

SIMATIC NET

PC software SIMATIC NET PC Software V17 SP1

Installation Manual

<u>Introduction</u>	1
<u>Installation of the SIMATIC NET PC software products</u>	2
<u>Installation and configuration with VMware vSphere</u>	3
<u>Configuration of the vCenter server environment and virtual machines for use of SIMATIC NET</u>	4
<u>SNMP service, SNMP OPC MIB compiler and profile files</u>	5
<u>Uninstalling the SIMATIC NET PC software products</u>	6
<u>Automated installation</u>	7
<u>Further Information</u>	8
<u>Appendix A</u>	A

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	Introduction	5
2	Installation of the SIMATIC NET PC software products.....	9
2.1	Requirements and notes on installation.....	9
2.1.1	Requirements and notes relating to the software.....	9
2.1.2	Requirements and notes relating to the hardware	11
2.1.3	Notes on installation	11
2.2	Released operating systems	12
2.3	Procedure	12
3	Installation and configuration with VMware vSphere	17
3.1	Requirements and notes	17
3.1.1	User experience	17
3.1.2	Requirements and notes relating to the software.....	17
3.1.3	Requirements and notes relating to the hardware	18
3.1.4	Restrictions.....	18
3.1.4.1	VMware vSphere vMotion	18
3.1.4.2	Options for operating the virtual machines.....	19
3.1.4.3	Intel SR-IOV	19
3.1.4.4	Configuration of the MAC address in STEP 7 projects	19
3.2	Overview	19
3.3	Installation of the SIMATIC NET PC software in a virtual machine	21
3.4	Upgrade	21
3.4.1	Upgrade procedure SIMATIC NET.....	21
3.4.2	Upgrading Hypervisor	22
4	Configuration of the vCenter server environment and virtual machines for use of SIMATIC NET	23
4.1	Configuration of the virtual Standard Switch (vSS).....	23
4.1.1	General	24
4.1.2	Security	24
4.1.3	Traffic Shaping	24
4.1.4	NIC Teaming	25
4.2	Configuration of the virtual machine	25
4.2.1	Hardware	25
4.2.1.1	CPU/RAM settings	25
4.2.1.2	Adding network adapter to the virtual machine	26
4.2.2	Options	26
4.2.2.1	Memory/CPU Hotplug	26
4.2.2.2	Boot options	26
4.2.2.3	Starting a virtual machine	26

5	SNMP service, SNMP OPC MIB compiler and profile files	27
5.1	Installing the SNMP service	27
5.2	SNMP OPC MIB compiler and profile files	29
6	Uninstalling the SIMATIC NET PC software products	31
7	Automated installation.....	33
7.1	Purpose and general description	33
7.2	Structure of the control file	34
7.3	Generating the control file automatically	35
8	Further Information.....	37
8.1	Documentation guide	37
8.2	Technical support, contacts and training	38
A	Appendix A	39
A.1	Security Events	39
A.1.1	Structure of the Security Events	39
A.1.2	Variables in Security Events.....	39
A.1.3	Access via untrusted networks	40
A.1.4	User account management	41
A.1.5	Nonrepudiation	42
A.1.6	Software and information integrity	42

Introduction

Purpose of this document

This document describes how to install the SIMATIC NET PC software products on your PG/PC.

Validity of this installation manual

This installation manual relates to the products on the DVD "SIMATIC NET PC Software V17 SP1".

The installation of STEP 7 Professional (TIA Portal) is described on the STEP 7 data medium.

The instructions in this manual for calling applications using the Start menu apply to Windows 10/Windows 11, Windows Server 2016 and Windows Server 2019.

Trademarks

The following and possibly other names not identified by the registered trademark sign ® are registered trademarks of Siemens AG:

HARDNET, SOFTNET, CP 5612, CP 5613, CP 5614, CP 5622

Industry Online Support

In addition to the product documentation, you are supported by the comprehensive online information platform of Siemens Industry Online Support at the following Internet address:

Link: (<https://support.industry.siemens.com/cs/de/en/>)

Apart from news, there you will also find:

- Project information: Manuals, FAQs, downloads, application examples etc.
- Contacts, Technical Forum
- The option submitting a support query:
Link: (<https://support.industry.siemens.com/My/ww/en/requests>)
- Our service offer:

Right across our products and systems, we provide numerous services that support you in every phase of the life of your machine or system - from planning and implementation to commissioning, through to maintenance and modernization.

You will find contact data on the Internet at the following address:

Link: (https://www.automation.siemens.com/aspa_app/?ci=yes&lang=en)

SITRAIN - Training for Industry

The training offer includes more than 300 courses on basic topics, extended knowledge and special knowledge as well as advanced training for individual sectors - available at more than 130 locations. Courses can also be organized individually and held locally at your location.

You will find detailed information on the training curriculum and how to contact our customer consultants at the following Internet address:

Link: (<https://new.siemens.com/global/en/products/services/digital-enterprise-services/training-services/sitrain.html>)

Industrial Networks Education

Training and certification for Industrial Networks

In our Industrial Networks Education courses you'll learn to design and implement wired and wireless data networks and connect them to a corporate network. You will also receive instruction on how to secure, diagnose and optimize communication networks. Certification can also be offered to supplement almost all training courses.

Link: (<https://www.siemens.com/industrial-networks-education>)

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 form one element of such a concept.

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. These systems, machines and components should only be connected to the enterprise network or the Internet if and only to the extent necessary and with appropriate security measures (firewalls and/or network segmentation) in place.

You can find more information on protective measures in the area of industrial security by visiting: (<https://www.siemens.com/industrialsecurity>).

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends performing product updates as soon as they are available and using only 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 (<https://www.siemens.com/industrialsecurity>).

Note on firmware/software support

Siemens only provides bug and security fixes for the last released firmware/software version. This means that Siemens only monitors the current firmware/software version for security vulnerabilities.

Security recommendations

To prevent unauthorized access, note the following security recommendations.

General

- You should make regular checks to ensure that the software meets these recommendations and/or other security guidelines.
- The "SIMATIC NET PC Software" undergoes continuous development to make it more secure. We strongly recommend that product updates are applied as soon as they are available and that the latest product versions are used. In addition, we recommend installing the latest security updates of the Microsoft .NET Framework and the Microsoft SQL Server 2019 on your PC systems. Also, make sure that the latest drivers are installed for the network cards you are using.
- When using the "SIMATIC NET PC Software" make sure that you have sufficient system resources for their use. Required resources and configuration of the PC station must match your specific application/configuration limit. General notes from Microsoft regarding memory usage and CPU load must be taken into account. If system resources are no longer available, error-free operation of the "SIMATIC NET PC Software" can no longer be guaranteed.
- When the internal and external network are disconnected, an attacker cannot access internal data. Therefore, operate the software only within a protected network area.
- We strongly recommend that you do not connect communication modules
 - without an activated firewall
 - without a VPN connectiondirectly to the Internet. Without suitable protective measures there is a risk of unauthorized access to the module.

Physical access

Restrict physical access to the device to qualified personnel.

Software (security functions)

- Keep the software up to date. Check regularly for security updates for the product. You can find information on this on the Internet pages at the following address: LINK: (<https://www.siemens.com/industrialsecurity>)
- Inform yourself regularly about security advisories and bulletins published by Siemens ProductCERT (<https://new.siemens.com/global/en/produkte/services/cert.html>).
- Only activate protocols that you really need to use the software.
- Restrict access to the software with a firewall or rules in an access control list (ACL - Access Control List).

SIMATIC NET glossary

The SIMATIC NET glossary describes terms that may be used in this document.

You will find the SIMATIC NET glossary in the Siemens Industry Online Support at the following address:

Link: (<https://support.industry.siemens.com/cs/ww/en/view/50305045>)

Recycling and disposal



The products are low in harmful substances, can be recycled and meet the requirements of the Directive 2012/19/EU for disposal of waste electrical and electronic equipment (WEEE).

Do not dispose of the products at public disposal sites.

For environmentally compliant recycling and disposal of your electronic waste, please contact a company certified for the disposal of electronic waste or your Siemens representative.

Note the different national regulations.

Installation of the SIMATIC NET PC software products

2

2.1 Requirements and notes on installation

User experience

To install the SIMATIC NET PC software products, you need to have experience of installing software on the operating system you are using.

To configure the communications modules, you should have experience and knowledge of the following:

- Structure of the plant involved.
- Configuration of the plant.

You should only undertake the installation and configuration described below if you have this knowledge.

Privileges required for installation

You need administrator privileges for the installation.

2.1.1 Requirements and notes relating to the software

Operating systems

The SIMATIC NET PC software products are intended for operation with Microsoft Windows operating systems; for details, refer to the section "Released operating systems (Page 12)".

Upgrade DVD for which versions?

"SIMATIC NET PC Software V17 SP1" is an upgrade DVD for the following software version:

- "SIMATIC NET PC Software V17"

The delivery release on the product support pages and the Readme provide you with a quick overview of available products.

Software licenses

To run the SIMATIC NET products, you require one software license per PC or virtual machine and product.

Example 1: If you have installed the product "HARDNET IE S7" on a PC and operate three CP 1623 modules with it, you require only one software license.

2.1 Requirements and notes on installation

Example 2: If you use SOFTNET PB S7 on a PC in three virtual machines, you require three licenses.

Screen savers

Using a screen saver during operation can cause system overload.

Some screen savers do not release parts of memory again. This leads to a continuous reduction in usable memory.

Virus scanners

The use of a virus scanner during runtime can impair or severely slow down communication. For this reason, dynamic virus protection in particular using gatekeeper mechanisms is not advisable.

Note

If you use a virus scanner, make sure that the PC has enough system resources.

The following virus scanners have been tested in conjunction with the SIMATIC NET PC software products (the default settings of the virus scanners were not changed for the test):

Virus scanner name	Tested with operating system
McAfee AntiVirus Plus	- Windows 11 Pro Version 21H2 - Windows 10 Pro Version 21H1
Norton Security	- Windows 11 Pro Version 21H2 - Windows 10 Pro Version 21H1
Kaspersky AntiVirus	- Windows 11 Pro Version 21H2 - Windows 10 Pro Version 21H1
Microsoft Defender	- Windows 11 Enterprise Version 21H2 - Windows 10 Pro Version 21H2 - Windows 10 Enterprise Version 21H1 - Windows Server 2016 - Windows Server 2019

Restore points

A system restore point is not created automatically and needs to be set as a manual restore point prior to the installation.

2.1.2 Requirements and notes relating to the hardware

Note

We recommend that you first install the software and license as described in this documentation and install the communications processors afterwards.

Bus collisions after reinstallation

With a new installation all PROFIBUS communications processors receive the bus address 0. If there are several communications processors connected to the same bus, this inevitably leads to address conflicts.

Solution

With such a constellation, set different bus addresses for the communications processors before attaching the communications processors to the bus. This can be done using the "Communication Settings" application.

Plug and play

If the plug-and-play mechanism does not find the driver after installing the communications processor and then rebooting the computer, you will need to start the search for drivers manually. Follow the steps outlined below:

1. Open the Device Manager.
2. Select the top expression in the list box (the local PC) and then the menu command "Action" > "Scan for hardware changes".
3. Confirm all the following dialogs with "Next".

Note

If a question appears in this dialog box asking whether or not you want to search for suitable drivers on the Internet, select "No, not this time" and then click "Next".

2.1.3 Notes on installation

Follow the instructions below step by step to install the SIMATIC NET PC software products and observe the following notes:

- During the installation, the PC is restarted several times depending on its configuration and the software you are installing. These restarts are unavoidable parts of the installation process.
- Following a restart of the PC, the installation will continue automatically with the next step. You only need to follow the installation instructions in this description. No further measures are necessary.

- Make sure that the same user is logged on following a restart.
- The installation dialog of the "SIMATIC NET PC Software" offers you the choice of "German" or "English". If you want to install on an Asiatic system (Chinese, Korean or Japanese), select the "English" language version.

2.2 Released operating systems

The "SIMATIC NET PC Software V17 SP1" DVD can be installed on the following operating systems:

Operating system	Minimum requirements
Windows 11 Enterprise, Pro Version 21H2 (OS Build 22000)	2.4 GHz PCs with 4 GB RAM, 2 cores
Windows 10 Enterprise, Pro Version 21H2 (OS Build 19044)	
Windows 10 Enterprise, Pro Version 21H1 (OS Build 19043)	
Windows 10 Enterprise, Pro Version 20H2 (OS Build 19042)	
Windows 10 (IoT) Enterprise 2021 LTSC (OS Build 19044)	
Windows 10 (IoT) Enterprise 2019 LTSC (OS Build 17763)	
Windows 10 (IoT) Enterprise 2016 LTSB (OS Build 14393)	
Windows Server 2016 (Standard, Datacenter)	2.4 GHz PCs with 4 GB RAM, 2 cores
Windows Server 2019 (Standard, Datacenter)	

You will find further information on multi-language versions for the supported operating systems in the readme file on the "SIMATIC NET PC Software" DVD.

For more detailed information on the minimum requirements for the PC, also refer to the readme file on the "SIMATIC NET PC Software" DVD.

2.3 Procedure

Installation of the "SIMATIC NET PC Software"

Proceed as follows to install the "SIMATIC NET PC Software":

1. Log in with the operating system using an account belonging to the group of administrators.
2. Close all active programs.

Note

Problems may occur during installation with active virus scanners. In this case, disable the virus scanner for the duration of the installation.

3. Insert the "SIMATIC NET PC Software" DVD and wait until installation is started automatically. If installation does not start after some time (about 30 seconds), the autostart function of your PC is not activated. In this case, start the "setup.exe" program in the main folder on the "SIMATIC NET PC Software" DVD.

4. Click the "Display Readme" button and read the information displayed. The readme file contains the latest information on the SIMATIC NET PC products.
5. Click the "Install Software" button and follow the instructions in the dialog boxes to select the language you require and to accept the license conditions. Depending on the operating system, there will be one or two dialog boxes relating to security settings and the energy saving mode that you can confirm with the "Install Software" button if you want the installation to be performed.
6. Select the programs to be installed by selecting the check box. The following programs can be selected:

Programs to be installed	Description and procedure
Automation License Manager	You can install or uninstall license keys with the "Automation License Manager".
SIMATIC NET PC Software	If the check box is selected, the SIMATIC NET PC software products are all installed at once.
SIMATIC NET PC Software Doc	Select this check box if you want to install the documents for installation and commissioning on your PC.
SOFTNET-IE RNA	The "SOFTNET-IE RNA" software allows the integration of PCs in redundant, parallel Ethernet structures based on the Parallel Redundancy Protocol (PRP) functionality. Select this check box if you want to install "SOFTNET-IE RNA".

Note

SIMATIC NET PC software products from an already installed SIMATIC NET PC software will be uninstalled automatically before the software products on this DVD are installed. The configuration data is retained.

You will see a further warning on the screen immediately before the previous software products are uninstalled.

7. Click the "Next" button. Installation starts and can take some time.
8. Click the "Transfer License Key" button if you want to transfer license keys. Alternatively, you can also transfer license keys after the installation using the "Automation License Manager" program. Current license keys are required for the products of the "SIMATIC NET PC Software" DVD. These ship with the product on a USB stick and must be transferred to your PC.
9. Once installation is complete, restart the PC and log in with the same account.

Transferring license keys

You can manage the license keys for running SIMATIC NET programs with the "Automation License Manager".

Follow the steps outlined below:

1. Start the "Automation License Manager" program.
2. Select the data storage medium containing the required license key in the left-hand list (navigation area).

2.3 Procedure

3. In the right-hand list (object area), select the license keys you want to transfer.
4. Click on the menu command "License Key" > "Transfer..." > "Transfer License Key" dialog box.
5. Select the local drive of your computer to which you want to transfer the license keys and confirm with "OK". The license keys are transferred.

Note

For more detailed information on the "Automation License Manager", refer to the online help for the program.

Communication settings

After you have transferred the license keys, the PC reports successful installation of the SIMATIC NET PC products. If multiple network adapters are installed on the PC, the "Communication Settings" dialog box opens.

Note

If the network adapters have not yet been installed, close the dialog with "Cancel" and continue with the instructions in the section "Installing communication modules". Once you are finished, the "Communication Settings" dialog box opens once again.

Note

To transfer a configuration with STEP 7 to a destination PC, a communication module is required in the destination PC that can receive the configuration data. If multiple network adapters are displayed, select the one that is connected to the same network and subnet as the PC on which STEP 7 is installed.

Proceed as follows to select a network adapter using the "Communication Settings" dialog:

1. Select the "Remote Communication" check box. This enables remote configuration.
2. Enter the password for the STEP 7 communication.
3. Select the desired network adapter.

Note

For security reasons, clear the "Remote Communication" check box if you do not need remote configuration.

Installing communication modules

Proceed as follows to install the communication modules to be used:

1. Read the installation manual or operating instructions for the communications module and any other relevant documentation.
2. Install the communications modules as explained.
3. Restart the PC.

Starting the configuration

After restarting the PC, you will need to log on with administrator privileges. It is possible that the Microsoft "Found New Hardware Wizard" will appear. You will then be asked whether or not you want to install the software automatically. Select this option, click "Next" and close the wizard when it has completed its work with "Finish". The PC now contains the SIMATIC NET communication software that still needs to be configured. The steps involved are described in the "Commissioning PC Stations" manual.

Installing further software components

Observe section "SNMP service, SNMP OPC MIB compiler and profile files (Page 27)" on installing optional software components.

SIMATIC NET PC Software as of V17 is installed in such a way that Security Events according to IEC 62443-3-3 are generated when security-relevant events occur.

You can find these Security Events in the Control Panel under "Administration" > "Event view" in the folder "Application and Service protocols" > "Siemens Automation" > "Simatic Net PC Software".

The events are suitable for further processing and automatic evaluation by a consumer such as a SIEM system (Security Information Event Management system). You can find a detailed description of the Security Events valid for the SIMATIC NET PC Software as of V17 in the section "Security Events (Page 39)".

2.3 Procedure

Installation and configuration with VMware vSphere

3

This section describes the requirements for installation as well as the installation of the "SIMATIC NET PC Software" on the "VMware vSphere Hypervisor ESXi 6.7 Update 3/ESXi 7.0 Update 3" platform. The steps in configuration described in this section relate to the vSphere Client. The descriptions apply correspondingly to the vSphere Web Client.

Note

VMware vSphere Hypervisor ESXi 6.7 Update 3 has only been released for operation with Windows 10.

3.1 Requirements and notes

3.1.1 User experience

To install and operate the SIMATIC NET PC software products with "VMware vSphere Hypervisor ESXi 6.7 Update 3/ESXi 7.0 Update 3", you require experience of the product "VMware (<http://www.vmware.com/>)".

To configure the communications modules, you should have experience and knowledge of the following:

- Structure of the plant involved
- Configuration of the plant
- "SIMATIC NET PC Software", see Further Information (Page 37)

Note

You should only undertake the installation and configuration described below if you have this knowledge.

3.1.2 Requirements and notes relating to the software

Operation on a VMware ESXi server

The "SIMATIC NET PC Software" is suitable for operation on virtual machines with the server operating system VMware vSphere.

3.1 Requirements and notes

Released guest operating systems

You will find a list with the guest operating systems compatible with the "ESXi 6.7 Update 3" and "ESXi 7.0 Update 3" servers that are suitable for operation as PC station in the section "Released operating systems (Page 12)".

Notes on licenses

Note

A license must be obtained for each virtual machine (VM). If, for example, you want to operate 5 VMs with the S7 protocol, you need to purchase the product that provides the S7 protocol functionality 5 times. The license keys then need to be installed on the VM in which the corresponding functionality is used.

Alternatively, you can also use a license server at the terminal bus.

3.1.3 Requirements and notes relating to the hardware

You will find a list with the server hardware compatible with the ESXi server on the Web page of VMware.

VMware compatibility list (<http://www.vmware.com/resources/compatibility/search.php>)

The requirements and restrictions for operation without virtualization also apply.

Minimum requirements of SIMATIC NET for a VM (virtual machine):

- 2.4 GHz (2 cores)
- 4 GB RAM

3.1.4 Restrictions

3.1.4.1 VMware vSphere vMotion

"vMotion" is the term used by VMware for moving virtual machines from one server to another during operation.

vMotion has been released for operation of SOFTNET-IE S7 via the virtual network adapter VMXNET3. When moving a VM, there will be interruptions in communication (drop out). Make sure that you take this into account when setting the monitoring times of the communications protocols.

3.1.4.2 Options for operating the virtual machines

The following option for operating virtual machines is released:

- Microsoft Remote Desktop connection
- vSphere client

See also the notes in the readme of Remote Desktop and Terminal Services.

Note

Operator control restriction

A virtual machine must not be operated via more than one console at any one time.

Make sure that the connection between the Remote PC and VM is not interrupted. Otherwise the VM can only be operated again after a fresh logon of the Remote Desktop client.

When using Remote Desktop, the connection must be established as an administrator to be able to use the full range of functions of the "SIMATIC NET PC Software". The call from the client uses `mstsc.exe /admin`.

3.1.4.3 Intel SR-IOV

SR-IOV stands for "Single Route I/O Virtualization" and allows several VMs direct access to a PCIe device at the same time.

The use of SR-IOV has not been released for SIMATIC NET communication.

3.1.4.4 Configuration of the MAC address in STEP 7 projects

The MAC address of a virtual network adapter is assigned automatically by VMware. If it is changes and the adapter involved is part of a configuration, the configuration may need to be changed.

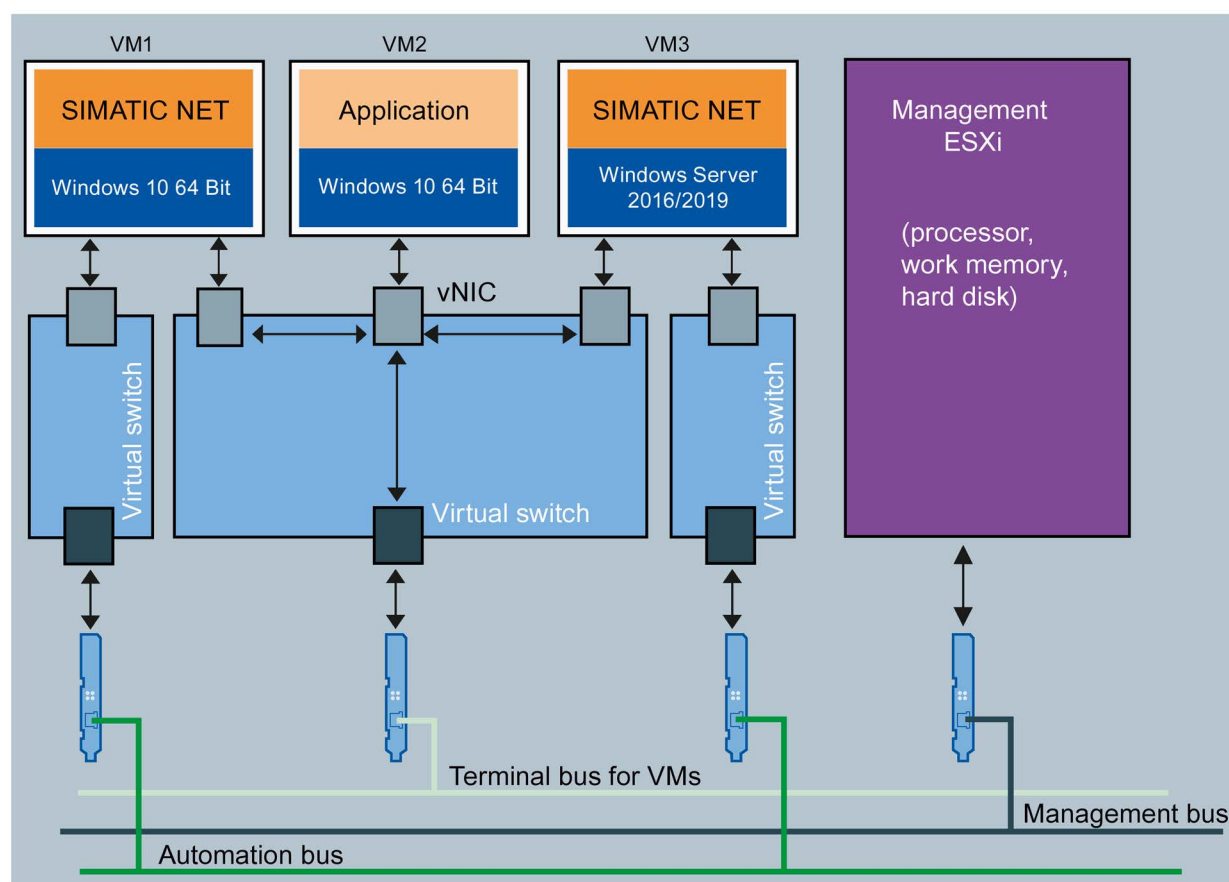
3.2 Overview

Note

VMware Passthrough is not supported for the SIMATIC NET PC CPs.

If the SIMATIC NET communication is exclusively via virtual networks, you can skip this section.

Following installation, the VMware ESXi server supports only standard hardware (main boards, processors, graphics cards, network adapters, ...) from the compatibility list of VMware (refer to the section "Requirements and notes relating to the hardware (Page 18)").



vNIC virtual network adapter

Figure 3-1 Division of the Ethernet networks

The Figure "Division of the Ethernet Networks" shows a suggestion for dividing up the Ethernet networks based on their tasks:

- VM1 uses a virtual Ethernet interface (SOFTNET IE) with a separate virtual switch for access to the automation network.
- VM2 is only connected to one virtual adapter on a separate virtual switch, at the same time it shares a real adapter with the other two virtual machines. No "SIMATIC NET PC Software" is installed.
- VM3 uses a virtual Ethernet interface (SOFTNET IE) with a separate virtual switch for access to the automation network.
- The management of the ESXi server also uses its own virtual switch to avoid disruptions (e.g. during backups).
- The terminal bus is intended for the connection of "Remote Desktop Service".

3.3 Installation of the SIMATIC NET PC software in a virtual machine

To reduce the number of restarts of virtual machines and the ESXi server required during installation, follow the steps below when commissioning:

1. Shut down all virtual machines.
2. All devices with pass-through capability are listed in the server settings on the property page "PCI devices" > "Passthrough-capable devices". If available, disable the "Passthrough" option for existing modules.
3. Restart the ESXi server.
4. Install the "SIMATIC NET PC Software" in the required virtual machine as described in section "Installation of the SIMATIC NET PC software products (Page 9)".
5. Restart the virtual machine.

3.4 Upgrade

3.4.1 Upgrade procedure SIMATIC NET

"SIMATIC NET PC Software V17 SP1" has been released for use with the following versions of VMware vSphere Hypervisor:

- ESXi 6.7 U3
- ESXi 7.0

To upgrade from "SIMATIC NET PC Software" V17 to "SIMATIC NET PC Software V17 SP1", the ESXi server must first be updated to version 6.7 U3 or version 7.0.

1. Run the update of the software VMware vSphere Hypervisor.
2. Following the server upgrade, update the virtual machines. To do this, the current VMware Tools must be installed on the virtual machines.
The supported virtual hardware versions are listed in the Readme file.
3. Then install the "SIMATIC NET PC Software V17 SP1".

3.4.2 Upgrading Hypervisor

"SIMATIC NET PC Software, V17 SP1" has been released for VMware vSphere Hypervisor ESXi 6.7 Update 3 (only with Windows 10) and ESXi 7.0 Update 3.

Follow the steps below to upgrade your server:

1. Shut down all virtual machines.
2. Make sure that you do not use any modules with pass-through functionality; otherwise, a host upgrade is not allowed. All devices with pass-through capability are listed in the server settings on the property page "PCI devices" > "Passthrough-capable devices". If available, remove the pass-through devices.
3. Restart the ESXi server.
4. Install the upgrade to VMware vSphere Hypervisor ESXi 6.7 Update 3. or ESXi 7.0 Update 3.
5. Update the "SIMATIC NET PC Software" to version V17 SP1.

Note

To use the "SIMATIC NET PC Software" to create and manage the virtual machines, the vSphere WebClient is required.

4.1 Configuration of the virtual Standard Switch (vSS)

For SIMATIC NET communication via SoftNet Ethernet products, a separate virtual Standard Switch (vSS) must be used. You will find a schematic diagram in the section Overview (Page 19), Figure 3-1 Division of the Ethernet networks.

Configuring a VMkernel port for server management tasks on this switch (vSS) is not permitted.

Note

SIMATIC NET communication is not released for the virtual Distributed Switch (vDS).

To be able to use SIMATIC NET communication via vSS, make the following settings in the properties of the vSwitch and the port groups.

Note

The settings can be specified separately for the vSwitch, individual port groups or individual VMkernel ports.

Remember that the settings for the port group/VMkernel port overwrite the settings on the vSwitch and therefore have priority.

You can open the properties as follows:

1. Open the vSphere Web Client.
2. Click on the server in the navigation tree on the left.
3. Click on the "Configuration" tab.
4. Click "Network" in the small "Hardware" dialog window.
5. To configure the network, click "Properties..." on the right above the network.
6. In the menu on the left, select the port group for the created network (the settings can be seen in the right-hand column).

4.1 Configuration of the virtual Standard Switch (vSS)

To change the settings, click the "Edit..." button at the bottom left.
The properties dialog and the settings to be made are explained in the following sections.

4.1.1 General

The name of the port group is assigned on this page. This name is the name of the network connection that can be selected in the "Properties of virtual machines".

The default setting for VLAN ID "None (0)" must be retained.

4.1.2 Security

For SIMATIC NET communication, the default settings for security must be retained.

- Promiscuous Mode: "Reject"
- MAC Address Changes: "Accept"
- Forged Transmits: "Accept"

4.1.3 Traffic Shaping

The VMware function "Traffic Shaping" allows central and distributed restriction of the usable bandwidth.

The VMware function "Traffic Shaping" has not been released for the "SIMATIC NET PC Software".

The default setting "Disabled" must be retained for "Traffic Shaping".

4.1.4 NIC Teaming

The settings in the "NIC Teaming" tab allow the settings for load balancing and failover configuration.

The default settings for NIC groupings must be retained.

Note

The server settings for assigning the MAC addresses must not be changed when using SIMATIC NET communication.

This involves the assignment type and the VMware OUI value (Organizationally Unique Identifier). The default values are as follows:

Assignment type: "VMware OUI assignment"

VMware OUI: for example "00:50:56" :xx:xx:xx

4.2 Configuration of the virtual machine

4.2.1 Hardware

Note

1:1 assignment between module and VM recommended

For optimum performance, a VM with "SIMATIC NET PC Software" should be assigned to its own physical module.

1. Open the vSphere client.
2. Click on the required machine in the navigation tree on the left.
3. To edit the properties of the virtual machine, open the shortcut menu (right-click) and select "Edit Settings".

Reaction: The "Virtual Machine Properties" window opens.

4.2.1.1 CPU/RAM settings

Select "Memory" on the left and configure the memory for 64-bit systems at least 4 GB.

Select "CPUs" and set 1 for the "Number of virtual sockets" and at least 2 for the "Number of cores per socket".

4.2 Configuration of the virtual machine

4.2.1.2 Adding network adapter to the virtual machine

SIMATIC NET communication has been released for the network adapter VMXNET 3.

The setting of the MAC address for SIMATIC NET communication must remain set to the default (automatic).

When adding an Ethernet adapter, you need to select the corresponding network based on the port group name (section "Configuration of the virtual Standard Switch (vSS) (Page 23)").

4.2.2 Options

The following settings relate to the advanced options in the "Options" tab.

4.2.2.1 Memory/CPU Hotplug

The settings for "Memory/CPU Hotplug" must remain set to the defaults:

- "Disable memory hot add for this virtual machine"
- "Disable CPU hot plug for this virtual machine"

4.2.2.2 Boot options

The "Boot options" must remain set to "EFI" for the specified boot firmware.

4.2.2.3 Starting a virtual machine

When "SIMATIC NET PC Software" is installed, a virtual Ethernet interface is automatically assigned to SOFTNET-IE and can be used for industrial communication.

Note

1:1 assignment between module and VM recommended

For optimum performance, a VM with "SIMATIC NET PC Software" should be assigned to its own physical module.

SNMP service, SNMP OPC MIB compiler and profile files

5.1 Installing the SNMP service

Purpose

The SNMP OPC Server requires the SNMP service in the operating system. Full use of the SNMP OPC Server is only possible if this Windows component is installed / enabled.

Introduction

Following standard installation of Windows, the full SNMP service is not yet available in the operating system. Without taking further steps, you can query items but cannot use SNMP traps.

Installing the SNMP service involves the following steps:

- Installing the SNMP service
- Adapting the network security settings to your own security needs

Requirement

You must be logged on as administrator or as a member of the "Administrators" group to be able to perform the installation.

Note

If programs already use the OPC server and the SNMP service was installed while an OPC Server was active, all programs that use the OPC Server must be closed and restarted. The OPC server must also be shut down with "Communication Settings" > "Exit OPC Server" and then restarted.

Note

If the computer is connected to a network, the general network settings may prevent installation of the SNMP services.

Step 1 - Installing the SNMP service

Procedure with Windows Server 2016

For the local server, add the "SNMP service" feature. The SNMP service starts automatically whenever you restart the system.

Note

Exit OPC server

If the SNMP service was installed on an OPC server that is already active, the OPC server must be shut down.

Close the OPC server with "Communication Settings" > "Exit OPC server" to ensure that the settings are adopted. With the next request, it will start up again automatically.

Procedure under Windows 10 and Windows Server 2019

Install the SNMP service as described below:

1. In the Control Panel, go to "Start > Settings > Apps > Optional Features + Add Features".
2. In the "Windows Features" list, click "Install" for "Simple Network Management Protocol (SNMP)". The SNMP service starts automatically whenever you restart the system.

Note

Exit OPC server

If the SNMP service was installed on an OPC server that is already active, the OPC server must be shut down.

Close the OPC server with "Communication Settings" > "Exit OPC server" to ensure that the settings are adopted. With the next request, it will start up again automatically.

Procedure with Windows 11

1. Set up an internet connection for the installation.

Note

If you cannot set up an internet connection on site, you can also install the SNMP service using "Features on Demand". More information is available here:

<https://docs.microsoft.com/en-us/windows-hardware/manufacture/desktop/features-on-demand-v2--capabilities?view=windows-11>).

2. In the Settings, go to "Apps" > "Optional features" and click on the "View features" button in "Add an optional feature".

3. In the list, select the "Simple Network Management Protocol (SNMP)" feature and click "Next".
4. Click the "Install" button to install the feature. The SNMP service will start automatically after installation.

Note**Exit OPC server**

If the SNMP service was installed on an OPC server that is already active, the OPC server must be shut down.

Close the OPC server with "Communication Settings" > "Exit OPC server" to ensure that the settings are adopted. With the next request, it will start up again automatically.

Step 2 - Adapting the network security settings to your own security requirements

When you install the SNMP service, not only the SNMP protocol but also an SNMP agent is installed.

Adapt the network security settings and the access permissions of the SNMP agent to your own security needs. To this end, open the properties of the Windows service "SNMP service", "Security" tab. You will find more detailed information in our manual "Commissioning PC Stations".

5.2 SNMP OPC MIB compiler and profile files

MIB compiler of STEP 7

The range of information that can be monitored by the devices with the SIMATIC NET SNMP OPC server depends on the particular device profile. With the integrated MIB compiler of STEP 7, existing profiles can be modified and new device profiles created for any SNMP-compliant device. It requires MIB files according to the SMIv1 standard.

MIB files for CP 1623

Suitable MIB files ship with STEP 7.

When you enter the required device in the plant configuration, the "device profile" parameter offers you the profiles with the name of the module, for example "CP1623_V10.txt" and they can be selected here.

The following MIB files are supported for the CP 1623:

- rfc1213.mib
- automationSystem.mib
- automationPS.mib
- automationTime.mib

Uninstalling the SIMATIC NET PC software products

6

Note

After uninstalling the SIMATIC NET PC software products, any CP installed in the PC will no longer be ready for operation because the associated device driver is also uninstalled. This is indicated in the device manager by a yellow exclamation point. You can remedy this situation by reinstalling the "SIMATIC NET PC Software" DVD. SOFTNET modules can also be operated with other SIMATIC products (e.g. STEP 7).

Uninstalling the SIMATIC NET PC products is achieved using "Control Panel" and the entry "Programs" or "Uninstall programs". Depending on what you installed from the data medium "SIMATIC NET PC Software" you can also uninstall these parts again:

- SIMATIC NET PC Software
- SIMATIC NET PC Software Doc
- SIMATIC NET SOFTNET-IE RNA
- Siemens Automation License Manager (only uninstall if no other product on your device uses license keys and after you have removed the license keys from the device)

If you uninstall "SIMATIC NET PC Software", you can also uninstall the following software if it is not required by other products:

- Microsoft SQL Server 2019 LocalDB
- Microsoft OLE DB Driver for SQL Server
- OPC UA Local Discovery Server

We do not advise uninstalling Microsoft Visual C++ Redistributables because it is needed by other software packages.

Note

Any license keys left on the PC can no longer be backed up without the "Automation License Manager".

Automated installation

7.1 Purpose and general description

Use in enterprises

Enterprises that install plants with large numbers of computers generally want to use the same installation everywhere. Automated installation provides this option. The settings are made with a control file.

Sequence

Installation only requires a few user decisions that generally need to be taken at the end of the installation.

Control file

The control file is generated during a sample run and is structured like an INI file. It is clear to read as an ASCII file and in exceptional cases can be corrected manually.

7.2 Structure of the control file

Description

The control file has the name "Ra_Auto.ini" and has the following structure:

```
[BUNDLEINFO]
CreatedWith=SIMATIC NET PC Software
RaSetupVersion=
[GENERAL]
AutoReboot=True
RebootOnEnd=True
Setuplanguage=en
IdName=
IdCompany=
IdNumber=
LicenseKeyDestinationDrive=C:
TransferLicenseManagerKey=False
InstallLanguage=de;en
OnlyUpdateInstallation=False
[DIALOGS]
DialogLicenseList=False
DialogDone=True

[PRODUCTCODE1]
DestinationDrive=C:
Selected=True
DestinationPath=[ProgramFilesFolder]SIEMENS\SIMATIC.NET
```

If necessary, the following parameters can be adapted, the other parameters should not be changed

[General] area

General settings are made in the [General] area.

Parameters	Value range	Description
AutoReboot	True/false	Automatic restart at the end
RebootOnEnd	True/false	Display of restart prompt
Setuplanguage	de=German en=English	Installed language

[Dialogs] area

The display of dialog boxes can be influenced in the [Dialogs] section.

Parameters	Value range	Description
DialogDone	True/false	Display of the closing dialog

[PRODUCTCODE1] area

The [Productcode1] area contains the product code as a title and the three following parameters. Examples of product codes are: [LICENSEMANAGER] or [SIMNETPC].

Parameters	Value range	Description
DestinationDrive	-	Installation drive, e.g. "C:\"
Selected	True/false	Product selection
DestinationPath	-	Installation path The installation path can be changed dynamically by a placeholder.

7.3 Generating the control file automatically

Description

The "Ra_Auto.ini" control file is generated by the setup program by making a trial installation and can then be used to control the installation program.

The setup program can be called by a batch file.

Note

The configuration of the PC on which you create the control file must correspond to the configuration of the destination PC.

If the "Microsoft Visual C++ 2012 Redistributable" is already installed on the destination PC, for example, the corresponding package in the control file is considered to be unnecessary:

```
[VCREDIST2012]
```

```
Selected=False
```

This would have the effect that the package would not be installed on all destination PCs and the product possibly could not be installed successfully.

Note

When installing a new version of the "SIMATIC NET PC Software", you also need to renew the control file because the software configuration can change with a new version.

Example of a batch file

The batch file shown here generates the control file "Ra-Auto.ini".

Create a batch file with the following content:

```
<LW>:
cd =\sw\x64
setup.exe /record
```

After starting the batch file, a dialog box is displayed in which you can make additional settings.

The lines of the batch file example have the following significance:

Line	Meaning
1	The program changes to the drive of the installation DVD.
2	The program changes to the working directory of the setup.
3	The program starts the manual test installation and generates the control file "Ra_Auto.ini" with the "/record" parameter. All user actions in the dialogs are stored there. The record action stops after the "component selection" and closes the program.

Note

During the automatic installation, note that the path for the "Ra_Auto.ini" file can be set with the following instruction:

```
sw\x64\setup.exe /silent=<Dr>:\<folder>\Ra_Auto.ini
```

Unless a path is specified, the Windows directory is searched.

If additional questions arise or error messages are displayed during installation, a suitable dialog box opens.

Further Information

8.1 Documentation guide

Readme file of the SIMATIC NET products

All the important information relating to the SIMATIC NET products and other information on configuration and operation can be found in the two readme files for the overall product (main directory of the product DVD).

Quick Start for SIMATIC NET products

You will find a quick start for configuration in the "Commissioning PC Stations" document if you have installed the documentation (Start menu "Start" > "Siemens Automation" > "Documentation" > "Manuals" > "English" > "SIMATIC NET - Commissioning PC Stations").

Commissioning PC Stations

The "Commissioning PC Stations" document contains overview information on all PC configuration programs (Start menu "Start" > "Siemens Automation" > "Documentation" > "Manuals" > "English" > "SIMATIC NET - Commissioning PC Stations").

The "Commissioning PC Stations" manual is a PDF document and can be read and printed out when required with the Acrobat Reader.

"Communication Settings" configuration program

Here, you will find information relating to a variety of topics, for example procedures manuals for the project engineering and configuration of connections. ("Communication Settings" > "Help" > "SIMATIC NET Configuration")

Manual Collection

The SIMATIC NET Manual Collection contains all SIMATIC NET documentation and is available on the web pages at Siemens Industrial Online Support at the following link:

Link: (<https://support.industry.siemens.com/cs/ww/en/view/109795412>)

8.2 Technical support, contacts and training

You will find information on this in the file "TechnicalSupport.pdf" in the "\doc" folder of the "SIMATIC NET PC Software" DVD.

Appendix A

A.1 Security Events

This section describes the Security Events. The structure of the Security Events is based on IEC 62443-3-3.

A.1.1 Structure of the Security Events

In Windows operating systems, the Security Events are saved as event log records¹ in an event log file^{2,3}. A consumer (e.g. an SIEM system) can subscribe to these Security Events for further processing⁴.

¹ (<https://docs.microsoft.com/en-us/windows/win32/eventlog/event-log-records>)

² (<https://docs.microsoft.com/en-us/windows/win32/eventlog/event-log-file-format>)

³ (<https://docs.microsoft.com/en-us/windows/win32/eventlog/reading-from-the-event-log>)

⁴ (<https://docs.microsoft.com/de-de/windows/security/threat-protection/use-windows-event-forwarding-to-assist-in-intrusion-detection>)

A.1.2 Variables in Security Events

The variables are displayed in the "Security Events" section in the "Message text" field within curly brackets {variable}.

The output Security Events can contain the following variables:

Variable	Description	Possible values or example
{IP address}	IPv4 address according to RFC1035 IPv6 address according to RFC4291 Section 2.2	192.168.1.105 2001:DB8::8:800:200C:417A
{Protocol}	Layer 4 protocol or service used that generated the event.	S7 Server
{User name}	String (without spaces) that identifies the authenticated user by his or her name.	PeterMaier
{Time seconds}	Number of seconds	44
{Failed login count}	Number of failed login attempts	10
{Max sessions}	Maximum number of sessions	10
{Trigger condition}	String (without spaces) for a trigger condition that activates the relevant function.	GUI-Switch Application
{Subject}	String (with spaces) for the "Subject" in the certificate. Is used as part of the certificate-based authentication and must include Unicode characters. This "Subject" is shown in parentheses.	(UaExpert@TESTPC)
{Local interface}	Symbolic name for the local interface	GUI

Variable	Description	Possible values or example
{file path}	String (with or without spaces) indicating the file path.	C:\templapp.exe
{Session id}	String without spaces for a GUID.	{01234567-abcd-bcde-b234-0123456789ab}
{Client}	String (with or without spaces) indicating the URL of the client application.	urn:TEST-PC:UnifiedAutomation:UaExpert
{Security mode}	String (without spaces) that specifies the security mode of the messages of the secure communication channel.	One of the values: None Sign SignAndEncrypt
{Security policy}	String (without spaces) that specifies the security policy of the secure communication channel.	Aes128_Sha256_RsaOaep
{Version}	Version information (without spaces)	V17.00.01.01

Note**Severity**

Some severities are grouped in the software:

- Info + Notice = Info

A.1.3 Access via untrusted networks

Message text	{Protocol}: Remote access enabled via {Trigger condition}.
Example	S7 Server: Remote access enabled via GUI-Switch.
Explanation	Remote access via S7 server is permitted.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.13

Message text	{Protocol}: Remote access disabled via {Trigger condition}.
Example	S7 Server: Remote access disabled via GUI-Switch.
Explanation	Remote access via S7 server is denied.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.13

A.1.4 User account management

Message text	{Protocol}: Authentication was enabled.
Example	OPC UA S7: Authentication was enabled.
Explanation	Authentication was enabled.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.3

Message text	{Protocol}: Authentication was disabled.
Example	OPC UA S7: Authentication was disabled.
Explanation	Authentication was disabled.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.3

Message text	{Protocol}: User {User name} disabled anonymous login.
Example	OPC UA S7: User PeterMaier disabled anonymous login.
Explanation	An authenticated user disabled anonymous login.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.3

Message text	{Protocol}: User {User name} enabled anonymous login.
Example	OPC UA S7: User PeterMaier enabled anonymous login.
Explanation	An authenticated user enabled anonymous login.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.3

A.1.5 Nonrepudiation

Message text	{Local interface}: User {User name} has changed configuration.
Example	GUI: User PeterMaier has changed configuration.
Explanation	The user has changed all of the configuration data by loading a new *.xdb file.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 2.12

Message text	{Protocol}: User {User name} has changed configuration.
Example	S7 Server: User PeterMaier has changed configuration.
Explanation	The user has changed the settings.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 2.13

Message text	User {User name} has changed configuration.
Example	User PeterMaier has changed configuration.
Explanation	The user has changed the configuration.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 2.14

Message text	The configuration was changed.
Example	The configuration was changed.
Explanation	The configuration was changed.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 2.14

A.1.6 Software and information integrity

Message text	Software integrity verification failed (path: {file path}).
Example	Software integrity verification failed (path: C:\templapp.exe).
Explanation	Integrity verification of the software failed.
Severity	Error
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 3.4