



**SIMATIC**

# PCS 7 Process Control System SIMATIC Logon Readme V1.6 Update 3 (online)

Readme

Security information

**1**

Overview

**2**

Notes on installation

**3**

Notes on SIMATIC Logon  
updates

**4**

Notes on usage

**5**

Version: 2020-11-07 (online)

## 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

<b>1</b>	<b>Security information .....</b>	<b>5</b>
<b>2</b>	<b>Overview .....</b>	<b>7</b>
<b>3</b>	<b>Notes on installation.....</b>	<b>9</b>
3.1	Introduction.....	9
3.2	Scope of delivery .....	9
3.3	Hardware requirements .....	9
3.4	Software requirements .....	10
3.4.1	Runtime environment .....	10
3.4.2	Memory requirements .....	11
3.5	New installation.....	11
3.5.1	Installation of SIMATIC Logon V1.6.....	11
3.5.2	Licensing of SIMATIC Logon V1.6.....	11
3.5.3	Deinstallation of SIMATIC Logon V1.6.....	12
<b>4</b>	<b>Notes on SIMATIC Logon updates.....</b>	<b>13</b>
4.1	Update of SIMATIC Logon V1.6.....	13
<b>5</b>	<b>Notes on usage .....</b>	<b>15</b>
5.1	General information.....	15
5.2	Notes on Windows workgroups .....	15
5.3	Note on smart card use .....	15
5.4	Notes on the SIMATIC Logon Event Log Viewer .....	16
5.5	Notes on the operating systems .....	16
5.6	Configuring SIMATIC Logon .....	17



# Security information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, systems, machines and networks.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens' products and solutions constitute one element of such a concept.

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.

For additional information on industrial security measures that may be implemented, please visit

<https://www.siemens.com/industrialsecurity>.

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed under

<https://www.siemens.com/industrialsecurity>.



# Overview

---

**Note****Notes on installation and use**

This information has priority over statements made in other documentation. Please read these notes carefully as they contain important information about the installation and use of SIMATIC Logon V1.6 Update 3.

---





# Notes on installation

## 3.1 Introduction

The installation notes include important information that you need to install the SIMATIC Logon V1.6 Update 3 software. Please read these notes prior to installation.

SIMATIC Logon V1.6 consists of the following components:

- SIMATIC Logon Service: provides access protection for SIMATIC applications
- SIMATIC Logon Role Management: manages the users of SIMATIC applications
- SIMATIC Electronic Signature: activates and logs actions with digital signatures for SIMATIC applications

## 3.2 Scope of delivery

You have received the following product with this delivery:

- SIMATIC Logon V1.6 Update 3
- Order number: 6ES7658-7BX61-0YA0
- The contents of this package include the following:
  - SIMATIC Logon V1.6 Update 3 software package with a trial license
  - 1 software product certificate for test license

## 3.3 Hardware requirements

The installation is subject to the conditions of SIMATIC PCS 7 V9.1.

To work with SIMATIC Logon V1.6 Update 3, you require a programming device or a PC equipped with the following:

- Processor with at least 800 MHz
- Minimum 512 MB RAM main memory

### Smart card reader

If you wish to work with a smart card reader, the device has to fulfill the following requirements:

- PC/SC V1.0 specification
- ISO 7816 Standard

### 3.4 Software requirements

SIMATIC PCS 7 catalog order no. 6ES7 652-0XX02-1XC0

#### The following smart card operating systems are supported:

- TCOS 3.0 (TCOS 3.0 on Philips P5CD036, TCOS 3.0 on Philips P5CT072, TCOS 3.0 on Philips P5CD072, TCOS 3.0 release 2 on Philips P5CD080, TCOS 3.0 on Infineon SLE 66CX642P, TCOS 3.0 on Infineon SLE 66CLX641P, TCOS 3.0 on Infineon SLE 66CLX640P, TCOS 3.0 on Infineon SLE 66CX680PE, TCOS 3.0 / NetKey 3.0) SIMATIC PCS 7 catalog order no. 6ES7652-0XX00-1XD2
- TCOS 2.0 (SLE44, SLE66, SLE66P, T-System Contactless TCOS Min, TeleSec NetKey Card Deutsche Post card)
- TCOS 1.2 (Telesec TCOS 1.2, CeloCom Card with TCOS 1.2)
- MTCOS 1.1

---

#### Note

Only TCOS 3 smart cards are currently supported when using two-factor authentication (authentication with PIN entry).

---

## 3.4 Software requirements

### 3.4.1 Runtime environment

SIMATIC Logon V1.6 requires the following operating systems:

- Windows 7 Ultimate/Enterprise/Professional SP1 64-bit
- Windows 8.1 Pro 64-bit
- Windows Server 2008 R2 Standard Edition 64-bit SP1
- Windows Server 2012 R2 Update Standard Edition 64-bit
- Windows 10 Enterprise 2015 LTSB 64-bit
- Windows 10 Professional 64-bit
- Windows 10 LTSC version 2019, 64-bit
- Windows Server 2016
- Windows Server 2019

MS Internet Explorer must be installed (at least V6.0 with ServicePack 1).

Using SIMATIC Logon in combination with PCS 7, WinCC, WinCC flexible

- Check the compatibility by using the following link:
  - Entry ID 64847781 (<https://support.automation.siemens.com/WW/view/de/64847781>)
  - The entry referenced in this link has the entry ID 64847781.

### 3.4.2 Memory requirements

SIMATIC Logon requires approximately 250 MB of space on your hard disk.

## 3.5 New installation

### 3.5.1 Installation of SIMATIC Logon V1.6

SIMATIC Logon is installed by the system setup on the CD. Select the entry "SIMATIC Logon V1.6".

You can install SIMATIC Logon over a previously installed version of SIMATIC Logon.

### 3.5.2 Licensing of SIMATIC Logon V1.6

Before you can work with SIMATIC Logon, you must transfer the license (usage authorization) to your computer from the USB stick with the license key. You have two options to do this:

- During the installation phase of SIMATIC Logon, the "Setup" program will display a message informing you that the appropriate license is not installed on your computer. You can then select whether you wish to have the "Setup" program install the license or whether you wish to install it later using the Automation License Manager program.
- If you cannot install the license with Setup, continue Setup without installing the license. You can install the license at a later time with the start menu command **Start > SIMATIC > License Management > Automation License Manager** or **Start > Programs > Siemens Automation > SIMATIC > License Management > Automation License Manager**.
- The license for SIMATIC Logon V1.6 must be installed on a local drive.

### 3.5.3 Deinstallation of SIMATIC Logon V1.6

---

#### Note

Software products must be removed according to Windows conventions.

To do this, open the Windows application "Add/Remove Software" (in the taskbar under

**Start > Settings > Control Panel > Add/Remove Software**) and remove "SIMATIC Logon V1.6".  
This is the only safe way to remove software under Windows.

---

## Notes on SIMATIC Logon updates

### 4.1 Update of SIMATIC Logon V1.6

---

**Note**

An update version with a larger number contains the corrections of the update versions with lower numbers.

---

Update 1 contains the following corrections:

- Optimizations in the area of PC resource management
- Improvements in the use of the on-screen keyboard
- Corrections in the area of role management

Update 2 contains the following corrections:

- Corrections for STEP 7
- SIMATIC WinCC optimizations
- Performance improvement (user authentication) for read-only domain controllers

Update 3 contains the following corrections:

- Support of LDAP signing and channel binding
- Support of the new "Plant and User Documentation Manager" (PUD Manager) online help
- SIMATIC WinCC optimizations
- Role management corrections

#### See also

Security Advisory (<https://cert-portal.siemens.com/productcert/pdf/ssa-931064.pdf>)



## Notes on usage

### 5.1 General information

---

**Note**

Please read these notes carefully; they contain important information and additional details about SIMATIC Logon V1.6.

These notes take precedence over statements made in the manuals and online help.

---

### 5.2 Notes on Windows workgroups

When using a central login computer in connection with a Windows workgroup, remote queries of user, computer, and group information cannot be executed under certain circumstances. This is the case if the role management of SIMATIC Logon does not list any users and groups after you select the central login computer.

If this happens, central user administration in connection with a Windows workgroup can be supported by activating the remote query of user, computer, and group information in Windows on the login computer. You can find details at:

Internet link (<https://docs.microsoft.com/en-us/windows/device-security/security-policy-settings/network-access-restrict-clients-allowed-to-make-remote-sam-calls>)

<b>NOTICE</b>
<b>Security information</b>
<ul style="list-style-type: none"><li>• Activating this function results in a decreased level of security on the local computer across the entire operating system and is not recommended. In such cases, however, remote access will continue to be logged in the Windows Event Log.</li><li>• We recommend using a domain environment to ensure central user administration in accordance with the latest security standards.</li></ul>



### 5.3 Note on smart card use

Make sure that you rewrite all smart cards that were written with a version of SIMATIC Logon prior to Version V1.3. This is necessary because SIMATIC Logon as of Version V1.3 uses an improved encryption for the smart card. You will not be able to log on with a smart card that has not been updated. However, you can always log on with your logon name and password.

If you have logged on with a smart card and remove this smart card during configuration in the SIMATIC Logon role management, all changes that you have not saved at this point are discarded. Reinserting the card will not solve this problem.

An error event may be reported in the Windows Event Viewer when a smart card is removed or inserted. This behavior is known and does not result in a malfunction with SIMATIC Logon. The same applies to permanent operation with smart card. [see also Microsoft Knowledge Base Article ID: 936156]

## 5.4 Notes on the SIMATIC Logon Event Log Viewer

If you want to print the events in the event log, proceed as follows:

- Click "Export" and export the events in XML or CSV format.
- Print the exported file.

In the filter dialog, the date and time are always displayed based on the settings you have made in Windows for the date and time. A display conforming to ISO 8601 is not possible.

## 5.5 Notes on the operating systems

You can see the a "SIMATIC Logon" link on the desktop. Clicking on the link opens the Windows Explorer with the actual links to the SIMATIC Logon programs. They can be immediately started by clicking on them.

---

### Note

Press the right mouse button on this link and select the menu command "Pin to Start" to make this link available on the start screen. This makes it faster and easier to open the program.

In order to ensure reliable operation of SIMATIC Logon, you may neither delete nor modify those files that can be selected via the menu command **Start > Programs > Siemens Automation > SIMATIC > SIMATIC Logon > Documents and Settings** or the link **"SIMATIC Logon" > Documents and Settings** with the exception of the files in the "Diagnostics" folder, which are used for diagnostic purposes and may be deleted if necessary.

---

If a computer is to be used as the logon computer for SIMATIC Logon, activate file and printer sharing as an exception in the Windows Firewall (search in the taskbar for "Windows Firewall", start it and click "Allow a program or feature through Windows Firewall". Activate file and printer sharing there).

### Slow response of on-screen keyboard

In Windows 8, Windows Server 2008 and Windows Server 2012, the "Microsoft OSK" and "HMI TouchInputPC" on-screen keyboards start very slowly. This delay is caused by the Internet certificate check with callback.



You can find measures to prevent possible delays from arising under entry ID 87057037 (<https://support.industry.siemens.com/cs/ww/en/view/87057037>) in the Industry Online Support

## 5.6 Configuring SIMATIC Logon

In contrast to the information provided in the "Configuring SIMATIC Logon" of the documentation, the following applies:

- The user logged on in Windows must be a member of this group:  
Windows group "Logon\_Administrator"
- The user to be logged on in "Configure SIMATIC Logon" must be a member of this group:  
Windows group "Logon\_Administrator"

This group is created automatically by the setup program on the local computer. If you also want to create and use this group on a domain, you have to add the domain group to the local Windows group "Logon\_Administrator" to ensure that the mechanism works.

