SIEMENS

SIMATIC NET

PC software
SIMATIC NET PC software V18

Installation Manual

11/2022

C79000-G8976-C233-17

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.

Siemens AG
Digital Industries
Postfach 48 48
90026 NÜRNBERG
GERMANY

C79000-G8976-C233-17
Ⓟ 11/2022 Subject to change

Copyright © Siemens AG 2022.
All rights reserved

Table of contents

Introduction 1

Purpose of this document

This document describes how to install "SIMATIC NET PC Software" products on your PG/PC.

Validity of this installation manual

The installation manual relates to products of the "SIMATIC NET PC Software V18".

The installation of "STEP 7 Professional (TIA Portal)" is described in the STEP 7 documentation.

The information in this manual on calling applications using the Start menu applies to Windows 10. This can be different for other released operating systems.

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: (https://www.siemens.com/sitrain)

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. (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 ensure that you are always informed about product updates, subscribe to the Siemens Industrial Security RSS feed at: (https://www.siemens.com/cert)

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: (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.

Security recommendations 2

To harden the system against security threats and to prevent unauthorized access to devices and/or the network, observe the following security recommendations.

General

- You should make regular checks to ensure that the software meets these recommendations and/or other security guidelines.
- Evaluate your plant as a whole in terms of security. Use a cell protection concept with suitable products.
- 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 adapters you are using.
  Check regularly for availability of newer versions of the Automation License Manager (ALM) and install the new version when available. You can find more information at: (https://support.industry.siemens.com/cs/de/en/view/114358)
- 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 connection

  directly to the Internet. Without suitable protective measures there is a risk of unauthorized access to the communications module.
- Check the user documentation of other Siemens products that are used together with the device for additional security recommendations or guidelines.
- Keep the operating system up to date. Check regularly for security updates of the operating system and apply them.
- Information on current security updates of the operating system or dependent components can be found at: (https://support.industry.siemens.com/cs/en/us/ps/15361/faq)
- No product liability will be accepted for operation of insecure infrastructure.

Access to the server

Limit access to the installed products of the "SIMATIC NET PC Software" to qualified personnel. The Windows operating system has a comprehensive system of access permissions. This system allows you to grant or deny users access to certain objects individually and according to need.

Physical access

- Restrict physical access to the communications module to qualified personnel. Use the security mechanisms of Windows.
- Protect the installed products of the "SIMATIC NET PC Software" from unauthorized access to the PC, for example, through installation in lockable racks, control cabinets or control rooms.

Software updates

- Keep the "SIMATIC NET PC Software" up to date. Always use the latest software version of the "SIMATIC NET PC Software". You can find information regarding product innovations and new software versions and updates at: (https://support.industry.siemens.com/cs/us/en/ps/15361/dl)
- The "SIMATIC NET PC Software" is signed. In this way it can be ensured that the software you download is unaltered software created by Siemens. To check this, you calculate the hash value of the downloaded file and compare it with the value indicated on the download page. (https://support.industry.siemens.com/cs/us/en/view/109483101)
- You can verify successful installation of the "SIMATIC NET PC Software" and updates to this software in the Control Panel under "Administrative Tools > Event Viewer" in folder "Applications and Services Logs > Siemens Automation > Simatic Net PC Software > Software Integrity > Operational". An entry along the lines of "User {User name} installed SIMATIC NET PC Software {Version}." indicates a successful installation of the "SIMATIC NET PC Software".

Security functions of the software

- Check regularly for security updates of the "SIMATIC NET PC Software". You can find information on this on the Internet at: (https://www.siemens.com/industrialsecurity)
- Make sure that a virus scanner is active to ensure secure operation of the SIMATIC NET PC Software products. You can also use practices such as "Application Whitelisting" (e.g. McAfee) as an alternative to active virus scanners. For more information regarding virus scanners that have been tested and released for the "SIMATIC NET PC Software", refer to section "Requirements and notes relating to the software" of the Installation Manual for "SIMATIC NET PC Software".
- Enable the protection from brute force attacks via the "Communication Settings" configuration program on the "Select OPC Protocol" properties page. You have the option of implementing the "Brute Force Prevention" on a user-specific or "IP-specific" basis. For more information on this, refer to the online help of the "Communication Settings" configuration program and the programming manual "Industrial Communication with PG/PC Volume 2 - Interfaces", section ""Brute Force Prevention" of the OPC UA server".

- The "SIMATIC NET PC Software" generates Security Events in accordance with IEC 62443-3-3 when security-relevant events occur. You can find these Security Events in the Control Panel under "Administrative Tools" > "Event Viewer" in folder "Applications and Services Logs" > "Siemens Automation" > "Simatic Net PC Software". You can find a detailed description of the Security Events valid for the SIMATIC NET PC Software in the Appendix of the Installation Manual, section "Security Events".
- Restrict access to the "SIMATIC NET PC Software" using a firewall or rules in an access control list (ACL).
- If Siemens detects and resolves Security Incidents in its products, this is published in Security Advisories. You can find the document for the "SIMATIC NET PC Software" at: (https://new.siemens.com/global/en/products/services/cert.html?s=SIMATIC%20NET%20PC%20Software#Subscriptions)

Passwords

- Define rules for use of the "SIMATIC NET PC Software" and assignment of passwords. Follow current recommendations on defining strong passwords, e.g. by the German Federal Office for Information Security: (https://www.bsi.bund.de/ENneu/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Sichere-Passwoerter-erstellen/sichere-passwoerter-erstellen_node.html)
- Regularly update the passwords to increase security.
- Only use passwords with high password strength. Avoid weak passwords, such as "password1", "123456789" and the like.
- Make sure that all passwords are protected and inaccessible to unauthorized personnel.
- Do not use the same password for different users and systems.
- If necessary, use a password manager for generating and managing passwords.

Certificates

- After installation of the "SIMATIC NET PC Software", self-signed certificates are automatically created for the OPC UA servers. If necessary, replace these certificates with self-created higher-quality certificates with key. Use certificates signed by a trusted external or internal certificate authority.
- Make sure that user-defined private keys are protected and inaccessible to unauthorized persons.
- If there is a suspected security violation, change all certificates and keys immediately.
- Verify certificates based on the fingerprint on the server side and client side to prevent "man in the middle" attacks. Use a second, secure transmission path for this.
- You can manage the OPC UA certificates in the "Communication Settings" configuration program. For more information on the OPC UA certificates, refer to the online help of the "Communication Settings" configuration program.
- The certificate management of the OPC UA certificates is based on OpenSSL and is located in a local directory structure. For more information, refer to document "Industrial

Communication with PG/PC Volume 2 – Interfaces", section "Certificate management for the OPC UA server".

- SIMATIC NET OPC UA Server Version 18.0 and higher supports certificate management services that can use a Global Discovery Server, for example. These management functions enable automated updating of OPC UA certificates, trusted lists and certificate revocation lists (CRLs) for the OPC UA servers. For more information, refer to document "Industrial Communication with PG/PC Volume 2 – Interfaces", section "Certificate management with GDS".

Guidelines for account management

Appropriate permissions are required to set up, configure and operate products of the "SIMATIC NET PC Software". The user account management of the operating system is used to assign permissions to a user or to applications. For this purpose, users are given a user account and assigned to one or more groups (roles). In this section, the term "role" is used synonymously with "group". After login with a user account (authentication), the user is given the permissions defined for this role (authorization).

- Assign only the group (role) that is absolutely needed for a user account to that account.
- Withdraw roles from a user account as soon as they are no longer needed by this account.

The following roles are available for account management in combination with the "SIMATIC NET PC Software":

- "Administrator" role

  The "Administrator" role has been predefined in the operating system but is not needed for operating the "SIMATIC NET PC Software" and can be disabled or remain disabled. This role includes broad permissions and should be assigned only for the following actions in the "SIMATIC NET PC Software" area:

  – Setup of users and assignment of roles

  – Installation and uninstallation of the "SIMATIC NET PC Software" products

  – Configuration, including configuration of security settings, such as

    - Settings for access to OPC

    - Certificate management

    - Brute force prevention

  – Configuration of modules and applications of a PC station

- "User" role

  The "User" role is suitable for operating applications of the "SIMATIC NET PC Software" once the runtime environment has been set up and configured for these applications. A group does not have to be assigned for this in the user administration of the operating system.

- "Remote Desktop user" role

  The "Remote Desktop user" role grants login permission from another system via the Remote Desktop of the operating system.

- "SIMATIC NET" and "SIMATIC HMI" role

  The "SIMATIC NET" and "SIMATIC HMI" roles grant permission for cross-computer operation of OPC DA (via DCOM) as well as the exact access permissions needed for operating the "SIMATIC NET PC Software". When you install the products of the "SIMATIC NET PC Software", existing accounts are automatically assigned to these roles. If you later create new accounts that are to be given this permission, you assign these roles to these accounts.

- Roles for operating OPC UA

  For information on this, read the description of the OPC UA services in document "Industrial Communication with PG/PC Volume 2 – Interfaces".

Services

Operation of the "SIMATIC NET PC software" requires specific services to be active. These services usually log in with the local system account.

File integrity

- The files of the "SIMATIC NET PC Software", such as *.exe and *.dll files, are signed by Siemens. You can view the signature and have the details displayed via the properties dialog of the file on the "Digital signatures" tab.
- During operation of the "SIMATIC NET PC Software" products, the files are monitored regularly and any replacement by a file not signed by Siemens is detected. In this case, the "SIMATIC NET PC Software" generates Security Events in accordance with IEC 62443-3-3. You can find these Security Events in the Control Panel under "Administrative Tools" > "Event Viewer" in folder "Applications and Services Logs" > "Siemens Automation" > "Simatic Net PC Software" > "Software Integrity". You can find a detailed description of the Security Events valid for the SIMATIC NET PC Software in the Appendix of the Installation Manual, section "Security Events". You are made aware of a new entry in this event log through an entry in the SIMATIC NET notification service and the flashing of its icon in the notification area of the taskbar on the bottom right.
- In addition, a checksum is published in Siemens Industry Online Support for downloadable files (e.g. *.iso, *.exe) with products or product updates of the "SIMATIC NET PC Software". After downloading the files, you can calculate the checksum and compare it with the published checksum.
- The data storage medium of the "SIMATIC NET PC Software" contains a file signed by Siemens named "content.cat" in the root directory. Double-clicking the file in Explorer opens a dialog window of the Windows app "Crypto shell extensions". Sha-256 checksums are listed for the files of the data storage medium on the "Security catalog" tab. You can calculate the checksum for a file on the data storage medium prior to installation, compare it with the provided checksum and thus check the integrity of the file.
- The procedure for calculating the checksum of a file can be found at: (https://support.industry.siemens.com/cs/us/en/view/109483101)

Protocols

Secure and non-secure protocols

- Only activate protocols that you really need for use of the "SIMATIC NET PC Software" products.
- Use secure protocols when access to the device is not secured by physical protection measures.
  The following protocol, for example, provides a secure alternative:
  - OPC COM / DCOM ⇒ OPC UA
- Avoid or disable non-secure protocols, such as OPC COM / DCOM. This protocol is still available for historical reasons. The OPC DCOM interface for receiving OPC COM protocols is disabled in the "SIMATIC NET PC Software" by default. We recommend that you do not make any changes to this setting.
- OPC UA protocol
  - Security modes
    For protecting your OPC UA communication, use the "Sign" or "Sign&Encrypt" security mode, as this guarantees the authenticity of the communication partners and the integrity of the data transfer.
    "None" does not support any safety objectives and should therefore be used only for commissioning your system.
  - Security policies
    For secure data exchange, use only the "Basic256SHA256", "AES256-SHA256-RsaPss" and "AES128-SHA256-RsaOaep" policies, which are state-of-the art.
    All other policies continue to be supported only for compatibility reasons and have been disabled by default.

List of available protocols

The following is a list of all available protocols and their ports via which the products of the "SIMATIC NET PC Software" can be accessed.

Explanation of the table:

- **Service**
  The services that the products of the "SIMATIC NET PC Software" support.
- **Protocol/port number**
  Port number assigned to the protocol.
- **Default port status**
  - Open
    The port is open after a new installation of the "SIMATIC NET PC Software".
  - Closed
    The port is closed after a new installation of the "SIMATIC NET PC Software".

  After an update installation, the settings of the previous configuration are retained.

- **Port configurable**
  - Yes
    The port number can be configured.
  - No
    The port number cannot be configured.
- **Authentication**
  Specifies whether an authentication of the communication partner takes place.
- **Encryption**
  Specifies whether the transfer is encrypted.

Service	Protocol/ Port number	Default port status	Port configurable	Authentication	Encryption
S7 protocol	TCP/102	Open	No	No	No
S7 optimized protocol	TCP/102	Open (only outgoing)	No	Yes	Yes
DCOM (OPC COM)	TCP/135	Open	No	No	No
SNMP (CP 1623)	UDP/161	Open	No	No	No
SNMP	UDP/162	Closed	No	No	No
DCOM	TCP/1025-1031	Closed	No	No	No
ALM	TCP/4410	Closed	Yes	No	No
OPC UA LDS	TCP/4840	Open	No	No	No
OPC UA/S7	TCP/55101	Closed	Yes	Yes	Yes
OPC UA/SR	TCP/55102	Closed	Yes	Yes	Yes
OPC UA/DP	TCP/55103	Closed	Yes	Yes	Yes
OPC UA/S7 optimized	TCP/55105	Closed	Yes	Yes	Yes

The following is a list of all available Layer 2 services via which the products of the "SIMATIC NET PC Software" are accessed.

The table includes the following columns:

- **Layer 2 service**
  The Layer 2 services that the "SIMATIC NET PC Software" supports.
- **Default status**
  Indicates whether the Layer 2 service is active or inactive after a new installation of the "SIMATIC NET PC Software".
- **Configurable**
  Indicates whether the Layer 2 service can activated/deactivated.

Layer 2 service	Default status	Configurable
DCP	Active	Yes
SNAP / S7-ISO	Inactive	Yes
LLDP	Active	Yes
PRP (SOFTNET-IE RNA)	Inactive	Yes

Guidelines for secure disposal (decommissioning)

To prevent unauthorized persons from accessing confidential data, perform the following steps for decommissioning the "SIMATIC NET PC Software":

- Uninstall all installed components of the "SIMATIC NET PC Software" on the device. You can find a description of this in section "Uninstallation of the SIMATIC NET PC Software" of the Installation Manual.
- Delete the following folders and all subfolders and files contained in them in the path: C:\ProgramData\Siemens\Automation\Logfiles\TraceConcept

Note on firmware/software support

Check regularly for new firmware/software versions or security updates and apply them. After the release of a new version, previous versions are no longer supported and are not maintained.

Intended operating environment

Security modules such as SCALANCE S or SCALANCE SC can be used to protect individual devices, automation cells or network segments of an Ethernet network.

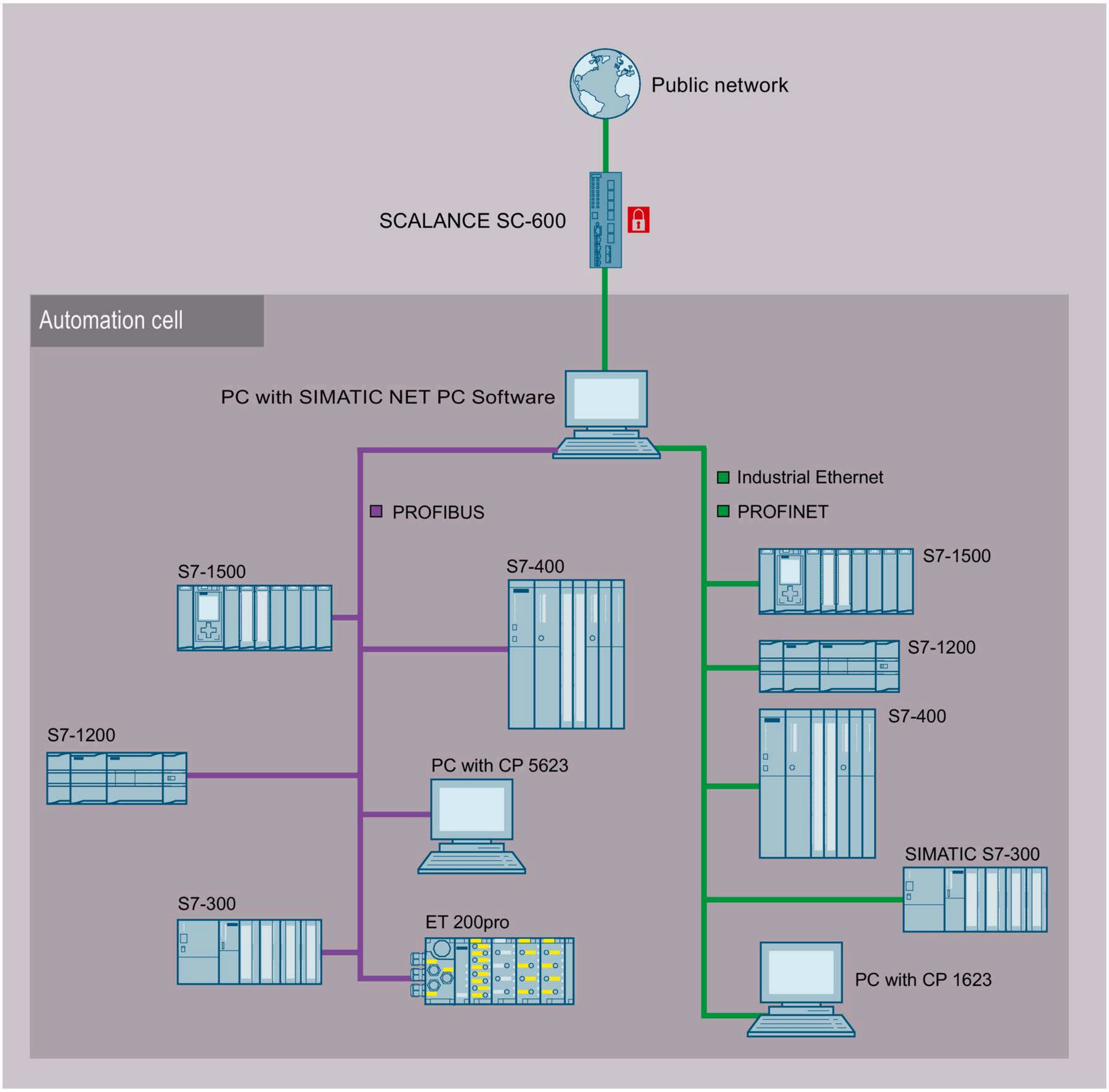


Figure 2-1 Configuration example with security module for a secure operating environment

Installation of the SIMATIC NET PC software products 3

3.1 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.

Notes on installation

Note the following information regarding the installation operation when installing "SIMATIC NET PC Software" products:

- 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.

3.1.1 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 24)".

Upgrade DVD for which versions?

"SIMATIC NET PC software V18" is an upgrade DVD for the following software version:

- "SIMATIC NET PC software V17 SP1"

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

Software licenses

To operate the "SIMATIC NET PC Software" products, exactly one software license per PC or virtual machine and product is required.

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.

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 21H2
Norton Security	• Windows 11 Pro Version 21H2 • Windows 10 Pro Version 21H2
Microsoft Defender	• Windows 11 Enterprise Version 21H2 • Windows 10 Pro Version 21H2 • Windows 10 Enterprise Version 21H2 • Windows Server 2016 • Windows Server 2019 • Windows Server 2022

Restore points

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

3.1.2 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. The "Communication Settings" configuration program can be used for this.

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".

3.2 Released operating systems

NOTICE

Install current security updates

Make sure that the current security updates for the operating system used are always installed.

The "SIMATIC NET PC software V18" DVD can be installed on the following operating systems:

Operating system	Minimum requirements
Windows 11 Enterprise, Pro Version 21H2 (OS Build 22000) Windows 10 Enterprise, Pro Version 21H2 (OS Build 19044) 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)	2.4 GHz PCs with 4 GB RAM, 2 cores
Windows Server 2022 (Standard, Datacenter) Windows Server 2019 (Standard, Datacenter) Windows Server 2016 (Standard, Datacenter)	2.4 GHz PCs with 4 GB RAM, 2 cores

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.

3.3 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. After installation, you will find the documents in subdirectory "%ProgramFiles%\Siemens\SIMATIC.NET\doc".
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).
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...". The "Transfer license key" dialog box then opens.
5. Select the local drive of your PC to which the license keys are to be transferred 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 Software" 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 needed in the destination PC to 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 and define a PSK (PSK = Pre Shared Key) for encrypted communication in the SIMATIC network. Make sure that you enter the same PSK for all communication partners in the SIMATIC network.
2. Select the desired network adapter.

   Note

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

3. If you now want to operate remote configuration, you must also enable OPC COM in the "Communication Settings" configuration program. For more information on this, refer to the online help of the configuration program.

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 55)" on installing optional software components.

"SIMATIC NET PC software" 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" in the section "Security Events (Page 67)".

Installation and configuration with VMware vSphere 4

This section describes the requirements for installation as well as the installation of the "SIMATIC NET PC software" on the "VMware vSphere Hypervisor ESXi 7.0 Update 3" platform. The steps in configuration described in this section relate to the "vSphere Client" configuration program.

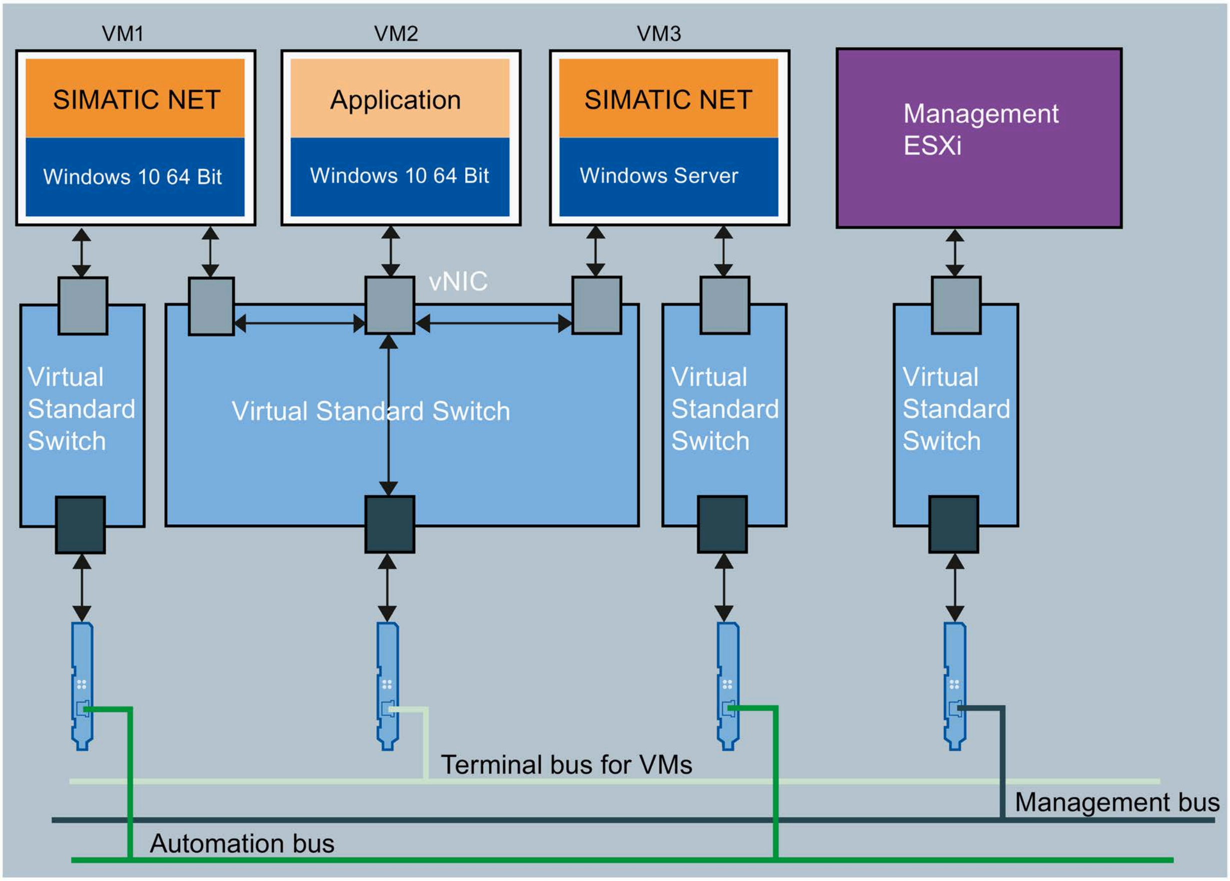
You will find information on "vSphere Client" at the following address: (https://docs.vmware.com/en/VMware-vSphere/index.html)

If you operate SIMATIC NET communication via SOFTNET-IE products, use either a separate virtual standard switch (vSS) or a separate distributed port group of the virtual distributed switch (vDS) for this. For more detailed information on the two specified options, refer to the section "Overview (Page 29)". You can find a description of the configuration options of the virtual switches in the section "Configuration of virtual machines for using SIMATIC NET PC software (Page 37)".

4.1 Overview

Following installation, the 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 33)").

Operation with virtual standard switch



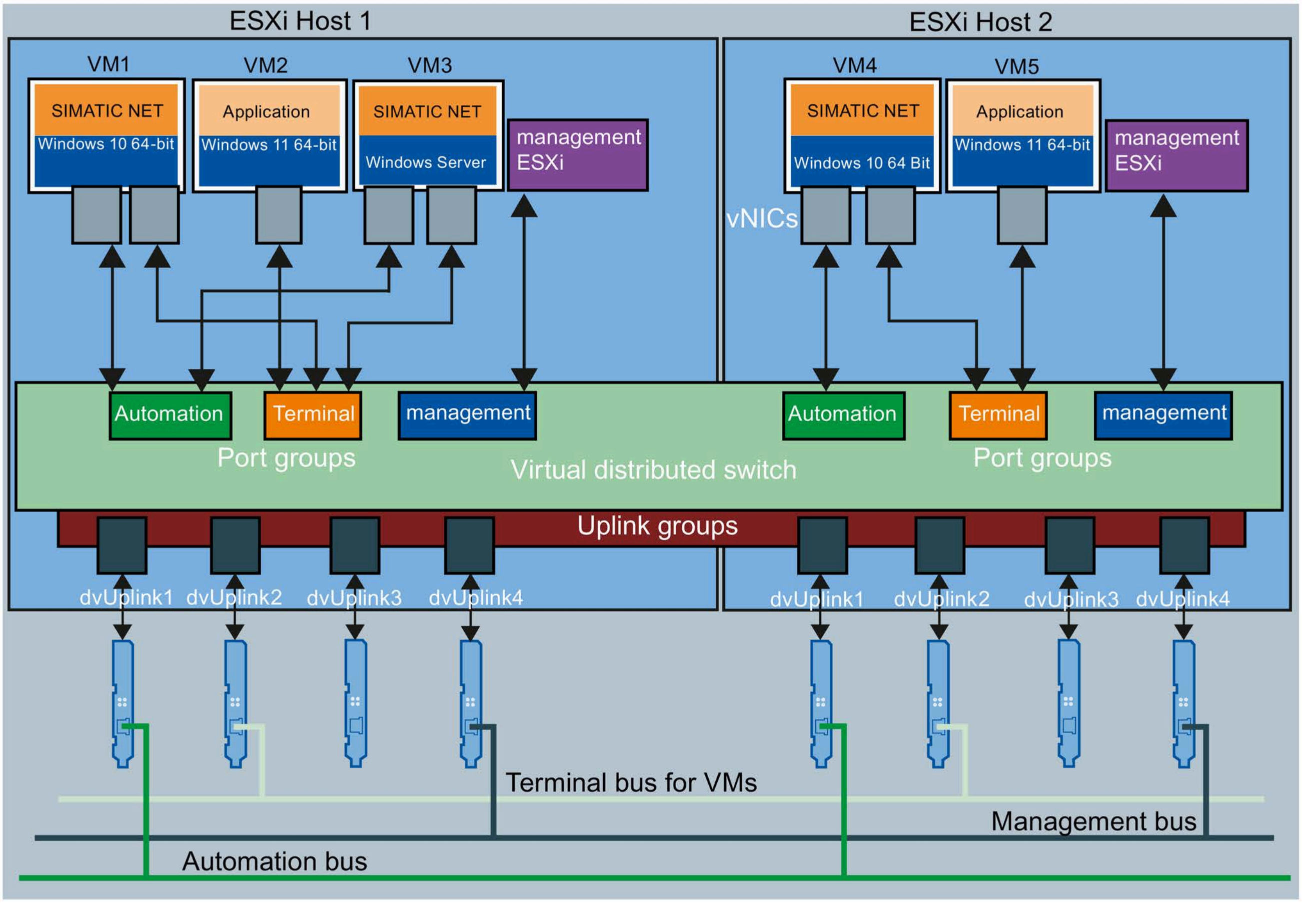
VM1 to VM3	Virtual machine 1 to 3
vNIC	Virtual network adapter

Figure 4-1 Division of the Ethernet networks using virtual standard switches (vSS)

The figure "Division of the Ethernet networks using virtual standard switches (vSS)" shows a suggestion for dividing up the Ethernet networks based on their tasks using virtual standard switches:

- 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".

Operation with virtual distributed switch



VM1 to VM5	Virtual machine 1 to 5
vNICs	Virtual network adapters
dvUplink 1 to 4	distributed virtual Uplink 1 to 4

Figure 4-2 Division of the Ethernet networks using virtual distributed switches (vDS)

The figure "Division of the Ethernet networks using virtual distributed switches (vDS)" shows a suggestion for dividing up the Ethernet networks based on their tasks using a virtual distributed switch:

- With a virtual distributed switch, the configuration of a port group is distributed via all ESXi hosts, so the "Automation" port group on ESXi Host 1 and the "Automation" port group on ESXi Host 2 have shared administration, for example.
- VM1 on Host 1 uses a virtual Ethernet interface (SOFTNET-IE) that is connected to a virtual port of the virtual port group "Automation" for access to the automation network.
- VM2 on Host 1 is only connected to one virtual port of the distributed port group "Terminal" of the virtual distributed switch; it shares a real adapter with the other two virtual machines VM1 and VM3. No "SIMATIC NET PC software" is installed.
- VM3 on Host 1 uses a virtual Ethernet interface (SOFTNET-IE) that is connected to a virtual port of the virtual port group "Automation" for access to the automation network.

- VM4 on Host 2 uses a virtual Ethernet interface (SOFTNET-IE) that is connected to a virtual port of the distributed port group "Automation" for access to the automation network.
- VM5 on Host 2 is only connected to one virtual port of the distributed port group "Terminal" of the virtual distributed switch; it shares a real adapter with the virtual machine VM4. No "SIMATIC NET PC software" is installed.
- The management of the ESXi server also uses its own distributed port group to avoid disruptions (e.g. during backups).
- The terminal bus is intended for the connection of "Remote Desktop Service".

4.2 Requirements and notes

4.2.1 User experience

To install and operate the SIMATIC NET PC software products with "VMware vSphere Hypervisor ESXi 7.0 Update 3/", you require experience of the product "VMware vSphere Hypervisor (https://www.vmware.com/products/vsphere-hypervisor.html)".

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 section "Further Information (Page 65)"

Note

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

4.2.2 Requirements and notes relating to the software

Operation on an ESXi server

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

Released guest operating systems

You will find a list with the guest operating systems compatible with the ESXi servers that are suitable for operation as PC station in the section "Released operating systems (Page 24)".

Notes on licenses

Note

You need to obtain one license for each virtual machine. If, for example, you want to operate 5 virtual machines with the S7 protocol, you need to purchase the product that provides the S7 protocol functionality 5 times. You need to install the "license keys" in the virtual machine in which the functionality will be used, e.g. the S7 protocol.

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

4.2.3 Requirements and notes relating to the hardware

You will find a list of the server hardware compatible with the ESXi servers at the following address: (https://www.vmware.com/resources/compatibility/search.php)

The requirements and restrictions for operation without virtualization also apply.

Minimum requirements of "SIMATIC NET PC software" for a virtual machine:

- 2.4 GHz (2 cores)
- 4 GB RAM, recommendation is 8 GB RAM

Note

With an additional installation of "STEP 7 Professional (TIA Portal)", make sure to observe the requirements described in the associated readme file.

Released hardware

The following hardware components are released for use of the SIMATIC NET PC software V18 under VMware vSphere Hypervisor ESXi 7.0 Update 3:

- CP 5711 communications processor
- Standard Ethernet adapters that are certified for VMware vSphere by VMware
- VMware VMXNET3 network adapter (virtual network adapter)

4.2.4 Restrictions

4.2.4.1 VMware passthrough

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

4.2.4.2 VMware vSphere vMotion

"vMotion" is the term used by VMware for moving virtual machines from one ESXi server to another during operation. The "vMotion" functionality has been released for operation of SOFTNET-IE S7 via the virtual network adapter "VMXNET3". Communication interruptions take place when moving a virtual machine. Take this into account when configuring the monitoring times of the communications protocols.

4.2.4.3 Options for operating the virtual machines

For the "SIMATIC NET PC software", the following operating option is released for the virtual machines:

- Microsoft Remote Desktop connection
- vSphere client

For more information on Remote Desktop and Terminal Services, refer to the readme file.

Note

Operator control restriction

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

It must be ensured that the connection between the remote PC and virtual machine is not interrupted. Otherwise, the virtual machine can only be operated again after a fresh logon of the Remote Desktop client.

When using "Remote Desktop", establish the connection as an administrator to be able to use the full range of functions of the "SIMATIC NET PC software". Calling on the Remote Desktop client takes place with the "mstsc.exe /admin" command.

4.2.4.4 Intel SR-IOV

The "SR-IOV" (Single Root I/O Virtualization) allows several virtual machines to access a PCIe device directly at the same time. The use of the "SR-IOV" functionality has not been released for SIMATIC NET communication.

4.2.4.5 Configuration of the MAC address in STEP 7 projects

The MAC address of a virtual network adapter is assigned automatically by VMware. If the MAC address is changed and the virtual network adapter is part of a STEP 7 configuration, you may need to adjust the STEP 7 configuration.

4.3 Installation of the "SIMATIC NET PC software" in a virtual machine

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

1. Shut down all virtual machines.
2. Make sure that you do not use any modules with pass-through functionality. 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 relevant virtual machine as described in section "Installation of the SIMATIC NET PC software products (Page 21)".
5. Restart the virtual machine.

4.4 Upgrade

4.4.1 SIMATIC NET PC software upgrade process

To upgrade from "SIMATIC NET PC software V17 SP1” to "SIMATIC NET PC software V18", you may need to update the ESXi server to version 7.0 update 3 first.

1. Run the update of "VMware vSphere Hypervisor".
2. Following the ESXi server upgrade, update the virtual machines. To do this, the current VMware Tools must be installed on the virtual machines. The hardware versions supported are listed in the readme file.
3. Then install "SIMATIC NET PC software V18".

4.4.2 VMware vSphere Hypervisor ESXi update process

Follow the steps below to upgrade your ESXi 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, disable the "Passthrough" option for existing modules.
3. Restart the ESXi server.
4. Install the upgrade to "VMware vSphere Hypervisor ESXi 7.0 Update 3".
5. Update the "SIMATIC NET PC software" to version V18.

Configuration of virtual machines for using SIMATIC NET PC software 5

Note

The "vSphere client" configuration program is required to create and manage the virtual machines in connection with the "SIMATIC NET PC software".

5.1 Configuration of the virtual Standard Switch (vSS)

Note

Configuration of a VMkernel port for server management tasks on a virtual standard switch is not released.

To use SIMATIC NET communication via a virtual standard switch, configure the properties of the virtual standard switch and the port groups. To perform the configuration, follow these steps:

Note

Configuration can be specified separately for the virtual standard switch, individual port groups or individual VMkernel ports.

Remember that the settings for the port group/VMkernel port overwrite the configuration on the virtual standard switch and therefore have priority.

1. Open the "vSphere Client" configuration program.
2. Click on the ESXi server on which the virtual standard switches are located in the navigation tree on the left.
3. Navigate via the "Configure > Network > Virtual switches" tab and then click on the virtual standard switch in the list.
4. Click the "Edit" tab for the virtual standard switch in the list to perform its configuration. If you want to configure a port group, right-click on the button with the three dots for the port group and select the "Edit settings" command to perform the configuration of individual port groups.

The settings to be made are described in the section "Configuring the settings (Page 38)".

5.2 Configuration of virtual distributed switch (vDS)

To use SIMATIC NET communication via a virtual distributed switch, configure the properties of the virtual distributed switch and the distributed port groups. To perform the configuration, follow these steps:

Note

Configuration can be specified separately for the virtual distributed switch, individual port groups or individual VMkernel ports, individual ports, individual uplink groups, individual uplinks.

Remember that the settings for the distributed port groups, VMkernel port, ports, uplink groups, uplinks overwrite the configuration on the virtual distributed switch and therefore have priority.

1. Open the "vSphere Client" configuration program.
2. Click on "Network" (globe icon) above the navigation and navigate to the virtual distributed switch.
3. Select the distributed port group for the created network of SIMATIC NET communication.
4. Right-click on the distributed port group and select the "Edit settings..." command.

The settings to be made are described in the section "Configuring the settings (Page 38)".

5.3 Configuring the settings

5.3.1 General/properties

The name of a port group is the name of the network connection that can be selected in the "Properties of virtual machines". There are the following ways to change the name of the port group of a virtual switch:

- Virtual standard switch: On the "Properties" page, change the name of the port group under "Network name".
- Virtual distributed switch: On the "General" page, change the name of the distributed port group under "Name".

5.3.2 Extended

On the "Extended" page (only for virtual distributed switch > distributed port group), do not make any changes and retain the default settings.

5.3.3 VLAN

Note

To use VLANs, you require prior knowledge of VLAN configuration under ESXi. You will find more information at the following address: (https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.networking.doc/GUID-7225A28C-DAAB-4E90-AE8C-795A755FBE27.html)

The "vSphere" configuration program supports the following three modes of VLAN tagging in the ESXi server:

- External Switch Tagging (EST)
- Virtual Switch Tagging (VST)
- Virtual Guest Tagging (VGT)

All three modes of VLAN tagging are released for SIMATIC NET communication.

To configure VLANs in a port group of a virtual standard switch, navigate to the "VLAN ID" parameter on the "Properties" page. The following configuration options are available:

- External Switch Tagging: Enter the value 0 in the input box.
- Virtual Switch Tagging: Enter a value of between 1 and 4094 in the input box.
- Virtual Guest Tagging: Enter the value 4095 in the input box.

To configure VLANs in a distributed port group of a virtual distributed switch, use the drop-down list on the "VLAN" page. The VLAN type corresponds to the VLAN tagging mode of the port group. The following configuration options are available:

- External Switch Tagging: Select the value "None" in the drop-down list. The real switch performs VLAN tagging.
- Virtual Switch Tagging: For the "VLAN ID", enter a number between 1 and 4094. The VLAN ID is the ID for the network segment for SIMATIC NET communication. The virtual switch identifies the data traffic with the entered tag.
- Virtual Guest Tagging: Enter a VLAN trunk area under "VLAN trunking". Note that SIMATIC NET communication is also configured within the VLAN trunk area. VLANs are realized by virtual machines. The virtual switch enables data traffic via each possible VLAN.

Note

For "Virtual Guest Tagging", only virtual network adapters of the type "VMNETX 3" are released for communication via SOFTNET-IE products.

5.3.4 Security

On the "Security" page, do not make any changes and retain the default settings. The following default settings are relevant:

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

5.3.5 Traffic Shaping

On the "Traffic Shaping" page, central and distributed restrictions of the usable bandwidth can be set. The "Traffic Shaping" functionality has not been released for the "SIMATIC NET PC software". The default setting "Disabled" must be retained for "Traffic Shaping".

5.3.6 Teaming and Failover

The settings for load balancing and failover configuration can be made in the "NIC Grouping" tab on the "Teaming and Failover" page. 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:

- Assignment type: "VMware-OUI-assignment"
- VMware-OUI: for example "00:50:56" :xx:xx:xx

5.3.7 Monitoring

On the "Monitoring" page (only for virtual distributed switch > distributed port group), do not make any changes and retain the default settings.

5.3.8 Other

On the "Other" page (only for virtual distributed switch > distributed port group), do not make any changes and retain the default settings.

5.4 Configuration of the virtual machine

5.4.1 Hardware

To configure the virtual machine, follow these steps:

1. Open the "vSphere Client" configuration program.
2. Click on the virtual machine in the navigation tree on the left.
3. Right-click on the virtual machine and select the "Edit settings..." command to be able to edit its settings.
4. Click on "Work memory" on the left and configure it to at least 4 GB for 64-bit systems. For better performance, Siemens recommends 8 GB for the "Work memory" of the virtual machine.
5. Select "CPUs" on the left and set the value 1 for the "Number of virtual sockets" and at least 2 for the "Number of cores per socket".
6. Make sure that you make the following default settings:
   – For CPU hot plug: "Enable CPU Hot Add" option is disabled
   – For work memory: "Activate" option is disabled

Using a CP 5711 in a virtual machine

Note that when installing a CP 5711, the virtual USB controller must already be installed in the virtual machine before you can assign the CP 5711 with the virtual machine turned off. The CP 5711 has not been released for use with vMotion.

5.4.1.1 Adding network adapters to the virtual machine

Note

1:1 assignment between network adapter and virtual machine recommended

For optimum performance, assign a separate physical network adapter to the virtual machine which uses the SOFTNET-IE communication of the "SIMATIC NET PC software".

SIMATIC NET communication has been released only for the "VMXNET 3" network adapter. The setting of the MAC address for SIMATIC NET communication must remain set to "Default (automatic)". When adding an Ethernet network adapter, you need to select the corresponding network via the name of the port groups, see section "Configuration of the virtual Standard Switch (vSS) (Page 37)" and "Configuration of virtual distributed switch (vDS) (Page 38)".

5.4.2 Options

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

Start options

In "Start options", the "EFI" value must remain set for the "Firmware" parameter.

As of Windows 11, the "Secure Boot" option must be enabled in addition in "Start options".

5.4.3 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.

Installation and configuration in Microsoft Hyper-V

6

This section describes the requirements for installation as well as the installation of the "SIMATIC NET PC software" on the "Microsoft Hyper-V" platform in the operating systems released for the "SIMATIC NET PC software", see section "Released operating systems (Page 24)".

6.1 Requirements and notes

6.1.1 User experience

To install and operate the SIMATIC NET PC software products with "Microsoft Hyper-V" you require experience of the host operating system and "Microsoft Hyper-V" (https://docs.microsoft.com/en-us/virtualization/hyper-v-on-windows/).

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"

Note

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

6.1.2 Requirements and notes relating to the software

Operation with Hyper-V

The "SIMATIC NET PC software" is suitable for operation on virtual machines (VMs) with the following SOFTNET-IE S7 products in Hyper-V.

- SOFTNET-IE S7 (Lean, Extended)
- SOFTNET-IE S7 REDCONNECT

To operate virtual machines, Hyper-V must be activated on the host operating system. To do this, the role "Hyper-V" must be added in Windows Server operating systems or the option "Hyper-V" must be enabled in Windows 10 and Windows 11. The "SIMATIC NET PC software" can be installed and used on the host operating system as well as on the guest operating system. Note the specific product and module releases in the following sections.

Released guest operating systems

You will find a list with the guest operating systems compatible with the "Hyper-V" and that are suitable for operation as PC station in the section "Released operating systems (Page 24)".

NOTICE

Use of PROFIBUS in virtual machines

Due to the lack of USB support of the guest operating systems, PROFIBUS cannot be used directly in Hyper-V. With routing, however, a CP 5711 (with the field PG CP 5711 Onboard) connected to the host can be used. You can find more information at the following address: (https://support.industry.siemens.com/cs/ww/en/view/100450795)

Note

Notes on licenses

You need to obtain one license for each virtual machine. If, for example, you want to operate 5 virtual machines with the S7 protocol, you need to purchase the product that provides the "S7 protocol" functionality 5 times. You need to install the "license keys" in the virtual machine in which the functionality will be used, e.g. the S7 protocol.

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

Enabling "Hyper-V" functionality

To enable "Hyper-V" on your PC under Windows, follow these steps:

1. Right-click on the Windows button and select "Apps and Features".
2. Select the "Programs and Features" option on the right-hand side under "Related settings".
3. Select "Turn Windows features on or off".
4. Select "Hyper-V" and click "OK".
5. Restart the PC.

6.1.3 Requirements and notes relating to the hardware

Compatible server hardware must be used for the host system. You can find more information at the following address: (https://docs.microsoft.com/en-us/windows-server/virtualization/hyper-v/system-requirements-for-hyper-v-on-windows)

The requirements and restrictions for operation without virtualization also apply.

Minimum requirements of SIMATIC NET for a virtual machine:

- 2.4 GHz (2 cores)
- 4 GB RAM, recommendation is 8 GB RAM

Note

With an additional installation of "STEP 7 Professional (TIA Portal)", make sure to observe the requirements described in the associated readme file.

6.1.4 Notes and restrictions

6.1.4.1 Microsoft "Live migration"

"Live migration" is the term used by Microsoft for moving virtual machines from one server to another during operation. The "Live migration" functionality is not supported by "SIMATIC NET PC software".

6.1.4.2 Options for operating the virtual machines

For the "SIMATIC NET PC software", the following operating option is released for the virtual machines:

- Microsoft Remote Desktop connection

For more information on Remote Desktop and Terminal Services, refer to the readme file.

Note

Operator control restriction

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

It must be ensured that the connection between the remote PC and virtual machine is not interrupted. Otherwise, the virtual machine can only be operated again after a fresh logon of the Remote Desktop client.

When using "Remote Desktop", establish the connection as an administrator to be able to use the full range of functions of the "SIMATIC NET PC software". Calling on the Remote Desktop client takes place with the "mstsc.exe /admin" command.

6.1.4.3 "Intel SR-IOV"

The "SR-IOV" (Single Root I/O Virtualization) allows several virtual machines to access a PCIe device directly at the same time. The use of the "SR-IOV" functionality has not been released for SIMATIC NET communication.

6.1.4.4 Configuration of the MAC address in STEP 7 projects

The MAC address of a virtual network adapter is assigned automatically by Hyper-V. If the MAC address is changed and the virtual network adapter is part of a STEP 7 configuration, you may need to adjust the STEP 7 configuration.

6.1.4.5 VLAN

The "VLAN" functionality is not supported. The configuration of the "VLAN ID" parameter has not been released for SIMATIC NET communication.

6.2 Installation of the "SIMATIC NET PC Software" in a virtual machine

Install the "SIMATIC NET PC software" in the relevant virtual machine as described in section "Installation of the SIMATIC NET PC software products (Page 21)".

6.3 Configuration of the guest and host operating systems

The "SIMATIC NET PC software" can also be installed on the host operating system. In contrast to the guest operating systems of "Hyper-V", all SIMATIC NET PC modules can be used here.

Note

Use of general Ethernet modules

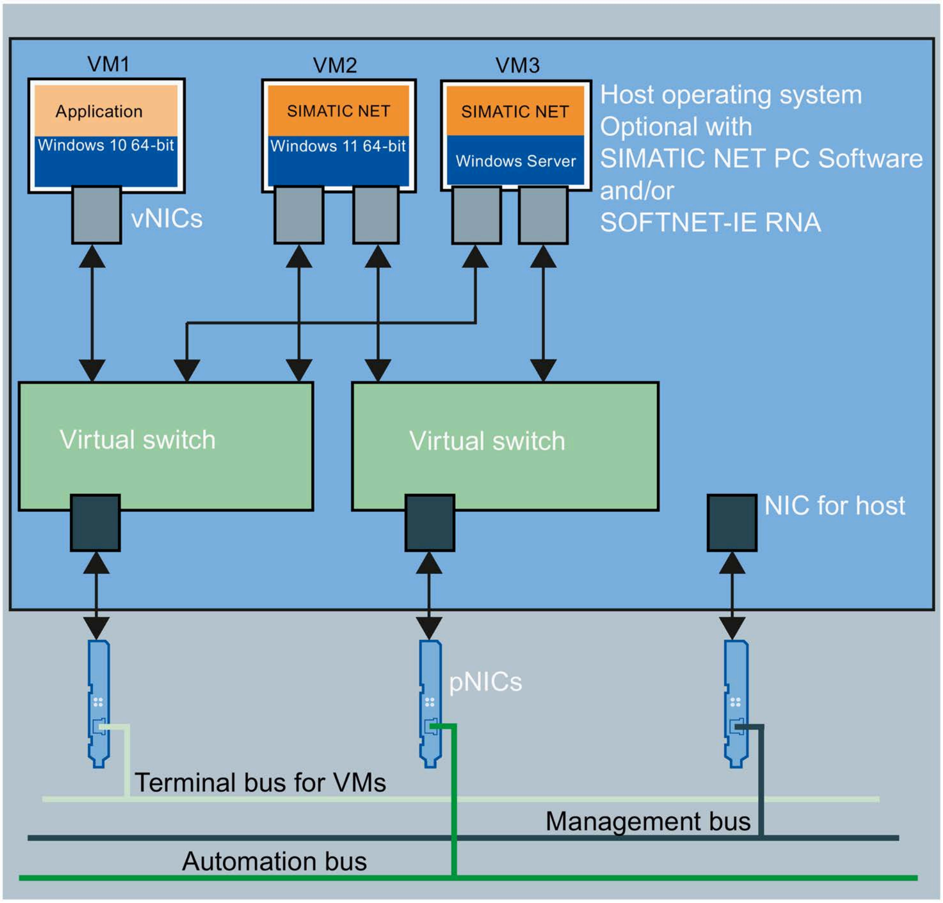
The "IE general" Ethernet modules are a special case, however. These can be assigned to a virtual switch. A change of the Ethernet modules used by "SIMATIC NET PC Software" is only permitted in offline mode. If a change needs to be made to the configuration, take the "IE general" Ethernet module out of the configured operation. You then need to end all applications of the "SIMATIC NET PC software" or the OPC server and restart the PC.

6.3.1 Example configuration of the guest and host operating systems

SIMATIC NET communication via guest operating systems is only possible using virtual Ethernet network cards.

To be able to use physical Ethernet network adapters on the physical PC, you need to install the "SIMATIC NET PC software" on the host operating system.

The following figure shows an example of the configuration of multiple guest operating systems by means of virtual switches on communication networks, as is commonly found in the industrial environment.



VM1 to VM3	Virtual machines 1 to 3
vNICs	Virtual network adapters
pNICs	Physical network adapters
NIC	Used by the host

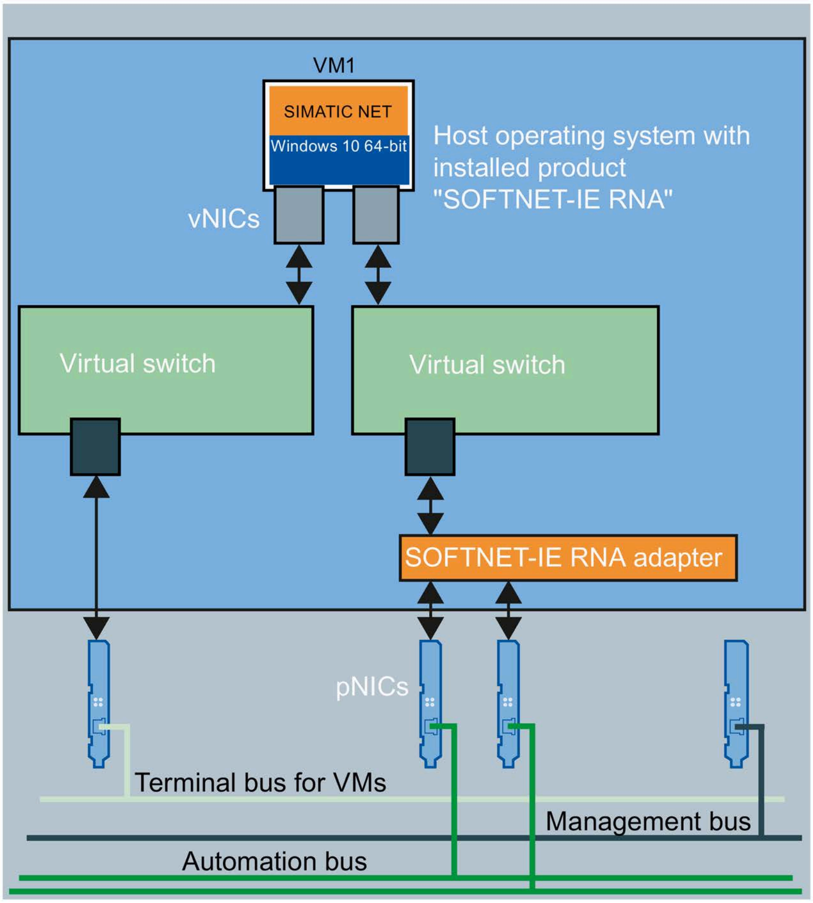
Figure 6-1 Configuration with "SIMATIC NET PC Software"

- VM1 is only connected to one virtual network adapter on a separate virtual switch. It shares a physical network adapter with the other two virtual machines.
- VM2 uses a virtual Ethernet interface (SOFTNET-IE) with a separate virtual switch to the automation network.
- VM3 also uses a virtual Ethernet interface (SOFTNET-IE) with the same virtual switch to the automation network. Make sure that the maximum bandwidth of the physical network adapter is not exceeded.

- Communication with the host operating system takes place via the management bus, through which the connection to virtual machines is established via "VMConnect", for example. A backup of virtual machines or the host operating system must also be via this network connection.
- The terminal bus is intended for the connection via "Remote Desktop Service".

6.3.2 Configuration of the host operating system with "SOFTNET-IE RNA"

The use of "SOFTNET-IE RNA" on guest operating systems is not possible. To use "SOFTNET-IE RNA", install "SOFTNET-IE RNA" on the host operating system and configure the SOFTNET-IE RNA network with the intended physical network adapters. You need 1 "SOFTNET-IE RNA" license for this configuration. When operating several virtual machines on a SOFTNET-IE RNA network, make sure that the bandwidth of the physical network is not exceeded. If necessary, define the network bandwidth at the associated virtual network adapter of the virtual machine.



VM1	Virtual machine 1
vNIC	Virtual network adapter
pNIC	Physical network adapter

Figure 6-2 Configuration with "SOFTNET-IE RNA"

7 Configuration of Hyper-V and virtual machines for use of SIMATIC NET PC software

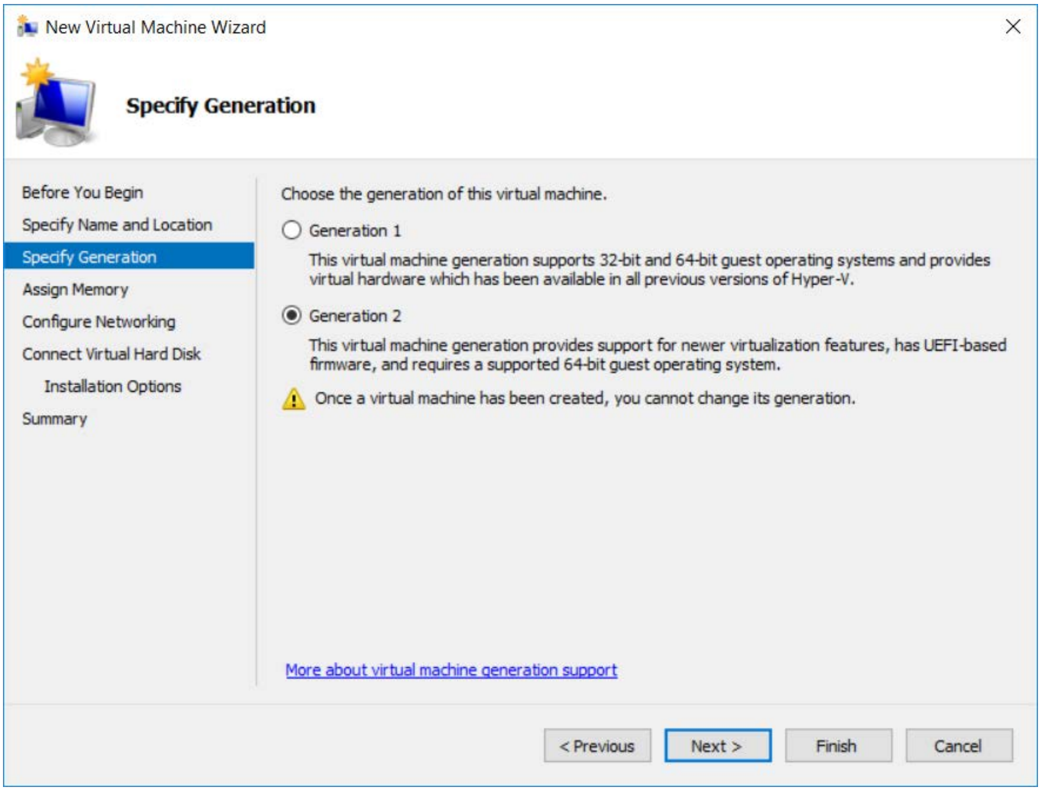
7.1 Configuration of a new virtual machine

This section describes the configuration of your Hyper-V environment for operation with the "SIMATIC NET PC software". Microsoft makes the following two options for selecting the virtual machine available for the configuration:

- Generation 1 - The option "Generation 1" is not released for the SIMATIC NET communication.
- Generation 2

To set up the new virtual machine, follow these steps:

1. Start the "Hyper-V Manager" program via "Windows button > Windows Administrative Tools > Hyper-V Manager" and confirm the prompt with "Yes".
2. In the "Hyper-V Manager", click "Action > New > Virtual computer" to show the wizard for new virtual computers.
3. If needed, enable the option "Generation 2" under "Specify Generation".
4. Before installing the guest operating system, assign adequate main memory and CPU resources to the virtual machine according to your intended use.



Choose the generation of this virtual machine.

○ Generation 1

This virtual machine generation supports 32-bit and 64-bit guest operating systems and provides virtual hardware which has been available in all previous versions of Hyper-V.

● Generation 2

This virtual machine generation provides support for newer virtualization features, has UEFI-based firmware, and requires a supported 64-bit guest operating system.

⚠ Once a virtual machine has been created, you cannot change its generation.

Figure 7-1 Selecting Generation 2

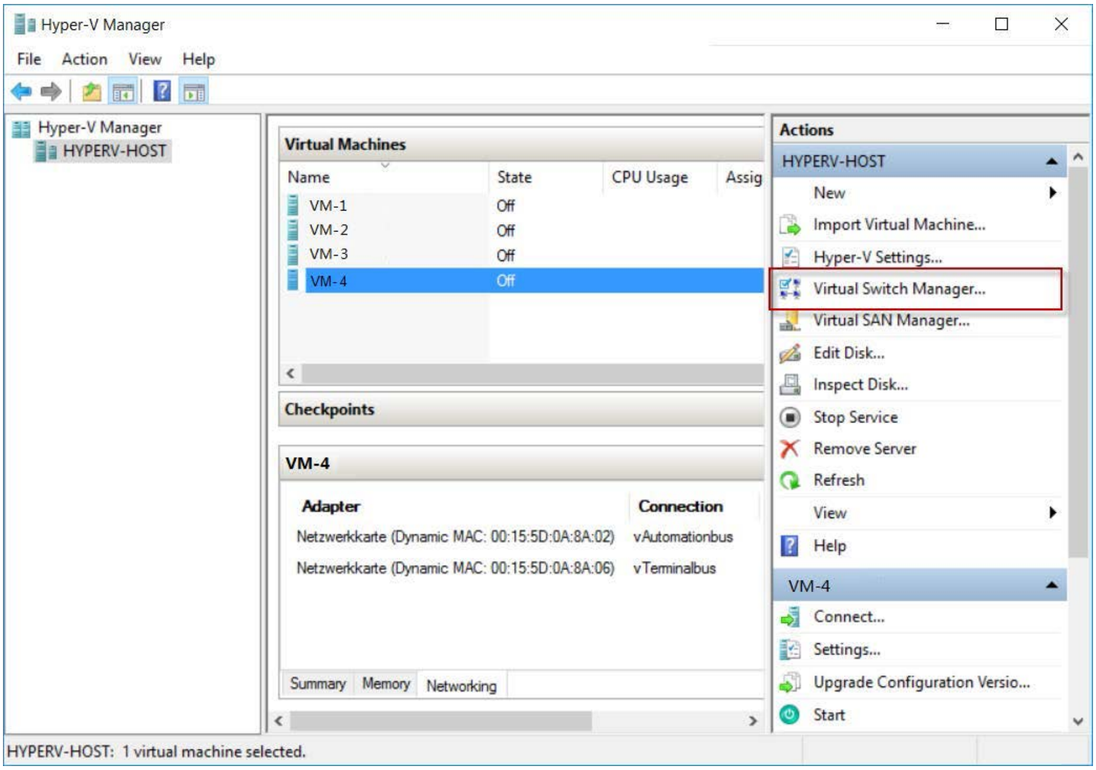
7.2 Configuration of the virtual switch

Note

End all applications of the "SIMATIC NET PC software" before you make configuration changes for the virtual switch.

To configure the virtual switch, follow these steps:

1. Start the "Hyper-V Manager" program via "Windows button > Windows Administrative Tools > Hyper-V Manager" and confirm the prompt with "Yes".
2. Select the corresponding Hyper-V host in the tree topology on the left.
3. Navigate to "Actions" on the right-hand side and call the command "Manager for virtual switches...".



Name	State	CPU Usage	Assig
VM-1	Off		
VM-2	Off		
VM-3	Off		
VM-4	Off		

Adapter	Connection
Netzwerkkarte (Dynamic MAC: 00:15:5D:0A:8A:02)	vAutomationbus
Netzwerkkarte (Dynamic MAC: 00:15:5D:0A:8A:06)	vTerminalbus

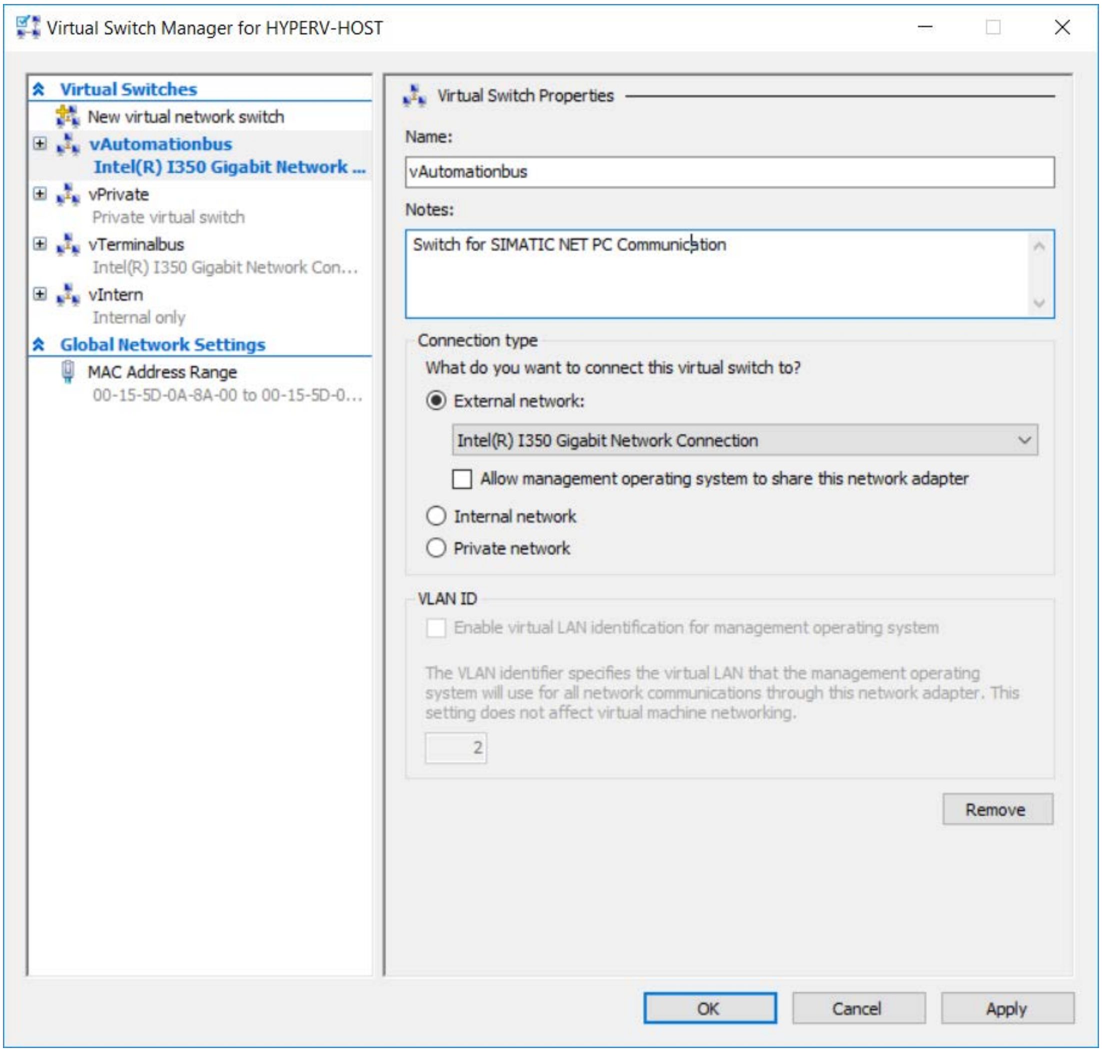
HYPERV-HOST: 1 virtual machine selected.

Figure 7-2 Hyper-V Manager

4. Click the command "Virtual switches > New virtual network switch" if you want to create and configure additional virtual switches.
5. Assign the virtual switch for the automation bus directly to a physical Ethernet network adapter.

Note

The option "Allow management operating system to share this network adapter" is not absolutely necessary for the terminal bus.



Virtual Switch Manager for HYPERV-HOST

Virtual Switches
- New virtual network switch
- vAutomationbus — Intel(R) I350 Gigabit Network ...
- vPrivate — Private virtual switch
- vTerminalbus — Intel(R) I350 Gigabit Network Con...
- vIntern — Internal only

Global Network Settings
- MAC Address Range — 00-15-5D-0A-8A-00 to 00-15-5D-0...

Virtual Switch Properties

Name: vAutomationbus

Notes: Switch for SIMATIC NET PC Communication

Connection type

What do you want to connect this virtual switch to?

● External network: Intel(R) I350 Gigabit Network Connection

□ Allow management operating system to share this network adapter

○ Internal network

○ Private network

VLAN ID

□ Enable virtual LAN identification for management operating system

The VLAN identifier specifies the virtual LAN that the management operating system will use for all network communications through this network adapter. This setting does not affect virtual machine networking.

2

Figure 7-3 Configuring properties of the virtual switch

7.3 Configuration of the virtual machine

Note

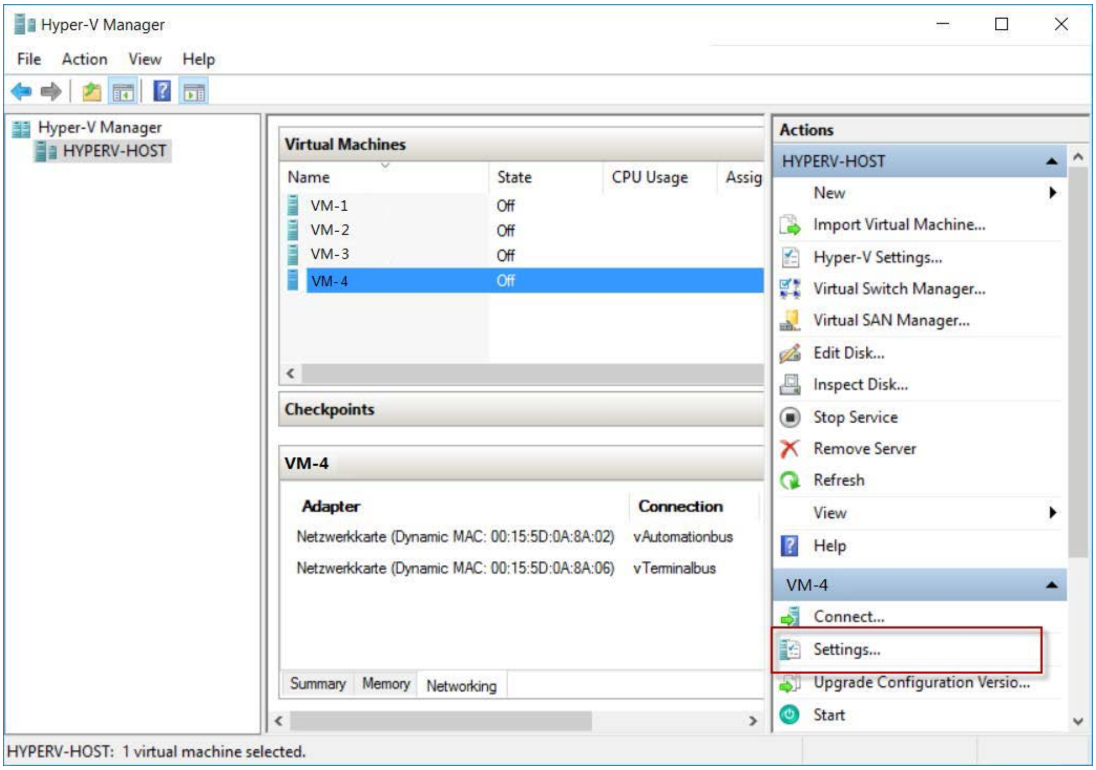
The configuration of the virtual machine by the integrated wizard is not adequate to operate the "SIMATIC NET PC Software". Changes are necessary.

Note

With an additional installation of "STEP 7 Professional (TIA Portal)", make sure to observe the requirements described in the associated readme file.

To configure the virtual machine, follow these steps:

1. Start the "Hyper-V Manager" program via "Windows button > Windows Administrative Tools > Hyper-V Manager" and confirm the prompt with "Yes".
2. Select the corresponding Hyper-V host in the tree topology on the left.
3. In the middle at "Virtual computers", select the virtual machine that you wish to configure.
4. On the right-hand side, navigate to the corresponding virtual machine and call the command "Settings...".



Name	State	CPU Usage	Assig
VM-1	Off		
VM-2	Off		
VM-3	Off		
VM-4	Off		

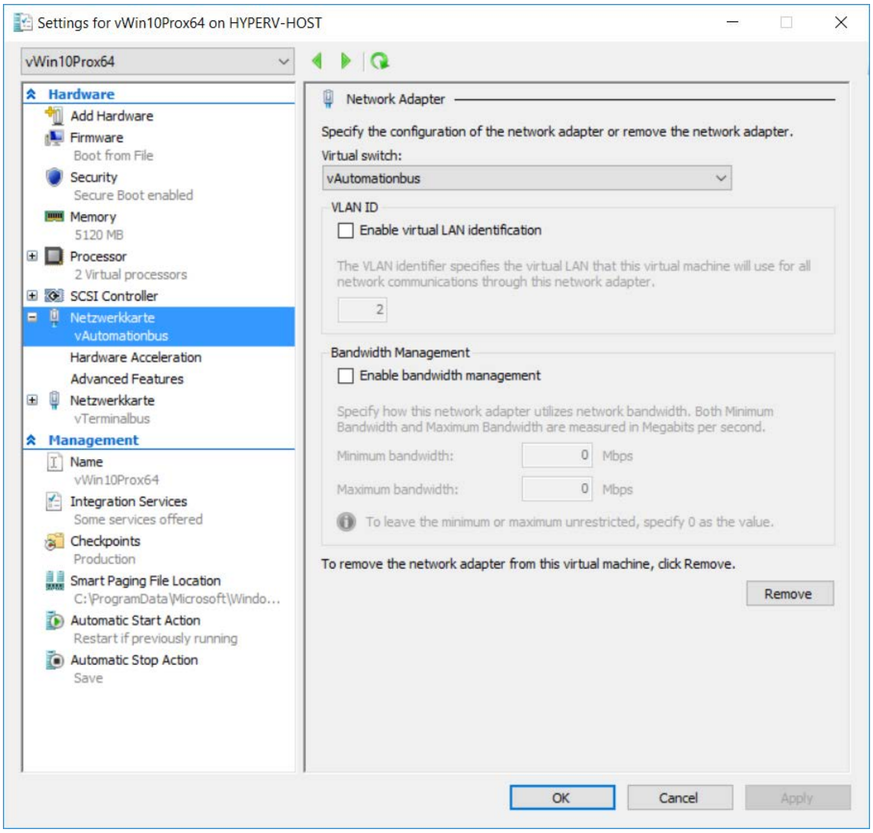
Adapter	Connection
Netzwerkkarte (Dynamic MAC: 00:15:5D:0A:8A:02)	vAutomationbus
Netzwerkkarte (Dynamic MAC: 00:15:5D:0A:8A:06)	vTerminalbus

HYPERV-HOST: 1 virtual machine selected.

Figure 7-4 Hyper-V Manager

5. On the left-hand side, click "Security" and enable the "Trusted Platform Module" there if you want to install Windows 11 or Windows Server 2022 on the virtual machine.

6. Click on "Processor" on the left-hand side and increase the number of cores to at least 2.
7. Click on "Work memory" on the left and configure it to at least 4 GB for 64-bit systems. For better performance, Siemens recommends 8 GB for the "Work memory" of the virtual machine.
8. Click the "Add hardware" command on the left if you want to add new network adapters to virtual machines and configure them.



Settings for vWin10Prox64 on HYPERV-HOST

vWin10Prox64

Hardware
- Add Hardware
- Firmware – Boot from File
- Security – Secure Boot enabled
- Memory – 5120 MB
- Processor – 2 Virtual processors
- SCSI Controller
- Netzwerkkarte – vAutomationbus
  - Hardware Acceleration
  - Advanced Features
- Netzwerkkarte – vTerminalbus

Management
- Name – vWin10Prox64
- Integration Services – Some services offered
- Checkpoints – Production
- Smart Paging File Location – C:\ProgramData\Microsoft\Windo...
- Automatic Start Action – Restart if previously running
- Automatic Stop Action – Save

Network Adapter

Specify the configuration of the network adapter or remove the network adapter.

Virtual switch: vAutomationbus

VLAN ID

□ Enable virtual LAN identification

The VLAN identifier specifies the virtual LAN that this virtual machine will use for all network communications through this network adapter.

2

Bandwidth Management

□ Enable bandwidth management

Specify how this network adapter utilizes network bandwidth. Both Minimum Bandwidth and Maximum Bandwidth are measured in Megabits per second.

Minimum bandwidth: 0 Mbps

Maximum bandwidth: 0 Mbps

To leave the minimum or maximum unrestricted, specify 0 as the value.

To remove the network adapter from this virtual machine, click Remove.

Figure 7-5 Properties of network adapters for virtual machines

9. Note the following when you make settings on the network adapters:
   - If several virtual machines are intended to access a physical network adapter, the bandwidth management needs to be set so that the maximum bandwidth of the physical network adapter cannot be exceeded.
   - Settings such as DHCP guards and router guards can interrupt the communication. Check the settings under "Setting > Network adapter > Extended features". These settings are disabled by default. Do not change these settings.
   - The setting "Network adapter > Extended features > Protected network" brings about an automatic "Live migration" if the network is interrupted. This happens as well if this parameter is enabled for any network adapter of the virtual machine. The "Live migration" functionality also causes a brief interruption of the network connection. Disable the "Live migration" functionality.

SNMP service, SNMP OPC MIB compiler and profile files 8

8.1 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 exited with the "Exit OPC Server" command in the "Communication Settings" configuration program 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 in Windows 10

Install the SNMP service as described below:

1. Navigate to "Start > Settings > Apps > Optional features > Add a feature".
2. In the "Windows Features" list, click "Install" for "Simple Network Management Protocol (SNMP)". The SNMP service starts automatically after a system restart.

Note

Exit OPC server

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

For security reasons, exit the OPC server using the "Exit OPC server" command in the "Communication Settings" configuration program. It is restarted automatically following a new request.

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. Navigate in the settings to "Apps" > "Optional features" and click the "View features" button of "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 exited.

For security reasons, exit the OPC server using the "Exit OPC server" command in the "Communication Settings" configuration program. It is restarted automatically following a new request.

Procedure in Windows Server 2016

Add the "SNMP service" feature for the local server. The SNMP service starts automatically after a system restart.

Note

Exit OPC server

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

For security reasons, exit the OPC server using the "Exit OPC server" command in the "Communication Settings" configuration program. It is restarted automatically following a new request.

Procedure in Windows Server 2019 and Windows Server 2022

Install the SNMP service as described below:

1. Navigate to "Start > Server Manager > Add Roles and Features > Select installation type > Select target server > Select server roles > Select features > Select SNMP service > Add features".
2. Click the "Install" button to install the feature. The SNMP service starts automatically after a system restart.

Note

Exit OPC server

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

For security reasons, exit the OPC server using the "Exit OPC server" command in the "Communication Settings" configuration program. It is restarted automatically following a new request.

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 information in manual "Commissioning PC Stations".

8.2 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 9

Note

Once "SIMATIC NET PC Software" products have been installed, any communications processor installed in the PC is no longer ready for operation because the associated device driver has also been 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". SOFTNET modules can also be operated with other SIMATIC products (e.g. STEP 7).

The SIMATIC NET PC products are uninstalled via "Programs and Features" and "Uninstall programs" in "Control Panel". 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 10

10.1 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.

10.2 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.

10.3 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++ 2015-2022 Redistributable (x64)" is already installed on the destination PC, for example, the corresponding package in the control file is considered to be unnecessary:

```
[VCREDIST2015X64]

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 meaning:

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 11

11.1 Documentation guide

Readme file for "SIMATIC NET PC Software" products

All important information on the "SIMATIC NET PC Software" products as well as additional information on configuration and operation is described in the Readme files for the overall product (main directory of the product DVDs).

Quick start for "SIMATIC NET PC Software" 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 as needed with Acrobat Reader.

"Communication Settings" configuration program

Here, you will find information on various topics such as procedures for planning and configuring connections.
(menu command "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)

11.2 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

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 records[1] in an event log file[2,3]. A consumer (e.g. a Security Information Event Management (SIEM) system) can subscribe to these Security Events for further processing[4].

[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.	OPC UA S7
{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.	(CN=UaExpert@TESTPC,
		O=Siemens,
		OU=DI PA DCP,
		C=DE)

{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:\temp\app.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)	V18.00.01.01
{Kind of certificate}	String (without spaces) that specifies the type of certificate.	One of the values: server | client | user

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:\temp\app.exe).
Explanation	Integrity verification of the software failed.
Severity	Error
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 3.4

A.1.7 User identification and authentication

Message text	{Protocol}: User {User name} logged in from {IP address} to session {Session id}.
Example	OPC UA S7: User PeterMaier logged in from ::ffff:127.0.0.1 to session {94c1c983-2573-4d70-adfa-a0c100012840}.
Explanation	Valid login information that is specified during login.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.1

Message text	{Protocol}: User {User name} failed to log in from {IP address} to session {Session id}.
Example	OPC UA S7: User PeterMaier failed to log in from ::ffff:127.0.0.1 to session {9ca0bd6a-cc86-42bb-bcab-802dbb40034d}.
Explanation	Incorrect user name or password specified during login.
Severity	Error
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.1

Message text	{Protocol}: User {User name} logged out from session {Session id}.
Example	OPC UA S7: User PeterMaier logged out from session {94c1c983-2573-4d70-adfa-a0c100012840}.
Explanation	User session ended - logged out.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.1

Message text	{Protocol}: Default user {User name} logged in from {IP address} to session {Session id}.
Example	OPC UA S7: Default user PeterMaier logged in from ::ffff:127.0.0.1 to session {94c1c983-2573-4d70-adfa-a0c100012840}.
Explanation	The default user is logged in via the IP address.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.1

Message text	{Protocol}: User {Subject} logged in from {IP address} to session {Session id}.
Example	OPC UA S7: User (CN=UaExpert@TESTPC, O=Siemens, OU=DI PA DCP, C=DE) logged in from ::ffff:127.0.0.1 to session {94c1c983-2573-4d70-adfa-a0c100012840}.
Explanation	Valid login information that is specified during login.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.1

Message text	{Protocol}: User {Subject} failed to log in from {IP address} to session {Session id}.
Example	OPC UA S7: User (CN=UaExpert@TESTPC, O=Siemens, OU=DI PA DCP, C=DE) failed to log in from ::ffff:127.0.0.1 to session {9ca0bd6a-cc86-42bb-bcab-802dbb40034d}.
Explanation	Incorrect or invalid user certificate specified on login.
Severity	Error
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.1

Message text	{Protocol}: User {Subject} logged out from session {Session id}.
Example	OPC UA S7: User (CN=UaExpert@TESTPC, O=Siemens, OU=DI PA DCP, C=DE) logged out from session {94c1c983-2573-4d70-adfa-a0c100012840}.
Explanation	User session ended - logged out.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.1

A.1.8 Unsuccessful login attempts

Message text	{Protocol}: User account {User name} for application {Client} is locked for {Time seconds} seconds after {Failed login count} unsuccessful login attempts.
Example	OPC UA S7: User account PeterMaier for application urn:TEST-PC:UnifiedAutomation:UaExpert is locked for 1800 seconds after 12 unsuccessful login attempts.
Explanation	If there were too many failed logins, the corresponding user account was locked for a specific period of time.
Severity	Warning
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.11

Message text	{Protocol}: {IP address} is locked for {Time seconds} seconds after {Failed login count} unsuccessful login attempts.
Example	OPC UA S7: ::ffff:127.0.0.1 is locked for 1800 seconds after 3 unsuccessful login attempts.
Explanation	If there were too many failed logins, the corresponding IP address was locked for a specific period of time.
Severity	Warning
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.11

A.1.9 Device identification and authentication

Message text	{Protocol}: Secure channel from subject {Subject} with message security mode {Security mode} and security policy {Security policy} successfully established.
Example	OPC UA S7: Secure channel from subject (CN=UaExpert@TESTPC, O=Siemens, OU=DI PA DCP, C=DE) with message security mode SignAndEncrypt and security policy Aes128_Sha256_RsaOaep successfully established.
Explanation	Client authentication was successful.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.2

Message text	{Protocol}: Secure channel from subject {Subject} with message security mode {Security mode} and security policy {Security policy} failed.
Example	OPC UA S7: Secure channel from subject (CN=UaExpert@TESTPC, O=Siemens, OU=DI PA DCP, C=DE) with message security mode SignAndEncrypt and security policy Aes128_Sha256_RsaOaep failed.
Explanation	Client authentication failed.
Severity	Error
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.2

Message text	{Protocol}: Connection to device {IP Address} subject {Subject} failed.
Example	S7 optimized: Connection to device 192.168.1.105 subject (CN=PLC-1/Communication-1, O=Siemens, OU=, C=DE) failed.
Explanation	Server authentication failed.
Severity	Error
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.2

A.1.10 Controlling simultaneous sessions

Message text	{Protocol}: The maximum number of {Max sessions} concurrent login sessions exceeded.
Example	OPC UA S7: The maximum number of 200 concurrent login sessions exceeded.
Explanation	The maximum number of parallel sessions has been exceeded.
Severity	Warning
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 2.7

A.1.11 Restoring the automation system

Message text	User {User name} installed SIMATIC NET PC Software {Version}.
Example	User PeterMaier installed SIMATIC NET PC Software V18.00.00.00.
Explanation	The user has successfully installed the software.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 7.4

A.1.12 Network and IT security settings

Message text	{Protocol}: Configuration of certificates changed ({Kind of certificate}).
Example	OPC UA S7: Configuration of certificates changed (client).
Explanation	The configuration of the trusted certificates has been changed. This can affect server, client and user certificates. Certificates of certificate publishers or their recall lists may have been changed.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 7.6