opened.
2. Enter your PIN.
3. Click "OK".

You are now logged on in the system.

Errors during the logon with 2-FA

Error messages can occur when you log on with 2-FA.

- Error message "The integration check of the data on the smart card is faulty."
Possible causes:
 - The entered PIN is faulty.
 - The data on the smart card are damaged.
 - The data on the smart card have been manipulated.

Note

You have 10 attempts to enter the PIN.

- To repeat the process, click the "Repeat" button. To cancel the process, click the "Cancel" button.
- Error message "The inserted smart card is a copy". The logon procedure is being aborted." Click "OK".
- Error message "The data on the smart card could not be read". The logon procedure is being aborted." Click "OK".

- Error message "The data on the smart card are not supported by SIMATIC Logon Installation". The logon procedure is being aborted."
Click "OK".
- Error message "The data on the smart card cannot be processed". The logon procedure is being aborted."
Click "OK".

Log off with smart card

To log off from the system remove the smart card from the smart card reader.

7.4.3.4 Logging on via another device

Introduction

"Other devices" can be used in addition to keyboards and smart card readers to identify users logging onto a computer. Devices are available, for example, that can identify fingerprints of users.

Available devices and drivers

Consult your Siemens representative to learn more about available systems, drivers and interface parameters.

7.4.3.5 Logon via a screen keyboard

Activating the screen keyboard

You activate the screen keyboard in the "Configure SIMATIC Logon" dialog box via the "Logon Device" tab.

Using the screen keyboard

You use the screen keyboard in addition to other input devices or as the sole logon method (when a logon device has failed, for example).

7.5 SIMATIC Logon Role Management

7.5.1 What is the SIMATIC Logon Role Management?

SIMATIC Logon Role Management

The SIMATIC Logon Role Management is the group of SIMATIC Logon components used to create roles and assign roles and assign groups and users of the operating system as well as the function rights to roles.

What is a role?

A role contains the rights of groups/users within applications to perform specific actions (for example, transferring data).

What is a phase?

A phase is a predefined period of time.

What is role management?

Role management is used to regulate access to applications and functions by users and groups.

- Access protection forces users to log on with the system if they want to use an application or function.
- Assigning specific tasks to roles simplifies the task of assigning rights to users and groups.
- User management is based on the users and groups of the operating system.

Note on copying in an image

Note

The groups and users are saved in the role management with a "security identifier". These identifiers are assigned by the operating system and also get a sequential number.

When a computer image is loaded, the numbering is continued at the position that was current when the image was created.

When groups and users are created again in the user management of the operating system, they may have a different "security identifier".

After loading an image, therefore, always check whether the roles have been assigned to the intended groups and users. If this is not the case at some points, you will need to adapt the assignment.

Requirements

The following requirements must be fulfilled to use SIMATIC Logon Role Management with an application:

- The users and groups of the operating system are set up.
- The "Access protection" and "User management" options must be activated in the application.

Opening SIMATIC Logon Role Management

SIMATIC Logon Role Management is started with the user interface of the application in which this service is embedded. It cannot be started in Windows.

Language

Default language setting for SIMATIC Logon Role Management:

- The language set for the respective application when this language has been installed for the SIMATIC Logon.
- English when the language set in the relevant application is not available.

7.5.2 Structure of SIMATIC Logon Role Management

Structure of the application dialog

The operation of the SIMATIC Logon Role Management application dialog is menu-guided. SIMATIC Logon Role Management has the following structure:

- Menu bar for operating SIMATIC Logon Role Management
- Toolbar for quick access to selected functions.
- The dialog window is divided into four groups:
 - Group 1: Configured roles and assignment types
 - Group 2: Details about the element selected in "Configured roles and assignment types"
 - Group 3: Available assignment types (groups and users, logon stations, function rights, etc.)
 - Group 4: Elements of the type selected in "Available assignment types"
- Shortcut menus and key combinations (shortcuts, hotkeys) help you to work in SIMATIC Logon.

Working in the application dialog

Operation using	Commands	Additional information available in the section
Menu commands	All functions in the SIMATIC Logon Role Management can be called using menu commands.	
Drag&Drop	Copy and paste: • Select an assignment type in the "Configured roles and assignment types" group • Select a corresponding assignment type in the "Available assignment types" group • Drag the required available objects to the detailed view of the "Configured roles and assignment types" group	
Shortcut menu	• Copy • Paste • Delete	Working with shortcut menus (Page 55)
Icons	• Copy • Paste • Delete	Toolbar (Page 56)
Key combinations	• Copy • Paste • Delete	Key combinations (Page 54)

Apply changes

Note

Changes in the SIMATIC Logon Role Management must be saved. Select the menu command **File > Save** to do this.

7.5.3 Assigning permissions for applications

7.5.3.1 Overview of the configuration tasks

Overview of the configuration tasks

Configuring the permissions for the application involves the following topics:

- Creating a role (Page 46)
- Configuring a role (Page 47)
- Changing the properties of a role (Page 51)
- Exporting the role management data (Page 52)
- Changing the assignment of groups and users (Page 53)
- Changing the project password (Page 53)

7.5.3.2 How to create a role

Procedure

1. Select the menu command **Edit > New Role**.
2. Enter a name for the role in the "Role name" text box.
3. You can provide a description for the role in the "Description" text box.
4. Optional: Assign phases to the roles: Use the following symbols for this:
 -  Assign available phases
 -  Delete unneeded phases
5. Click "OK".

Result

The "new role" is entered in the "Configured roles and assignment types" navigation view. The following folders are created in the "New Role" folder:

- Groups and Users
- Function Rights
- Security Areas
- Logon Stations

An application generally does not support all specified categories. Refer to the corresponding application documentation to learn about the types and options supported by an application.

Applying changes

Note

All changes made in SIMATIC Logon Role Management must be saved. To do this, select the menu command **File > Save**.

Users in a Windows domain

Note

SIMATIC Logon users must be direct members of a Windows group. Members of a sub-group cannot be authenticated.

7.5.3.3 How to configure a role

Introduction

A role can be assigned the following assignment types:

- Groups and users
- Function rights
- Logon stations
- Phases

Groups, users and logon stations can be assigned Security Areas.

Usually, an application does not support all defined assignment types. The corresponding documentation of the application lists the assignment types which are supported.

Expanding the role configuration

Proceed as follows in order to expand the configuration of a role:

1. Select the assignment types you want to add to the role by clicking these in the "Configured roles and assignment types" list.
2. Select the **Edit > Edit** menu command.
The corresponding dialog box opens:
 - Edit groups and users (Page 48)
 - Edit function rights (Page 49)
 - Edit Logon Stations (Page 49)
 - Edit Phases (Page 50)
 - Edit Security Areas (Page 50)
3. The assignment types of the role are displayed when you exit the dialog box with "OK".

Deleting objects of the assignment types of a role

You can only delete configured objects of the assignment types.

1. Select the assignment type you want to delete from this role by clicking it in the "Configured roles and assignment types" list.
 - Groups and users
 - Function rights
 - Logon Stations
 - Phases
 - Security areas
2. Select the objects of the assignment type you want to delete by clicking in the "Role: <name of the selected role>" list.
3. Select the **Edit > Delete** menu command
The "Role: <name of the selected role>" list shows all remaining objects of the assignment type of the role.

Activating changes

Note

All changes made in SIMATIC Logon Role Management must be saved. Select the **File > Save** command.

Operating by means of shortcut menu

The configured assignment types can be also edited using the shortcut menu commands. An overview of the shortcut menu functions is available in the section "New role" (Page 55) shortcut menu.

7.5.3.4 How to assign a role to groups and users

Roles can be assigned to user groups and users by means of the user management functions of the operating system.

Procedure

1. From the "Domain/Computer" drop-down list, select the desired computer or domain for which you want to edit the configuration.
2. Enter the name of a user or user group in the "Name" text box. You can add "*" to the name or use only the "*" character to perform filtering.
3. Click "Find Now" to create a list of groups and users. Click "Stop" to stop compiling the list.
4. Select the groups and users you want to assign to a role from the list of "Available groups and users".

5. Click .
The selected groups and users are moved to the list of "Configured groups and users".
6. Click  in order to remove groups and users from the list of "Configured groups and users".
7. Repeat steps 1 to 4 for each station.
8. Click "OK" to activate the groups and users configured in list of "Configured groups and users" for the role.

Note

Certain applications only allow the assignment of a single group or single user. The application documentation provides information on corresponding supported functionality.

7.5.3.5 How to assign function rights to a role

You can assign function rights to a role.

Procedure

1. Select the function rights you want to assign to a role from the list of "Available function rights".
2. Click .
The selected entries are moved to the list of "Configured function rights".
3. Click  in order to delete an entry from the list of "Configured function rights".
4. Click "OK" to activate the function rights configured in list of "Configured function rights" for the role.

Note

Certain applications do not support this functionality. The application documentation provides information on corresponding supported functionality.

7.5.3.6 How to assign Logon Stations to a role

You can assign Logon Stations to a role.

Procedure

1. Select the Logon Stations you want to assign to a role from the list of "Available Logon Stations".
2. Click .
The selected entries are moved to the list of "Configured Logon Stations".

3. Click  in order to remove an entry from the list of "Configured Logon Stations".
4. Click "OK" to activate the Logon Stations configured in list of "Configured Logon Stations" for the role.

Note

Certain applications do not support this functionality. The application documentation provides information on corresponding supported functionality.

7.5.3.7 How to assign Phases to a role

You can assign phases to a role.

Procedure

1. Select the phases you want to assign to a role from the list of "Available Phases".
2. Click .
The selected entries are moved to the list of "Configured Phases".
3. Click  in order to an entry from the list of "Configured Phases".
4. Click "OK" to activate the phases configured in list of "Configured Phases" for the role.

Note

Some applications only allow the assignment of a single group or single user. The application documentation provides information on corresponding supported functionality.

7.5.3.8 How to assign Security Areas to groups and users or to Logon Stations

You can assign one or several assign security areas to groups and users or to Logon Stations.

Procedure

1. Select the security areas you want to assign to groups and users or to Logon Stations from the list of "Available Security Areas".
2. Click .
The selected security areas are moved to the list of "Configured Security Areas".
3. Click  in order to an entry from the list of "Configured Security Areas".
4. Click "OK" to activate the security areas configured in list of "Configured Security Areas".

Note

Some applications only allow the assignment of a single group or single user. The application documentation provides information on corresponding supported functionality.

7.5.3.9 How to delete a role

You can only delete roles you actually created. The default roles included with an application cannot be deleted.

A list of default roles included in the calling application is available in its corresponding documentation.

Procedure

1. Select a role.
2. Select the menu command **Edit > Delete**.
The role is deleted with the permission groups.

Activating changes

Note

All changes made in SIMATIC Logon Role Management must be saved. Select the **File > Save** command.

Additional information

For information on deleting Phases from a role, refer to the chapter "How to edit the properties of a role (Page 51)".

7.5.3.10 How to change the properties of a role

Introduction

A role has the following properties:

- Role name
- Role description
- Phases to be available in the role

Note

Only applications that support "phases" can edit phases.

Requirement

The custom role has already been created.

Procedure

1. Select a role from the "Configured roles and assignment types" field.
2. Select the command **Properties** in the shortcut menu.
The "SIMATIC Logon AdminTool - Role Properties" dialog box opens.
3. Rename the role and/or edit its description as required.
4. Assign the phases to the roles:
 -  Assign the available phases
 -  Remove assignment of unneeded phases
5. Click "OK".
The modified phases are activated.

Applying changes

Note

All changes made in SIMATIC Logon Role Management must be saved. Select the **File > Save** command.

7.5.3.11 How to export role management data

Procedure

1. Select the menu command **File > Export**
The "Save File As..." dialog box of the Windows Explorer opens.
2. Change to the required folder.
3. Go to the "File name" field to edit the displayed file name in accordance with your project settings, for example, "Roles_ProjectA_20050930".
4. Select the file format.
 - Comma separated (*.txt)
 - XML (*.xml)
5. Click "Save".

Result

Role management data is saved to the selected folder by the name you entered.

7.5.3.12 How to assign groups and users to another computer

Introduction

You assigned groups and users of a specific computer to the roles when they were created. If you change the configuration, in other words, if you use another computer, you need to assign the groups and users to this computer.

Requirements

- The original logon computer is available.
- All groups and users must be available on the new computer under the same names.

Procedure

1. Select the menu command **Edit > Reassign Groups and Users....** .
The "SIMATIC Logon AdminTool - Reassign Users and Groups" dialog box opens.
2. Enter the name of the previous computer.
3. Enter the name of the new computer.
4. Click "OK".
The assignment of the groups and users is changed.

Apply changes

Note

Changes in the SIMATIC Logon Role Management must be saved. Select the menu command **File > Save** to do this.

7.5.3.13 How to change the project password

Introduction

The project can be protected by a password in some applications. We recommend that you change this password after setting up the project and then at regular intervals.

Requirement

The application supports the "Project Password" feature.

Procedure

1. Select the menu command **Edit > Change Project Password....**
The "SIMATIC Logon Role Management - Change Project Password" dialog box opens.
2. Enter the password in the corresponding box.
3. Confirm the password in the "Confirm Password" box.
4. Click "OK".
The project password is changed.

Apply changes

Note

Changes in the SIMATIC Logon Role Management must be saved. Select the menu command **File > Save** to do this.

7.5.3.14 Key combinations

List of functions

Many functions available as menu commands can also be executed with key combinations in SIMATIC Logon.

Key combination	Function
<F1>	Call the online help
<F10>	Activate the menu bar in the active program
<Ctrl + A>	Select all
<Ctrl + E>	Edit
<Ctrl + C>	Copy
<Ctrl + N>	New role
<Ctrl + R>	Reassign groups and users
<Ctrl + S>	Save changes
<Ctrl + V>	Paste
<Ctrl + W>	Change project password
	Delete
<Alt + underscored letters in a menu name>	Displays the corresponding menu
<Alt + underscored letter in a menu name + underscored letter in a menu command>	Execute relevant menu command

7.5.3.15 Folder icons of the SIMATIC Logon Role Management

List of icons

The folder icons of the SIMATIC Logon Role Management have the following meanings:

	Folder for ...
	Roles
	User groups and Windows groups
	Single users
	Logon stations
	Function rights
	Phases
	Domain linked computers
	Groups or users whose name cannot be identified, for example, because the connection to the corresponding computer is down

7.5.4 Calling dialog boxes from the shortcut menu

7.5.4.1 Working with shortcut menus

Shortcut menu

Many actions available as menu commands can also be called in the shortcut menus of SIMATIC Logon.

Selecting a menu command from the shortcut menu

If a shortcut menu is available, you can select the menu command by following the steps outlined below:

1. Select the object.
2. Right-click on it.
3. Select the menu command in the open shortcut menu.

7.5.4.2 "New Role" shortcut menu

This shortcut menu opens the dialog box for creating a role:

1. Select the "Roles" folder in the tree view of the "Configured roles and assignment types" group.
2. Select the shortcut menu command **New Role**.
3. Proceed as described in the section "How to create a role (Page 46)".

7.5.4.3 "Edit" shortcut menu

This shortcut menu opens a dialog box in which you can configure a role.

1. In the "Configured Roles and Assignment Types" group, select the desired assignment type, for example "Groups and Users" for the role you want to edit.
2. Select the shortcut menu command **Properties**.
3. Proceed as described in the section "How to configure a role (Page 47)".

7.5.4.4 "Properties" shortcut menu

A detailed description about this is available in the section "How to change the properties of a role (Page 51)".

7.5.4.5 "Delete" shortcut menu

Introduction

You can delete roles using this shortcut menu.

Deleting a role

1. Select a role to delete from the "Configured roles and assignment types" group.
2. Select the **Delete** command in the shortcut menu.

Applying changes

Note

All changes made in SIMATIC Logon Role Management must be saved. Select the menu command **File > Save**.

7.5.5 The toolbar and menu bar of SIMATIC Logon Role Management

7.5.5.1 Toolbar

Introduction

In the SIMATIC Logon Role Management, the toolbar is used as a shortcut for calling selected commands.

Toolbar



The following functions can be executed using the toolbar:

Symbol	Menu Command	Key shortcuts	Meaning
	Edit > New Role...	<Ctrl + N>	Opens the dialog box to create a new role
	File > Save	<Ctrl + S>	Saves the changes
	Edit > Copy	<Ctrl + C>	Copies objects from the area "Available objects" to the clipboard. Note: Application only in connection with the function Paste
	Edit > Paste	<Ctrl + V>	Assigns the objects on the clipboard to the role selected in the "Roles" area. Note: Application only in connection with "Copy"
	Edit > Delete		Deletes the objects selected in the object area.
	Help > Help on SIMATIC Logon	<F1>	Opens the information on the selected object or menu command in the SIMATIC Logon help.

Representation of the active toolbar functions

Note

A pressed button indicates that a specific status (for example, function enabled/disabled) is active.

A grayed out symbol indicates the following:

- the function linked with this symbol is not active

or

- the function linked with this symbol is not available

7.5.5.2 Menu bar of SIMATIC Logon Role Management

Menu bar

The menu bar of SIMATIC Logon Role Management contains the following menus:

- File menu (Page 58)
- Edit menu (Page 58)
- Help menu (Page 59)

7.5.5.3 File menu

File menu

The following commands can be executed using the **File** menu:

Menu command	Icon	Key combination	Meaning
Save		<Ctrl + S>	Saves changes
Export		<Ctrl + E>	Exports the data of role management
Exit			Closes SIMATIC Logon Role Management

7.5.5.4 Edit menu

Edit menu

The following functions can be executed using the **Edit** menu:

Menu Command	Symbol	Key shortcuts	Meaning
New role...		<Ctrl + N>	Opens the dialog box to create a new role
Copy		<Ctrl + C>	Copies objects from the area "Available objects" to the clipboard. Note: Application only in connection with the function Paste
Insert		<Ctrl + V>	Assigns the objects on the clipboard to the role selected in the "Roles" area. Note: Application only in connection with "Copy"
Delete			Deletes the objects selected in the object area.
Edit		<Ctrl + B>	To edit the selected role
Select all		<Ctrl + A>	Selects all objects in the area of available objects
Reassign groups and users...		<Ctrl + R>	Opens the dialog box to alter the group and user assignment
Change the project password...		<Ctrl+W>	Opens the dialog box to change the project password

7.5.5.5 Help menu

Help menu

The following functions can be executed using the **Help** menu:

Menu command	Icon	Key combination	Description
Help on SIMATIC Logon			Opens the online help on SIMATIC Logon
About			Opens the dialog displaying the version of SIMATIC Logon.

7.6 SIMATIC Logon Event Log

7.6.1 What is the SIMATIC Event Log Viewer?

Introduction

The SIMATIC Logon Event Log Viewer is a component that takes on the task of recording and displaying events for an application. The recording of events is triggered by the application, the display occurs in the "SIMATIC Logon Event Log Viewer (Page 60)" dialog box.

The documentation of the application describes how to display this dialog box.

Backing up SIMATIC Logon Service events to a database

Events are saved in the "EventLog.mdb" database. This database is located in the directory "...\\SIMATICLogon\\Logging" after installation with default settings.

Recommendation: Backup the database in short intervals. This will protect against loss of data (in the event of hard disk failure, for example).

To prevent damage to the database, do not perform the backup when applications are running.

If no database exists, a new database is created automatically.

Backing up the events of applications

Applications that use SIMATIC Logon save the events in a location defined by these applications.

If no database exists, a new database is created automatically.

Refer to the manual for the application to learn where the database is stored and move it from there to the desired directory.

7.6.2 The "SIMATIC Logon Event Log Viewer" dialog box

Meaning of the elements in the dialog box

The following table shows the meaning of the elements in the "SIMATIC Logon Event Log Viewer" dialog box.

Element		Meaning
Displays	Filter status	"Filter enabled" / "Filter disabled"
	Number of events	Number of events to be recorded in the file.

Element		Meaning
Event displays	"Type" column	Type of the event: information, warning or error
	"Time stamp" column	Time when the event occurred
	"Source" column	Application reporting the event
	"Category" column	Classification of events (based on the application)
	"Event" column	Information about the event
	"Work object" column	Object involved in the event (based on the application)
	"User" column	User who triggered the event
	"Computer" column	Computer on which the event was triggered
	"Comment" information field	Information about the event generated by the user or system
"Update" button	Displays events since the last refresh was performed	Events that occurred since you last refreshed are then displayed.
"Comment" button	Opens the dialog box for entering comments. You need to logon to authenticate yourself.	The information is displayed and saved in the log file: • Comment • Date • Time • Computer name • User
"Filter..." button	Opens the "Filter Events" dialog box	Setting filter criteria Additional information is available in the section "The "SIMATIC Logon Eventlog Viewer - Filter events" dialog box (Page 61)".
"Export..." button	Opens the "Export..." dialog box	Settings for exporting the events
"Close..." button	Closes the "Event Log Viewer" dialog box	
"Help" button	Opens the online help for the SIMATIC Logon Eventlog Viewer	

7.6.3 The "SIMATIC Logon Event Log Viewer - Filter Events" dialog box

Introduction

You can set a filter for occurring events in this dialog box.

The filter becomes automatically enabled when you close the dialog box with "OK". When a filter is enabled in the Event Log Viewer, the text "Filter enabled" appears in the status bar.

The Event Log Viewer only shows the filtered events.

Displayed events

You can use filters to control the display in the Eventlog Viewer.

Criteria:

- **Type**
Selection by activating check boxes for the individual event types
- **Time period**
Specification of the time period (Start/End). You can activate both points in time (date and time of day) with the check boxes.
- **Event displays**
String used to search within the specified column.

Character string	Find in column	Meaning
Source	"Source" column	Application reporting the event
Category	"Category" column	Classification of events (based on the application)
Event	"Event" column	Information about the event
Work object	"Work object" column	Object involved in the event (based on the application)
User	"User" column	User who triggered the event
Computer	"Computer" column	Computer on which the event was triggered
Comment	"Comment" information field	Information about the event generated by the user or system

Note

Not all characters are allowed in strings.
If you enter a prohibited character, it will be ignored and a signal tone sounds.

7.6.4 How to Track Logons and Logoffs with the SIMATIC Logon Event Log Viewer

Introduction

SIMATIC Logon records all authentications, logons and logoffs in a file. With the SIMATIC Logon Event Log Viewer, you can view this data and add comments on the individual entries.

Procedure

1. Select the menu command **Start > SIMATIC > SIMATIC Logon > SIMATIC Logon Event Log Viewer**.
2. Confirm the prompt asking if you want to open the viewer with "Yes".
The "SIMATIC Logon Event Log Viewer" dialog box opens displaying all recorded events. The comments on the currently selected event are displayed in the "Comments to the selected event" box.
3. Click "Update" to refresh the display of events.
This will then show the events that have occurred since the last update.

4. Click "Comment" to enter a comment for the event.
A dialog box opens in which you must authenticate yourself by logging on.
5. Enter a comment and click "OK".
The comment is displayed with the date, time, computer name, author and comment in the comment box and save to the file.
6. Click "Close" to close the dialog box.

7.7 SIMATIC Electronic Signature

7.7.1 What is SIMATIC Electronic Signature?

SIMATIC Electronic Signature

SIMATIC Electronic Signature is the *SIMATIC Logon* component that can be used to create an electronic signature. An electronic signature is a verification created and archived to fulfill a requirement such as important or critical operator input in an automation system.

These verifications contain information about an operation, for example:

- Name of the person or persons responsible for performing the operation
- Date and time of the operation to be performed
- Significance of the signatures (an authorization, for example)
- Author (for example, of a Batch recipe).

Example

An electronic signature is required for the configured "Activation of motor" operation.

Basic principle of operation

SIMATIC Electronic Signature works as explained below:

- If an electronic signature is required for an operation, configure the appropriate requirement in the corresponding application. SIMATIC Electronic Signature queries and evaluates the information to be entered.
- SIMATIC Electronic Signature requests the information on the configured operations, checks it and transfers it to the calling application for storage.
- The requested operation is released only when all necessary signatures have been entered for the operation.

Opening SIMATIC Electronic Signature

The SIMATIC Electronic Signature dialog box is displayed by the application with a specific call. How you activate the application-specific call for SIMATIC Electronic Signature is described in the documentation of the relevant application.

7.7.2 Rules for Electronic Signatures

Rules

Electronic signatures made with **Electronic Signature** fulfill the following requirements:

- Electronic signatures are unique:
 - They consist of a user name and password.
 - If the information for several or different users are requested, they are prompted to enter their user name and password.
- Once entered, electronic signatures cannot be reused ("copied").
- Once entered, electronic signatures cannot be reassigned to another person.
- The electronic signature contains the following:
 - Name of the person signing
 - Date and time of the signature
 - Name of the operator station
 - Comments (optional)
- During configuration, the administrator can make settings so that the object is released only after one or more signatures have been entered (4-eyes principle). It is also possible to define certain rules that must be adhered to, for example:
 - Different user roles (see section "SIMATIC LOGON")
 - That signatures must be entered in a fixed order

Note

Take into account that the user name must always be unique within a system.

- A user name may not be assigned to two different users.
 - Different users must always have different user names.
-

7.7.3 Signing operations

7.7.3.1 The "SIMATIC Electronic Signature: Acquire Signatures" dialog box

Introduction

In this dialog box, you can sign an operation such as an action or state change.

Note

Users can only enter their signature once within a dialog box. This also applies to users which have been allocated to several required users roles.

Scope and functions of the "SIMATIC Electronic Signature dialog box: Acquire Signatures" dialog box

Area	Object	Meaning
Element	Element	Object name (in SIMATIC BATCH, for example: batch, recipe procedure, partial recipe procedure, recipe operation, recipe function, transition)
Information	Status transition	- From / To: Display of the status transition - Operation Display of operator input
	Input	- All: All user signatures must be entered in order to be able to confirm the dialog box with "OK". - Separate: Signatures can be entered separately by the users. The signature dialog box can be opened several times on different clients.
	Order of entries	- Any: A specific order of the entries of multiple signatures is not specified. - Default: If several signatures are required for operator input, each signature must be entered in accordance with the displayed order of roles.
	Times (optional display)	- Request: Time at which the signatures were requested. - Validity: Time within which the signature has to be entered.
Signatures	Signatures	Shows the user roles assigned to users who are required to enter a signature. Any specified and listed order of entries must be maintained. Click the role in the list of the "Sign" group in order to enter your signature. Click "Sign" to enter your signature.
Canceling a signature	Cancel signature (optional display)	Shows the user who canceled the signing operation. This cancel option is only available if not all signatures were entered. The signature request can be deleted using the "Cancel signature operation" button. This function is only available to users who are listed in the user roles in the "Signatures" display.

7.7.3.2 How to sign actions and state changes**Initial situation**

After an operator action or during a state change, the "SIMATIC Electronic Signature: Sign" dialog box opens automatically. As the representative of a user role, you will be requested to sign the operation.

Procedure

You user role is displayed in the "SIMATIC Electronic Signature: Log Signatures" dialog box, "Signatures" table:

1. Click "Sign".
The "SIMATIC Logon Service - Signature" dialog box opens.
2. Enter your user name and password and select the appropriate domain or station.
Enter a comment as required, provided the calling tool supports comment entries.
3. Click "OK".
The "Signatures" table displays the data of signatures.
 - If the "All" check box is activated the "OK" button is only activated after all necessary signatures were entered.
 - If the "Separate" check box is set, the "SIMATIC Logon Service - Signature" can be closed by clicking "OK" after all necessary signatures were entered.

The signature operations are only completed after all signatures were entered.
4. Confirm the changes made in the "SIMATIC Logon Service - Signature" dialog box by clicking "OK".

Note

The entry of signatures may be monitored by a timeout function. The time and timeout settings are displayed in the "Times" area of the "SIMATIC Logon Service - Signature" dialog box.

7.8 SIMATIC Logon Development Kit

7.8.1 What is the SIMATIC Logon Development Kit?

SIMATIC Logon Development Kit

The Development Kit is intended for programmers who wish to integrate SIMATIC Logon in a customer application.

Additional information

You will find the following files in the directory "...\\SimaticLogon\\developmentkit":

- SL_ProgrammingGuide.pdf
The "*SL_ProgrammingGuide.pdf*" contains the English language manual *SIMATIC; SIMATIC Logon Development Kit; Programming Guide*.
- SL_Example.zip
The "SL_Example.zip" file contains a example application. The *SIMATIC Logon Development Kit* programming guide uses an example application to demonstrate how to integrate SIMATIC Logon in a customer application.

Index

A

- Actions and state changes, 66
 - Signing, 66
- Assigning groups and users, 53
 - Changing, 53
- Automatic logoff, 33
 - Configuring, 33

C

- Certificate, 34
 - Configuring, 34
- Components of SIMATIC Logon, 15, 16, 20
 - Installing, 15, 16
 - Removing, 20
- Configuration, 47
 - Role, 47
- Configuration of SIMATIC Logon, 26, 27, 28, 30, 32, 33, 34
 - Automatic logoff, 33
 - Beginning, 26
 - Certificate, 34
 - Dialog box, 27
 - General, 28
 - Logon, 32
 - Working environment, 30
- Configuration tasks, 46
 - Overview, 46

E

- Electronic signature, 9, 64, 65
 - and user management, 9
 - Rules, 65
 - with SIMATIC Electronic Signature, 64
- Export, 52
 - Role management data, 52
 - Roll management data, 52
- Exporting, 52

F

- Folder icons of the SIMATIC Logon Role management, 55

G

- General settings, 28
- Groups and users, 53
 - Changing an assignment, 53

I

- Icons, 55
 - Folder icons of the SIMATIC Logon Role management, 55
- Installation, 15, 16
 - SIMATIC Electronic Signature, 16
 - SIMATIC Logon, 15, 16
- Integrating SIMATIC Logon into a customer application, 68

K

- Key combinations, 54

L

- Logon, 32, 37, 38, 42
 - Logon via another device, 42
 - Via a smart card reader, 38
 - Via logon dialog box, 38
 - with SIMATIC Logon - an overview, 37
- Logon and log off, 62
 - Tracking, 62
- Logon events, 62
 - Tracking, 62
- Logs, 62
 - Logon tracking, 62

M

- Menu, 55, 57, 58, 59
 - ? - Help, 59
 - Edit, 58
 - File, 58
 - Menu bar in SIMATIC Logon Role Management, 57
 - Menu bar of SIMATIC Logon Role Management, 57
 - Shortcut menu, 55

O

- Operating system, 17
 - Settings, 17
- Operator input and status transition, 66
 - Sign, 66
- Overview of the configuration tasks, 46
- Overview of the required configuration tasks, 25

P

- Principle of logging on via the SIMATIC Logon Service, 23
- Principle of user logon by means of SIMATIC Logon Service, 23
- Project password, 53
 - Changing, 53
- Properties of a role, 51, 56
 - Changing, 51, 56

R

- Removal, 20
 - SIMATIC Logon, 20
- Requirements, 11
 - Hardware, 11
 - Operating system, 11
- Role, 46, 47, 51
 - Changing properties, 51
 - Configuring, 47
 - Creating, 46
 - Deleting, 51
- Role management, 52, 55
 - Exporting data, 52
- Role management data, 52
 - Export, 52
- Roll management data, 52
 - Exporting, 52

S

- Scope of delivery for SIMATIC Logon, 13
- Settings, 17
 - in the operating system, 17
- Shortcut menu, 55, 56
 - Delete, 56
 - Edit, 56
 - New role, 55
 - Using, 55

- Signing actions and state changes, 66
- Signing status transition and operator input, 66
- SIMATIC Electronic Signature, 16, 64
 - Installing, 16
- SIMATIC Electronic Signature dialog box, 65
 - Acquire signatures, 65
- SIMATIC Event Log Viewer, 60
- SIMATIC Logon, 13, 15, 20, 26, 27
 - Beginning configuration, 26
 - Configuring, 27
 - Installing, 15
 - Removing, 20
 - Scope of delivery, 13
 - Service, 26
- SIMATIC Logon Event Log Viewer, 62
- SIMATIC Logon Role Management, 43, 44, 55
 - Folder icons, 55
 - Purpose, 43
 - Structure, 44
- SIMATIC Logon server, 19
 - Preparing for failure, 19
- SIMATIC Logon server failure, 19
 - Retaining functionality, 19
- SIMATIC Logon working environment, 30
 - Configuring, 30
- State changes and actions, 66
 - Sign, 66
- Status transition and operator input, 66
 - Sign, 66

T

- Tab, 28, 32
 - General, 28
 - Logon, 32
- The SIMATIC Logon Event Log Viewer - Filter Events dialog box, 61
- Toolbar, 56
 - Toolbar, 56

U

- User, 36
 - Adding, 36
 - Deleting, 36
- User management and electronic signatures, 9

W

- What is the SIMATIC Event Log Viewer?, 60

Windows, 17
 Settings, 17

