

SIMATIC

Process Control System PCS 7 Compendium Part F - Industrial Security (V9.1)

Configuration Manual

<u>Security information</u>	1
<u>Preface</u>	2
<u>What's new?</u>	3
<u>Security strategies</u>	4
<u>Network security</u>	5
<u>System hardening</u>	6
<u>User Administration and Operator Permissions</u>	7
<u>Patch management</u>	8
<u>Protection against malware using virus scanners</u>	9
<u>Backing up and restoring data</u>	10
<u>Disposal of systems and components</u>	11
<u>Remote access</u>	12
<u>Definitions and Abbreviations</u>	13
<u>Service and support</u>	14

Valid for PCS 7 V9.1

Legal information

Warning notice system

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

DANGER

indicates that death or severe personal injury **will** result if proper precautions are not taken.

WARNING

indicates that death or severe personal injury **may** result if proper precautions are not taken.

CAUTION

indicates that minor personal injury can result if proper precautions are not taken.

NOTICE

indicates that property damage can result if proper precautions are not taken.

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

Qualified Personnel

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

Proper use of Siemens products

Note the following:

WARNING

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

Trademarks

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

Disclaimer of Liability

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

Table of contents

1	Security information	7
2	Preface	8
3	What's new?	11
4	Security strategies	12
4.1	General information	12
4.2	Concept of "defense in depth"	12
4.3	Example configuration.....	16
5	Network security	18
5.1	Automation and security cells	18
5.2	Addressing and segmenting.....	20
5.2.1	Subnet.....	20
5.2.2	Network class	21
5.2.3	Example configuration: Division into subnets	21
5.2.4	Example configuration: Setting of IP addresses and subnet mask.....	24
5.3	Name resolution	27
5.3.1	Computer name.....	27
5.3.2	Changing the computer name.....	28
5.3.3	NetBIOS name	28
5.3.4	Fully Qualified Domain Name.....	28
5.3.5	NetBIOS name resolution	29
5.3.6	NetBIOS name resolution with the Lmhosts file	29
5.3.7	NetBIOS name resolution with a NetBIOS name server.....	30
5.3.8	Host name resolution with the Hosts file	30
5.3.9	Host name resolution (DNS name resolution)	31
5.3.10	Example configuration: Name resolution.....	32
5.4	Managing networks and network services	33
5.5	Access points to the security cells.....	34
5.5.1	Overview	34
5.5.2	Automation Firewall Next Generation	35
5.5.3	Example configuration: Access rules.....	36
5.5.4	Example configuration: Securing the PCS 7 Web server on the front-end firewall	42
5.5.5	Example configuration: Access to the OpenPCS 7 server in the perimeter network	44
5.5.6	Example configuration: Securing the PCS 7 Web server at the back-end firewall	45
5.5.7	Example configuration: Securing the PCS 7 IS server at the front-end firewall	45
5.5.8	Network Intrusion Prevention / Network Intrusion Detection System.....	46
5.6	Secure communication between security cells.....	46
5.6.1	Data exchange between automation systems.....	47
5.6.1.1	Introduction	47
5.6.1.2	Establishing secure communication between security cells with SCALANCE SC.....	48
5.6.2	Operation and observation with remote OS clients	49

5.6.3	Quarantine station as data exchange point.....	52
5.6.3.1	Required firewall rules	52
5.6.3.2	FTPS server configuration	53
5.6.3.3	Patch management, virus protection and whitelisting	59
5.6.4	Secure data exchange between OS and AS stations	60
5.6.5	Using dynamic firewall rules	61
5.7	Configuration of the SCALANCE X network components	63
5.7.1	Disabling non-required ports.....	64
5.7.2	System password for the switch configuration	64
5.7.3	Disabling non-required protocols	64
6	System hardening.....	65
6.1	Overview.....	65
6.2	Installation of the operating system	65
6.2.1	Disabling services	66
6.2.2	Setting of data protection and telemetry data in Windows 10	68
6.2.3	Additional hardening measures to be configured manually.....	71
6.2.3.1	Parameter assignment of the ALM as license server	71
6.2.3.2	SMB signing.....	73
6.2.3.3	Remote Desktop Security setting	74
6.2.3.4	Disabling SMBv1	75
6.2.3.5	Support of LDAP signing and channel binding	76
6.2.3.6	Disabling outdated SSL/TLS communication procedures.....	76
6.3	Security Controller	78
6.4	Windows Firewall	79
6.5	BIOS settings	84
6.6	Working with mobile data media.....	84
6.6.1	Blocking access to all USB storage media	86
6.6.2	Regulating the use of USB storage media and devices.....	86
6.6.3	Disabling AutoRun / AutoPlay for external drives and storage media	94
6.6.3.1	Disabling the AutoPlay function using a group policy.....	95
6.6.3.2	Disabling all AutoRun functions using a group policy	97
6.7	Whitelisting	99
6.7.1	McAfee Application Control	99
6.7.2	Local administration of McAfee Application Control.....	100
6.7.3	Centralized management of McAfee Application Control	100
6.8	Hardening of devices by Industrial Security Services	101
6.9	SIMATIC S7 CPUs.....	101
6.10	SIMATIC NET- Industrial Ethernet CPs	102
6.10.1	Requirements	103
6.10.2	Procedure.....	103
6.10.3	Diagnostic options	105
6.11	PROFINET	106
6.12	Time synchronization of system	106
6.13	Handling of digital signatures for applications	107

6.14	OPC server in the plant.....	107
6.15	Hardening of the Process Historian server.....	108
6.16	Hardening of the Information Server	108
6.17	Disabling non-required network interfaces	108
6.18	Hardening of the Internet Information Server (IIS)	108
6.19	Hardening of the Internet Explorer (IE).....	111
7	User Administration and Operator Permissions	112
7.1	Overview	112
7.2	Windows workgroup or Windows domain	113
7.2.1	Operation of the system in a Windows workgroup.....	113
7.2.2	Operation of the system in an Active Directory	114
7.3	Administration of computers and users	115
7.3.1	Implementation.....	115
7.3.2	SIMATIC permission model.....	117
7.3.3	SIMATIC PCS 7	117
7.3.4	SIMATIC NET	118
7.3.5	Siemens TIA Engineer	118
7.3.6	SIMATIC BATCH.....	119
7.3.7	SIMATIC Route Control.....	119
7.3.8	SIMATIC Management Console	120
7.3.9	Logon_Administrator.....	120
7.3.10	Example configuration.....	121
7.4	Password policies.....	125
7.5	Domain Controller	128
7.5.1	Installation and configuration of the first domain controller (DC1).....	131
7.5.1.1	Configuration of the DNS server	132
7.5.2	Installation and configuration of an additional domain controller (DC2-DCn) in an existing domain	135
7.5.3	Check of network settings on the DCs	136
7.5.4	WINS installation and configuration	137
7.5.4.1	WINS installation	137
7.5.4.2	Entering the WINS server in the IPv4 configuration	137
7.5.4.3	Checking the configuration of the WINS server	138
7.5.5	Operations master roles (FSMO).....	138
7.5.6	Users and user groups.....	141
7.6	Operator authorizations – Rights management of the operator.....	141
7.6.1	SIMATIC Logon	141
7.6.2	Access protection for projects/libraries on the engineering station	142
7.6.3	Change log	146
7.6.4	ES log	147
7.6.5	Access protection for operator stations.....	148
7.7	Protection level concept.....	148

8	Patch management	150
8.1	Overview	150
8.2	Windows Server Update Service (WSUS)	152
8.2.1	Integration of the WSUS server in the system	152
8.2.2	Procedure for patch management with the WSUS.....	153
8.2.3	Configuration of the group policies on the systems	158
8.2.4	Firewall rules for operation of the WSUS.....	162
8.2.5	Installing updates from the SIMATIC Management Console	163
8.3	Manual update	163
8.4	SIMATIC PCS 7 Updates.....	164
9	Protection against malware using virus scanners	165
9.1	Overview.....	165
9.2	Update source	167
9.3	Firewall rules	167
9.4	Distribution of virus signature files	168
9.5	Further settings for the Microsoft Defender AV.....	172
9.6	Procedure after malware infection	174
10	Backing up and restoring data.....	176
10.1	Backup strategy	176
10.1.1	Scope of the backups	177
10.1.2	Interval for creating backups.....	178
10.2	Storage location of backups.....	179
10.3	Archiving.....	179
10.4	Restoration.....	179
11	Disposal of systems and components	181
12	Remote access	183
12.1	Remote maintenance based on the Remote Services platform	183
12.2	Creating a remote service concept	185
12.3	Connection to the Remote Services platform	185
12.4	Implementation of your own remote access solution.....	186
13	Definitions and Abbreviations.....	187
14	Service and support.....	188

Security information

Security information

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

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

Customer is responsible for preventing unauthorized access to its plants, systems, machines, and networks. Systems, machines, and components should only be connected to the enterprise network or the Internet if and to the extent necessary and with appropriate security measures (e.g. use of firewalls and network segmentation) in place.

Additionally, Siemens' guidance on appropriate security measures should be taken into account. You can find more information about Industrial Security at <https://www.siemens.com/industrialsecurity>.

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

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed or Security Newsletter under <https://www.siemens.com/industrialsecurity>.

Preface

Subject of the manual

As a distinctly open system, SIMATIC PCS 7 can be flexibly adapted to a wide range of customer needs. The system software provides the configuration engineer with a great deal of freedom in terms of project configuration, as well as in the design of the program and visualization.

Experience has shown that subsequent modernization or plant expansion work is made much easier if the project is configured "in conformance with PCS 7" as far as possible right from the start. This means users must adhere to certain basic rules to ensure that the provided system functions will offer optimum usability in the future.

This manual serves as a compendium in addition to the product documentation for SIMATIC PCS 7. The basic steps for project creation and parameter assignment are described in the form of instructions with numerous figures.

This compendium is based on the "Security Concept PCS 7 & WinCC (Basic) (<https://support.industry.siemens.com/cs/ww/en/view/109780811>)" document.

The compendium directly reflects the recommended method through the security configuration of a SIMATIC PCS 7 system (defense-in-depth concept in accordance with IEC 62443), which is based on the results of a great deal of practical experience. The description relates to working with the project and the parameter settings of the components it contains but not the application itself.

Subject of Part F-"Industrial Security"

In the production and automation environment, it is primarily about the availability of the system. The protection of information and data is of secondary importance.

"Industrial Security" must not be reduced to information security in the automation environment. The transmitted information controls and monitors physical and/or chemical processes, directly and deterministically. The actual information is therefore comparatively unimportant when viewing the possible IT-based damages in the production environment (exception: company secrets, for example, recipes). What is important is the possible (and intended) direct effect of information on the process control and process monitoring based on the use of automation technology. When this information flow is disrupted, a series of consequences can be expected:

- Limited process availability up to the loss of process control
- Direct maloperation
- System standstills, production downtimes, quality losses and product contamination
- Damages to the system
- Danger to life and limb
- Dangers to the environment
- Violations of legal or official conditions
- Criminal or civil charges
- Loss of public reputation (damage to public image)
- Financial losses

As result, the objectives of protection in process automation and in traditional information technology differ significantly: For office applications, confidentiality and data protection are most important. For automation systems, maintaining operational safety without exception and protecting life and limb are of the highest priority. The decisive prerequisite in this case is maintaining the availability of the system and, as a result, the unrestricted control over the process. The consequence resulting from this is that the proven methods and approaches in the office environment cannot be applied one-to-one in automation engineering.

General notes for the secure operation of a SIMATIC PCS 7 system

- The settings described in the SIMATIC PCS 7 compendium Part F are necessary for secure operation of SIMATIC PCS 7. This applies to all systems.
- System-specific hardening measures must be established as the result of a risk evaluation.
- Hardening measures depend on the respective operating phase, for example, commissioning or runtime operation.
- Prior to the installation of SIMATIC PCS 7 on a system, all available updates must be installed on it. During subsequent operation of the systems, the availability of new updates must be checked regularly, and they must be installed as quickly as possible.
- All measures that are written to and implemented on Microsoft Windows Client systems must also be applied to Microsoft Windows Server systems.

Validity

This manual incorporates the statements provided in the documentation for SIMATIC PCS 7 and specifically in the "Security Concept PCS 7 & WinCC". It can be used for plants and projects that are automated with SIMATIC PCS 7.
The configuration guide is valid for SIMATIC PCS 7 V9.1.

For components that are outside the scope of SIMATIC PCS 7 as described in this document, further possible security measures must be applied:

- "SIMATIC PCS 7 Add-on and device-specific libraries"
<https://support.industry.siemens.com/cs/ww/en/view/109782749>
- Manuals for the Industrial Ethernet switches of the SCALANCE X product series

SIMATIC PCS 7 in Industry Online Support

An overview of the most important technical information and solutions for SIMATIC PCS 7 is available at www.siemens.de/industry/onlinesupport/pcs7.

SIMATIC PCS 7 documentation

You can find the documentation of SIMATIC PCS 7 in the Siemens Industry Online Support under the following link:

- SIMATIC PCS 7 V9.1 Software Technical Documentation
(<https://support.industry.siemens.com/cs/ww/en/view/109794065>)

What's new?

The existing contents were updated for SIMATIC PCS 7 V9.1. Changes and additions were made in the following sections in particular:

- Windows 10 Enterprise LTSC 2019 and Windows Server 2019 operating systems
- Using SCALANCE SC modules
- Automation Firewall Next Generation based on the Palo Alto Next Generation Firewalls
- Windows Update (WU) relevant settings on the WSUS and the WU clients
- Microsoft Defender Antivirus (AV) as approved virus scanner product and its configuration
- Integrity check of software packages prior to the installation of SIMATIC PCS 7 from the SIMATIC Management Console
- Central update management of the SIMATIC Management Console
- Disabling other Microsoft Windows services that are not required

Security strategies

4.1 General information

The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) supports system operators in the case of expert security reports, with preparation of additional defensive measures for protection against computer and network security risks.

ICS-CERT recommends:

- Minimization of vulnerabilities in the network for all control system devices. Important devices must not have direct access to the Internet.
- Placement of control system network and remote devices behind a firewall and isolation of these from the company network.
- If remote access is needed, secure methods such as Virtual Private Networks (VPNs) must be used. Keep in mind that VPN is only as secure as the connected devices.

4.2 Concept of "defense in depth"

The concept of defense-in-depth is a security strategy in which several layers of the defense position themselves around the system to be protected, in this case the automation system (like "peeling an onion").

The implementation of a defense-in-depth requires a combination of various security measures. They include:

Plant security

- Physical security measures
Control of physical access to spaces, buildings, individual rooms, cabinets, devices, equipment, cables and wires. The physical security measures must be based around the security cells and the responsible persons. It is also important to implement physical protection at remote single station systems.
- Organizational security measures
Security guidelines, security concepts, set of security rules, security checks, risk analyses, assessments and audits, awareness measures and training.

Network security

- Division into security cells

A comprehensively secured network architecture subdivides the control network into different task levels.

Perimeter zone techniques should be employed for this. This means that systems set up in the perimeter network (DMZ) are shielded by one or more firewalls (front-end firewall and back-end firewall or three-homed firewall) from other networks (e.g. Internet, office network). This separation enables access to data in the perimeter network without having to simultaneously allow access to the internal network to be protected (e.g. automation network). As a result, risks of access violations can be significantly reduced.

- Securing access points to the security cells

A single access point to each security cell (should be realized by a firewall) for authentication of users, employed devices and applications, for direction-based access control, for assignment of access authorizations, and for detection of intrusion attempts.

The single access point functions as the main access point to the network of a security cell and serves as the first point of a control of access rights to a network level.

- Securing the communication between two security cells over an "insecure" network
Certificate-based, authenticated and encrypted communication should always be used when the perimeter zone technique is used and there is communication across the access points. Tunnel protocols such as L2TP (Layer Two Tunneling Protocol) and IPSec (IPSecurity) or OpenVPN can be used for this. Furthermore, communication is possible using protocols that are secured by server-based certificates, such as RDP (Remote Desktop Protocol) or a website published via HTTPS. In this case, communication takes place across the firewall using TLS (Transport Layer Security) technology.

System integrity

- System hardening
Adjustments to a system to make it more resistant to malware attacks.
- User management and role-based operator authorizations
Task-based operation and access authorizations (role-based access control).
- Patch management
Patch management is the systematic procedure for installing updates on plant systems.
- Malware detection & prevention
Use of suitable and correctly configured virus scanners or other Endpoint Detection and Response (EDR) software.
- Security Information and Event Management (SIEM)
A SIEM system performs a real-time analysis of security events from different sources like operating systems, applications and network components.

Note

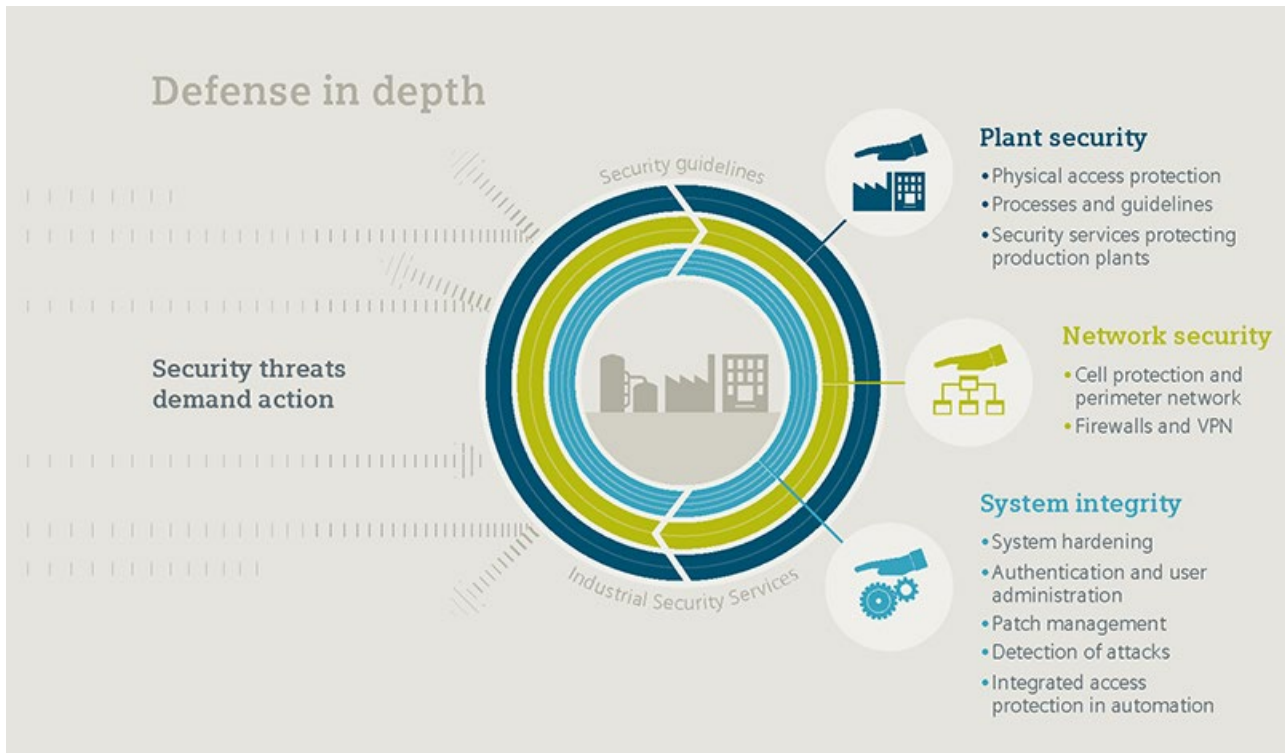
The following information is available in the SIMATIC PCS 7 environment for a SIEM system:

- Windows Eventlogs for user logons, system changes and other events
- Security Events of SIMATIC PCS 7 CPU 410-5H and CPU 410E (firmware V8.2 and higher)
- Events of network components or of an optional network management system

The following sources are available for additional security-relevant evaluations:

- SIMATIC Logon Events for logons to SIMATIC PCS 7
 - ES Audit
 - WinCC option "Audit Trail"
-

The following figure shows the "defense-in-depth" strategy:



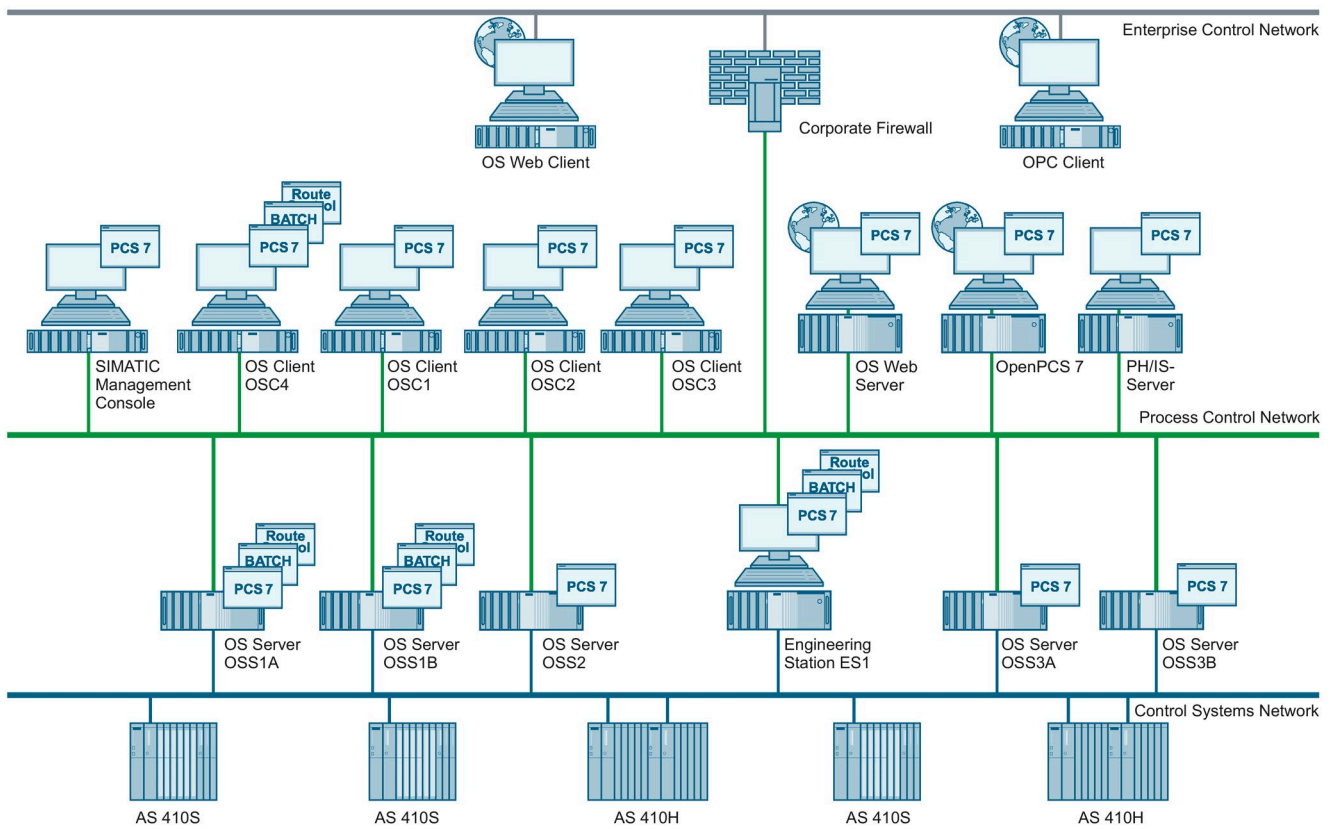
4.3 Example configuration

This compendium orients itself on the concept of defense-in-depth in its design and structure. In line with the concept, the individual sections are divided into network security measures (division into security cells, securing access points and secure communication between components in different security cells) and system integrity measures. This includes the sections "System hardening", "User management & operator authorization", "Patch management" and "Virus scanners".

Note

Note that the example configuration presented in this section depicts a plant configuration without any safety measures. The example configuration shown below is a negative example from a security point of view. This document presents a step-by-step description of how this plant configuration can be made more secure by implementing security measures.

The measures presented in this compendium and configuration examples are illustrated using the following example configuration:



The example configuration consists of a total of five S7 controllers (partially redundant) that assume the measuring and control tasks within the process-related system. Five OS servers (two redundant pairs of servers and a single OS server) and four OS clients are planned for controlling and monitoring. In addition, a Web server is envisaged for operator control and monitoring via the corporate network and the Internet. For this, the terminal bus is connected to the corporate network which, in turn, provides Internet access. An engineering station is available for configuring the overall plant.

The SIMATIC Management Console is available for installation of the SIMATIC PCS 7 software on the systems. In addition, central diagnostic data of the plant can be collected from here (e.g. software and firmware versions). A PH/IS server handles archiving and reporting of process values. Finally, an OpenPCS 7 system is available for OPC functionalities.

The industrial process plant is divided into two or more independent units. Three S7 controllers are used for the measuring and control tasks of Unit A, while two S7 controllers are used for those of Unit B. The four OS clients should allow both units to be operated and monitored. For this purpose, Unit A and B are each assigned a redundant OS server pair. Unit A also features another OS server, which is not configured redundantly. An OS client is to serve as a local operating station at a filling station.

Network security

5.1 Automation and security cells

The strategy for dividing plants and connected plants into security cells increases the availability of the overall system. Failures or security threats that result in failure can thereby be restricted to the immediate vicinity. During the planning of the security cells, the plant is first divided into process cells and then into security cells based on the security measures.

You can learn about the criteria for dividing a system into automation and security cells in the document "Security Concept PCS 7 & WinCC (Basic)" (<https://support.industry.siemens.com/cs/ww/en/view/109780811>).

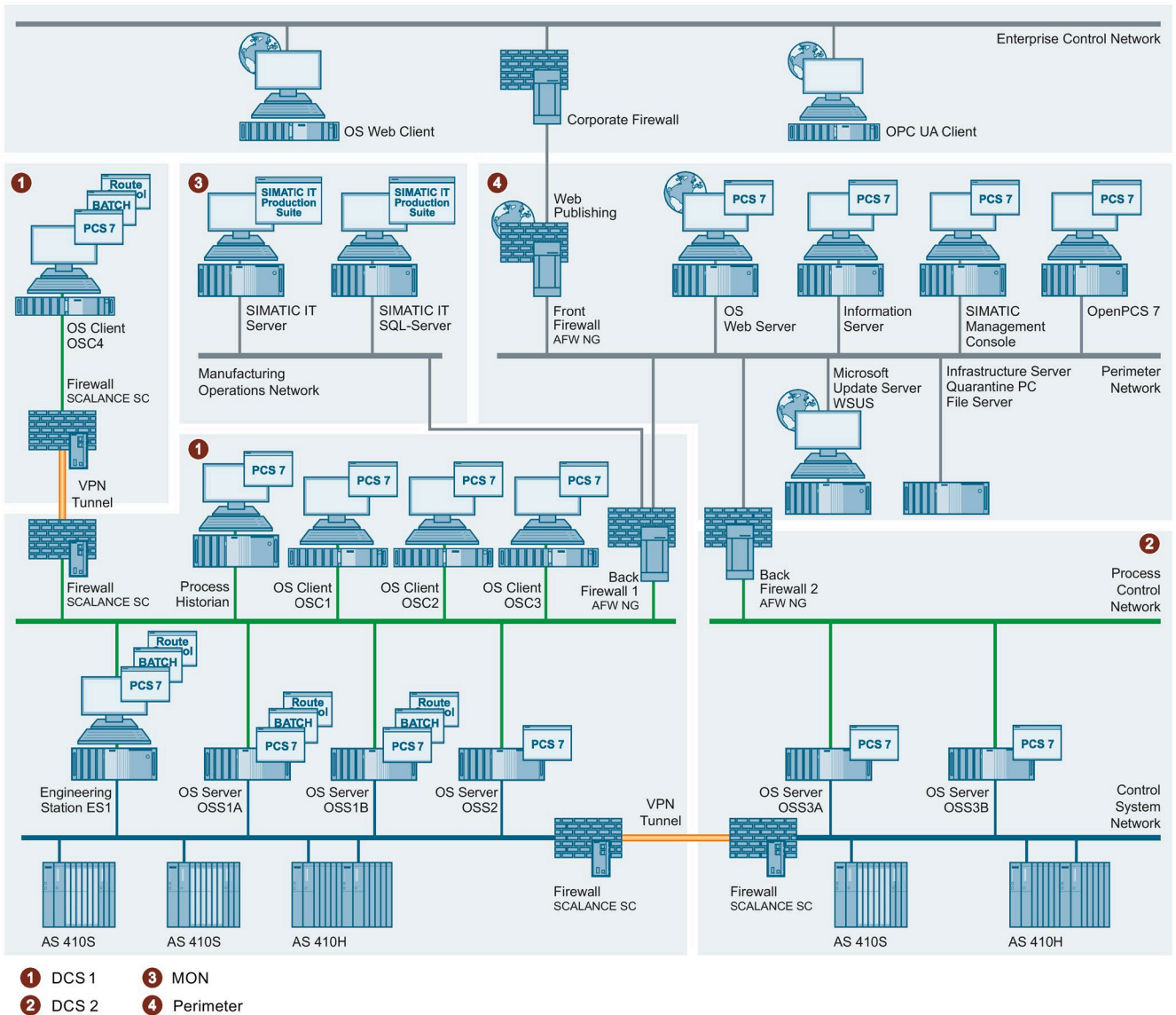
Example configuration: Division into security cells

The example configuration consists of two independent units with a common operating and monitoring level. Hence, a security cell for Unit A can be formed with the S7 controllers and OS servers assigned to Unit A in each case. A separate security cell is formed for Unit B and the controllers and OS servers assigned to this unit.

The division of the overall plant into a security cell for Unit A as well as Unit B also demands the separation of plant bus and terminal bus (Control Systems Network and Process Control Network). The OS clients, on which operating and monitoring of the entire process (Units A and B) is to be performed, are assigned to the security cell of Unit A. As a result, a communication between the security cells of Unit A and B must be ensured.

The Web server, which is used for operating and monitoring from the corporate network or from the Internet, is placed in a separate security cell (perimeter). The virus scanner server and update server are also placed in this security cell. A quarantine PC is also implemented in the perimeter security cell for data exchange (project data/project backup) between the security cells.

The components of the production planning interface (SIMATIC IT), in turn, are combined in a separate security cell (MON/MES). This results in four different security cells (DCS1, DCS2, MON and Perimeter) for the example configuration, which are shown in the following figure:



5.2 Addressing and segmenting

Note

The term "IP Address" used in this document means an IPv4 address, as opposed to an IPv6 address. IPv6 addressing is not covered in this document.

An IP address consists of 32 bits. Usually, a notation is used with four decimal numbers (from 0 to 255) delimited by periods (decimal point notation). Each decimal number, also known as an octet, represents 8 bits (1 byte) of the 32-bit address:

IPv4 address				
Binary	1100 0000	1010 1000	0000 0001	0000 1010
Hexadecimal	C 0	A 8	0 1	0 A
Decimal	192	168	1	10

5.2.1 Subnet

The strategy of a spatial and functional division of an automation plant must also be reflected in the network configuration. This can be achieved by the selection of the IP address range and the formation of subnets associated with it. Subnets are used to subdivide an existing network into additional, smaller networks (PCN, CSN, MON, perimeter, etc.) without requiring additional Class A, Class B or Class C IP addresses.

A subnet therefore refers to a network section for the Internet protocol (IP). The subnet groups several sequential IP addresses by means of a subnet mask. Hence, the subnet mask divides an IP address into a network part and a host part. It has the same structure as an IP address (4 bytes). By definition, all bits of the network part must be set to TRUE = 1 and all bits of the host part to FALSE = 0.

Network and host part of an IP address					
IP address	192.168.65.2	1100 0000	1010 1000	0110 0101	0000 0010
Subnet mask	255.255.255.0	1111 1111	1111 1111	1111 1111	0000 0000
Network	192.168.65.0	1100 0000	1010 1000	0110 0101	0000 0000
		0000 0000	0000 0000	0000 0000	1111 1111
Host	2	0000 0000	0000 0000	0000 0000	0000 0010

5.2.2 Network class

The address classes were defined by the Internet Assigned Numbers Authority (IANA) in order to systematically assign address prefixes to networks of varying size. The class of addresses indicates how many bits are used for the network ID and how many bits are used for the host ID. The address classes also specify the possible number of networks and the number of hosts per network. Of the five address classes, classes A, B and C are reserved for IPv4 unicast addresses. Private IP address ranges have also been defined within these three network classes. From a network security point of view, these private IP address ranges have the advantage that they cannot be forwarded (routed) on the Internet. As a result, a direct attack from the Internet on a system PC is already being prevented.

Network address range	CIDR notation	Number of addresses	Network class
10.0.0.0 – 10.255.255.255	10.0.0.0/8	$2^{24} = 16,777,216$	Class A: 1 private network with 16,777,216 addresses
172.16.0.0 – 172.31.255.255	172.16.0.0/12	$2^{20} = 1,048,576$	Class B: 16 private networks with 65,536 addresses each
192.168.0.0 – 192.168.255.255	192.168.0.0/16	$2^{16} = 65,536$	Class C: 256 private networks with 256 addresses each

5.2.3 Example configuration: Division into subnets

Addresses from the private IP address range for Class C are to be used for addressing the automation networks in the example configuration (plant bus/CSN, terminal bus/PCN, etc.). This range features:

- 256 Class C networks (subnet 192.168.0.x to 192.168.255.x)
- 254 hosts per network (IPv4 address 192.168.x.1 to 192.168.x.254)

The network address 192.168.2.0 used in the example configuration is divided into four subnets of equal size (same number of hosts in the subnet). The division into four networks (Perimeter Network, Process Control Network 1, Process Control Network 2 and Manufacturing Operations Network) requires 2 bits ($2^2 = 4$).

This enables segmentation into four networks with the following subnet mask:

1111 1111.1111 1111.1111 1111.1100 0000 = 255.255.255.192

(in a different notation: /26 (26 bits of subnet mask are set))

5.2 Addressing and segmenting

This results in the following networks:

- Network 1: Manufacturing Operations Network (IP addresses of MON, 192.168.2.0/26)

Network 1: Manufacturing Operations Network	
Network address	192.168.2.0
Address of the first host	192.168.2.1
Address of the last host	192.168.2.62
Broadcast address	192.168.2.63

- Network 2: Process Control Network 1 (IP addresses of the PCN1 (Unit A), 192.168.2.64/26)

Network 2: Process Control Network 1	
Network address	192.168.2.64
Address of the first host	192.168.2.65
Address of the last host	192.168.2.126
Broadcast address	192.168.2.127

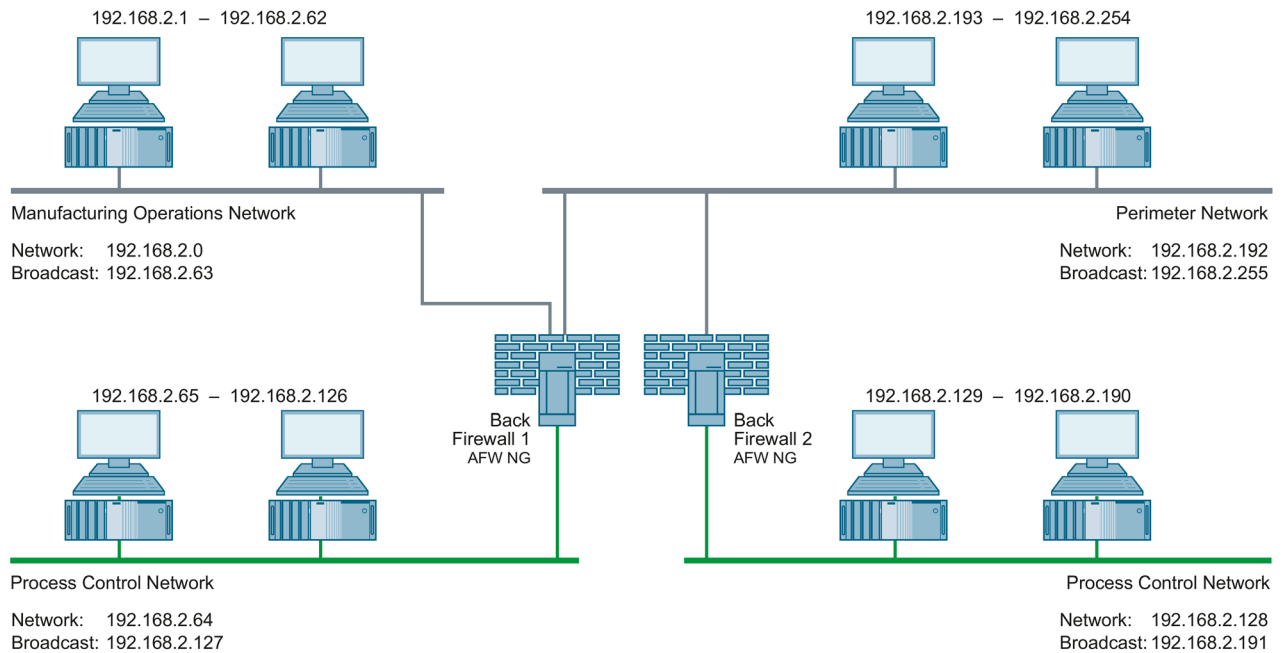
- Network 3: Process Control Network 2 (IP addresses of PCN2 (Unit B), 192.168.2.128/26)

Network 3: Process Control Network 2	
Network address	192.168.2.128
Address of the first host	192.168.2.129
Address of the last host	192.168.2.190
Broadcast address	192.168.2.191

- Network 4: Perimeter network (IP address of Perimeter network, 192.168.2.192/26)

Network 4: Perimeter Network	
Network address	192.168.2.192
Address of the first host	192.168.2.193
Address of the last host	192.168.2.254
Broadcast address	192.168.2.255

Example: The four computers with the IP addresses 192.168.2.10, 192.168.2.100, 192.168.2.149 and 192.168.2.201 are located in different subnets among which the routing must be performed. This means broadcast addresses in the Manufacturing Operations Network are not transmitted to the other subnets. Failures in individual subnets will remain localized to these subnets.



The gateway functionality between the different networks is taken up by the two back-end firewalls in the aforementioned configuration. This requires establishing an appropriate network rule within the firewall used.

If systems have to communicate with one another in the different subnets, the corresponding routing must be configured there, specifying the gateways.

5.2.4 Example configuration: Setting of IP addresses and subnet mask

Procedure

The following procedure is described using the example of a "Windows 10" operating system.

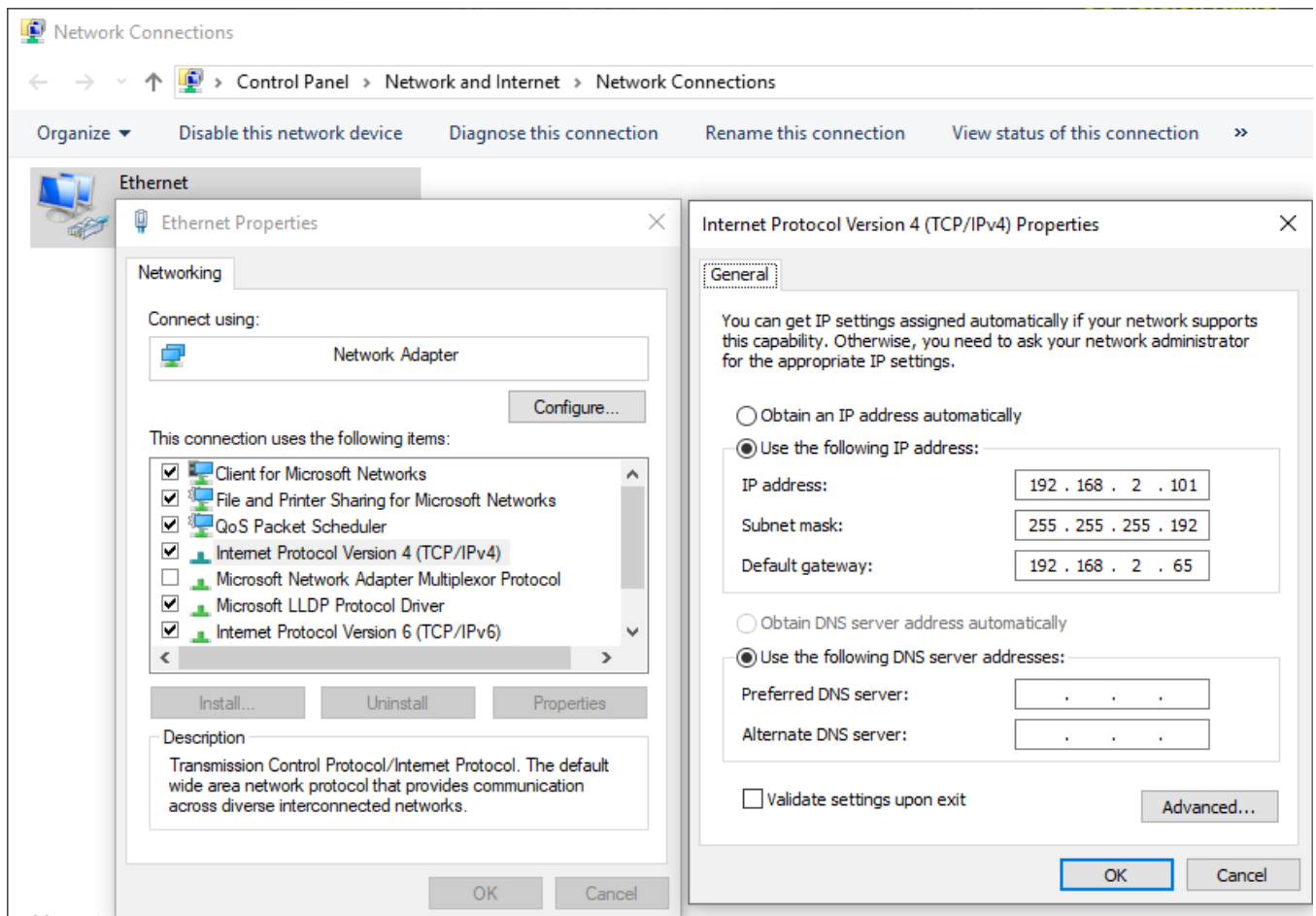
To configure the IP address, subnet mask and default gateway, follow these steps:

1. In the Window Start menu, right-click the "Network connections" command from the shortcut menu.
The "Network connections" dialog box opens.
2. Now, under "Change network settings", open the option "Change adapter options".
3. Double-click on the corresponding network adapter icon to open the status display of the corresponding network connection (Process Control Network 1 or 2, Perimeter Network or Manufacturing Operations Network).
The status display dialog of the network connection opens.
4. Click the "Properties" button.
Enter the administrator password, if required. If you are logged on as an administrator, confirm the execution of the application.
The "Local Security Policy" dialog box opens.
5. Select the "Internet Protocol Version 4 (TCP/IPv4)" option and click on the "Properties" button.
The properties dialog of the "Internet Protocol Version 4 (TCP/IPv4)" option opens.
6. Select "Use the following IP address" option and enter the IP address of the corresponding computer in the "IP address" box.
7. In the "Subnet mask" box, enter the subnet mask of the computer.
8. If necessary, enter the corresponding IP address in the "Default gateway" field.
9. Confirm the changes with "OK".

Example

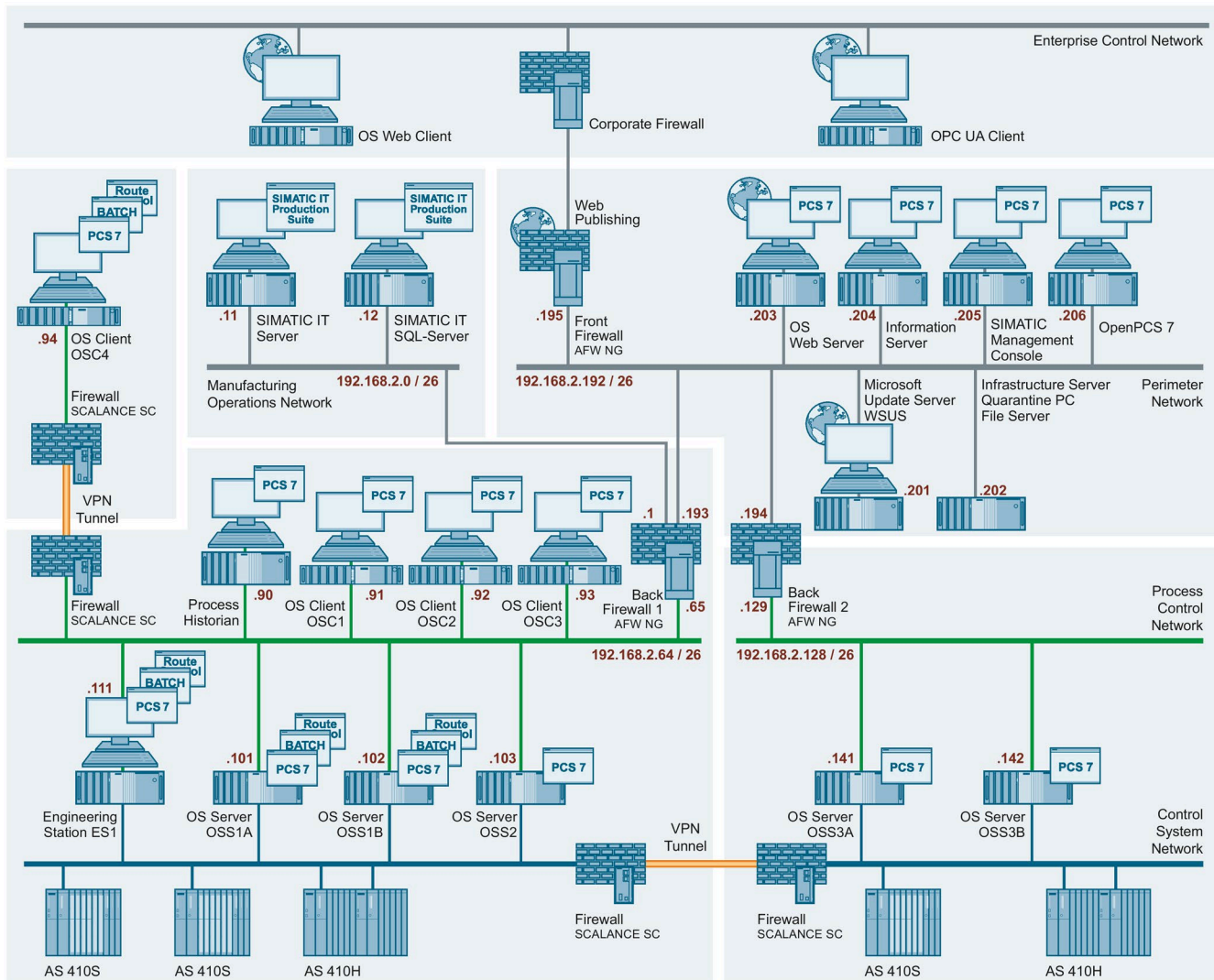
In the following figure, a computer located in Process Control Network 1 is addressed. The OS server with the name "OSS1A" has a network connection to the Process Control Network 1. The subnet mask 255.255.255.192 was specified for this network by the division into subnets. Hence, the IP addresses available within this network are the addresses from 192.168.2.65 to 192.168.2.126.

The IP address 192.168.2.101 was specified for the OS server "OSS1A" and inserted in the "IP address" box of the properties dialog for "Internet Protocol Version 4 (TCP/IPv4)". The subnet mask 255.255.255.192 specified above was entered in the "Subnet mask" box.



5.2 Addressing and segmenting

This procedure is used to assign the corresponding IP address to all computers.



5.3 Name resolution

5.3.1 Computer name

A computer can be identified within a network by the computer name. The name has to be uniquely associated with the computer. This ensures that a computer is reliably found in the network with its name. Entering computer names twice inadvertently can result in unforeseen behavior during communication.

The NetBIOS name is derived from the computer name (see NetBIOS name) and must be unique for the NetBIOS resolution and operation of the system. The computer name should allow the function of the computer to be inferred.

The following rules apply to the computer name:

- The computer name starts with a letter.
- The computer name contains only letters and numbers.
- The computer name is a maximum of 15 characters.

Note

You can learn about the rules for assigning the computer name in the installation manual "SIMATIC PCS 7 PC Configuration"

(<https://support.industry.siemens.com/cs/ww/en/view/109794377>).

Refer also to the following documents:

- FAQ "Why is the underscore character not permitted in computer names in PCS 7?" (<https://support.industry.siemens.com/cs/ww/en/view/67794551>)
- Microsoft Support Center: "Naming conventions in Active Directory for computers, domains, sites, and OUs" (<https://docs.microsoft.com/en-us/troubleshoot/windows-server/identity/naming-conventions-for-computer-domain-site-ou>)

You can find more naming conventions in the following documents:

- Manual "SIMATIC PCS 7 Engineering System" (<https://support.industry.siemens.com/cs/ww/en/view/109800500>) section "Rules for naming in the PH"
 - Online help WinCC information system "Working with projects > Appendix > Invalid characters"
-

5.3.2 Changing the computer name

NOTICE

The computer name may be changed only prior to the installation of SIMATIC PCS 7.

For information on changing the computer name, refer to the installation manual "SIMATIC PCS 7 PC Configuration" (<https://support.industry.siemens.com/cs/ww/en/view/109794377>) (section 5.3.3 - "Changing the computer name").

Procedure

The following procedure is described using the example of a "Windows 10" operating system.

To change the computer name, follow these steps:

1. In the Window Start menu, right-click the "System" command from the shortcut menu.
2. Click the "System Info" link in the "Related Settings" area.
3. Click on the "Change settings" link in the "Computer name, domain, and workgroup settings" section.
If prompted, enter the administrator password as required. If you are already logged on as an administrator, confirm the execution of the application.
The "System Properties" dialog box opens.
4. Click "Change" in the "Computer name" tab.
The "Computer Name/Domain Changes" dialog box opens.
5. In the "Computer name" box, enter the name of the computer.

5.3.3 NetBIOS name

Source: Microsoft Support Center "TCP/IP Fundamentals for Microsoft Windows"

A NetBIOS name is a 16-byte (16-character) name based on the computer name that designates a NetBIOS application in the network. The service uses the first 15 characters of the computer name plus the character 0x20 as the 16th character as the exact name. A NetBIOS name is either a unique (exclusive) name or a (non-exclusive) group name. If a NetBIOS application communicates with a specific NetBIOS application on a single computer, unique names are used. If a NetBIOS process communicates with several NetBIOS applications on different computers, a group name is used.

5.3.4 Fully Qualified Domain Name

The "Fully Qualified Domain Name" (FQDN) is comprised of the computer name and the domain name and must not be used multiple times.

5.3.5 NetBIOS name resolution

Source: Microsoft Support Center "TCP/IP Fundamentals for Microsoft Windows"

NetBIOS name resolution is the process of assigning an IPv4 address to a NetBIOS name. The following methods can be used for the successful NetBIOS name resolution:

- Methods of NetBIOS name resolution in the order they are executed by Windows

Method	Description
NetBIOS name cache	A local table stored in RAM that contains the NetBIOS names with the corresponding IPv4 addresses recently resolved by the local computer.
NBNS	A server that provides the NetBIOS names. For WINS, this is the Microsoft implementation of an NBNS.
Local broadcast	NetBIOS Name Query Request broadcast messages that are transmitted to the local subnet.
Lmhosts file	Local text file in which NetBIOS names are assigned to their IPv4 addresses. The Lmhosts file is used for NetBIOS applications that are executed on computers in remote subnets.
Local host name	Configured host name of the computer
DNS resolution cache	Local RAM-based table that contains domain names and IPv4 address assignments from entries in the local HOSTS file as well as the names to be resolved via DNS.
DNS server	Server that manages databases with assignments of IPv4 addresses to host names.

5.3.6 NetBIOS name resolution with the Lmhosts file

Source: Microsoft Support Center "TCP/IP Fundamentals for Microsoft Windows"

The Lmhosts file is a static text file with NetBIOS names and IPv4 addresses. NetBT uses the Lmhosts file to resolve NetBIOS names for NetBIOS applications that are executed on remote computers in a network without NBNS (e.g. WINS). The Lmhosts file features the following characteristics:

- Entries consist of an IPv4 address and a NetBIOS computer name, for example:
192.168.2.101 OSSRV01A
- The entries are not case-sensitive.
- A separate file is located on every computer in the folder %windir%\system32\Drivers\etc.

This folder also contains an Lmhosts sample file (Lmhosts.sam). You can create your own file with the name Lmhosts or copy Lmhosts.sam in this folder to Lmhosts.

The entries in the Lmhosts file are to be supplemented with the keyword #PRE. The keyword #PRE specifies which entries will be loaded into the NetBIOS name cache as permanent entries at the restart of Windows. This reduces network broadcasts and increases the name resolution performance because names are resolved using the cache if necessary instead of through broadcast queries.

Example:

```
192.168.2.101 OSSRV01A #PRE
192.168.2.102 OSSRV01B #PRE
```

5.3.7 NetBIOS name resolution with a NetBIOS name server

Source: Microsoft Support Center "TCP/IP Fundamentals for Microsoft Windows"

A NetBIOS name server (NBNS) can be used for NetBT to resolve NetBIOS names of NetBIOS applications that run on local computers or remote computers. If an NBNS is used, the name resolution is performed as follows:

1. NetBT checks the NetBIOS name cache for assignments of NetBIOS names to IPv4 addresses.
2. If the name cannot be resolved with the NetBIOS name cache, NetBT sends a NetBIOS Name Query Request unicast message to the NBNS that contains the NetBIOS name of the target application.
3. If the NBNS can resolve the NetBIOS name for an IPv4 address, the NBNS returns the IPv4 address to the transmitting host with a positive NetBIOS name query response message. If the NBNS cannot resolve the NetBIOS name for an IPv4 address, the NBNS sends a negative NetBIOS name query response message.

A Windows system attempts to find the primary NBNS server three times. If no response is received or a negative NetBIOS name query response message indicates that the name resolution has failed, a computer running Windows attempts to contact additional NBNS servers.

WINS (Windows Internet Name Service) is the Windows implementation of a NetBIOS Name Server (NBNS), which provides a distributed database for registering and querying dynamic assignments of NetBIOS names to the IPv4 addresses used in the network.

5.3.8 Host name resolution with the Hosts file

Source: Microsoft Support Center "TCP/IP Fundamentals for Microsoft Windows"

The Hosts file is a static text file with host names and IPv4 addresses. The Hosts file exhibits the following:

- Entries consist of an IPv4 address and a computer name, for example: 192.168.2.101
OSSRV01A
- The entries are not case-sensitive.

Each computer has its own file in the folder %windir%\system32\Drivers\etc.

5.3.9 Host name resolution (DNS name resolution)

Source: Microsoft Support Center "TCP/IP Fundamentals for Microsoft Windows"

Host name resolution refers to the correct assignment of a host name to an IP address. A host name is an alias name that was assigned to an IP node. The IP node is, therefore, identified as TCP/IP host. The host name can consist of up to 255 characters. It can contain alphabetical and numerical characters, hyphens and periods. You can assign multiple host names to the same host.

For Winsock programs (Windows Sockets), e.g. Internet Explorer and the FTP utility, one of two values can be set for the desired target: The IP address or a host name. If the IP address is specified, the name resolution is not required. If a host name is specified, it must be resolved in an IP address before IP communication with the required resource can start.

Different types of host names can be used. A freely selectable name and a domain name are usually used. Such a name is called the FQDN (see above). The freely selectable name is an alias name for an IP address that is assigned to individual IP nodes (hosts) and can then be used (e.g. www). A domain name is a structured name in a hierarchically organized namespace that is referred to as DNS (Domain Name System). An example of a domain name is microsoft.com. For example, this yields www.microsoft.com for an FQDN.

Freely selectable names can be resolved via entries in the "Hosts" file. This file is located in the folder "%windir%\System32\Drivers\etc".

To resolve FQDNs, a DNS client sends DNS name queries to a configured DNS server. The DNS server is a computer on which entries with assignments of host and domain names (zones) to IP addresses or information about other DNS servers are stored. The DNS server resolves the requested FQDN into an IP address and returns the result to the requesting DNS client.

If one or more DNS servers are available in your network, you must configure your computers in the network settings with the IP address of this responsible DNS server. This will enable your computers to resolve FQDNs into IP addresses. Active Directory-based computers (systems that are members of a Windows domain) always require this configuration.

5.3.10 Example configuration: Name resolution

The example configuration was divided into multiple security cells (DCS1, DCS2, MON and Perimeter). A WINS server is not available for the NetBIOS name resolution in any of these security cells. A DNS server for the host name resolution is also lacking in every security cell. To ensure trouble-free name resolution in this case, the "lmhosts" and "hosts" file must therefore be configured on each computer.

First, a computer name must be assigned to each computer. To do so, proceed as described under the heading "Changing the computer name". Note that the computer name may be changed only prior to installation of SIMATIC PCS 7.

Note

You need administrator rights for the configuration of the Lmhosts and Hosts file described below.

After a computer name and an IP address have been specified for every computer, you can configure the lmhosts file. Proceed as follows:

1. Open the file "Lmhosts.sam" (e.g. using "Notepad").
It is located in the directory "%windir%\system32\Drivers\etc" and is a sample file that can be used as a template to create the individual "Lmhosts" file.
2. Add a new line at the end of the file for each computer of the plant.

```
lmhosts - Notepad
File Edit Format View Help
#
# Note that the whole file is parsed including comments on each lookup,
# so keeping the number of comments to a minimum will improve performance.
# Therefore it is not advisable to simply add lmhosts file entries onto the
# end of this file.

192.168.2.101 OSS1A #PRE
192.168.2.102 OSS1B #PRE
192.168.2.103 OSS2 #PRE
192.168.2.111 ES1 #PRE
192.168.2.90 PH1 #PRE
192.168.2.91 OSC1 #PRE
192.168.2.92 OSC2 #PRE
192.168.2.93 OSC3 #PRE

192.168.2.141 OSS3A #PRE
192.168.2.142 OSS3B #PRE

192.168.2.11 SITS1 #PRE
192.168.2.12 OITS2 #PRE

192.168.2.201 PCS7WSUS #PRE
192.168.2.202 QPC #PRE
192.168.2.203 PCS7WEBSRV1 #PRE
192.168.2.204 PCS7IS #PRE
192.168.2.205 PCS7SMC #PRE
192.168.2.206 PCS7OPC #PRE

Windows (CRLF) Ln 98, Col 1 100%
```


3. Configure all computers, including those located in the security cells "MON", "Perimeter", "DCS1" and "DCS2".
4. Save the file with "Save As" and assign the name "lmhosts" (without file extension) to the file.
5. Add the entries made in the "lmhosts" file to the "hosts" file.
6. Copy both files from the computer on which you have created them to the directory listed under 1. on all computers in the plant.

5.4 Managing networks and network services

The administration of network settings and required network services of a process control system can be organized in a decentralized or central manner. Mixed configurations of central and decentralized administration are possible.

Central administration (Windows domain, Active Directory)

All required information and settings can be configured centrally:

- IPv4 addresses, subnet mask, default gateway, DNS server via DHCP
- DNS and NetBIOS name resolution via DNS and WINS
- Time synchronization via NTP and/or NT5DS
- Additional system-related settings as per group policies (GPOs) (e.g. password guidelines)

Distributed administration (Windows workgroup)

All of the required information and settings must be configured locally on every individual computer within the process control system.

RADIUS

RADIUS (Remote Access Dial In User Service) is a network protocol that provides central authentication, authorization and user account management. The central user authentication of network components should preferably be performed using a central RADIUS server, e.g. the Network Policy Server (NPS) as part of the Microsoft Active Directory.

You can find information on the configuration of RADIUS options for network devices in the application example "User administration for SCALANCE devices with RADIUS protocol" (<https://support.industry.siemens.com/cs/ww/en/view/98210507>) and in the manuals for the SCALANCE X network devices.

DHCP

DHCP (Dynamic Host Configuration Protocol) allows computers and other TCP/IP-based network devices to be automatically provided with IP addresses. In this way, additional configuration parameters needed by these systems, such as DNS server, WINS server, default gateway and NetBIOS mode, can also be provided.

DHCP was developed with the following two application scenarios in mind:

- Large networks with frequently changing topologies and nodes
- Users who want to have "only a network connection" and do not want to deal with the network configuration in more detail (e.g. WLAN hotspots)

Neither of these use scenarios usually apply to an automation system, which is why use of a DHCP server is not recommended in such an environment.

Note

If a DHCP server is used in a SIMATIC PCS 7 system, static address reservations must be used.

5.5 Access points to the security cells

5.5.1 Overview

One of the factors for designing the security cells is that they should only have one access point. Any access to the security cell via this access point may occur only after verifying the legitimacy (persons and devices have to be authenticated and authorized) and must be logged. The access points should prevent unauthorized data traffic to the security cells while allowing authorized and necessary traffic for smooth operation of the system.

The access point to a security cell can be designed differently depending on requirements of the configuration and functionality.

You can find information about the various concepts in the manual "SIMATIC Process Control System PCS 7 Security Concept PCS 7 & WinCC (Basic)"

(<https://support.industry.siemens.com/cs/ww/en/view/109780811>).

5.5.2 Automation Firewall Next Generation

To implement the different solutions for access points according to the SIMATIC PCS 7 & WinCC security concept (front-end/back-end firewall, three-homed firewall or access point firewall), the Automation Firewall Next Generation is available as a SIMATIC PCS 7 add-on.

The Automation Firewall Next Generation, in its different versions, is a solution from Palo Alto Networks with the Linux-based operating system PAN-OS. The Automation Firewall Next Generation (AFW NG) is a firewall that goes beyond protocol and port-based filtering and can control and analyze the data traffic at the application level. Moreover, additional safety functions like Threat Detection, Antivirus, Anti-Spyware, URL filtering, File Blocking, WildFire Analysis, Data Filtering and DoS Protection are implemented (some are fee-based functions).

Note

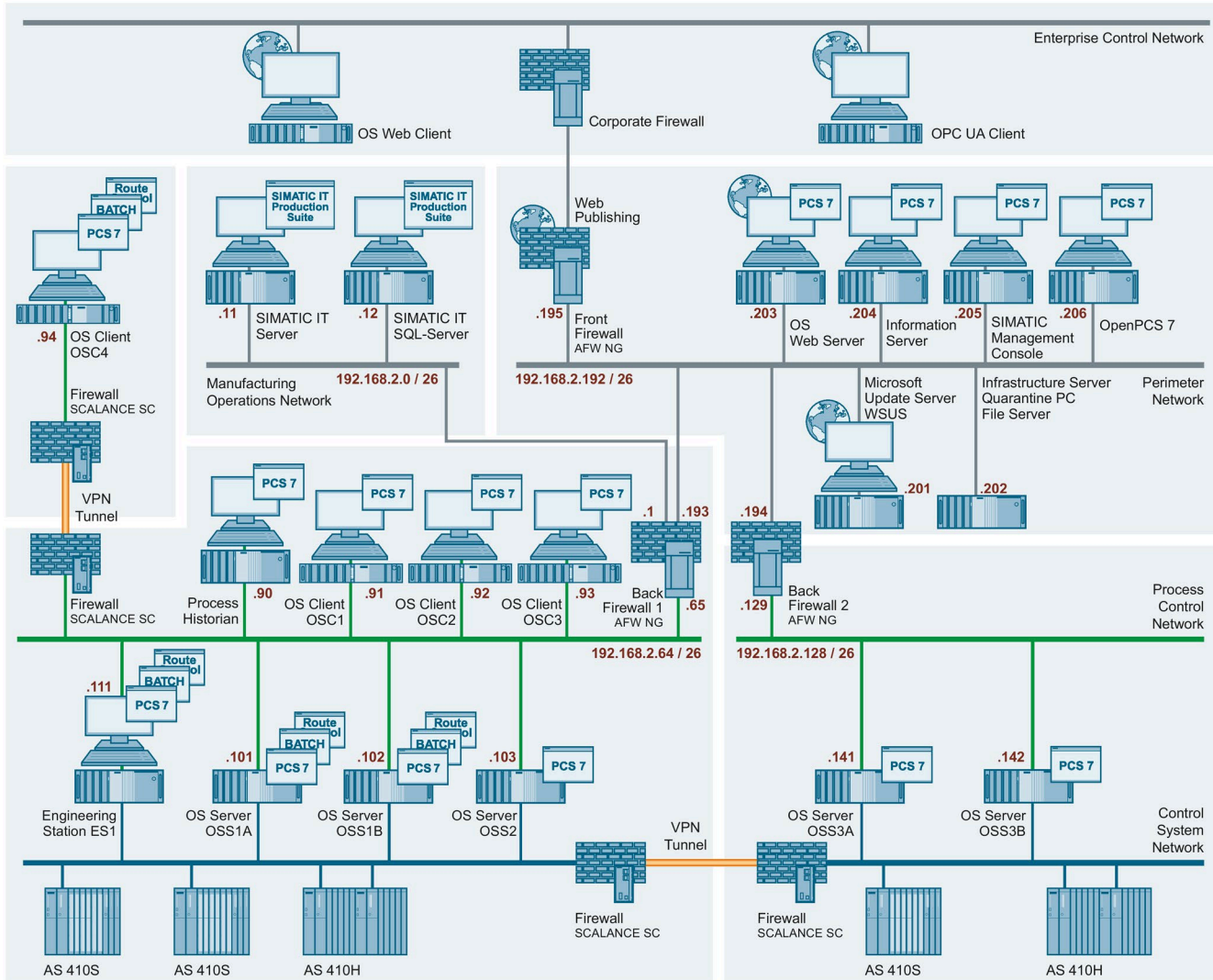
The necessary firewall rules will be formulated neutrally in the remainder of the document.

You can find the complete range of products for Automation Firewall Next Generation in the PCS 7 Add-on catalog. You can download this catalog from the SIMATIC PCS 7 website (<https://w3.siemens.com/mcems/process-control-systems/en/simatic-pcs-7/Pages/simatic-pcs-7.aspx>).

Information for more support for this product can be found under "Automation Firewall Next Generation" (<https://support.industry.siemens.com/cs/ww/en/sc/4984>).

5.5.3 Example configuration: Access rules

In the example configuration, the access points to the four security cells (DCS1, DCS2, MON and Perimeter) are protected by firewalls. The result is a front-end/back-end firewall solution (with two back-end firewalls).



Data exchange between the different security cells is required to ensure unrestricted operation of the system. To ensure this data exchange, corresponding access rules must be stored in the firewalls that serve as an access point to the security cells.

The table below lists the necessary data exchange across security cells:

Security cell	Security cell	Via	Purpose
Perimeter	DCS1	Back-end firewall 1	<ul style="list-style-type: none"> • Distribution of Windows updates (security patches and critical patches) via WSUS to all computers within the PCN1 • Distribution of virus signature files via VSCAN to all computers within PCN1 and status of virus scan clients • Communication between PCS7WEBSRV1 and OSS1A/B, OSS2 and ES1 • File transfer from ES1 to quarantine station / File Server • Communication between OpenPCS 7 and OSS1A/B, OSS2 and ES1 • Communication between PH and IS • Communication between SMMC and the plant computers
Perimeter	DCS2	Back-end firewall 2	<ul style="list-style-type: none"> • Distribution of Windows updates via WSUS to all computers within PCN2 • Distribution of virus signature files via VSCAN to all computers within PCN2 and status of virus scan clients • Communication between PCS7WEBSRV1 and OSS3A/B • Communication between OpenPCS 7 and OSS3A/B • Communication between PH and IS • Communication between SMMC and the plant computers
Perimeter	MON	Back-end firewall 1	<ul style="list-style-type: none"> • Distribution of Windows updates via WSUS to all computers within the MON • Distribution of virus signature files via VSCAN to all computers within PCN2
MON	DCS1	Back-end firewall 1	Communication between the SIMATIC IT servers and OSS1A/B and OSS2
DCS1	DCS2	Back-end firewalls 1 and 2	<ul style="list-style-type: none"> • Communication between OSS3A/B in PCN2 and the OS clients in PCN1 • Communication between OSS3A/B in PCN2 and the ES1 in PCN1

5.5 Access points to the security cells

Based on the table above, the following access rules apply to back-end firewalls 1 and 2:

- Example configuration: Access rules for back-end firewall 1

Name	Action	Protocols	From	To
PCN1 to Perimeter WSUS #1	Allow	HTTPS (alternatively: Port 8531)	[All] [192.168.2.64/26]	[WSUS] [192.168.2.201]
Perimeter IS to PCN1 PH Server #1	Allow	IPSec ¹	[IS] [192.168.2.zz]	[PH Server PCN1] [192.168.2.aa]
Perimeter SMMC to PCN1 PCS 7 Systems #1	Allow	IPSec ¹	[PCN1 Network] [SMMC] [192.168.2.yy]	[SMMC] [192.168.2.yy] [PCN1 Network]
PCN1 ES to Perimeter OpenPCS 7 #1	Allow	IPSec ¹	[ES] [192.168.2.111] [OpenPCS 7] [192.168.2.xx]	[ES] [192.168.2.111] [OpenPCS 7] [192.168.2.xx]
PCN1 OS Server to Perimeter OpenPCS 7 #1	Allow	IPSec ¹	[OS Server] [192.168.2.101, 192.168.2.102] [192.168.2.103]	[OpenPCS 7] [192.168.2.xx]
Perimeter OpenPCS 7 to PCN1 OS Server #1	Allow	IPSec ¹	[OpenPCS 7] [192.168.2.xx]	[OS Server] [192.168.2.101, 192.168.2.102] [192.168.2.103]
PCN1 ES to Perimeter OS Web Server #1	Allow	IPSec ¹	[ES] [192.168.2.111] [OS Web Server] [192.168.2.203]	[ES] [192.168.2.111] [OS Web Server] [192.168.2.203]
PCN1 OS Server to Perimeter OS Web Server #1	Allow	IPSec ¹	[OS Server] [192.168.2.101, 192.168.2.102] [192.168.2.103]	[OS Web Server] [192.168.2.203]
Perimeter OS Web Server to PCN1 OS Server #1	Allow	IPSec ¹	[OS Web Server] [192.168.2.203]	[OS Server] [192.168.2.101, 192.168.2.102] [192.168.2.103]
Bidirectional Ping between Perimeter and PCN1 #1	Allow	ICMP/Ping	Perimeter PCN1	Perimeter PCN1
PCN1 ES to Perimeter Quarantine Station ²	Allow	TCP/445 ²	[ES] [192.168.2.111]	[Quarantine Station] [192.168.2.202]

¹) The use of the "IPSec" protocol type requires a tunneled and encrypted IPSec connection between the components in the various security cells that conforms to the SIMATIC PCS 7 security concept.

For SIMATIC PCS 7, it is possible to activate the encrypted communication in the SIMATIC Shell. The configured port must then also be opened in the back-end firewall with the TCP/UDP protocols.

Moreover, SQL database communication between the ES and systems in other subnets (for example, the Perimeter network) must be allowed.

In addition, the bidirectional communication for Windows data transfer (using drive shares) and ICMP/ping between the SIMATIC PCS 7 systems involved must be enabled in this case.

If there is no possibility to configure such tunneled and encrypted connections, an "All outbound traffic" firewall rule must be configured bidirectionally in each case. Dedicated port filtering is not used in this case. This configuration can have advantages when a firewall with application-specific analysis and IDS (Intrusion Detection System) functionalities is used (for example, Automation Firewall Next Generation), because it enables a detailed check of the data traffic.

Moreover, the Multicast Proxy Configuration in the SIMATIC Shell must be taken into account.

The configuration of these rules is thus dependent on the requirements of the project, the firewall options and the anticipated risks.

²) Alternatively, an FTPS server can be set up on the quarantine station (see the section "Quarantine station as data exchange point" for more information).

- Example configuration: Access rules for back-end firewall 2

Name	Action	Protocols	From	To
PCN2 to Perimeter WSUS #1	Allow	HTTPS (alternatively: Port 8531)	[All] [192.168.2.128/26]	[WSUS] [192.168.2.201]
Perimeter SMMC to PCN2 PCS 7 Systems #1	Allow	IPSec ¹	[PCN2 Network] [SMMC] [192.168.2.yy]	[SMMC] [192.168.2.yy] [PCN2 Network]
PCN2 OS Server to Perimeter OpenPCS 7 #1	Allow	IPSec ¹	[OS Server] [192.168.2.141, 192.168.2.142]	[OpenPCS 7] [192.168.2.xx]
Perimeter OpenPCS 7 to PCN2 OS Server #1	Allow	IPSec ¹	[OpenPCS 7] [192.168.2.xx]	[OS Server] [192.168.2.141, 192.168.2.142]
PCN2 OS Server to Perimeter OS Web Server #1	Allow	IPSec ¹	[OS Server] [192.168.2.141, 192.168.2.142]	[OS Web Server] [192.168.2.203]
Perimeter OS Web Server to PCN2 OS Server #1	Allow	IPSec ¹	[OS Web Server] [192.168.2.203]	[OS Server] [192.168.2.141, 192.168.2.142]
Bidirectional Ping between Perimeter and PCN2 #1	Allow	ICMP/Ping	Perimeter PCN ²	Perimeter PCN2

¹) The use of the "IPSec" protocol type requires a tunneled and encrypted IPSec connection between the components in the various security cells that conforms to the SIMATIC PCS 7 security concept.
For SIMATIC PCS 7, it is possible to activate the encrypted communication in the SIMATIC Shell. The configured port must then also be opened in the back-end firewall with the TCP/UDP protocols.
In addition, the bidirectional communication for Windows data transfer (using drive shares) and ICMP/ping between the SIMATIC PCS 7 systems involved must be enabled in this case.
Moreover, SQL database communication between the ES and systems in other subnets (for example, the Perimeter network) must be allowed. If there is no possibility to configure such tunneled and encrypted connections, an "All outbound traffic" firewall rule must be configured bidirectionally in each case. Dedicated port filtering is not used in this case. This configuration can have advantages when a firewall with application-specific analysis and IDS (Intrusion Detection System) functionalities is used (for example, Automation Firewall Next Generation), because it enables a detailed check of the data traffic.
Moreover, the Multicast Proxy Configuration in the SIMATIC Shell must be taken into account.
The configuration of these rules is thus dependent on the requirements of the project, the firewall options and the anticipated risks.

²) Alternatively, an FTPS server can be set up on the quarantine station (see the section "Quarantine station as data exchange point" for more information).

5.5 Access points to the security cells

The example configuration contains only one engineering station in security cell DCS1, which is also used for configuring the OS servers OSS3A and OSS3B. To enable configuring in this case, especially the OS loading, you must configure the following access rules on the back-end firewalls 1 and 2:

Name	Action	Protocols	From	To
PCN2 OS Server to PCN1 ES Engineering Station #1	Allow	IPSec ¹	[OS Server] [192.168.2.141, 192.168.2.142]	[ES Engineering Station] [192.168.2.111]
PCN ES Engineering Station to PCN2 OS Server #1	Allow	IPSec ¹	[ES Engineering Station] [192.168.2.111]	[OS Server] [192.168.2.141, 192.168.2.142]

¹⁾ The use of the "IPSec" protocol type requires a tunneled and encrypted IPSec connection between the components in the various security cells that conforms to the SIMATIC PCS 7 security concept. For SIMATIC PCS 7, it is possible to activate the encrypted communication in the SIMATIC Shell. The configured port must then also be opened in the back-end firewall with the TCP/UDP protocols. In addition, the bidirectional communication for Windows data transfer (using drive shares) and ICMP/ping between the SIMATIC PCS 7 systems involved must be enabled in this case. Moreover, SQL database communication between the ES and systems in other subnets (for example, the Perimeter network) must be allowed. If there is no possibility to configure such tunneled and encrypted connections, an "All outbound traffic" firewall rule must be configured bidirectionally in each case. Dedicated port filtering is not used in this case. This configuration can have advantages when a firewall with application-specific analysis and IDS (Intrusion Detection System) functionalities is used (for example, Automation Firewall Next Generation), because it enables a detailed check of the data traffic. Moreover, the Multicast Proxy Configuration in the SIMATIC Shell must be taken into account. The configuration of these rules is thus dependent on the requirements of the project, the firewall options and the anticipated risks.

Operator control and monitoring of the OS servers OSS3A and OSS3B in the DCS2 from the OS clients in the DCS1 should also be possible. To ensure this, you must configure the following access rules on the back-end firewalls 1 and 2:

Name	Action	Protocols	From	To
PCN2 OS Server to PCN1 OS Client #1	Allow	IPSec ¹	[OS Server] [192.168.2.141, 192.168.2.142]	[OS Client] [192.168.2.91]
PCN2 OS Server to PCN1 OS Client #2	Allow	IPSec ¹	[OS Server] [192.168.2.141, 192.168.2.142]	[OS Client] [192.168.2.92]
PCN2 OS Server to PCN1 OS Client #3	Allow	IPSec ¹	[OS Server] [192.168.2.141, 192.168.2.142]	[OS Client] [192.168.2.93]
PCN2 OS Server to PCN1 OS Client #4	Allow	IPSec ¹	[OS Server] [192.168.2.141, 192.168.2.142]	[OS Client] [192.168.2.94]
PCN1 OS Client to PCN2 OS Server #1	Allow	IPSec ¹	[OS Client] [192.168.2.91]	[OS Server] [192.168.2.141, 192.168.2.142]
PCN1 OS Client to PCN2 OS Server #2	Allow	IPSec ¹	[OS Client] [192.168.2.92]	[OS Server] [192.168.2.141, 192.168.2.142]
PCN1 OS Client to PCN2 OS Server #3	Allow	IPSec ¹	[OS Client] [192.168.2.93]	[OS Server] [192.168.2.141, 192.168.2.142]

Name	Action	Protocols	From	To
PCN1 OS Client to PCN2 OS Server #4	Allow	IPSec ¹	[OS Client] [192.168.2.94]	[OS Server] [192.168.2.141, 192.168.2.142]
PCN2 OS Server to PCN1 PH	Allow	IPSec ¹	[OS Server] [192.168.2.141, 192.168.2.142]	[PH Server] [192.168.2.90]
PCN1 PH to PCN2 OS Server	Allow	IPSec ¹	[PH Server] [192.168.2.90]	[OS Server] [192.168.2.141, 192.168.2.142]

¹⁾ The use of the "IPSec" protocol type requires a tunneled and encrypted IPSec connection between the components in the various security cells that conforms to the SIMATIC PCS 7 security concept. For SIMATIC PCS 7, it is possible to activate the encrypted communication in the SIMATIC Shell. The configured port must then also be opened in the back-end firewall with the TCP/UDP protocols. In addition, the bidirectional communication for Windows data transfer (using drive shares) and ICMP/ping between the SIMATIC PCS 7 systems involved must be enabled in this case. Moreover, SQL database communication between the ES and systems in other subnets (for example, the Perimeter network) must be allowed. If there is no possibility to configure such tunneled and encrypted connections, an "All outbound traffic" firewall rule must be configured bidirectionally in each case. Dedicated port filtering is not used in this case. This configuration can have advantages when a firewall with application-specific analysis and IDS (Intrusion Detection System) functionalities is used (for example, Automation Firewall Next Generation), because it enables a detailed check of the data traffic. Moreover, the Multicast Proxy Configuration in the SIMATIC Shell must be taken into account. The configuration of these rules is thus dependent on the requirements of the project, the firewall options and the anticipated risks.

Note

In the various networks (PCN1, PCN2, Perimeter, MON), dedicated routing entries to the other subnets in each case must be configured on the two back-end firewalls.

For simplification, the assigned back-end firewalls can be configured as the default gateway on the terminal devices.

Note

Setup of an Active Directory (Windows domain) is recommended from a security perspective. In this case, other protocols and ports may need to be configured on the firewalls to enable communication between the domain controllers as well as communication of domain members with the domain controllers.

You can find additional information under the following link "Active Directory and Active Directory Domain Services Port Requirements" (<https://technet.microsoft.com/en-us/library/8daead2d-35c1-4b58-b123-d32a26b1f1dd>)

5.5.4 Example configuration: Securing the PCS 7 Web server on the front-end firewall

For access to a PCS 7 Web server in the Perimeter network by PCS 7 Web clients from an external network, two functions of the Automation Firewall NG (AFW NG) have to be used:

1. Hiding the IP address of the PCS 7 Web server (DNAT)

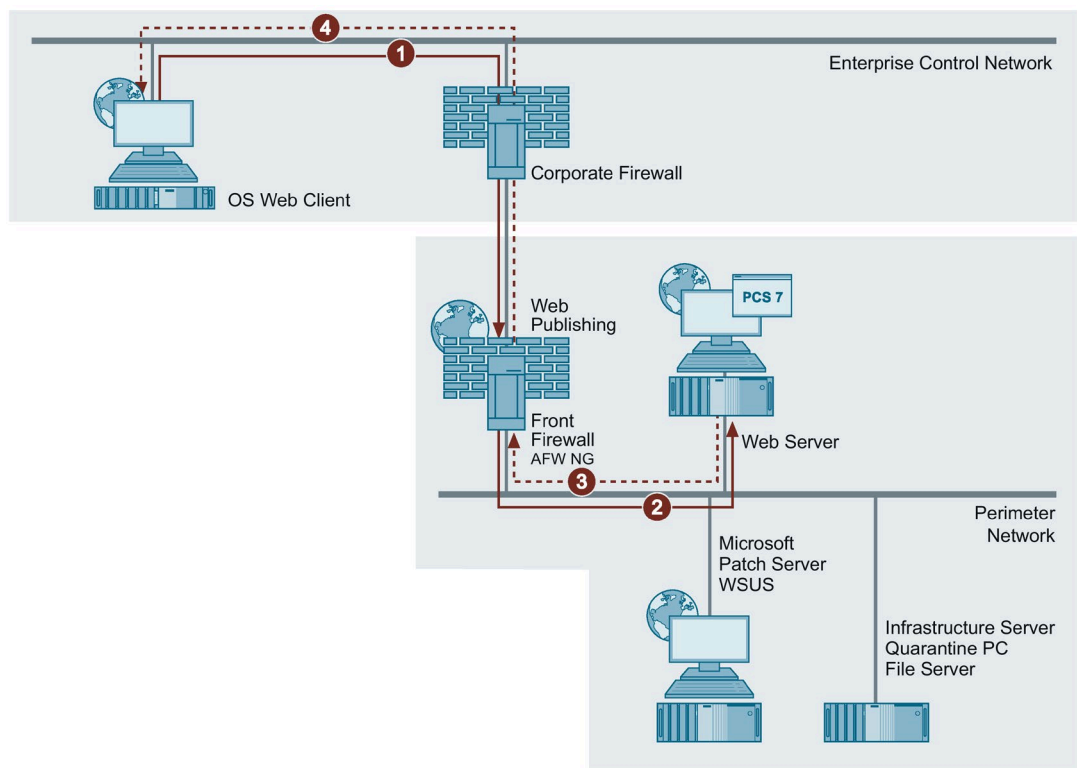
For access to the PCS 7 Web server from an external network, a destination NAT rule must be created on the AFW NG. This means the PCS 7 Web client does not access the IP address of the PCS 7 Web server directly but uses the external interface of the AFW NG (1). An address conversion to the address of the PCS 7 Web server is performed here (2). Thus, the internal address of the PCS 7 Web server remains hidden from the client user. The analyzed data traffic is made available to the PCS 7 Web client in the reverse order (3,4).

2. Deep Packet Inspection (DPI)

The incoming data traffic is analyzed by means of the safety functions of the AFW NG. To that end, the rules for Threat Detection, Antivirus, Antispyware and File Blocking must be activated. By using SSL Inbound Inspection, even encrypted HTTPS data traffic can be analyzed at the AFW NG and using the aforementioned protective mechanisms, analyzed and, if required, blocked.

Note

This recommendation for firewall configuration (DNAT with DPI) for access to the PCS 7 Web server or to other SIMATIC PCS 7 systems within the Perimeter network is referred to as "Web Publishing" in all network configuration overviews in this document.

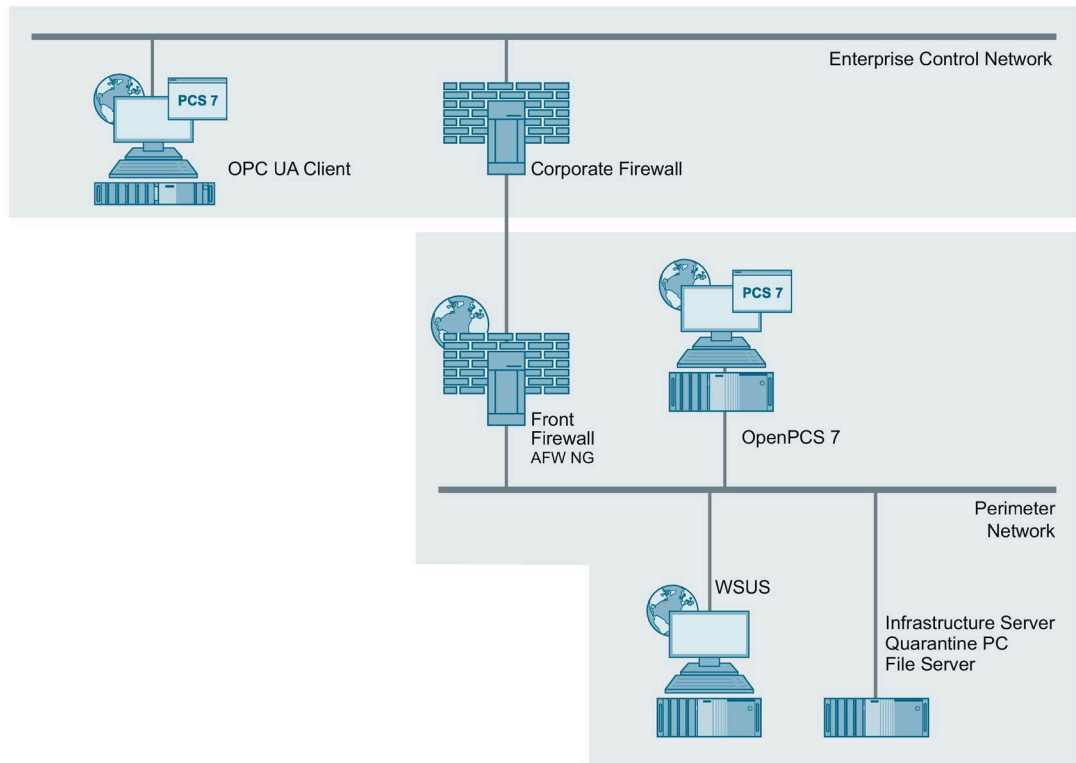


Only HTTPS should be permitted between the PCS 7 Web client in the external network and the Automation Firewall Next Generation. In this way, the authenticity of AFW NG can be guaranteed via a server certificate and communication between the PCS 7 Web client, firewall and PCS 7 Web server can be encrypted, thereby protecting it against manipulation and sniffing.

Note

The steps for configuring the PCS 7 Web server and the settings of the PCS 7 Web client are described in the manual "SIMATIC Process Control System PCS 7 Web Option" (<https://support.industry.siemens.com/cs/de/en/view/109794376>).

5.5.5 Example configuration: Access to the OpenPCS 7 server in the perimeter network



The OpenPCS 7 server allows access to the plant over defined OPC interfaces. The (local Windows) firewall must be configured so that only authorized systems can access the OpenPCS 7 server. The OPC clients must be also protected by a comprehensive defense-in-depth concept.

OPC access must be limited to the plant units necessary to meet the requirements. The risk caused by the access has to be evaluated. Critical plant units, such as safety-instrumented systems (SIS), should not be accessible from outside the plant (e.g. from the ECN).

Note

The steps for configuring the OpenPCS 7 server are listed in the manual "SIMATIC Process Control System PCS 7 OpenPCS 7"

(<https://support.industry.siemens.com/cs/de/en/view/109794368>).

Note

The use of encrypted and digitally signed OPC UA communication is recommended between the OPC client and the OPC server (OpenPCS 7). By adaptation of the OpenPCS 7 XML configuration file, it is possible to bring about a situation that only this type of secure communication is permitted between OPC UA client and OPC UA server.

The OPC UA client must support the algorithms that are configured in this process for communication to take place.

The description of this configuration can be found under "How do I configure OpenPCS 7 for secure communication with an OPC UA client?"

<https://support.industry.siemens.com/cs/de/en/view/109799626>

5.5.6 Example configuration: Securing the PCS 7 Web server at the back-end firewall

To reach the PCS 7 Web server located in the Perimeter network from another internal network, e.g. from the Manufacturing Operations Network (MON), via a PCS 7 Web client, access to the PCS 7 Web server must be secured via the back-end firewall 1.

In this context, see the recommended configuration in section 5.5.4, "Example configuration: Securing the PCS 7 Web server at the front-end firewall" (Page 42).

5.5.7 Example configuration: Securing the PCS 7 IS server at the front-end firewall

For accessing IS Web clients from an external network to the IS Web server in the Perimeter network, the Web server must be published over the front-end firewall.

To reach the PCS 7 IS server located in the Perimeter network from an external network, for example, from the Enterprise Control Network (ECN), via an IS Web client, access to the IS Web server must be secured via the front-end firewall.

In this context, see the recommended configuration in section 5.5.4, "Example configuration: Securing the PCS 7 Web server at the front-end firewall" (Page 42).

5.5.8 Network Intrusion Prevention / Network Intrusion Detection System

An intrusion detection or intrusion prevention system (IDS/IPS) is an essential part of a modern, secure Web gateway.

The PAN-OS operating system used in the Automation Firewall Next Generation contains a high-performance IDS/IPS solution that is designed to detect and prevent attacks on operating systems, networks and applications. It has the functionalities Antivirus, Anti Spyware, Vulnerability Protection, URL-Filtering, File Blocking, Data Filtering, DoS Protection and Wildfire, some of which must be purchased additionally as service subscriptions.

The IDS/IPS of the Automation Firewall Next Generation provides protection from known attacks with a deep level network protocol inspection. Each data packet is analyzed for protocol status, structure and content of the message. The system checks the received data packet after it has been checked by the firewall policy and any assigned Web or application filters.

To keep the detection rates as high as possible, the AFW NG must be automatically provided with pattern updates.

5.6 Secure communication between security cells

In many cases, data exchange between components located in different security cells is required for operation of a plant. The following variants have to be differentiated here:

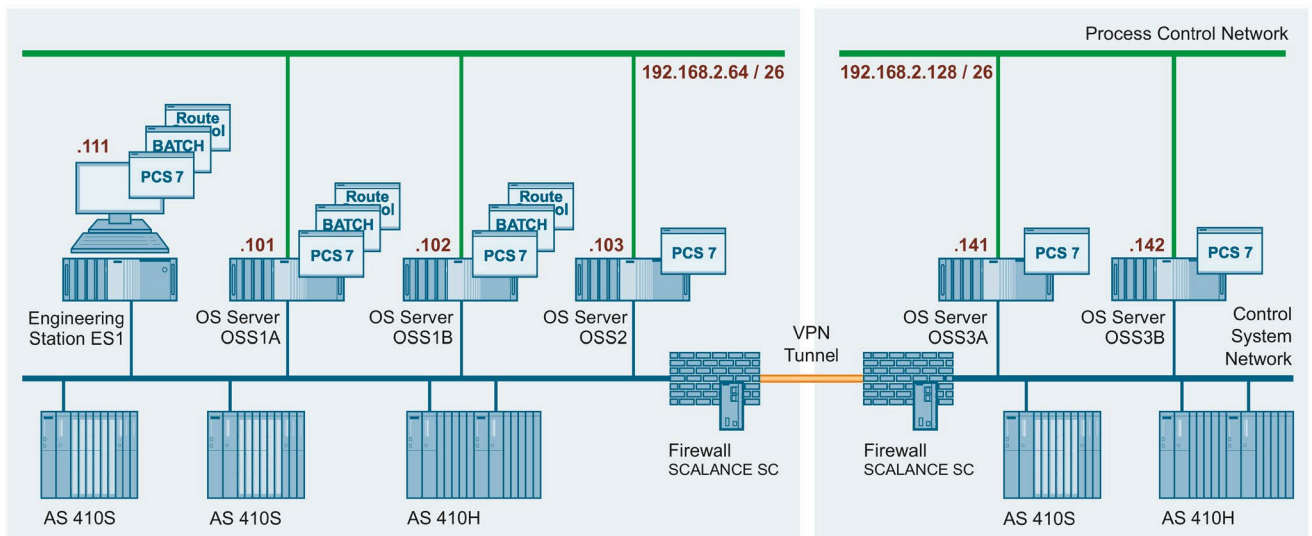
- Data exchange on the CSN level
Data exchange between automation systems in different security cells
- Data exchange on the PCN level
Data exchange for operating and monitoring with remote OS clients, which means OS clients located in other security cells than the corresponding OS server(s).

5.6.1 Data exchange between automation systems

5.6.1.1 Introduction

The data exchange between automation systems in different security cells should be performed via VPN connection (for example, OpenVPN). This communication can be established using two SCALANCE SC security modules.

The following figure shows the structure of automation systems in different security cells and the resulting communication options between these systems:



SCALANCE SC modules allow the tunneling of communication using the OpenVPN protocol. This technique is used here to interconnect the two protected internal networks via secure data connection through the (possibly) insecure external network. This enables automation systems to communicate with one another across security cells through a secure connection.

The data exchange of the devices via the OpenVPN tunnel in the VPN has the following properties as a result:

- The exchanged data are interception-proof so that the confidentiality of the data is secured.
- The exchanged data are tamper-proof, which secures the integrity of the data.
- Authenticity

Note

The most recent firmware, but at least version V2.2, must always be installed on the SCALANCE SC modules.

„Firmware Update V2.2 for SCALANCE SC622-2C, SC632-2C, SC636-2C, SC642-2C and SC646-2C" (<https://support.industry.siemens.com/cs/ww/en/view/109802584>)

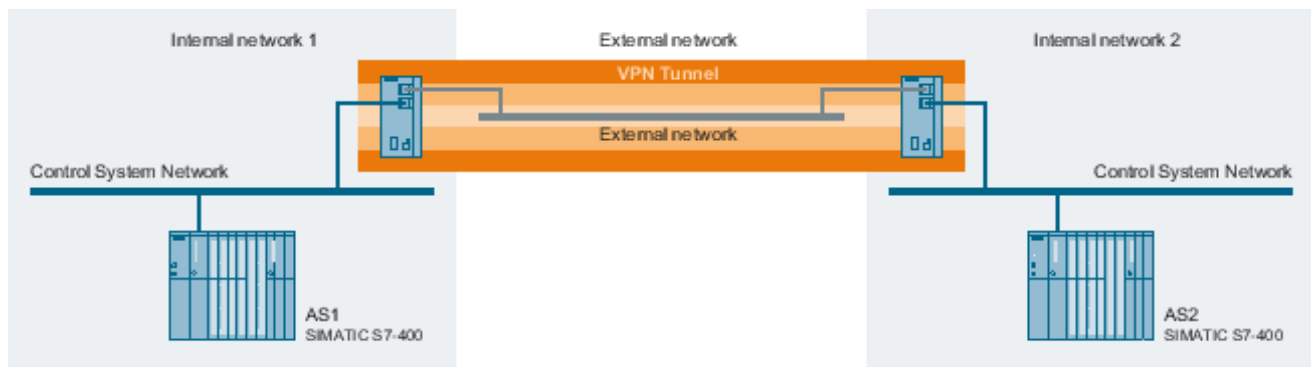
You can find additional information on SCALANCE SC in the manual "SIMATIC NET Industrial Ethernet Security Basics and Application" (<https://support.industry.siemens.com/cs/ww/en/view/109747342>) and in the manual "SIMATIC NET: Industrial Ethernet Security SCALANCE SC-600 Web Based Management (WBM)" (<https://support.industry.siemens.com/cs/ww/en/view/109754815>)".

5.6.1.2 Establishing secure communication between security cells with SCALANCE SC

Introduction

In this example configuration, the tunnel function is configured in the "Default mode" configuration view. In this example, SCALANCE SC Module 1 and SCALANCE SC Module 2 form the two endpoints of the tunnel for the secured tunnel connection.

The following figure shows an example of a VPN tunnel (OpenVPN tunnel with two SCALANCE SC modules):



It is a requirement of the L2 bridge configuration performed in the following documents that the same IP subnet is used in the internal network 1 and 2. No further configuration is necessary in any of the networks involved in the communication between these two networks, for example, no routing must be defined, or gateway set up. Communication between the internal networks is fully transparent for all network participants.

In a more advanced configuration, users can define firewall rules on the SCALANCE SC modules which limit communication to selected participants, protocols and ports.

For configuring the SCALANCE SC modules, proceed as described in one of the following articles.

Configuring with the TIA portal

(<https://support.industry.siemens.com/cs/de/en/view/109792357>)

Configuring with the SCT tool

(<https://support.industry.siemens.com/cs/ww/en/view/109792637>)

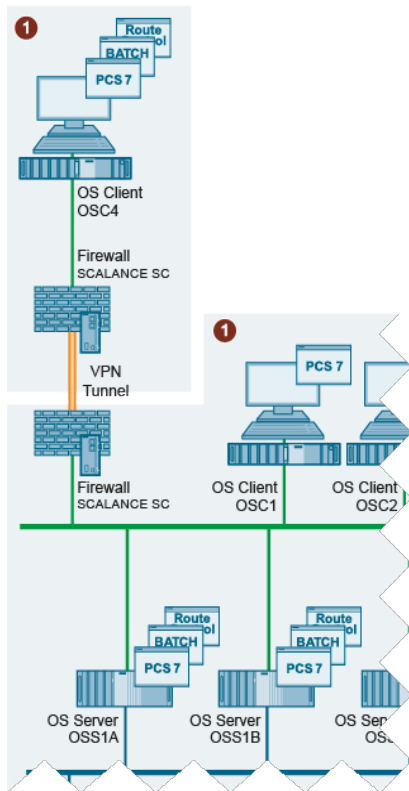
5.6.2 Operation and observation with remote OS clients

Remote, but trusted process control OS clients without direct process interface are integrated via encrypted and authenticated communication into the security cell.

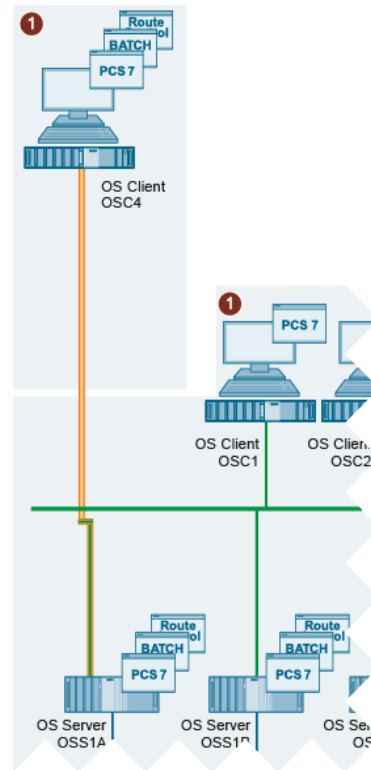
Such encrypted communication can, on the one hand, be established by means of two SCALANCE SC security modules, as shown and described in the previous section (see variant 1 in the figure below). On the other hand, such encrypted communication can also be configured directly on the relevant PCS 7 OS stations (see variant 2 in the figure below). This configuration is described in the following.

5.6 Secure communication between security cells

Regardless of this, it must be ensured that only authorized personnel are granted access to the remote PCS 7 OS station.



Version 1: Communication with two SCALANCE SC modules



Version 2: Encrypted communication directly from the OS server to the OS client (example)

The two variants shown here differ in two important aspects. One difference is the end point of the encryption. With version 1, the end point is the respective SCALANCE SC security module. With version 2, the end points are, on the one hand, the PCS 7 OS client and, on the other hand, the PCS 7 OS server and the ES on the terminal bus (PCN).

The second major difference is the scope of the encryption. In the first version, the entire communication is encrypted by the encrypted tunnel that exists between the SCALANCE SC security modules. In version 2, only the internal communication between the PCS 7 OS client and PCS 7 OS servers and ES is encrypted. Other possible communication modes, if not supported by the corresponding protocol, are not encrypted in variant 2.

Depending on the result of a risk assessment, a combination of the two variants can also be used. Another alternative would be to use an external firewall between the remote station and the OS servers/ES in the plant to limit the data communication only to the protocols and ports needed for operation.

Encrypted communication

When encrypted communication between PCS 7 OS systems is configured and used, only SIMATIC PCS 7-relevant communication connections for which an identical common Pre Shared Key (PSK) has been specified are established between computers. Only these systems can communicate with one another via PCS 7 mechanisms. The Windows "Security Support Provider Interface" (SSPI) is used for this type of communication. This interface allows authenticated and encrypted communication between the participating PCS 7 OS systems.

A fixed port is set for this communication. This fixed communication port is only used for TCP-based and UDP-based PCS 7 communication between participating SIMATIC PCS 7 systems. This enables a dedicated port filtering of communication through a firewall.

Note

Additional data communication is required between PCS 7 systems for proper operation (e.g. use of file sharing, SQL client/server, ICMP-ping, domain communication, time synchronization) which must be allowed on firewalls.

This additional data communication is not taken into account by the aforementioned SIMATIC PCS 7 function ("Encrypted communication"), that is, not encrypted.

Note

Encrypted communication is to be configured on all PC stations containing the SIMATIC Shell.

If the participating SIMATIC PCS 7 systems are located in different subnets, the so-called multicast proxy configuration must be performed in the SIMATIC Shell.

Proceed for the configuration as described in the "SIMATIC Process Control System PCS 7 - PC Configuration (V9.1)" (<https://support.industry.siemens.com/cs/ww/en/view/109794377>) manual.

Note

If a computer in the system is compromised or is being shut down, the PSK key must be changed on all the other computers.

Note

Migration mode should be disabled again after migration is complete.

You can find information on migration mode in the "SIMATIC Process Control System PCS 7 – PC Configuration (V9.1)" (<https://support.industry.siemens.com/cs/ww/en/view/109794377>) manual.

Note

In SIMATIC PCS 7 V9.1, you must adapt the "MTU Size" when using SIMATIC NET Softnet IE-RNA and encrypted communication (see "PCS 7 Readme" (<https://support.industry.siemens.com/cs/ww/en/view/109780270>)), section 4.14).

5.6.3 Quarantine station as data exchange point

A quarantine station is a central data communication point in a plant.

A quarantine station is used to transfer data (for example, configuration data) of computers of the automation system (preferably the ES) from or to the station. This means the data transfer must always start from computers of the automation system.

Data transfer to external systems or from external systems (for example, in the ECN) to the quarantine station must also always originate at the quarantine station.

The use of a quarantine station can be important when the recommendations relating to system hardening and, here in particular, for blocking all USB ports on PCS 7 stations are implemented (see section "Working with mobile data media (Page 84)").

As a central data communication point, the quarantine station should be especially protected from a security point of view. For this reason, local security measures (for example, firewall, virus scanner, security updates, etc.) must be implemented and configured very strictly, if necessary.

As shown in the example configuration, the quarantine station should be positioned in the Perimeter network. Corresponding rules must be configured in the firewalls to ensure communication between computers in the DCS1 and DCS2 security cells and the quarantine station via the back-end firewall(s) as well as between computers in the ECN and the quarantine station.

5.6.3.1 Required firewall rules

If Automation Firewall Next Generation is used as the back-end firewall, the quarantine station (configured as FTPS server) can be secured at the back-end firewall for the DCS1 and DCS2 security cells (see section 5.5.4 "Sample configuration: Securing the PCS 7 Web server at the front-end firewall") (Page 42).

For the situation in which a firewall is used that does not offer the possibility of securing the FTPS connection, the following tables show the required firewall rules:

- Front-end firewall (NAT between the Perimeter network and ECN is not used)

Name	Action	Protocols	From	To
ECN computer to perimeter quarantine station	Allow	FTPS	IP address of the computer in the office network	IP address of quarantine station in the Perimeter network

If a NAT (Network Address Translation) from the Perimeter network to the ECN is configured on the front-end firewall, a port forwarding rule must be set up:

Name	Action	Protocols	From	To
ECN computer to perimeter quarantine station	Forward	FTPS	IP address of the computer in the office network	IP address of quarantine station in the Perimeter network

The rule on the front-end firewall is only required if FTPS data access from the ECN (Enterprise Control Network) to the quarantine station in the Perimeter network is needed.

- Back-end firewall

Name	Action	Protocols	From	To
PCN 1/2 to perimeter quarantine station	Allow	FTPS	IP address of the computer in PCNx (e.g. ES1)	IP address of quarantine station in the Perimeter network

Note

The use of a NAT is not permitted on the back-end firewall if the PCS 7 communication is performed across it (e.g. PCS 7 Web Server – PCS 7 OS Server).

5.6.3.2 FTPS server configuration

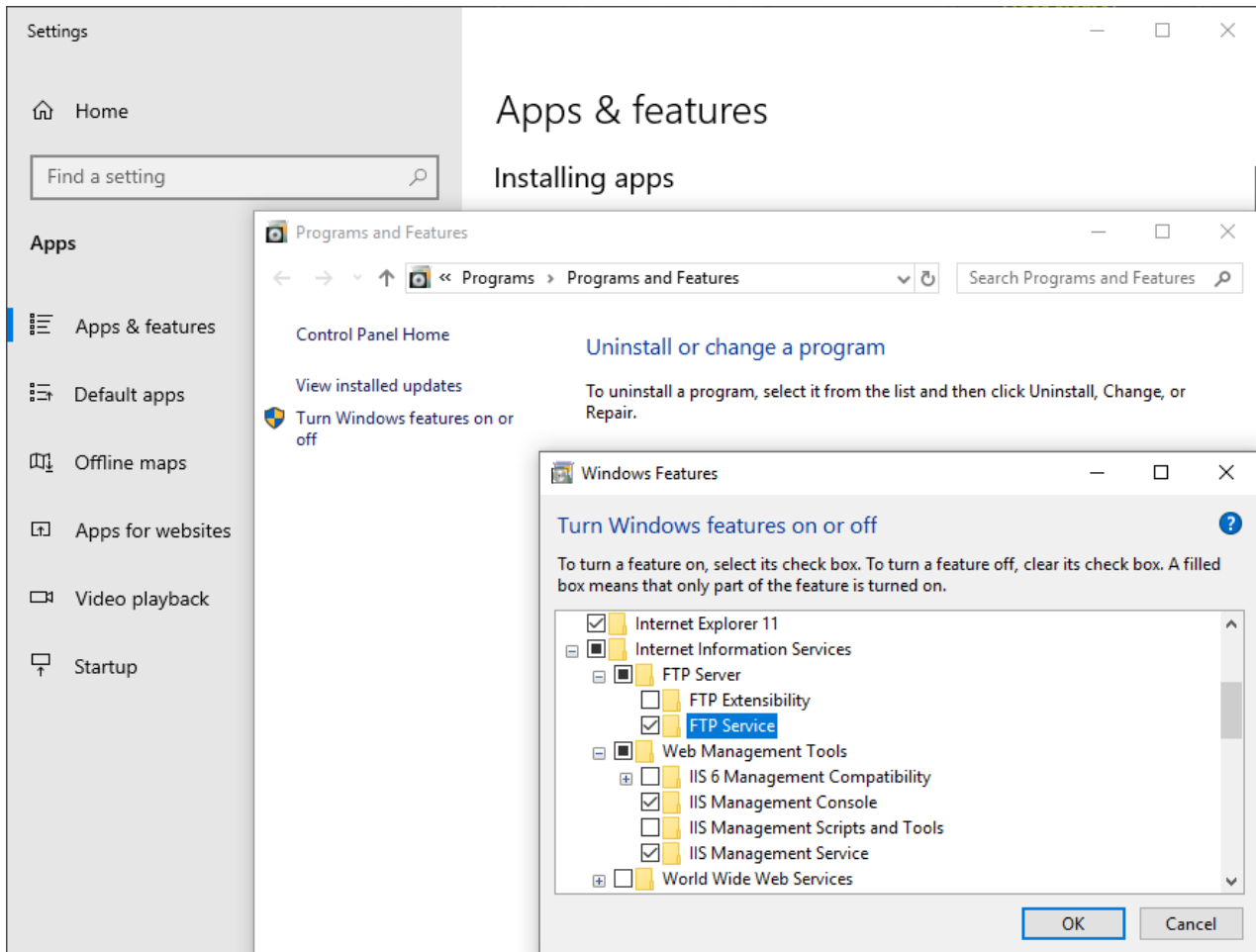
The procedure is described using the example of a "Windows 10" operating system.

Enabling FTP Service

To enable FTP Service on the quarantine station, follow these steps:

1. In the Window Start menu, right-click the "Apps and Features" command from the shortcut menu. The "Apps & feature" dialog is opened.
2. Under "Related Settings", click "Programs and Features".
3. The "Apps & Features" dialog is opened.
4. Click the "Turn Windows features on or off" button.
Enter the administrator password, if required. If you are already logged on as an administrator, confirm the execution of the application.
The "Windows Features" dialog box opens.
5. Enable the "FTP Service" feature in the area "Internet Information Services > FTP Server".

6. Enable the "IIS Management Console" and "IIS Admin Service" features in the "Web Management Tools" area.



7. Click "OK" to apply the changes
The selected features are enabled.

Starting FTP Service

To launch the Microsoft FTP Service, follow these steps:

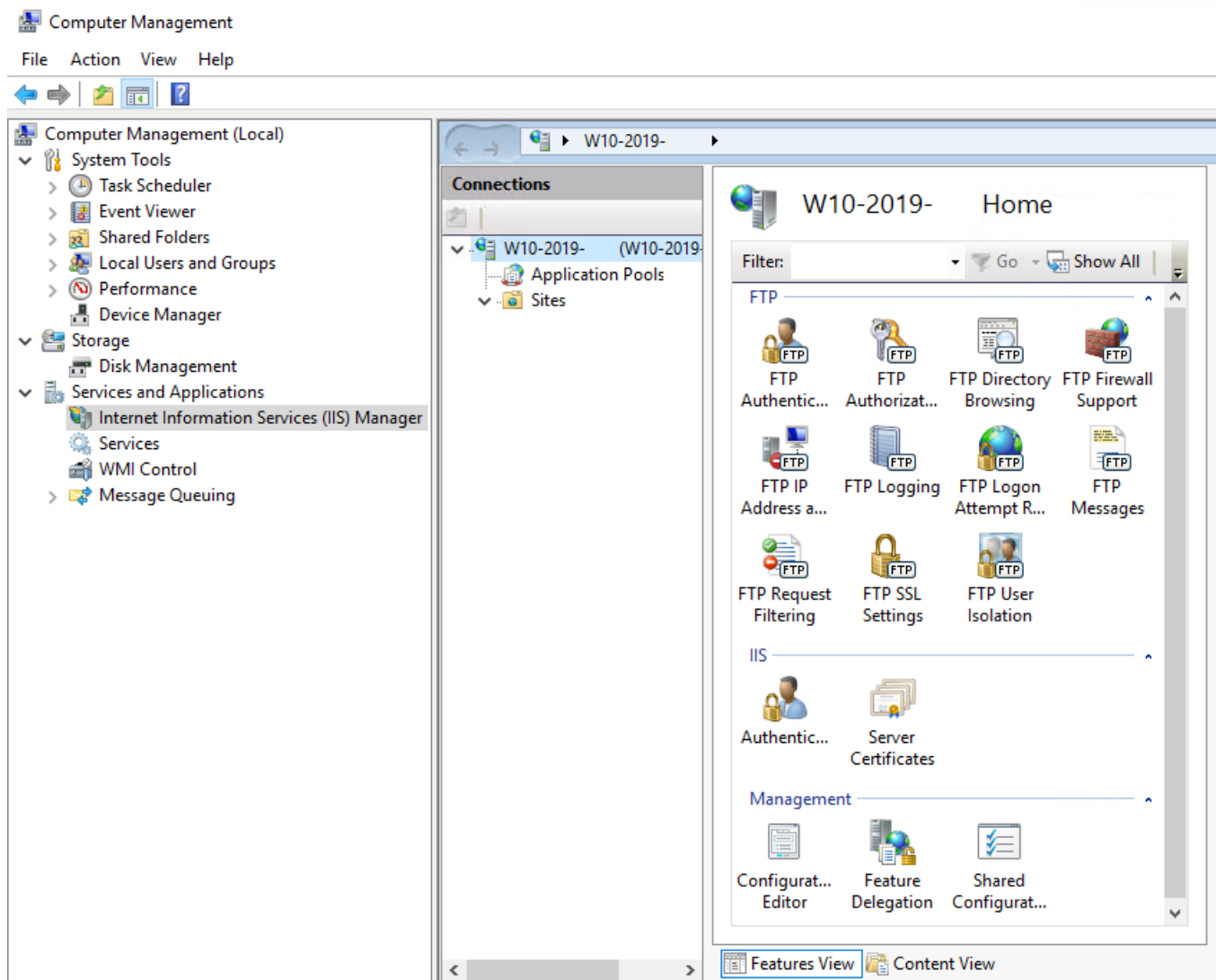
1. In the Window Start menu, right-click on the "Computer Management" command from the shortcut menu.
Enter the administrator password, if required. If you are already logged on as an administrator, confirm the execution of the application.
The "Computer Management" dialog opens.
2. In the navigation pane, select "Services and Applications > Services".
The right pane of the dialog lists all available services .
3. Select "Microsoft FTP Service" and check the following properties:
 - Startup type: Automatic
 - Status: Running

If the property values differ, open the "Properties" dialog from the shortcut menu of the service and change the properties as described above.

Configuring the FTP server

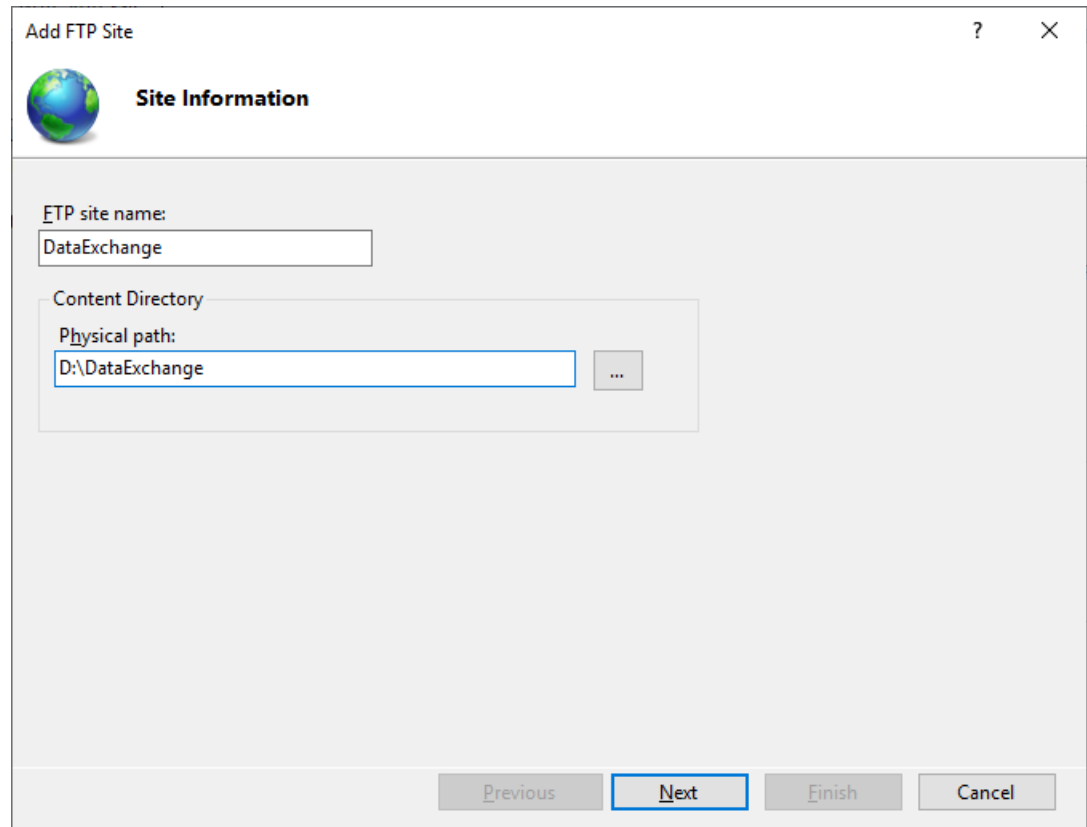
To configure the FTP server, follows these steps:

1. In the Window Start menu, right-click on the "Computer Management" command from the shortcut menu.
Enter the administrator password, if required. If you are already logged on as an administrator, confirm the execution of the application.
The "Computer Management" dialog opens.
2. In the navigation pane, click on the item "Services and Applications > Internet Information Services (IIS) Manager."
The Internet Information Services (IIS) Manager window opens in the right pane of the "Computer Management" dialog.



3. To add an FTP site as the FTP root directory, create a new folder on the data partition (D:\) with the name "Data Exchange" (D:\Data Exchange).

- Right-click on the "Sites" icon. Select the "Add FTP Site" command from the shortcut menu. The "Add FTP Site" dialog opens.
- In the "Add FTP Site" dialog, enter a name for the FTP site and the physical path to the directory you have created (D:\Data Exchange).



- Click "Next".
The "Binding and SSL Settings" dialog opens.

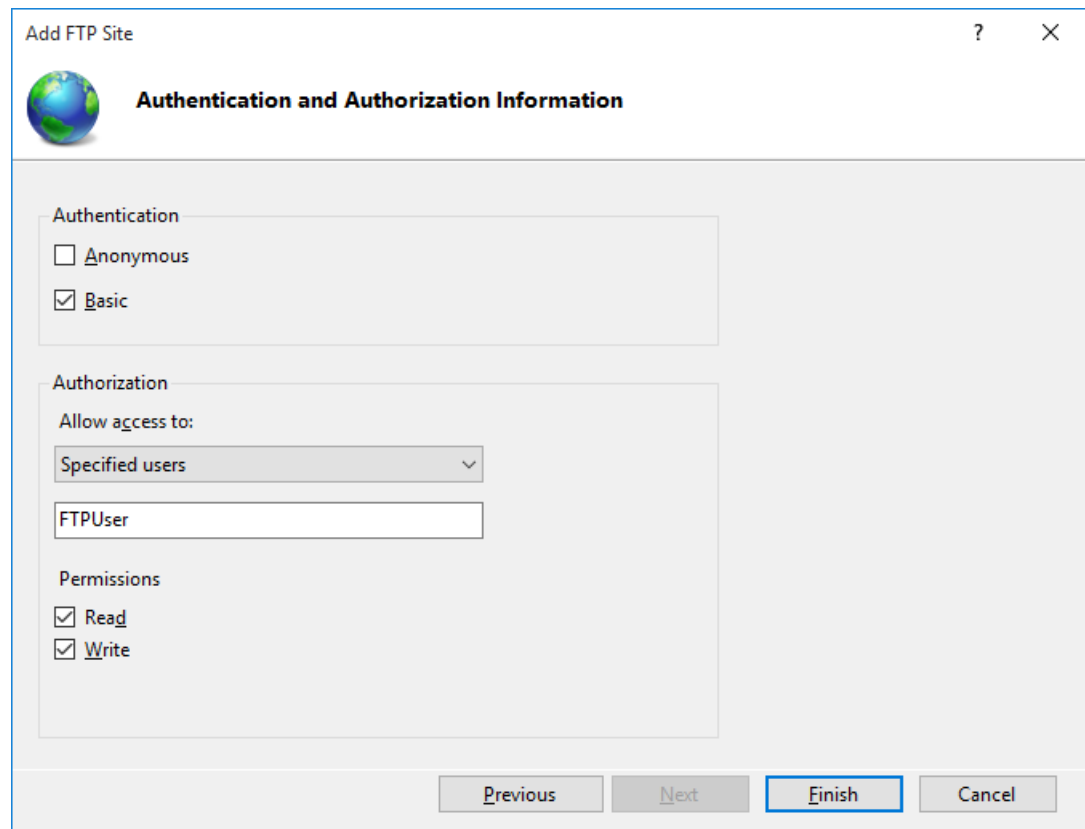
5.6 Secure communication between security cells

7. Make the following settings in the "Binding and SSL Settings" dialog:
 - The "Binding" area, "IP address" box: Select "All Unassigned" in the drop-down list.
 - SSL area: Enable the "SSL" option, and select the certificate generated for the FTPS server from the selection list.

The screenshot shows the "Add FTP Site" dialog box with the "Binding and SSL Settings" tab selected. The "Binding" section includes an "IP Address" dropdown menu set to "All Unassigned" and a "Port" text box containing "21". There is an unchecked checkbox for "Enable Virtual Host Names" and an empty text box for "Virtual Host (example: ftp.contoso.com)". The "Start FTP site automatically" checkbox is checked. The "SSL" section has three radio buttons: "No SSL", "Allow SSL", and "Require SSL", with "Require SSL" selected. Below the radio buttons is an "SSL Certificate" dropdown menu showing a certificate name ending in ".local", and two buttons: "Select..." and "View...". At the bottom of the dialog are four buttons: "Previous", "Next" (highlighted with a blue border), "Finish", and "Cancel".

8. Click "Next".
The "Authentication and Authorization Information" dialog opens.

9. Make the following settings in the "Authentication and Authorization Information" dialog:
 - "Authentication" area: Select the "Standard" check box.
 - "Authorization > Allow access to" area: Select the entry "Specified users" from the drop-down list and enter the authorized users in the box below. The users must have been created in the Windows User Administration beforehand.
 - "Permissions" area: Enable the check boxes "Read" and "Write".



The screenshot shows the "Add FTP Site" dialog box with the "Authentication and Authorization Information" tab selected. The "Authentication" section has the "Basic" checkbox checked. The "Authorization" section has "Allow access to:" set to "Specified users" and "FTPUser" entered in the text box. The "Permissions" section has the "Read" and "Write" checkboxes checked. At the bottom, there are buttons for "Previous", "Next", "Finish", and "Cancel".

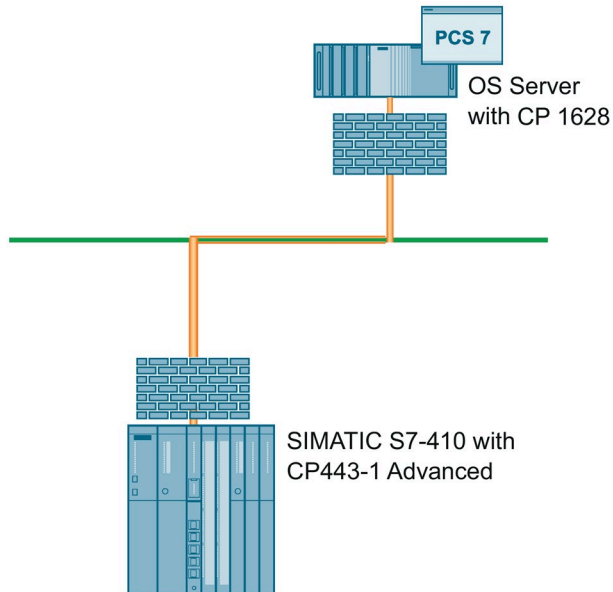
10. Click "Finish" to complete the configuration.

5.6.3.3 Patch management, virus protection and whitelisting

The quarantine station is an "entrance gate" for data to the automation system. Hence, malware can also enter the system via this station. For this reason, this station must be integrated in the patch management and virus protection concept of the system. That is, the quarantine station must be supplied with the latest Windows Updates as quickly as possible. The WSUS server, which is also located in the Perimeter network, can serve as the update source. In addition, a virus scanner must be installed on the quarantine station. The virus scanner and the virus definitions must always have the latest updates installed. This is done through a corresponding server (for example, WSUS), which is also located in the Perimeter network. Whitelisting is an additional protection measure that can also be implemented on the quarantine station (see the corresponding sections of this document).

5.6.4 Secure data exchange between OS and AS stations

In addition to the scenarios in which secure data exchange of systems in different security cells is described, the communication between PCS 7 OS stations and the automation systems (AS) on the system bus (PCN) can also be secured via IPsec. Furthermore, the data exchange configured in this way ensures the integrity of the transmitted data and guarantees the authenticity of the communication partners involved. This requires SIMATIC NET security modules, such as the CP1628 (in the OS station) and CP443-1 Advanced (in the AS rack).



Note

Configuration of secure communication on the system bus is described in section 6.10.

Note

You can find additional information on this configuration in "Industrial Ethernet Security – Security Basics and Application – Configuration Manual" (<https://support.industry.siemens.com/cs/ww/en/view/109747342>) (sections 1.2, 1.8 and 1.9).

Note

The CP1628 module is type-cancelled. Therefore, the use of secured communication using this module is only recommended if it is still in stock. There are no successor or substitute types for this module.

(Announcement of type cancellation for SIMATIC NET Ethernet PC module CP 1628 (<https://support.industry.siemens.com/cs/de/en/view/109793063>))

Note

The component CP443-1 Advanced (GX30) module will not be monitored for security loopholes any longer. This means that it is not now possible to ensure that there will be firmware updates for critical security loopholes.

(Critical limitations to security with the CP 443-1 Advanced (6GK7443-1GX30-0XE0) (<https://support.industry.siemens.com/cs/de/en/view/109799025>))

5.6.5 Using dynamic firewall rules

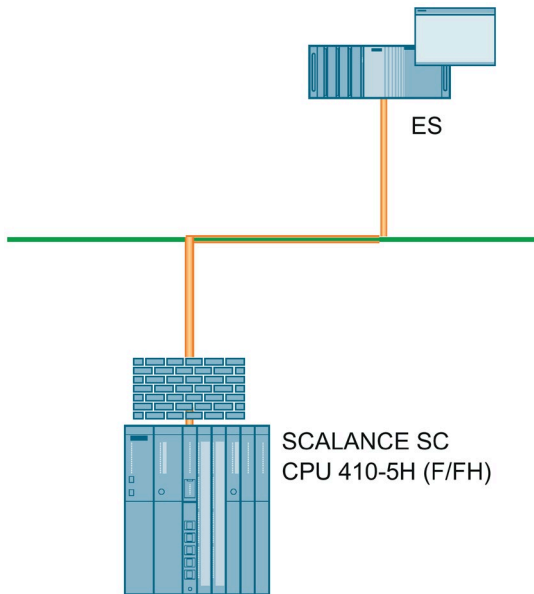
The configuration of dynamic (previously user-specific) firewall rules can be beneficial under enhanced security requirements.

This includes, for example, the use of a common Engineering System (ES) for configuring both normal CPU data as well as safety-relevant data on fail-safe CPUs (F-CPU).

To provide further security when loading security-relevant data to the F-CPU, apart from entering a project password, a firewall can be inserted before such CPUs. This makes it possible to permit loading of the F-CPU only after logon by an authorized engineer with his user name and password at the firewall. This can also be done by a RADIUS based authentication.

5.6 Secure communication between security cells

This logon activates a dynamic set of rules, which permits the loading process between the ES and F-CPU. To that end, a corresponding configuration for the set of rules on the firewall (for example, SCALANCE SC) required for the purpose has to be carried out.



You can find additional information on configuring dynamic firewall sets of rules with the example of a SCALANCE SC module in the manual "SIMATIC NET: Industrial Ethernet Security SCALANCE SC-600 Web Based Management (WBM)" (<https://support.industry.siemens.com/cs/ww/en/view/109754815>).

5.7 Configuration of the SCALANCE X network components

The following should be observed when configuring the network components (e.g. Ethernet switches):

- Disabling non-required ports
- Changing the preconfigured default password
- Disabling non-required protocols, e.g. FTP, TELNET

Note

Read the operating instructions for the corresponding devices for configuring and hardening the SCALANCE X Industrial Ethernet switches.

If you use Ethernet switches from third-party manufacturers to configure the various networks segments, follow the corresponding operating instructions of the third-party manufacturer when configuring these devices.

Note

When configurable network components (e.g. Ethernet switches) that support the "IGMP Snooping" function and the like are used, this function must be disabled for proper operation of SIMATIC PCS 7.

You can find more information and support for the configuration of the measures specified below in the following manuals:

- SIMATIC NET: Industrial Ethernet Switches SCALANCE X-200 Configuration Manual (<https://support.industry.siemens.com/cs/ww/en/view/109757352>)
- SIMATIC NET Industrial Ethernet Switches SCALANCE X-300 / X-400 Configuration Manual (<https://support.industry.siemens.com/cs/ww/en/view/109773473>)
- SIMATIC NET: Industrial Ethernet Switches SCALANCE XB-200/XC-200/XF-200BA/XP-200/XR-300WG Web Based Management Configuration Manual (<https://support.industry.siemens.com/cs/ww/en/view/109799818>)
- SIMATIC NET: Industrial Ethernet switch SCALANCE XM-400/XR-500 Web Based Management (WBM) Configuration Manual (<https://support.industry.siemens.com/cs/ww/en/view/109798663>)

Support for implementing network security in your plant is available from Industrial Security Services. You can find additional information and the corresponding contacts at Industrial Security website (<https://www.siemens.com/industrial-security>).

5.7.1 Disabling non-required ports

Unused ports of the switch that are not required and to which no terminal devices are connected should be disabled.

5.7.2 System password for the switch configuration

On SCALANCE X switches, in the WBM menu "Security" - "Passwords", change the passwords for the users "Admin" and "User" to passwords that conform to the latest version of the security recommendations.

You need to log on as the administrator to change the passwords.

Note

When SCALANCE X switches with current firmware are used, a prompt to set an administrator password appears automatically during initial setup. A customized, secure password must be selected.

5.7.3 Disabling non-required protocols

Access possibilities to the IE switch, among other things, are specified on SCALANCE X switches in the "Agent – Agent Configuration" WBM menu. Furthermore, the network configuration for the IE switch can be defined here.

Specifying protocols

We recommend that you specify only the "HTTPS" protocol for access to the IE switch. To do this, disable all protocols (for example, FTP, TELNET, E-mail) in the "Agent Configuration" dialog and select only the "HTTPS only" protocol.

Note

If the IE switch is to be time-synchronized, the protocol used for that must be enabled (e.g. SNTP or SIMATIC Time).

If PCS 7 Asset Management is used, the SNMP protocol must be enabled.

If a SIEM system is used, the Syslog protocol must be enabled. The events to be taken into consideration can be enabled using the Agent Event configuration.

See also

Managing networks and network services (Page 33)

System hardening

6.1 Overview

Source: <https://www.bsi.bund.de>

The term "hardening" in information security is understood to mean the removal of all software components and functions that are not absolutely necessary to fulfill a given task.

In other words, hardening summarizes all measures and settings with the goal of

- Reducing the opportunities to exploit vulnerabilities in software
- Minimizing potential methods of attack
- Limiting the tools available for a successful attack
- Minimizing the available rights following a successful attack
- Increasing the probability of detecting a successful attack

This is intended to increase local security and the resilience of a computer to withstand attacks.

It follows that a system can be described as "hardened" if:

- The software components and services installed are limited to those that are required for the actual operation
- A restrictive user and rights management is implemented
- The local Windows Firewall is enabled and it is restrictively configured

6.2 Installation of the operating system

The operating system and SIMATIC PCS 7 software are pre-installed on the SIMATIC PCS 7 Industrial Workstation systems (IPC).

Note

When performing a manual installation, you need to comply with the requirements and procedures described in the following documents:

- Manual "SIMATIC Process Control System PCS 7 Readme" (<https://support.industry.siemens.com/cs/ww/en/view/109780270>).
 - Manual "SIMATIC Process Control System PCS 7 PC Configuration" (<https://support.industry.siemens.com/cs/ww/en/view/109794377>)
-

For a SIMATIC PCS 7 computer that fulfills a specific function in an automation system (OS server, OS client, engineering station), certain programs that were installed during installation of the operating system are not required for operation. These programs should be removed.

6.2.1 Disabling services

In accordance with the specifications for hardening a system, unneeded services should be disabled in addition to the software packages that are not required for the operation of a system.

The following services can be disabled for all operating systems supported by SIMATIC PCS 7 V9.1:

- Bluetooth Audio gateway service
- Bluetooth support service
- Bluetooth support service for users
- Diagnostic Service Host
- Diagnostic Policy Service
- Wireless Management service
- Geolocation service
- Performance logs and alerts
- Managers for downloaded cards
- Telephone service
- WalletService
- Windows Media Player network approval service
- Windows Presentation Foundation Font Cache
- Windows service for mobile hotspots
- Windows Color System
- Windows Insider service
- Windows Connect Now - Config Registrar
- Xbox Accessory Management Service
- Xbox Live Authentication Manager
- Xbox Live Network Service
- Saving Xbox Live games
- Payment and NFC/SE manager
- Certificate distribution

Note

If you select the "System hardening" option during installation via the SIMATIC PCS 7 Setup, the services listed are disabled by the installation.

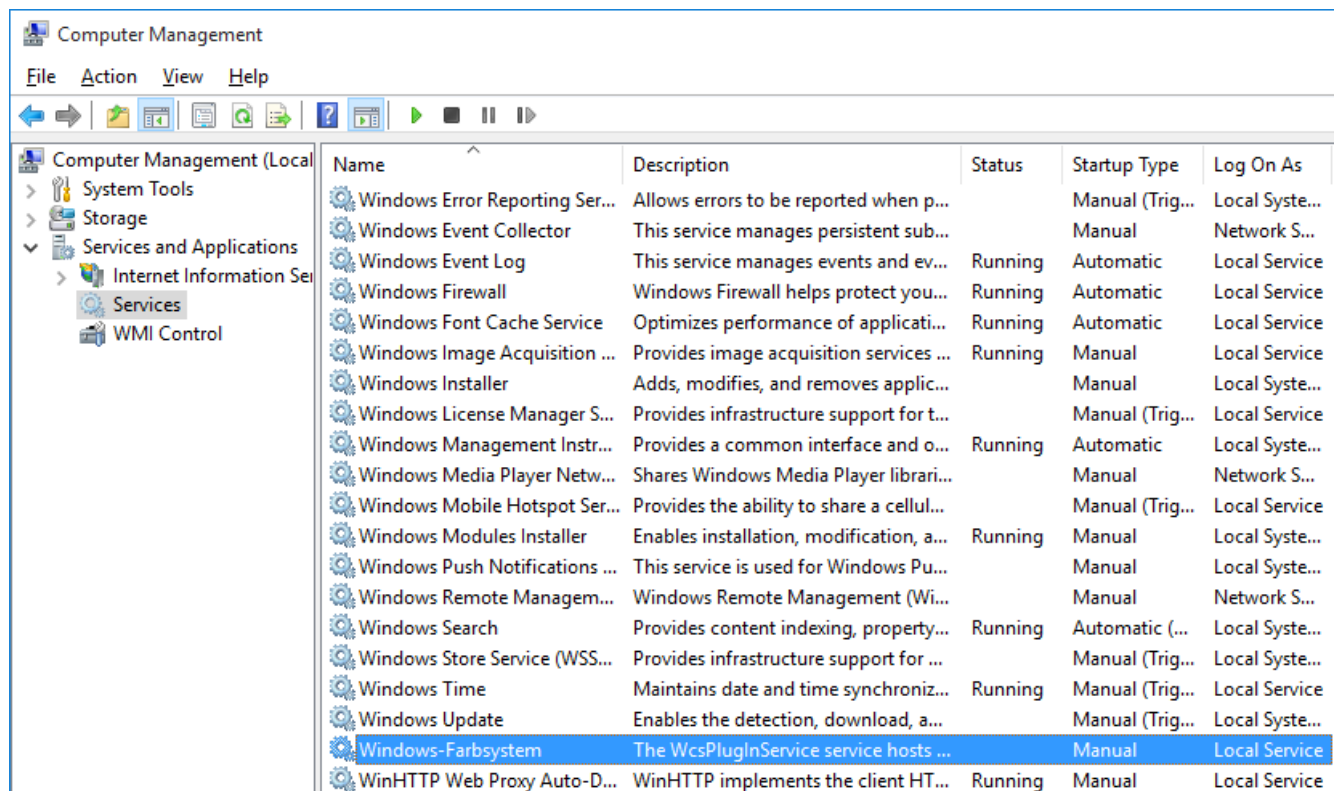
Note

In this context, note the advanced recommendations from Microsoft (article applies to Windows Server 2019): "Guidance on disabling system services on Windows Server 2016 with Desktop Experience" (<https://docs.microsoft.com/en-us/windows-server/security/windows-services/security-guidelines-for-disabling-system-services-in-windows-server>).

Procedure

To disable the above-mentioned services manually, follow these steps (using Windows 10 as an example):

1. In the Window Start menu, right-click on the "Computer Management" command from the shortcut menu.
Enter the administrator password, if required. If you are already logged on as an administrator, confirm the execution of the application.
The "Computer Management" dialog opens.
2. In the navigation pane, select "Services and Applications > Services".
The right pane of the dialog lists all available services. The "Status" column indicates whether the service is currently running. The "Startup Type" column shows whether and how the service is started - "Manual", Manual (Start by Trigger)", "Automatic", "Automatic (Delayed Start)" or "Disabled" (service cannot be started).



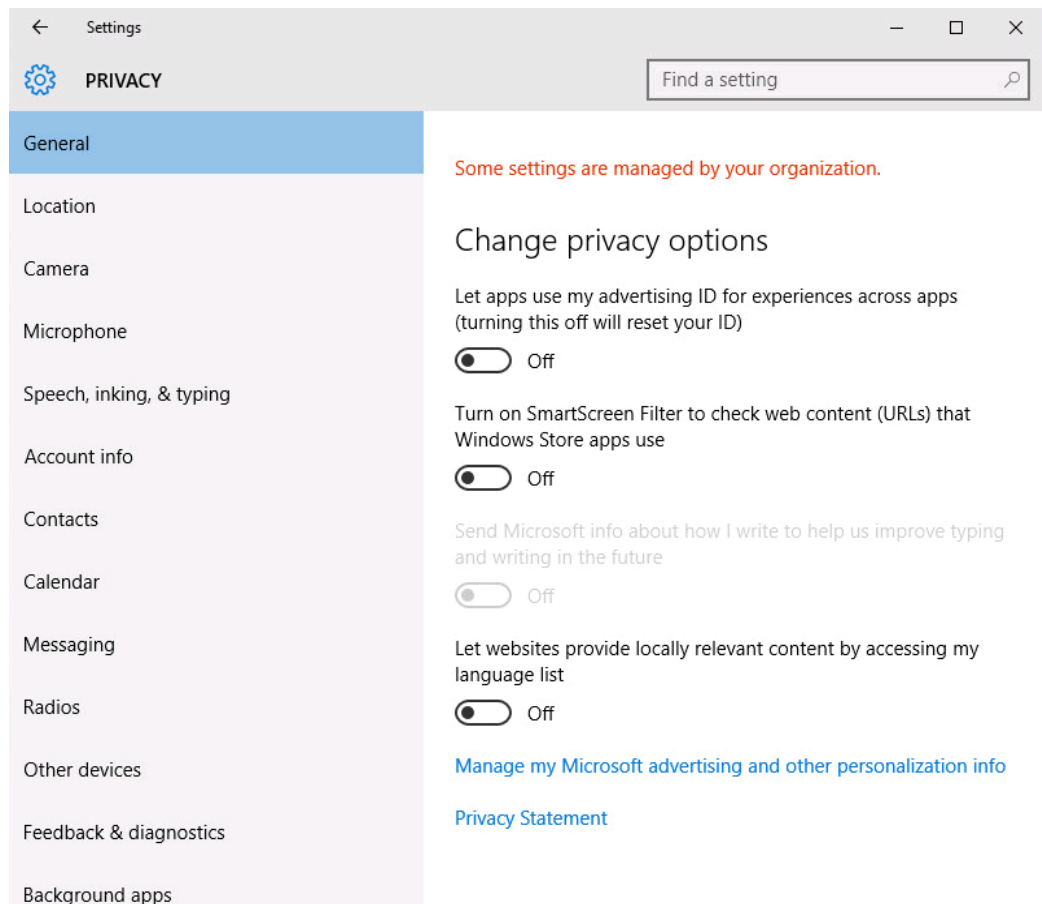
3. In the right area, select the service to be disabled, and open the properties dialog of the service by double-clicking on it. Only the services listed above may be disabled.
4. Under "Service status", click "Stop" to stop the service.
5. Select "Disabled" as the startup type and confirm your changes with "OK".

6.2.2 Setting of data protection and telemetry data in Windows 10

The following procedure is described using the example of a "Windows 10" operating system.

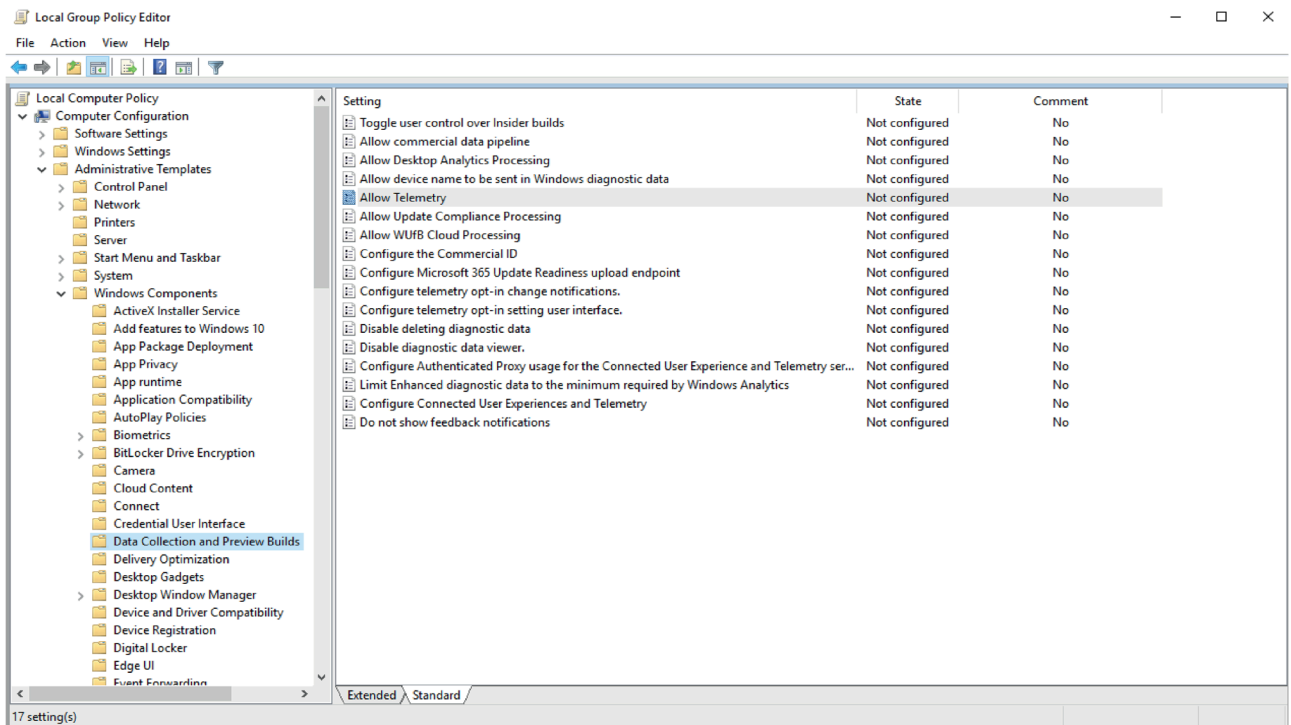
To set the data protection and telemetry data in Windows 10, for example, follow these steps:

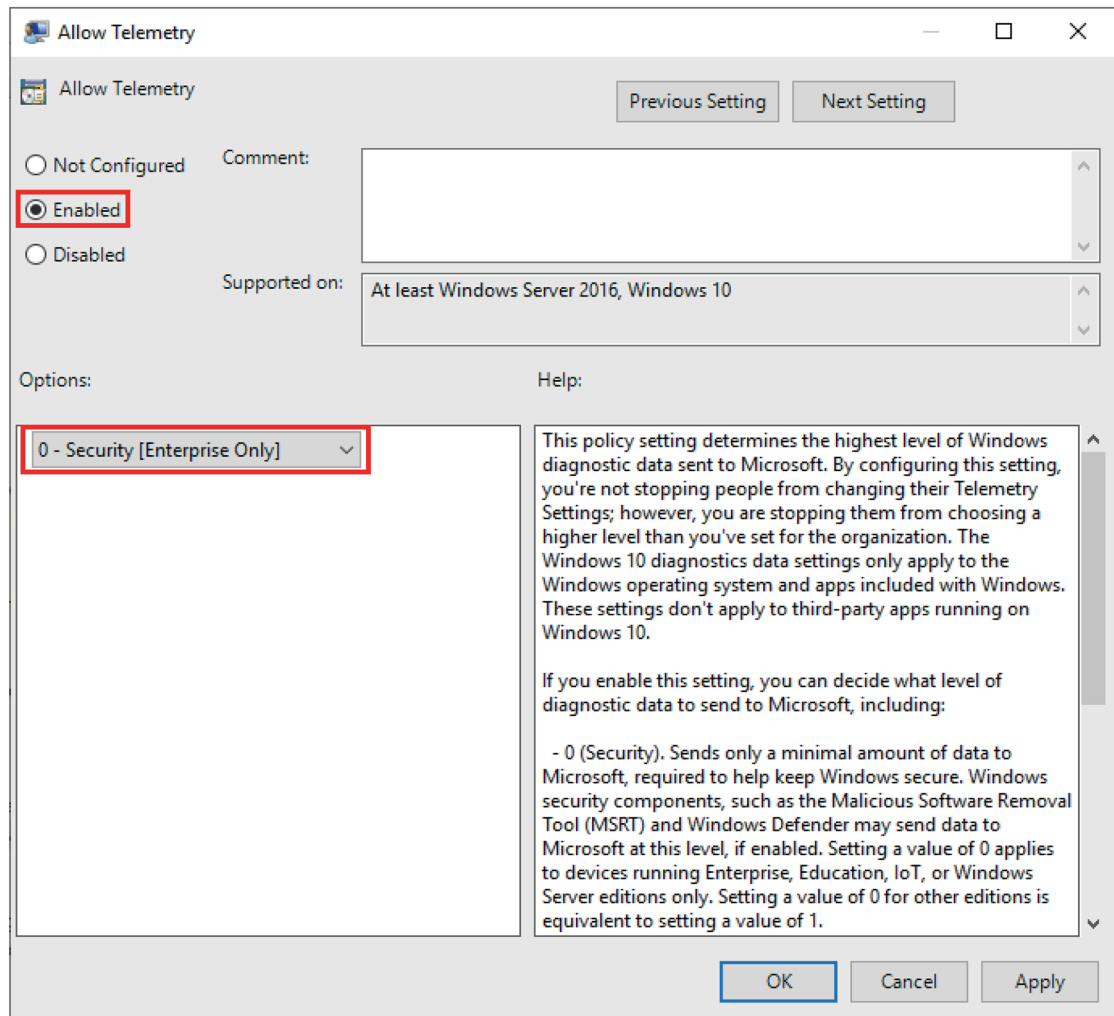
1. Select the "Notifications" icon in the Windows taskbar.
The "ACTION CENTER" opens.
2. Select the "All settings" option.
3. In the "Settings" navigation area, click the "Data Protection" option,
The privacy settings are displayed.
4. Go step by step through the privacy settings and disable them if this is possible and you wish to do so.



5. Close the "Settings" window.

Additional Windows 10 data protection functions can be enabled via group policy settings. To do this, start the Group Policy Editor for the local group policies "gpedit.exe" in an administrative command prompt (these settings can be made centrally in a domain) and configure the following policy settings (Group Policy Object or GPO).





Note

Additional information on the data protection settings and the acquisition of telemetry data by Windows 10 can be found on the Microsoft website (<https://docs.microsoft.com/en-us/windows/configuration/manage-connections-from-windows-operating-system-components-to-microsoft-services>).

Note

Additional information on the configuration of Windows 10 can be found in the following documents:

- Manual "SIMATIC Process Control System PCS 7 Readme" (<https://support.industry.siemens.com/cs/ww/en/view/109780270>)
 - Manual "SIMATIC Process Control System PCS 7 PC Configuration" (<https://support.industry.siemens.com/cs/ww/en/view/109794377>)
-

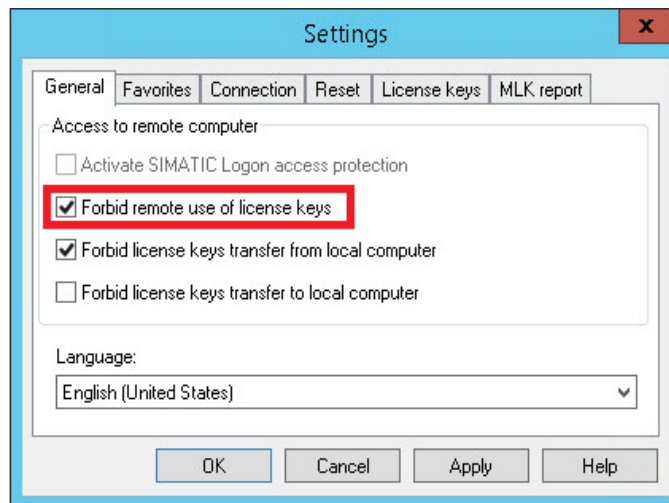
6.2.3 Additional hardening measures to be configured manually

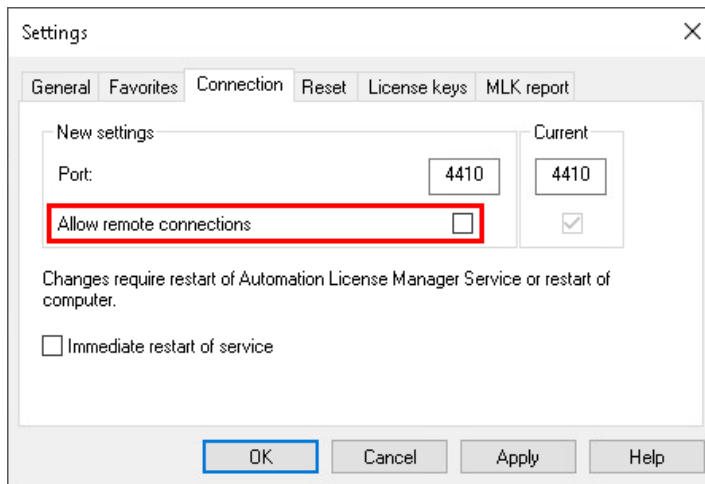
6.2.3.1 Parameter assignment of the ALM as license server

The Automation License Manager (ALM) is installed by default on SIMATIC PCS 7 systems and can be optionally configured as the license server. However, this function is only required if the system is also to be used as a remote license server. This may be helpful during commissioning of a plant, for example, so that a central license server is available on which all SIMATIC PCS 7 licenses required for the plant are stored. This makes it easier to commission the systems.

If the plant is in operation, we recommend not using the ALM license server functionality.

These settings can be checked or made in the ALM application. You can find these settings in "File > Settings > General > Forbid remote use of license keys" and "File > Settings > Connection > Allow remote connections". These options must be checked for the current settings and enabled or disabled, if necessary, so that the license server functionality is disabled.





Note

SIMATIC PCS 7 systems (for example, ES, OS Server, OS Client) should not be used as the license server. This function should therefore be generally disabled on these systems. If a license server is required in the plant, install a dedicated ALM license server for this purpose. Depending on the number of simultaneous accesses to this license server, you can use a system with Microsoft Windows desktop or server operating system and an ALM installation. In addition, all SIMATIC PCS 7 licenses required for the plant are stored on this system.

Note

On PCS 7 SIMATIC Batch servers, it can be necessary to set up the ALM as a license server to avoid long wait times when batch functionalities are invoked. Here, it must be ensured that in the local Windows firewall of the batch server, only the participating batch systems get access to the ALM license server. This can be achieved through the corresponding configuration of the "area" for permitted "Remote IP addresses" in the inbound firewall rule for the ALM. Further information on licensing of batch functionalities can be found in the documentation "SIMATIC Process Control System PCS 7 SIMATIC BATCH" (<https://support.industry.siemens.com/cs/ww/en/view/109794450>).

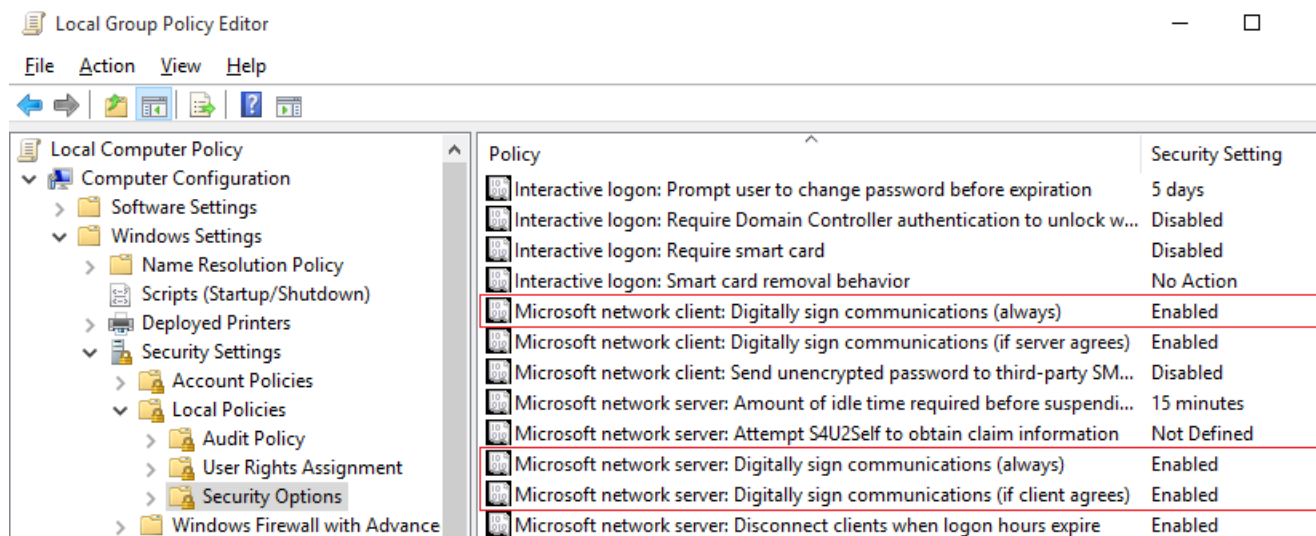
6.2.3.2 SMB signing

Additional Windows security functions can be enabled via group policy settings. To do so, start the Group Policy Editor for the local group policies "gpedit.exe" in an administrative command prompt (these settings can be made centrally in a domain).

The following settings are found under policy setting "Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options":

- Microsoft network (client): Digitally sign communication (always)
- Microsoft network (server): Digitally sign communication (always)
- Microsoft network (server): Digitally sign communication (if client agrees)

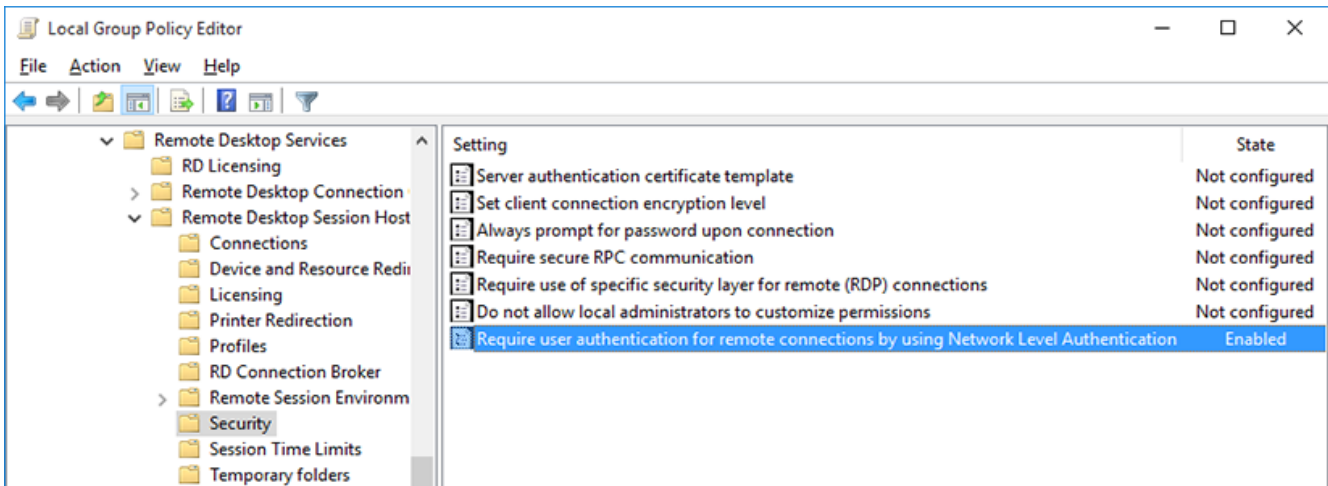
These three settings must be enabled for use of SMB signing.



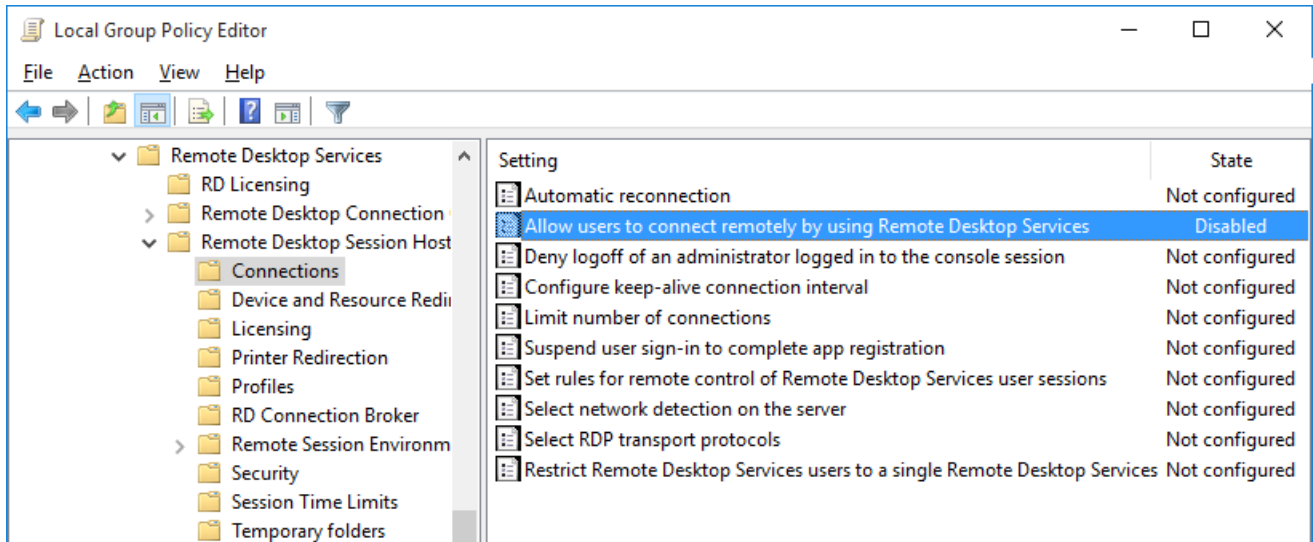
6.2.3.3 Remote Desktop Security setting

If required, e.g. when an OS client is accessed via the Remote Desktop Protocol (RDP), an additional security measure should be taken. To do so, start the Group Policy Editor for the local group policies "gpedit.exe" in an administrative command prompt (this setting can be made centrally in a domain) to make the appropriate group policy setting.

The setting "Require user authentication for remote connections by using Network Level Authentication" can be found under policy setting "Computer Configuration > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Security". This setting must be enabled.



On all SIMATIC PCS 7 systems, except when necessary on OS clients (e.g. in virtual environments), the setting "Computer Configuration > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Connections > Allow users to connect remotely using Remote Desktop Services" must be disabled. This prevents users from logging on to systems using RDP.



6.2.3.4 Disabling SMBv1

In the currently approved operating systems for SIMATIC PCS 7, the SMBv1 protocol is not active after reinstalling the operating systems:

"No default installation of SMBv1 in Windows 10, Version 1709, Windows Server, Version 1709 and higher versions" (<https://docs.microsoft.com/en-US/windows-server/storage/file-server/troubleshoot/smbv1-not-installed-by-default-in-windows>)

For checking or disabling the use of an outdated version of the SMB protocol on your system, proceed as described in the following manual:

Detect, enable and disable SMBv1, SMBv2, and SMBv3 in Windows (<https://support.microsoft.com/de-de/help/2696547>)

Note

Disable only SMBv1.

If additional SMB protocols are disabled, the proper function of Microsoft Windows or SIMATIC PCS 7 is no longer guaranteed.

When SMBv1 is disabled, no more communication to older operating systems (e.g. Windows XP or Windows Server 2003) is possible.

6.2.3.5 Support of LDAP signing and channel binding

LDAP is a directory protocol that is used in an Active Directory for the authentication, authorization and access to the address and user directories.

The LDAP protocol offers possibilities to better secure the LDAP-based domain communication. You can find more information here:

"Microsoft Guidance for Enabling LDAP Channel Binding and LDAP Signing (<https://msrc.microsoft.com/update-guide/en-en/vulnerability/ADV190023>)"

I.e. it is enough to copy the Windows updates (or the most recent ones) specified in the aforementioned Microsoft article to all domain controllers (DCs). Additional settings, especially in the SIMATIC PCS 7 systems, do not have to be made.

6.2.3.6 Disabling outdated SSL/TLS communication procedures

For Windows to not use any outdated SSL-/TLS communication procedures, the outdated processes must be disabled in the Windows Registry. These include all SSL versions and TLS versions before version 1.2.

Information on these processes and their configuration is available on the Microsoft web page "Transport Layer Security (TLS) registry settings" (<https://docs.microsoft.com/en-us/windows-server/security/tls/tls-registry-settings>).

To disable outdated processes, the following settings must be implemented on all SIMATIC PCS 7 systems via registry settings. Please create a backup before making changes to the Registry.

Recommended registry settings:

Disabling SSL V2.0:

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 2.0\Client]
```

```
"DisabledByDefault"=dword:00000001
```

```
"Enabled"=dword:00000000
```

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 2.0\server]
```

```
"DisabledByDefault"=dword:00000001
```

```
"Enabled"=dword:00000000
```

Disabling SSL V3.0:

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\Client]
```

```
"DisabledByDefault"=dword:00000001
```

```
"Enabled"=dword:00000000
```

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\Server]
```

```
"DisabledByDefault"=dword:00000001
```

```
"Enabled"=dword:00000000
```

Disabling TLS V1.0:

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Client]
```

```
"DisabledByDefault"=dword:00000001
```

```
"Enabled"=dword:00000000
```

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Server]
```

```
"DisabledByDefault"=dword:00000001
```

```
"Enabled"=dword:00000000
```

Disabling TLS V1.1:

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Client]
```

```
"DisabledByDefault"=dword:00000001
```

```
"Enabled"=dword:00000000
```

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Server]
```

```
"DisabledByDefault"=dword:00000001
```

```
"Enabled"=dword:00000000
```

Enabling TLS V1.2:

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Client]
```

```
"DisabledByDefault"=dword:00000000
```

```
"Enabled"=dword:00000001
```

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Server]
```

```
"DisabledByDefault"=dword:00000000
```

```
"Enabled"=dword:00000001
```

Note

These recommended settings are already pre-configured on SIMATIC PCS 7 IPC bundle computers.

6.3 Security Controller

The Security Controller is a program that makes application-specific security settings on the system.

The Security Controller is integrated by default in SIMATIC PCS 7.

The option of enabling the Security Controller to automatically perform the required settings must be explicitly confirmed when the PCS 7 programs are installed.

Communication to non-configured devices, in other subnets, as well as use by non-configured users is not possible or extremely restricted.

When changing the system configuration (e.g. network settings, incorporation of systems in a Windows domain), be aware that the local firewall configuration or additional system parameters must be adapted. The Security Controller must be restarted to do so.

Note

Next, the local firewall rules might have to be adapted manually (for example, when installing SIMATIC PCS 7 systems in different subnets).

Settings are made in the following areas by the Security Controller:

- Windows Firewall
- DCOM
- Registry
- User groups
- File system rights

These settings are made depending on the installation (PCS 7 OS server, PCS 7 OS client, PCS 7 ES).

Note

You can also find information on this in the manual "SIMATIC Process Control System PCS 7 PC Configuration" (<https://support.industry.siemens.com/cs/ww/en/view/109794377>).

6.4 Windows Firewall

As described in section 6.3 "Security Controller", the "Security Controller" program carries out settings on the local Windows Firewall. With respect to the sample configuration in which communication of SIMATIC PCS 7 computers between various subnets must be possible, additional manual adjustments to the Windows Firewall must be made depending on the version of the Security Controller.

Example configuration: Windows Firewall

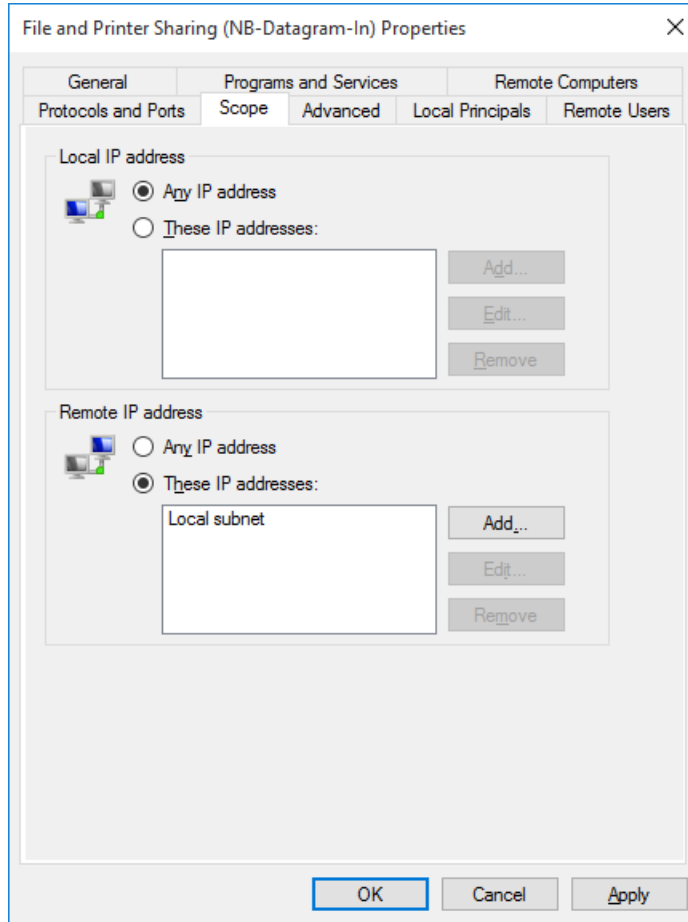
The following procedure is described using the example of a "Windows 10" operating system.

To prevent the Windows Firewall from blocking the communication, for example, between the OS Web server with the IP address 192.168.2.203 and the OS server OSS1A with the IP address 192.168.2.101, which are located on different subnets (Perimeter network and PCN1), the following changes must be made to the firewall rules of the Windows Firewall of the systems involved:

1. Open the Windows Firewall with the command "Start (Windows logo) - right mouse button > Network Connections > Windows Firewall > Extended Settings.
The "Windows Defender Firewall with Advanced Security" dialog opens.
Enter the administrator password if required. If you are logged on as an administrator, confirm the execution of the application.
2. In the left navigation pane, click "Inbound Rules". The inbound rules are displayed on the console on the right.

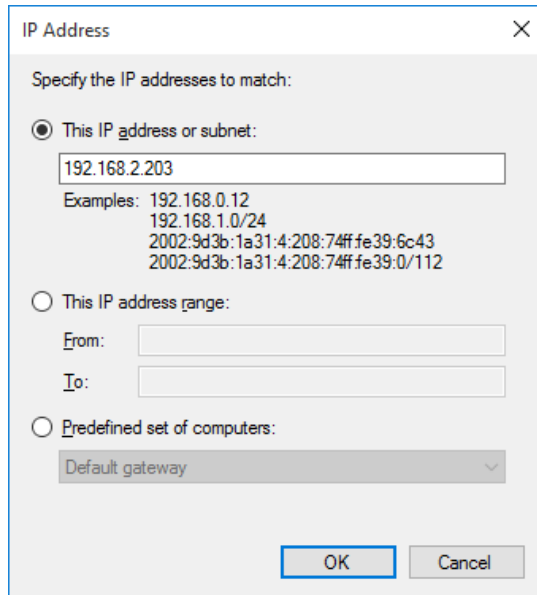
Inbound Rules		
Name	Group	Profile
File and Printer Sharing (Echo Request - ICMPv4-In)	File and Printer Sharing	Private, Public
File and Printer Sharing (Echo Request - ICMPv4-In)	File and Printer Sharing	Domain
File and Printer Sharing (Echo Request - ICMPv6-In)	File and Printer Sharing	Domain
File and Printer Sharing (Echo Request - ICMPv6-In)	File and Printer Sharing	Private, Public
File and Printer Sharing (LLMNR-UDP-In)	File and Printer Sharing	All
File and Printer Sharing (NB-Datagram-In)	File and Printer Sharing	Domain
File and Printer Sharing (NB-Datagram-In)	File and Printer Sharing	Private, Public
File and Printer Sharing (NB-Name-In)	File and Printer Sharing	Domain
File and Printer Sharing (NB-Name-In)	File and Printer Sharing	Private, Public
File and Printer Sharing (NB-Session-In)	File and Printer Sharing	Domain
File and Printer Sharing (NB-Session-In)	File and Printer Sharing	Private, Public
File and Printer Sharing (SMB-In)	File and Printer Sharing	Domain
File and Printer Sharing (SMB-In)	File and Printer Sharing	Private, Public
File and Printer Sharing (Spooler Service - RPC)	File and Printer Sharing	Domain
File and Printer Sharing (Spooler Service - RPC)	File and Printer Sharing	Private, Public
File and Printer Sharing (Spooler Service - RPC-EPMAP)	File and Printer Sharing	Domain
File and Printer Sharing (Spooler Service - RPC-EPMAP)	File and Printer Sharing	Private, Public

3. Open the properties of an active file and printer sharing rule (according to the network profile domain used in the system, Private or Public) with a double-click. The properties dialog of this rule opens.
4. Open the "Scope" tab.
The "Remote IP address" area shows the IP address range for which this firewall rule is valid and, for example, does not block the inbound communication.
In the case of the figure below, the communication is allowed only with computers in the "Local subnet". Communication of computers in a different subnet is thus blocked.



5. In order to allow communication of OS server "OSS1A" to the OS Web server with the IP address 192.168.2.203 in the subnet "Perimeter network", click the "Add" button in the "Remote IP Address".

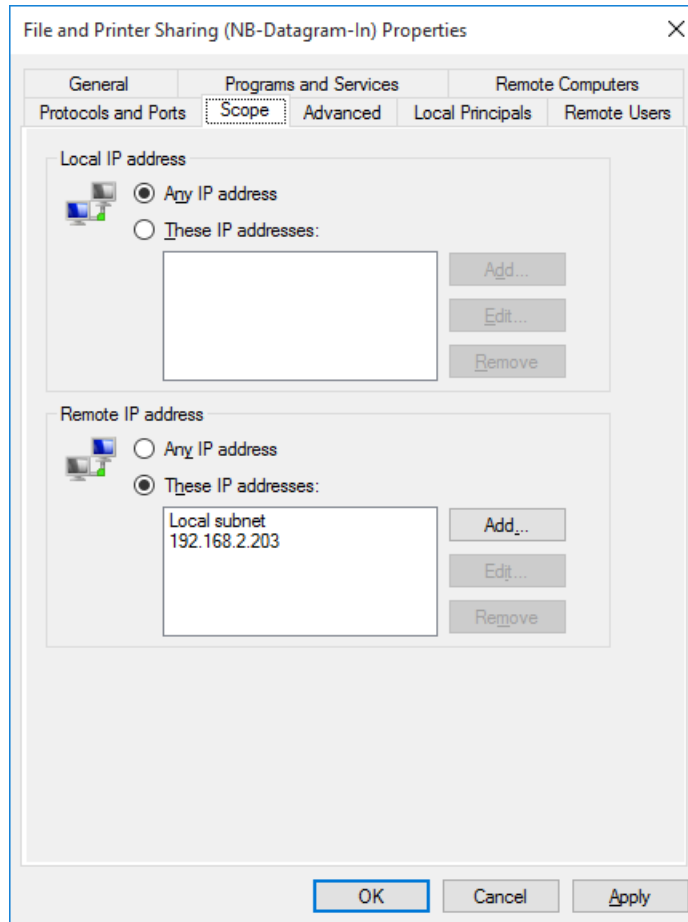
The configuration dialog opens.



The image shows a dialog box titled "IP Address" with a close button (X) in the top right corner. The dialog contains the following elements:

- A label: "Specify the IP addresses to match:"
- A radio button selected: "This IP address or subnet:"
- A text input field containing "192.168.2.203".
- Examples listed below the input field:
 - 192.168.0.12
 - 192.168.1.0/24
 - 2002:9d3b:1a31:4:208:74ff:fe39:6c43
 - 2002:9d3b:1a31:4:208:74ff:fe39:0/112
- A radio button: "This IP address range:"
- Two text input fields labeled "From:" and "To:".
- A radio button: "Predefined set of computers:"
- A dropdown menu showing "Default gateway".
- Two buttons at the bottom: "OK" and "Cancel".

6. Select the option "This IP address or subnet:" and enter the IP address of the communication partner. When you configure the firewall rules on OS server "OSS1A", enter the IP address of the OS Web server 192.168.2.203 in this dialog and confirm the entry with the "OK" button.



7. Confirm the change with "OK".
8. Adapt all inbound and outbound rules marked in the following figure according to your environment (e.g. private network profile, Windows domain, subnets). In addition, all inbound rules of the "Automation ..." "SIMATIC ..." "SQL Server ..." and "STEP 7" groups must also be checked or adapted.

Inbound Rules		
Name	Group	Profile
File and Printer Sharing (Echo Request - ICMPv4-In)	File and Printer Sharing	Private, Public
File and Printer Sharing (Echo Request - ICMPv4-In)	File and Printer Sharing	Domain
File and Printer Sharing (Echo Request - ICMPv6-In)	File and Printer Sharing	Domain
File and Printer Sharing (Echo Request - ICMPv6-In)	File and Printer Sharing	Private, Public
File and Printer Sharing (LLMNR-UDP-In)	File and Printer Sharing	All
File and Printer Sharing (NB-Datagram-In)	File and Printer Sharing	Domain
File and Printer Sharing (NB-Datagram-In)	File and Printer Sharing	Private, Public
File and Printer Sharing (NB-Name-In)	File and Printer Sharing	Domain
File and Printer Sharing (NB-Name-In)	File and Printer Sharing	Private, Public
File and Printer Sharing (NB-Session-In)	File and Printer Sharing	Domain
File and Printer Sharing (NB-Session-In)	File and Printer Sharing	Private, Public
File and Printer Sharing (SMB-In)	File and Printer Sharing	Domain
File and Printer Sharing (SMB-In)	File and Printer Sharing	Private, Public
File and Printer Sharing (Spooler Service - RPC)	File and Printer Sharing	Domain
File and Printer Sharing (Spooler Service - RPC)	File and Printer Sharing	Private, Public
File and Printer Sharing (Spooler Service - RPC-EPMAP)	File and Printer Sharing	Domain
File and Printer Sharing (Spooler Service - RPC-EPMAP)	File and Printer Sharing	Private, Public

Note

More information on the configuration of the local Windows firewall for this application can be found in the FAQ "How to ensure that the WinCC client-server communication is sustained upon switching on a firewall?"

(<https://support.industry.siemens.com/cs/de/en/view/109798700>).

Note

If a HW RAID controller from Adaptec is used in the system, note that a new rule that allows access only from and for the local system (localhost) must be added for access to the Adaptec maxview Web server.

6.5 BIOS settings

Make the following BIOS settings on each computer in your plant:

- Access to the BIOS should be protected with a password. The password should be set by an administrator and handled as confidential.
- The order of the boot media of the computer must be set in such a way in the BIOS, that the first boot attempt is from the integrated system hard disk containing the operating system installation and SIMATIC PCS 7. The BIOS boot manager should be disabled. These measures will make it difficult to boot from other media, such as from a CD, DVD or a USB stick.
- USB ports should be disabled, unless they are required for peripheral devices, such as a mouse or keyboard.

Note

The possible BIOS settings for a computer depend on the installed BIOS (e.g. manufacturer or version). Take into account the corresponding system description.

6.6 Working with mobile data media

In addition to the definition and designation of mobile data media, this section provides information about the settings to be performed with respect to mobile data media.

Mobile data media

Source:

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Umsetzungshinweise/Umsetzungshinweise_2021/Umsetzungshinweis_zum_Baustein_SYS_4_5_Wechseldatentraeger.html

Exchangeable media are often used to transport data, to save data, or to access data in a mobile situation. Exchangeable media include, for example, external hard disks, CD-ROMs, DVDs, memory cards, magnetic tapes and USB sticks.

Data storage media are classified according to whether they are only readable, or can be written to just once, or are rewritable. There are also differences in the type of data storage (analog or digital), how they can be processed or even in their design. Thus, there are exchangeable data storage media (for example, integrated hard disks) or external data storage media (for example, USB sticks).

Given this multitude of forms and application areas, not all of the required security considerations are taken into account at all times.

Mobile data media can be used for

- data exchange,
- data transport between IT systems that are not networked with each other, or between different locations,
- archiving or storing backups, if other automated methods are not appropriate,
- storing data that are too sensitive to be stored on workstations or servers,
- mobile data usage or data generation (e.g. MP3 player, digital camera, etc.).

Handling USB storage media

A variety of optional equipment can be connected to a PC via the USB interface. This includes hard disks, CD / DVD burners and memory sticks, for example. USB memory sticks consist of a USB connector and a memory chip. Despite their large capacity, they are small enough that they can be designed as key chains, for example, and they can fit into any pocket. The drivers for USB mass storage devices are already integrated in modern operating systems so that no software installation is necessary to operate them. In general, this measure does not relate exclusively to USB memory media, but generally to all USB devices that can store data. Among others, USB printers and USB cameras can be "misused" to save the data. This is especially true for "smart" USB devices such as PDAs, which can take on any USB identity if they are equipped with special software.

Similarly to floppies, uncontrolled information and programs can be read or written via USB storage media. Therefore, USB storage media should generally be dealt with similar to conventional storage media. The access to floppy drives can be prevented relatively easily. In contrast, the operation of USB storage media can be very difficult to prevent when the USB interface is used for other devices. For example, there are laptops that only offer the USB interface for connecting a mouse. For this reason, use of a "USB Lock" or disabling of the interface by other mechanical means is recommended. The use of interfaces should therefore be regulated by assigning appropriate rights on the operating system level or with the help of additional programs.

Handling USB ports

In addition to the possible BIOS settings for disabling USB ports (see section 6.5, "BIOS settings (Page 84)"), unwanted access can also be restricted using Windows settings. By disabling/restricting the USB ports via the BIOS or Windows settings, you ensure that the use of USB storage media and devices not known to the system is prevented or impeded.

Restricting access to USB storage media and devices using Windows

Various procedures that show how Windows resources can be used to prevent or restrict access to USB storage media and devices are described below:

- Regulating the use of USB storage media and devices using a group policy
- Disabling the Autoplay function using group policy
- Disabling the Autorun functions using group policy

6.6.1 Blocking access to all USB storage media

On modern systems, a general blocking of access to USB storage media is not recommended, since this could result in unforeseen function limitations.

Restrictions on USB access should be implemented if required as described in section 6.6.2, "Regulating the use of USB storage media and devices (Page 86)".

Note

Hotswap hard disks and/or partitions created on these hard disks (does not apply to hard disks operated in RAID configurations) can be recognized as removable data storage medium under newer Windows operating systems (e.g. Windows 10). The result may be that with a general blocking of access to USB storage media, no more access is possible to these hard disks or partitions that are located on them.

Check the BIOS settings of the system in this case to see whether hard disks can be configured as not hotswap-compatible. If this option exists, make this setting for all hard disks except for those configured in RAID arrays.

If the BIOS does not permit this configuration, the blocking of USB storage media must not be used.

Note

When using USB Hardlocks, this setting must not be made until after commissioning and use of the USB Hardlocks.

6.6.2 Regulating the use of USB storage media and devices

Before using a USB storage medium or device on a computer, the medium/device must first be installed. The operating system does this automatically when the device is connected to a computer the first time. This installation can be influenced on Windows by group policy settings:

- The installation of explicitly defined devices by the user can be allowed (positive list)
- The installation of explicitly defined devices by the user can be disallowed (negative list)
- Read and write access to mobile data media, such as USB sticks, USB HDDs, diskettes, CD/DVD burners, can be configured.

Note

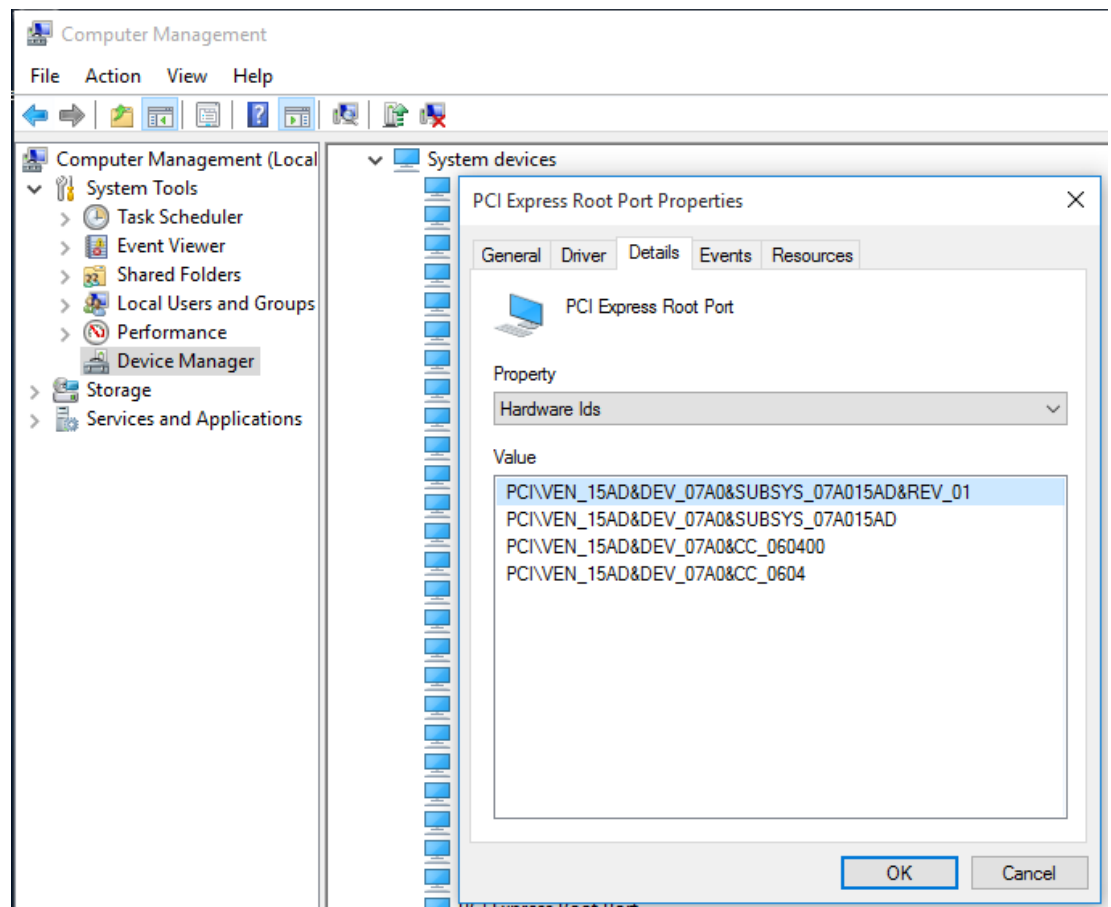
For security reasons, creating a positive list is recommended. In this manner, it is only possible to use USB storage media and devices known to the system.

Determining the hardware ID of a device

To influence the installation of a device by settings of the group policies as in the cases described above, you need to know the hardware ID of the device.

To determine the hardware ID of a device, follow these steps:

1. Connect the device with a Windows PC and wait until the installation of the corresponding driver finishes.
Successful installation is indicated with the message "Your device is ready to use".
2. After successful device driver installation, open the Device Manager.
3. In the properties of the corresponding device, open to the "Details" tab.
4. Select the option "Hardware IDs" from the property to display the hardware IDs of the device.
You need the hardware IDs to configure the respective group policies.

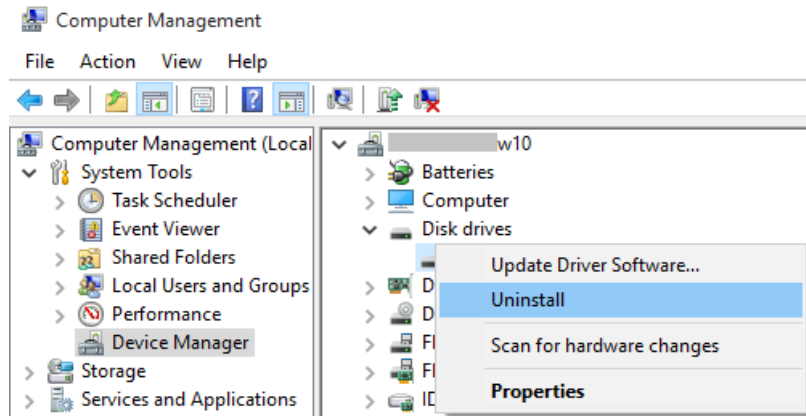


Uninstalling the device

In order to explicitly enable installation of the device via group policies, the device must first be uninstalled again after determination of the hardware ID.

To uninstall the device, follow these steps:

1. Right-click the device in the Device Manager and select the "Uninstall" command.

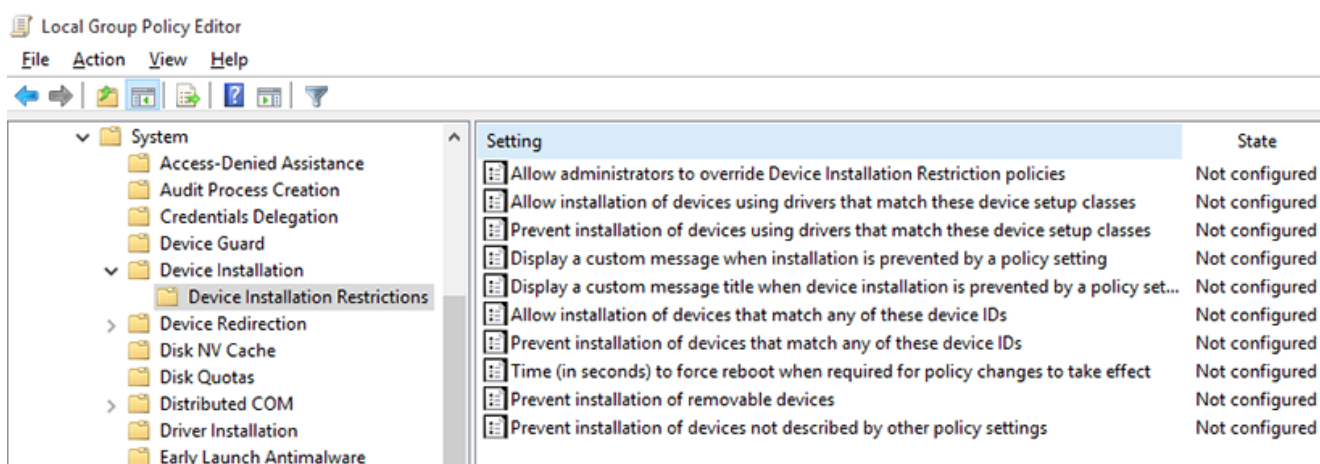


2. Click "OK" in the final dialog.
3. If a question appears here regarding uninstalling the relevant drivers, then if there are other identical devices still being operated with this driver, the driver can be left on the device.

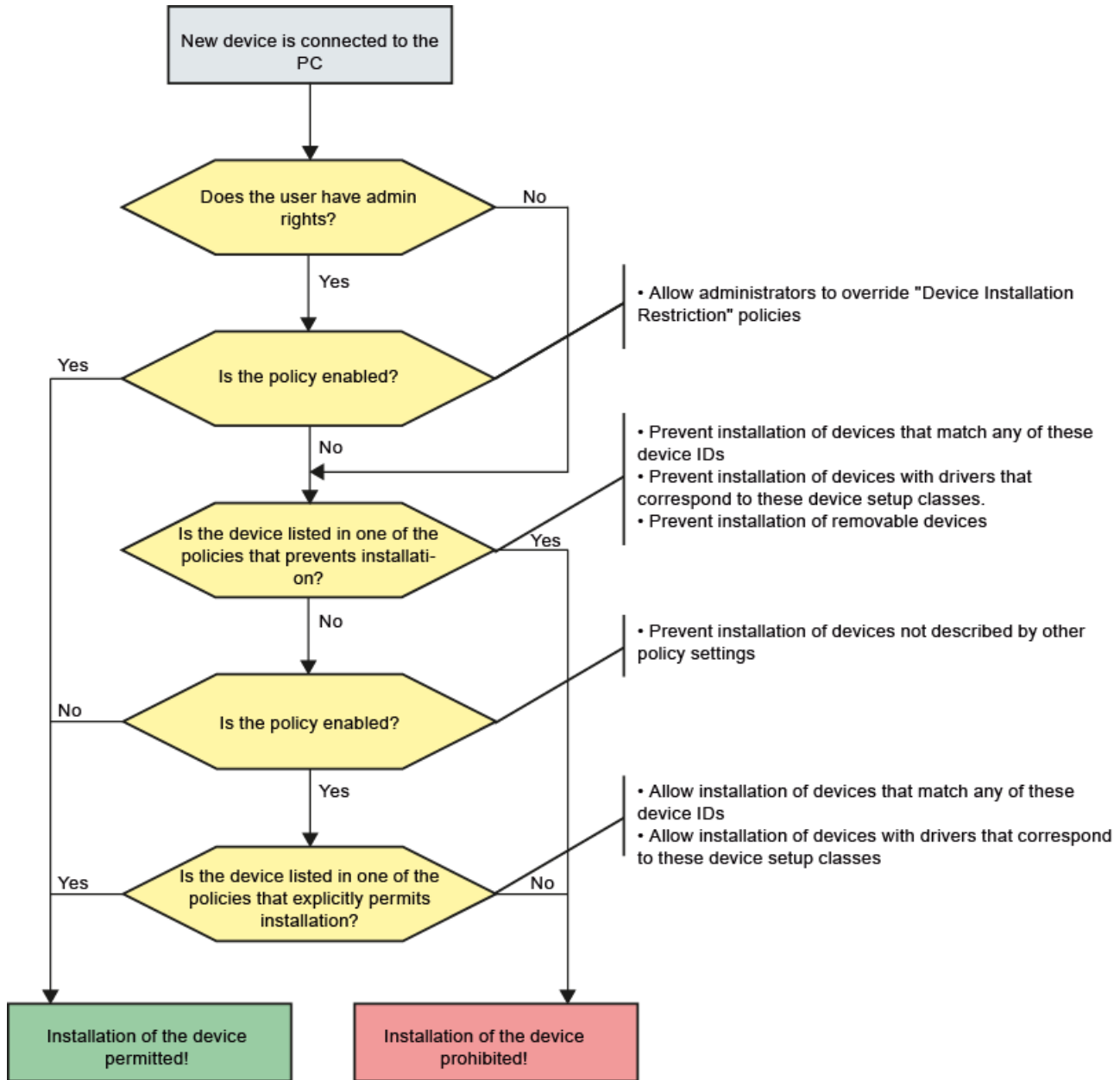
Correlation of group policies

The device installation characteristics can be specified through group policies. You can view these group policies in the Group Policy Editor under "Computer Configuration > Administrative Templates > System > Device Installation > Device Installation Restrictions". It contains the following policies:

- Allow administrators to override "Device Installation Restriction" policies
- Prevent installation of devices not described by other policy settings
- Allow installation of devices that match any of these device IDs
- Prevent installation of devices that match any of these device IDs
- Allow installation of devices with drivers that correspond to these device setup classes
- Prevent installation of devices with drivers that correspond to these device setup classes
- Prevent installation of removable devices



The correlation of the above-mentioned group policies is shown in the following diagram:



To allow only very specific devices on a computer based on the above-mentioned group policies, follow these steps:

1. Prevent the installation of all devices on the computer.
2. Explicitly allow a specific device to be installed.

To prevent the installation of all devices on the computer, proceed as follows (local administrator rights are required for this purpose):

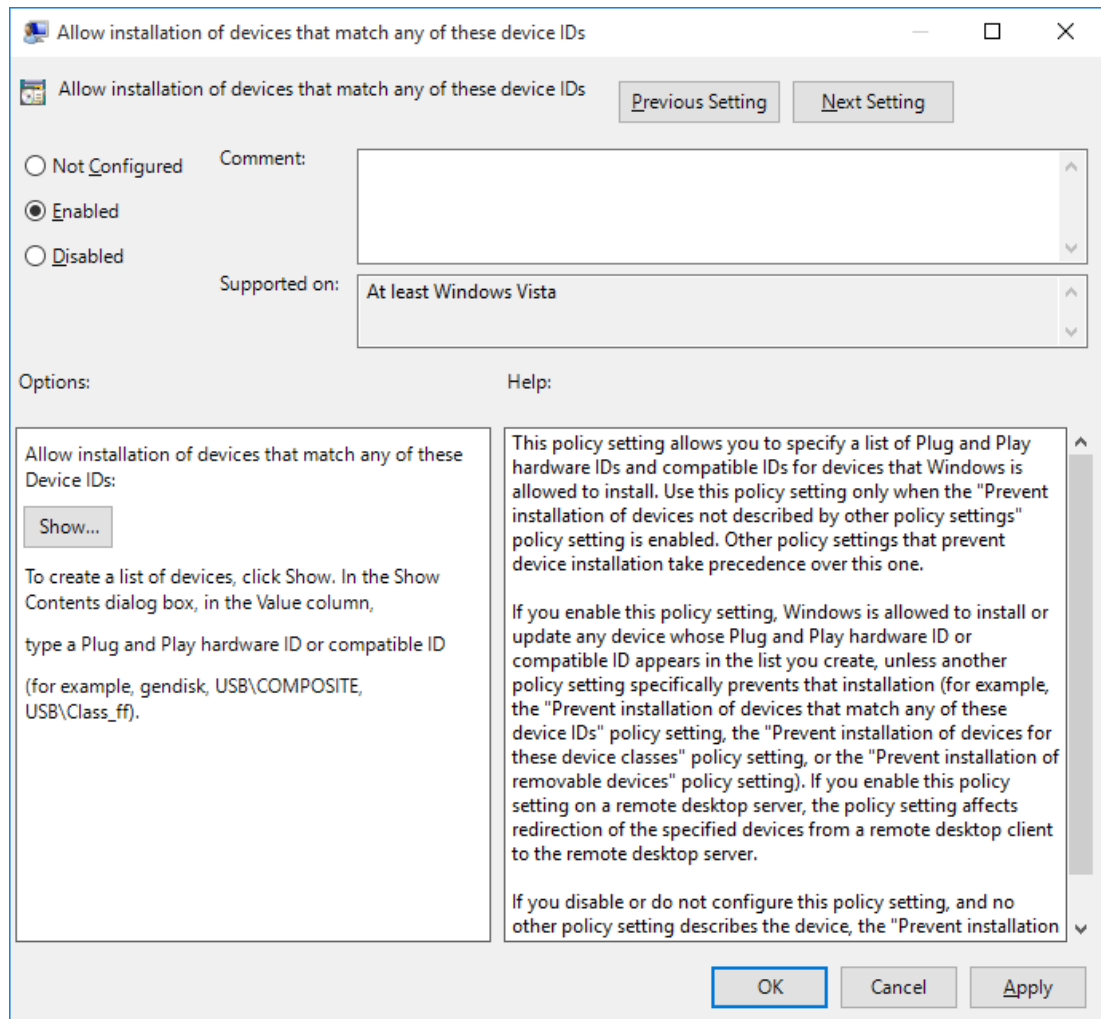
1. Ensure that all devices involved are uninstalled in the Device Manager.
2. Open the Group Policy Editor and navigate to the folder "Computer Configuration > Administrative Templates > System > Device Installation > Device Installation Restrictions". The group policies are displayed in the right pane of the editor.
3. Open the properties of the group policy "Prevent installation of devices not described by other policy settings" by double-clicking on the policy. The properties dialog of the group policy opens.
4. Enable the group policy by selecting the "Enabled" option and confirm your setting with the "OK" button.
This setting prohibits the installation of any other devices (not just USB media) on the computer.

In the next step, you have to allow the users with administrator rights to suspend the policies under "Device installer compliance". This then allows administrators to install hardware drivers on the computer using the Add Hardware Wizard when restricted device installation is enabled. To enable this group policy, follow these steps:

1. Open the properties of the group policy "Prevent installation of devices not described by other policy settings" by double-clicking on the policy. The properties dialog of the group policy opens.
2. Enable the group policy by selecting the "Enabled" option and confirm your setting with "OK".

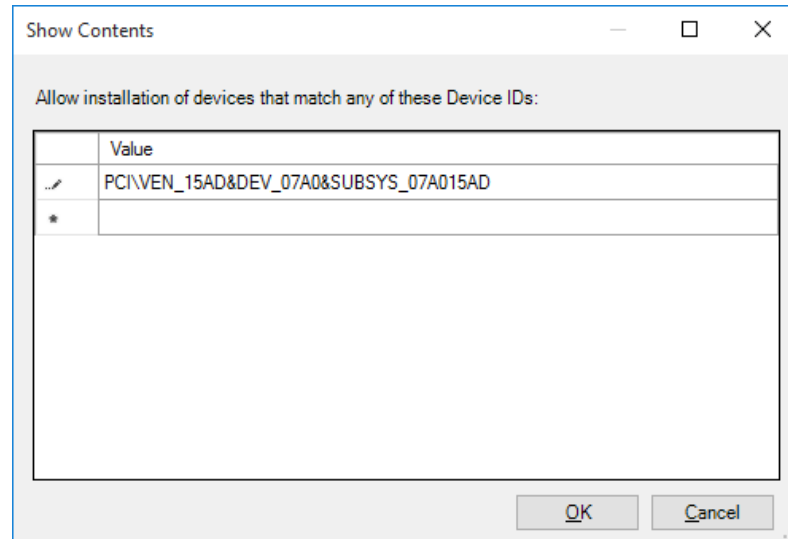
In the next step, you have to explicitly permit the installation of certain devices (positive list). Proceed as follows:

1. Open the properties of the group policy "Allow installation of devices that match any of these device IDs" by double-clicking on the policy. The properties dialog of the group policy opens.
2. Enable the group policy using the "Enabled" option.



3. Click the "Show" button to display the devices that are enabled on your computer for installation.

The released devices are displayed in the "Show content" dialog.



4. To release additional devices for installation on your computer, enter the hardware IDs of the devices in the dialog.
You can determine the hardware IDs of the device using the Device Manager (see above, under "Determining the hardware ID of a device").
5. Confirm the settings with "OK".
The installation and use of the specified devices are allowed by the user on your computer. The administrator is not subject to this restriction.

Note

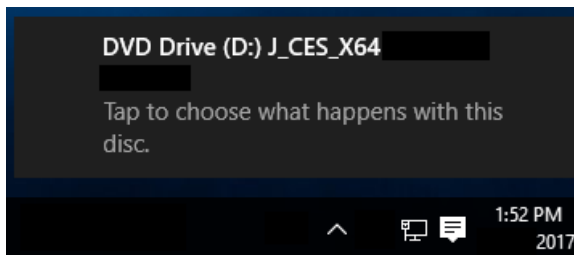
In an Active Directory (Windows domain), the use of USB exchangeable storage media and devices can be configured and restricted by means of central domain group guidelines for all the member computers in the domain.

6.6.3 Disabling AutoRun / AutoPlay for external drives and storage media

The main purpose of Autorun is to respond to hardware actions that are started on a computer on the software side. Autorun offers the following features:

- Double-click
- Shortcut menu
- Autoplay

These features are typically called from removable media or network shares. With Autoplay, a search is made for the "Autorun.inf" file on the medium and it is analyzed, if found. This file specifies the commands to be executed by the system. Usually, this functionality is used to start installation programs.



The AutoRun and AutoPlay functions are influenced by the "Shell hardware detection" service (ShellHWDetection).

Note

Malware, such as a Trojan horse, can be started via the AutoRun and AutoPlay functions.

In an Active Directory (Windows domain), the functions AutoRun and AutoPlay can be configured and restricted by means of central domain group policies for all the member computers in the domain.

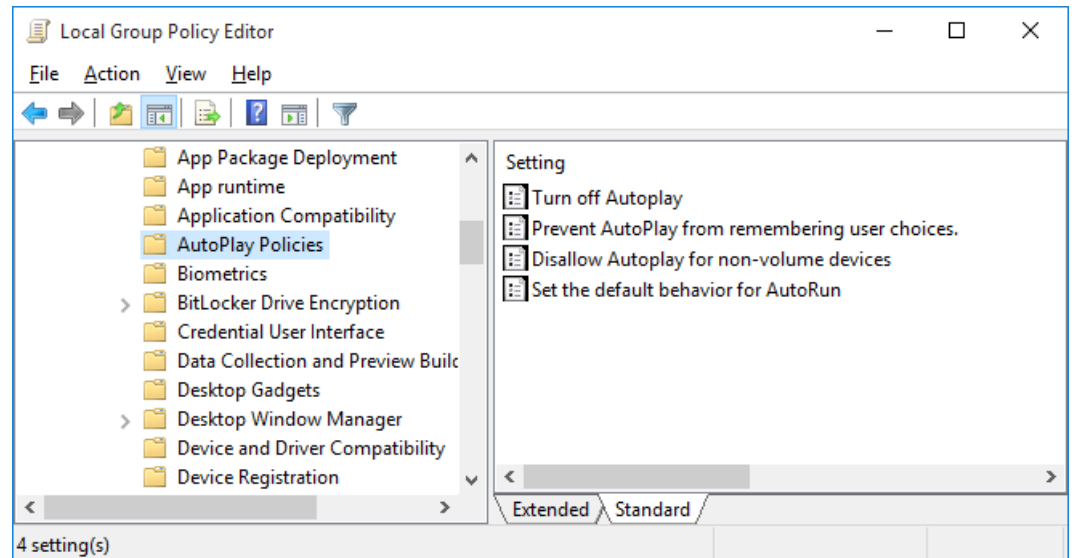
6.6.3.1 Disabling the AutoPlay function using a group policy

Procedure

To disable the AutoPlay function in Windows via a group policy, follow these steps:

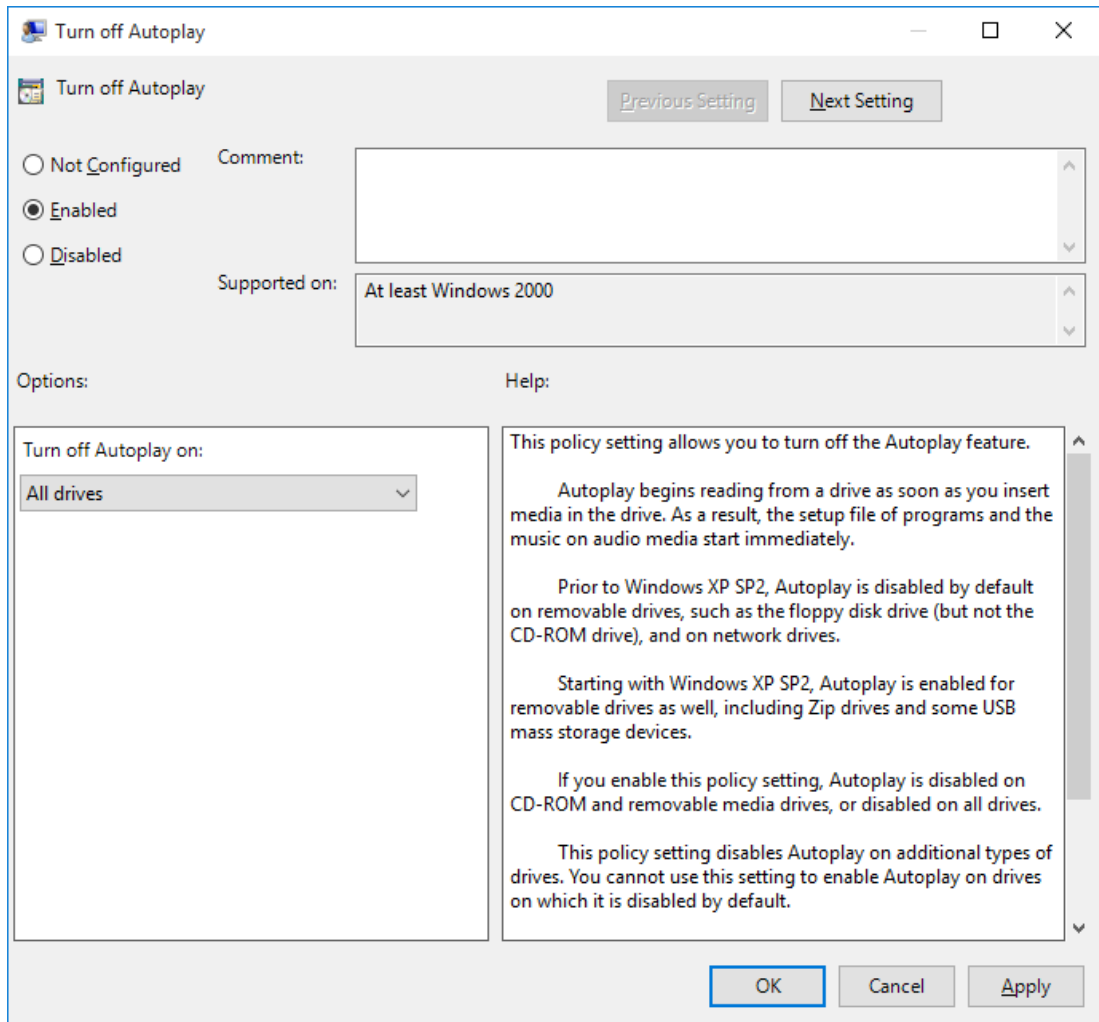
1. Start the Group Policy Editor for the local group policies "gpedit.exe" in an administrative command prompt (these settings can be made centrally in a domain) and configure the following policy settings (Group Policy Object or GPO).
2. Select the folder "Computer Configuration > Administrative Templates > Windows Components > Autoplay Policies".

The associated policies for the folder are displayed in the right pane of the editor.



3. Double-click the group policy "Turn off Autoplay". The properties dialog of the group policy opens.

4. Select the "Enabled" option, and from the drop-down list in the "Turn off Autoplay on:" area, select the "All drives" option.



5. Confirm the settings with "OK".
6. Reboot the computer.

6.6.3.2 Disabling all AutoRun functions using a group policy

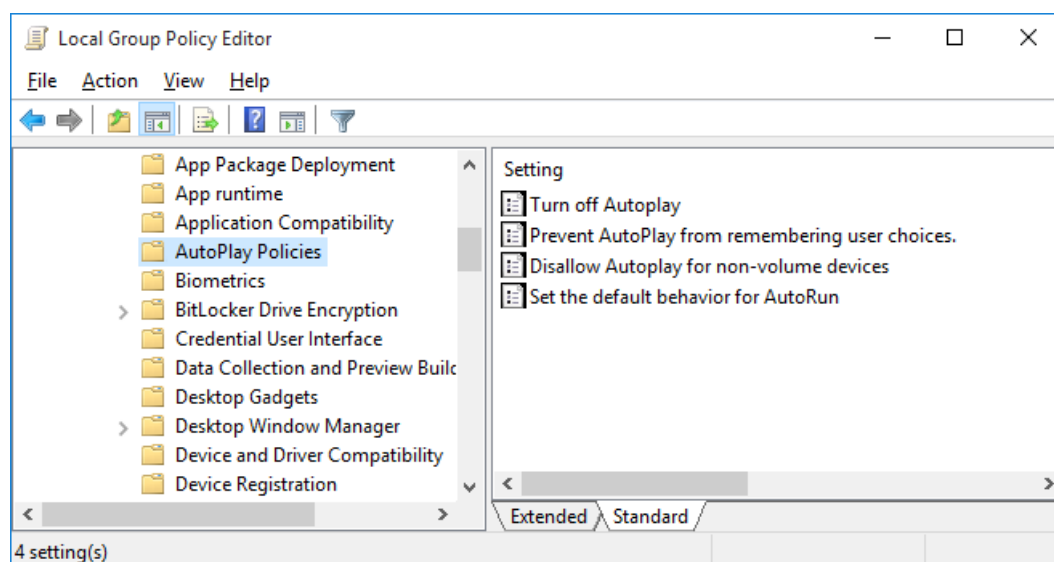
Procedure

To disable the AutoRun function in Windows via a group policy, follow these steps:

1. Start the Group Policy Editor for the local group policies "gpedit.exe" in an administrative command prompt (these settings can be made centrally in a domain) and configure the following policy settings (Group Policy Object or GPO).

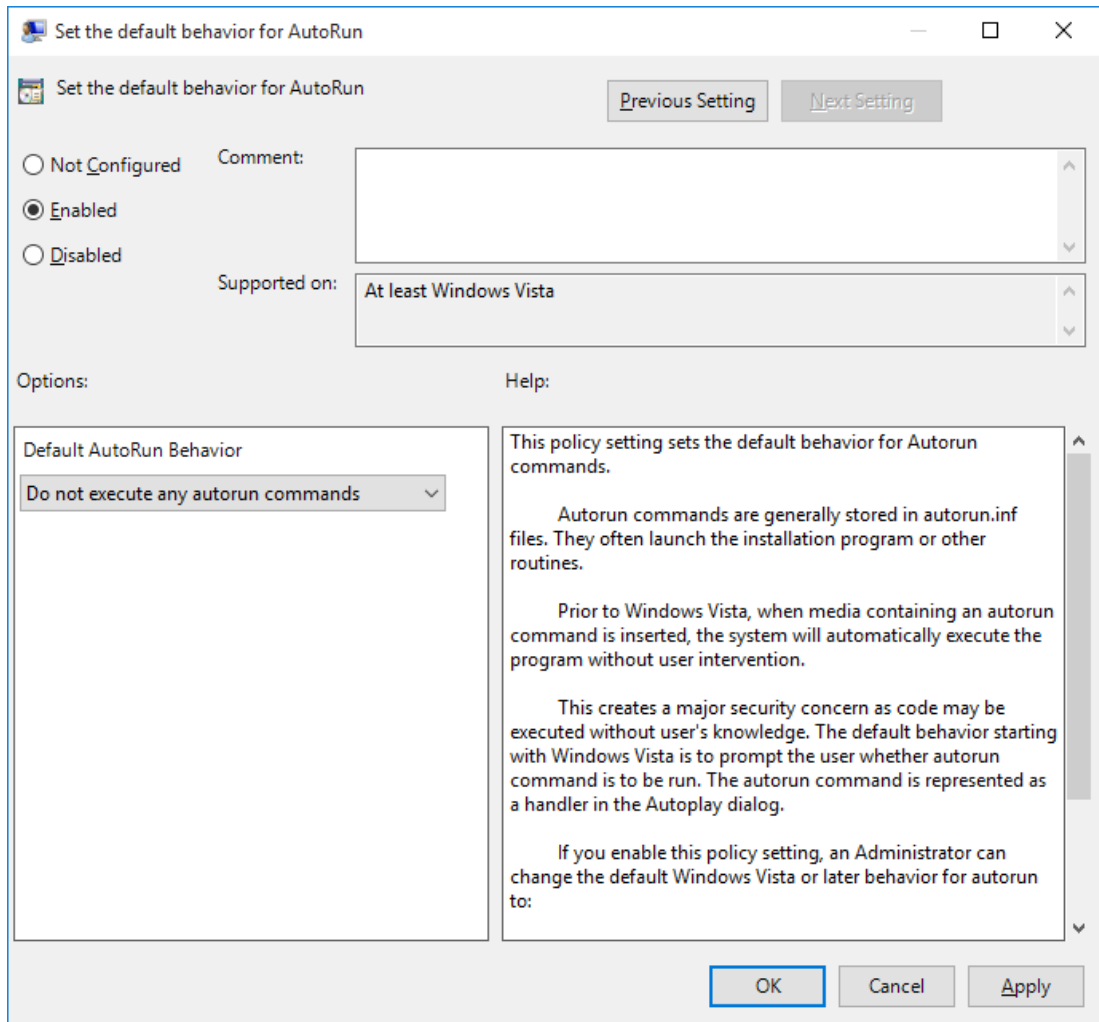
2. Select the folder "Computer Configuration > Administrative Templates > Windows Components > Autoplay Policies".

The right pane of the editor shows the policies associated with the folder.



3. Double-click the group policy "Specify Default Autorun Behavior". The properties dialog of the group policy opens.

4. Select the "Enabled" option, and from the drop-down list in the "Default Autorun Behavior" area, select the "Do not execute any autorun commands" option.



5. Confirm the settings with "OK".
6. Reboot the computer.

6.7 Whitelisting

The approach of whitelisting is that only applications deemed as trustworthy are allowed to run on the computer system. These applications are maintained in a positive list (whitelist). Based on this technique, it is not necessary to constantly adapt to new threats, e.g. new malware.

6.7.1 McAfee Application Control

McAfee Application Control allows blocking of unauthorized applications on servers and workstations. This means that after the installation and activation of McAfee Application Control on a computer system, all executable files are protected against changes and unknown executable files (not whitelisted) are prevented from being launched.

In contrast to simple whitelisting designs, McAfee Application Control uses a dynamic trustworthiness model. This makes time-consuming manual updates of lists of approved applications unnecessary. Updates can be installed in different ways:

- By trusted users
- By trustworthy manufacturers (certificate)
- From a trusted directory
- By means of binary file
- Using an updater (update programs such as WSUS or virus scanners)

Moreover, McAfee Application Control offers a feature that monitors memory, protects against buffer overflow, and protects the files that run in memory.

McAfee Application Control can be administered in the following ways:

- Locally on a computer system (standalone)
- Centrally using McAfee ePolicy Orchestrator (ePO)

The decision as to whether McAfee Application Control is to be administered centrally or locally should be made based on the number of systems to be maintained.

The following procedure applies regardless of the type of administration:

- After installing McAfee Application Control on a computer, a so-called white list must first be generated. This means that all connected local drives are scanned for executable files. The duration of this procedure depends on the data volume and hardware used and may take several hours.
- After enabling McAfee Application Control, the computer must be restarted. All executable files (exe, com, dll, bat, etc.) found during the scan are now protected against changes (renaming, deletion, manipulation, etc.) and the whitelisting mechanism is activated. This prevents the start of executable files newly copied to the system.

6.7.2 Local administration of McAfee Application Control

Local administration is handled exclusively by means of command line input. The commands are clear and self-explanatory. McAfee also provides detailed documentation on configuration. McAfee Application Control can also be configured and controlled using scripts.

6.7.3 Centralized management of McAfee Application Control

The centralized management (installation, configuration and monitoring) of McAfee Application Control instances is carried out using the McAfee ePolicy Orchestrator (ePO) application. McAfee ePO software is a management tool that can manage all McAfee products and includes numerous network management and monitoring functionalities.

As in the case of the Active Directory (Windows domain), centralized management via ePO can be advantageous when there are at least 10 managed systems. All McAfee Application Control commands and options are also available remotely via the ePO. Some are available through pre-defined tasks and the remainder through remote command line options. In comparison to local management, ePO offers centralized monitoring of the system and a clearly arranged event management.

McAfee ePO must be installed on a dedicated computer with up-to-date hardware. If the system already contains an infrastructure computer (for example, WSUS), McAfee ePO can also be installed on this computer.

Note

McAfee ePO must not be installed on a PCS 7 system or a domain controller.

Additional information

The whitelisting solution "McAfee Application Control" is approved for different SIMATIC PCS 7 versions. You can find details about the compatibility with SIMATIC PCS 7 in the Compatibility tool (<https://support.industry.siemens.com/cs/ww/de/view/88653385>).

You can find a description of the recommended procedure and configuration with McAfee Application Control in the application example "Use of Whitelisting with McAfee Application Control in the PCS 7 / WinCC environment" (<https://support.industry.siemens.com/cs/ww/en/view/88653385>).

You can find the McAfee Knowledge Center with the latest documentation on McAfee products in the McAfee Knowledge Center (<https://support.mcafee.com/ServicePortal/faces/knowledgecenter>).

See also

SIMATIC PCS 7 compatibility tool (<http://www.siemens.com/kompatool>)

6.8 Hardening of devices by Industrial Security Services

In addition to the system hardening possibilities described above, there are additional options that also include topics such as hardening of devices (e.g. network devices and automation systems). They are part of the industrial security services. You can find more information and the corresponding contacts at (<https://www.siemens.com/industrial-security>).

6.9 SIMATIC S7 CPUs

In a holistic examination of security, it is recommended that the S7-400 automation systems be considered as critical components in a PCS 7 configuration and that a password and a suitable protection level be assigned. The password should have sufficient complexity. This means, for example, that the password should consist of letters, numbers and special characters and be at least 8 characters long.

For S7-400 CPUs, a protection level can be defined in the project to prevent unauthorized access to the CPU program.

You can choose between three protection levels. Protection level 1 means no access restriction and protection level 3 has the strictest access restriction.

It is recommended that you configure at least protection level 2.

We also recommend that you use the increased password security option. The increased password security is only relevant for the engineering system. When this option is selected, the password entered in the data management is stored encrypted. This setting increases the password security. The setting has no effect on the behavior in password mode.

Note

If S7-400 CPUs with an integrated Web server (S7-400 PN standard) are used, ensure that the Web server is disabled in the CPU.

To achieve the highest level of protection from unauthorized access, access to the S7-410 CPU over the DP or the PNIO interface should be blocked. To do this, all functions that are not required for the automation task at hand can be disabled. This level of protection can be configured for each interface for incoming connections in HW Config by enabling the setting "Enable additional protection at the interface (Field Interface Security)". This setting prevents external bus nodes from establishing a connection. All connection requests are rejected by the CPU. The connections required for IO mode are still being established by the CPU.

Additional information

Detailed information about possible protection levels of the S7-400 and S7-410 CPUs, know-how protection of blocks and other security functions for the S7-410 CPUs, can be found in the following entries:

- Manual "SIMATIC S7-400H Fault-tolerant Systems (<https://support.industry.siemens.com/cs/ww/en/view/82478488>)"
- Manual "SIMATIC Process Control System PCS 7 CPU 410 Process Automation (<https://support.industry.siemens.com/cs/ww/en/view/109748473>)".
- FAQ "How can you install block protection for self-created blocks?" (<https://support.industry.siemens.com/cs/ww/de/view/10025431>)

6.10 SIMATIC NET- Industrial Ethernet CPs

In addition to an integrated Web server, Industrial Ethernet CPs (e.g. CP 443-1) include a variety of other integrated servers (depending on the CP 443-1 type). For the purpose of system hardening, you have to proceed as described in the preceding sections: All services and procedures that are not required should be switched off or disabled. This means that the integrated servers, such as Web server, FTP server as well as SNMP (if Asset Management is not being used), should be disabled.

When the CP 443-1 Advanced V3 or higher is used in combination with a CP 1628, appropriate security settings must be made from SIMATIC Manager using the Security Configuration Tool (SCT). This enables configuration and use of firewall functionalities and VPN tunnel (via IPSec) on the plant bus (PCN).

Note

The CP1628 module is type-cancelled. Therefore, the use of secured communication using this module is only recommended if it is still in stock. There are no successor or substitute types for this module.

(<https://support.industry.siemens.com/cs/de/en/view/109793063>)

Note

The component CP443-1 Advanced (GX30) module will not be monitored for security loopholes any longer. This means that it is not now possible to ensure that there will be firmware updates for critical security loopholes.

<https://support.industry.siemens.com/cs/de/en/view/109799025>

Note

For configuring, pay attention to the notes in the following document "Industrial Ethernet CP 443-1 Advanced (GX30) - Equipment Manual Manual Part B", section 6.14:

<https://support.industry.siemens.com/cs/ww/en/view/59187252>

6.10.1 Requirements

Make sure that the following requirements are met:

- All systems with connection to the system bus either have a CP 1628 (computer) or CP 443-1 Advanced (CPU S7-400) installed
- The latest firmware is installed on all CP modules listed above
- The basic configuration of the PCS 7 project including all CP components must be completed and functioning
- A backup of the project has been created
- The SCT Tool (SIMATIC Configuration Tool) in its latest version has been installed on the ES
- An NDIS IP address at the system bus has been configured on the ES for the CP 1628 (for diagnostic purposes from within the SCT Tool)
- Runtime is stopped during initial download of the CP configuration to the OS server
- You have ensured that only known and trusted network components are connected to the system bus.

6.10.2 Procedure

Proceed as described in sections 4.2, 4.3 and 6.2 of the document "SIMATIC NET Industrial Ethernet Security Setting Up Security" (<https://support.industry.siemens.com/cs/ww/en/view/109742841>) when configuring the encrypted communication (VPN tunnel).

The following items must be taken into consideration:

- The configuration calls for a thorough approach; otherwise it may be difficult to access modules that were configured incorrectly and to make changes.
- During initial activation of the "Enable security" function you are prompted to enter a user name and password (credentials). Enter a user name and a secure password. You will need these credentials later to open the security project during configuration or in the SCT Tool. These credentials must be assigned (additionally) independently of the Windows and PCS 7 project environment.
- On the CP 443-1 Advanced, the X1 interface has been connected to the system bus and configured for the VPN tunnel. The X2 interface is "networked" with a "dummy network" (The network is only configured virtually in the project. A physical network is not necessary).
- Enable the "Activate security" function on all participating CP modules and save this setting.
- After the security of all CP modules has been enabled, open the SCT Tool. You can start the SCT with the command "HW Config > Edit > Security Configuration Tool".

- The following information only applies to the initial configuration(!):
 - You can find all configured CP modules in the module overview. Create a new VPN group and drag all modules to this group using the mouse.
 - Disable the "Tunneled communication" option in the properties of the CP 1628 module, and enable the "Allow IP communication" and "Allow MAC layer communication" options.
 - Enable the "Advanced mode" and configure the log level from "Error (3)" to "Informational (6)" in the "Log settings > Configure system events". This setting can be retained permanently.
 - Save this configuration in the SCT Tool and go back to HW Config.
 - Note that the following download processes are only possible over the MAC addresses of the CP modules.
 - Compile the CP 1628 configuration for the ES and download the project to the module. Now compile and download all additional CP modules one after the other.
 - Once all download processes are completed successfully, open the SCT Tool again.
 - In the SCT Tool, reset the CP 1628 modules of the ES listed above to the default settings. To do this, enable the option "Tunneled communication" in the properties of the CP 1628 module, and disable the options "Allow IP communication" and "Allow MAC layer communication".
 - Save the SCT project and exit SCT.
 - Now compile and download the CP 1628 module of the ES again in HW Config. This completes the initial configuration of the encrypted communication (VPN tunnel).
- Additional changes and downloads can now be made as usual.

6.10.3 Diagnostic options

You have a variety of options in the SCT Tool and under Windows to diagnose the secure communication (VPN tunnel).

- Checking the interfaces in the SCT Tool
 - Start the SCT Tool and use the corresponding icon to enable the "Online mode".
 - Select the CP 1628 module of the ES.
 - You open a status view with "Edit > Online diagnostics > Interfaces", in which a "Yes" must be entered in the "Reachability" column of all modules.
- The SCT Tool offers additional diagnostic options for each CP module of the project.
- Checking the system log in the SCT Tool
 - Switch to online mode and select the CP 1628 module of the ES.
 - Start the online diagnostics and execute the "Start Reading" command in the "System log" tab.
 - To finish checking, close the online diagnostics and exit online mode.
- Checking using the "ping" command
 - Execute the "ping" command for all configured CP 443-1 Advanced modules of the project on the ES in a command prompt.

Additional information

You can find additional information on Industrial Security with SIMATIC NET in the following manuals:

- SIMATIC NET Industrial Ethernet Security Setting Up Security Getting Started (<https://support.industry.siemens.com/cs/ww/en/view/109742841>)
- SIMATIC NET Industrial Ethernet Security, Security Basics and Application (<https://support.industry.siemens.com/cs/ww/en/view/109747342>)

6.11 PROFINET

In plants today, the field level must also be integrated into the security concept, because modern field devices are connected to the automation systems via PROFINET. The security measures published by PROFIBUS & PROFINET International (PI) must be taken into consideration.

For configuration and diagnostics of the PROFINET field devices, the PCS 7 Engineering Station (ES) must also have access to these devices. Temporarily and for as long as the configuration or diagnosis takes, the so-called Service Bridge is used for this purpose; it may be preceded by an upstream firewall to increase network security.

Additional information

Information on the PROFINET security concept is available in the "PROFINET Security Guideline" (https://www.profibus.com/download/profinet-security-guideline/?return_url=download%2Fspecifications-standards%2F).

Information on how to use the Service Bridge and protect access through it is available in the application example "Service Bridge – Setup and Configuration" (<https://support.industry.siemens.com/cs/ww/en/view/109747975>).

6.12 Time synchronization of system

A comprehensive security concept includes consideration of the time synchronization of the system. A trustworthy and available time source is the basis for stable operation of the system. Among other things, this ensures that all systems run with the same time and the authentication (Kerberos Tickets) and replication between the domain controllers is guaranteed within an Active Directory (Windows domain), fault and alarm messages of the system enable descriptive diagnostics and archives are kept consistent.

Note

The time source (for example, Bürk Mobatime) should be located in the system's security cell.

Additional information

You can find additional information on the configuration of time synchronization in SIMATIC PCS 7 systems in the "SIMATIC Process Control System PCS 7 Time Synchronization" (<https://support.industry.siemens.com/cs/de/de/view/109794383>) manual.

6.13 Handling of digital signatures for applications

A mechanism is available in Windows that is used to check the digital signatures of binary files that are signed with the Windows Authenticode Signature Format. The new standard behavior for checking the Windows Authenticode Signature no longer permits irrelevant information in the WIN_CERTIFICATE structure. Afterwards, Windows no longer recognizes incompatible binary files as signed.

Additional information

You can find information on measures for preventing delays that might occur and checking the validity of certificates and thus improving the security in the FAQ "What can cause the start of SIMATIC PCS 7 applications being delayed?"

(<https://support.industry.siemens.com/cs/ww/en/view/87057037>).

6.14 OPC server in the plant

If an OPC connection is used in the system, it is recommended that it should be established by OPC UA (Unified Access). It is a currently valid OPC standard that makes it possible, among other things, to run encrypted and digitally signed communication between the OPC client and OPC server.

For this purpose, an OpenPCS 7 system should be used as an OPC UA server, which is to be placed in the Perimeter network. This system should be reachable only for authorized systems and only via the communication protocols used for OPC UA. Depending on the system configuration, this must be ensured by the corresponding firewall rules on the frontend, backend or three-homed firewall.

When OPC UA is used, it must be ensured, through configuration of the OPC server, in this case, the OpenPCS 7 system, that only encrypted and digitally signed communication is used between the OPC UA clients and the OPC UA server. The OPC clients must support this recommended type of secured configuration and communication. Otherwise, a OPC UA connection is not possible.

Notes regarding the recommended configuration of the OpenPCS 7 system can be found in the FAQ "How do I configure OpenPCS 7 for secure communication with an OPC UA client?" (<https://support.industry.siemens.com/cs/de/en/view/109799626>)

Note

When the OPC (UA) server function is active on SIMATIC PCS 7 systems (for example, PCS 7 OS server, Process Historian), make sure that only authorized systems can access this function. This can be ensure, for example, through corresponding (local) firewall rules.

6.15 Hardening of the Process Historian server

To restrict the rights for the required communication services (PH-Ready Service and Information Server Ready) of the Process Historian server (PH), the instructions given in sections 1.2.8 and 1.2.9 of the "Process Historian – System Manual" (<https://support.industry.siemens.com/cs/de/en/view/109795088>) must be observed.

6.16 Hardening of the Information Server

The Windows authentication function should be enabled on the Information Server. You can find the relevant information in section 4.2.1 of the document "Installation and Commissioning of Process Historian/Information Server in the PCS 7 Environment" (<https://support.industry.siemens.com/cs/de/en/view/66579062>) in the application example chapter "Installation and Commissioning".

With separate PH/IS installations, make sure that only authorized systems can access this function. This can be ensured, for example, through corresponding (local) firewall rules.

6.17 Disabling non-required network interfaces

On systems such as computers, switches, firewalls and others, network interfaces and ports to which no terminal units are connected should be disabled.

6.18 Hardening of the Internet Information Server (IIS)

When a PCS 7 Web server and/or Information Server (IS) is used in the plant, the following hardening measures can be applied. This approach prevents header information that allows conclusions on the IIS used.

Procedure

1. Create a backup of the Windows registry.
2. Add the following key in the Windows registry or adjust the existing key:
HKLM\SYSTEM\CurrentControlSet\Services\HTTP\Parameters
DisableServerHeader == 1 (DWORD)

3. Create a backup of the "web.config" file.

Note

You can find the relevant "web.config" files of the Web server in the following directories:

- PCS 7 Web Server
C:\Program Files (x86)\Siemens\WinCC\Webnavigator\Server\Web\web.config
- Information Server
C:\inetpub\wwwroot\Siemens\Informationserver\web\Web.config

The measures recommended below must be repeated or checked after each download of the PCS 7 Web server, each start of the Web Configurator in WinCC or each start of the SIMATIC Web Configurator (IS).

4. Add or change the "web.config" file of the Web server in the corresponding sections with the following parameters:

```
<configuration>
  <system.web>
    <httpRuntime enableVersionHeader="false" />
    <httpCookies httpOnlyCookies="true" requireSSL="true" />
    <customErrors mode="RemoteOnly" defaultRedirect="~/Error.aspx" />
  </system.web>
  <system.webServer>
    <httpProtocol>
      <customHeaders>
        <add name="X-Frame-Options" value="DENY" />
        <add name="X-XSS-Protection" value="1; mode=block" />
        <add name="Content-Security-Policy" value="default-src 'none'; script-src
'self'; connect-src 'self'; img-src 'self'; style-src 'self';" />
        <remove name="X-Powered-By" />
      </customHeaders>
    </httpProtocol>
  </system.webServer>
</configuration>
```

5. If you have installed a certificate for your Web server (recommended configuration), the following supplement in the "web.config" file will ensure that the Web server can only be accessed over https.

```
<configuration>
  <system.webServer>
    <httpProtocol>
      <customHeaders>
        <add name="Strict-Transport-Security" value="31536000" />
      </customHeaders>
    </httpProtocol>
  </system.webServer>
</configuration>
```

In addition, it must be ensured through the following Web server configuration that calls to the Web server are always rerouted to the encrypted website (https):

- Stop the PCS 7 Web server / Information Web server (IS) with the Internet Information Services Manager (IIS Manager).
 - Use the IIS Manager to check the available websites on the PCS 7 Web server /IS.
 - One "Default website" and an additional "Virtual website" called "WebNavigator" or "InformationServer" should exist
(If there is only one "Default website" for the PCS 7 Web server, delete the WebNavigator and SCSWebBridge directories within this "Default website. Next you start the Web Configurator in WinCC and publish the WebNavigator as "virtual" website. Any changes to the web.config file must be made again afterward).
 - Now you can also make a separate configuration for each of the ports 80 (http) and 443 (https).
 - On the "Default website", you configure the connection to port 80 (http) (other relationships must be deleted)
(Comment: All options must be disabled on the "Default website" in the SSL settings.)
 - You configure the connection to port 443 (https) on the Web Navigator website (other relationships must be deleted)
(Comment: On the WebNavigator website, the option "SSL required" and "Required" should be enabled in the SSL settings, if required (use of client certificate)).
 - A "default.htm" must be created once for the "Default website" in the default website directory (default: c:\inetpub\wwwroot).
 - Insert the following HTML code in the default.htm file (whereby the host name must be entered without < and >):
<meta http-equiv="Refresh" content="0;URL=https://<PCS7 Webserver Hostname>" />.
 - Rename the original "iisstart.htm" file contained in this folder (e.g. "_iisstart.htm").
6. Reboot the PCS 7 Web server / IS.

6.19 Hardening of the Internet Explorer (IE)

To limit vulnerabilities of the Internet Explorer (IE), the IE updates published by Microsoft must be applied regularly and the following settings should be made:

- Changing the security and data protection settings for Internet Explorer 11 (<https://support.microsoft.com/de-de/windows/%C3%A4ndern-der-sicherheits-und-datenschutzeinstellungen-f%C3%BCr-internet-explorer-11-9528b011-664c-b771-d757-43a2b78b2afe>)

User Administration and Operator Permissions

7.1 Overview

Administration of user authorizations, group authorizations, and operation authorizations involves the assignment of authorizations in the Windows environment as well as the assignment of users to activity-oriented roles. These procedures are rigorously separated from each other, but both are strictly applied under the principle of minimum required rights. A simple check can be performed with the following questions:

- Who has to do what?
- Who is allowed to do what?

When logging on to the operating system, the user may receive only the rights that are required for accomplishing his/her tasks.

When logging onto the control system (e.g. the OS client operating station or the engineering system, etc.), the operator/configuring engineer may only receive the permissions required for his/her role, e.g. as operator/configuring engineer of a unit.

Note

The following chapters describe which permissions and settings are required for the corresponding roles. We recommend that a user **only** gets the minimum rights that he requires to fulfil his tasks. If a task requires higher rights temporarily, it is recommended to use a special account with the required rights and not to work with the higher rights permanently.

Note

Users in an Active Directory (Windows domain) should be managed according to the Least-Privilege principle.

See also

Microsoft articles: "Implementing Least-Privilege Administrative Models"
(<https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/implementing-least-privilege-administrative-models>)

7.2 Windows workgroup or Windows domain

SIMATIC PCS 7 can be operated in two different Windows system environments:

- Windows workgroup (default setting)
- Active Directory (Windows domain)

When a Windows workgroup is used, the computers and users/groups are administered in a decentralized manner and locally on each individual computer. Within an Active Directory, centralized administration of computers, users, and groups is possible.

7.2.1 Operation of the system in a Windows workgroup

Operation of a system without centralized Windows management is recommended under the following conditions:

- The system has no more than approximately 10 computers.
- The plant does not undergo changes on a routine basis (for example, adding new users, changing computers, introducing new security policies, changing passwords, etc.).
- The operation of a Windows domain infrastructure cannot be guaranteed due to a lack of appropriately trained personnel.
- The consistency of network settings, computer configurations, security policies, users and passwords can be guaranteed by centralized plant documentation.

Special attention should be given to the following:

- User passwords must always be changed in the same way on all computers involved.
- User accounts that are no longer needed must be disabled/removed everywhere.
- All computers of the system must be configured with the same security policies (for example, use of the LanManager NTLMv2 protocol, signing of SMB communication, password complexity and password age).
- Centralized documentation of assigned computer names and IP addresses must be created and kept up-to-date.
- When local LMHosts and Hosts files are used for name resolution, these files must always be simultaneously updated on all systems.
- Secure operation of a system can be jeopardized by the incorrect configuration of a single computer. Moreover, troubleshooting in such cases is often difficult and time-consuming.

7.2.2 Operation of the system in an Active Directory

Configuration and use of centralized Windows management (Active Directory) is recommended under the following conditions:

- The system has more than 10 computers, the number of computers, accounts, and users to be administered is very large, or users and/or group memberships from an existing Windows domain are needed.
- Changes are regularly made in the system (e.g. addition of users, replacement of computers, introduction of new security policies, periodic password changes, etc.).
- A centralized, high-availability user administration is required.
- A centralized configuration of the computers is required.
- The company requires security policies that can be fulfilled only by a Windows domain (e.g. use of Kerberos tickets).

Additional criteria for centralized management can be:

- Legal requirements and guidelines must be met (e.g. use of Kerberos tickets as an authentication method, centralized logging of logon events, etc.).
- Centralized (including redundantly possible) IP address assignment via DHCP

Note

The use of a DHCP server under PCS 7 requires the configuration of static IP address assignment for the SIMATIC PCS 7 computers.

- Centralized administration of name resolution and registration of computers via DNS/WINS.
- Use of a certificate server (PKI/CA) based on Active Directory to enable the following services:
 - Secure Web services with encrypted communication via Transport Layer Security (TLS) (server and client certificates)
 - Signatures for applications and documents
 - Authentication
 - Certificate-based IP security communication protocols and tunneling protocols such as the Layer Two Tunneling Protocol (L2TP) or OpenVPN
 - Certificate-based Radius server

7.3 Administration of computers and users

The strategy of role-based access control includes the limiting of rights of users, operators, devices, network components and software components to the minimum rights required.

The users to be created in the operating system environment can be managed distributed or from a central location.

Note the following in this regard:

- With the distributed management of users in workgroups, proceed according to the ALP principle (Add User Account to Local Group and Assign Permission) recommended by Microsoft. This means that local users must be grouped first so that the required permissions (folder, releases, etc.) can be assigned to these groups.
- If management is performed centrally using an Active Directory, the AGLP principle (Account, Global, Domain local, Permission) must be observed. According to this principle, the domain user accounts are initially assigned to the domain-global groups in the Active Directory. These groups are then assigned to local computer groups which, in turn, receive the permissions to the objects.

7.3.1 Implementation

An automation system features stations/computers that must be permanently operational and are used by several persons. An example is the operator control and monitoring device (OS client). This station is operated continuously and is used by different operators for process control.

SIMATIC PCS 7 uses three different user accounts and related authorizations:

- User accounts that are used for logging on to the operating system and starting the applications (for example, the "PCS 7-Runtime" of the PCS 7 OS server/clients, PCS 7 Web server, OpenPCS 7)
(Remark: These are also used at the start of the OS server runtime as a service.)
- User accounts that are used for logging on to the operating system on the PCS 7 Engineering System (ES) and the start of the applications installed there (for example, SIMATIC Manager).
- User accounts that are used for logon of operators on the user interface ("PCS 7 Runtime").

Note

It is recommended that these user accounts be defined and handled separately. The option exists to consolidate user accounts and to use only one user account for accessing a SIMATIC PCS 7 system.

For user accounts that are used for logging onto the operating system and starting applications on continuously used operator control and monitoring stations, the use of "non-personalized", device-specific user accounts is recommended. The user accounts should be suitable for establishing a reference to the respective computer (e.g. OSClient5User).

This account must be used when using "Autologon" for logging onto the operating system followed by Autostart of the PCS 7 Runtime (as recommended).

Note

For device-specific user accounts, password changes are only permissible during a maintenance phase (PCS 7 runtime mode stopped), because these user accounts are used for authentication of the communication between SIMATIC PCS 7 systems, among other things.

Password changes of the affected user accounts must be made simultaneously on all involved systems, otherwise proper operation cannot be ensured. We therefore recommend that you disable password aging for these user accounts.

Personalized user accounts lend themselves to the engineering station that is used by different users/configuring engineers for configuring and that is not continuously in operation or on which no one is logged on when not in use. No "Autologon" should be configured at the engineering station for logging on to the operating system.

Note

When an engineer exits the ES, they must close the SIMATIC Manager and all other applications that have been started and log out of the ES. This prevents the system from being blocked (for example, by a screen saver) and other engineers having no access to the ES.

The user accounts used for logon in PCS 7 Runtime are set up as stand-alone (personalized) users (e.g. operators, shift supervisors, engineers) and assigned to operator groups according to their authorization. These groups are assigned the necessary rights within the configuration for PCS 7 Runtime (WinCC User Administrator). SIMATIC Logon is required for assignment of rights using Windows group membership in the SIMATIC PCS 7 Runtime. If "Autologon" is configured for a user account, the account should only get read authorization.

Note

The use of a user account from the administrator group or with administrator rights is only needed for commissioning and configuring the computer and installation of SIMATIC PCS 7.

Administrative rights are not needed for operation of SIMATIC PCS 7 (PCS 7 Runtime).

7.3.2 SIMATIC permission model

All the permissions to shares and folders in conjunction with SIMATIC products can be assigned using the SIMATIC permission model. For this, local groups are created during the installation and then assigned to the SIMATIC objects including all the required permissions. This simplifies the assignment of the necessary rights, because the respective user account or the group only has to be added to the local SIMATIC groups that are needed for operation of SIMATIC products. Depending on the SIMATIC products being installed, the number of added groups may differ.

Note

While membership in the "SIMATIC HMI" user group allows access to projects, it does not grant the permission to access the operating system or to locally log on to the desktop.

Therefore, membership in the local default group "Users" is also required in addition to the groups created by the SIMATIC PCS 7 Setup program.

7.3.3 SIMATIC PCS 7

During installation of the SIMATIC WinCC component via the SIMATIC PCS 7 setup program, the following three new user groups are created, which are used for assignment of rights to project shares, project file accesses and interprocess communication:

- **SIMATIC HMI**
The members of this group may create, edit, start and remotely access local projects. By default, the user installing SIMATIC PCS 7 and the local administrator are automatically added to this group. Other user accounts must be manually added to this group by a user with administrative rights.
- **SIMATIC HMI CS**
The members of this group may only perform configurations; they may not make direct changes to the runtime components. This group is empty by default and is reserved for later use.
- **SIMATIC HMI VIEWER**
The members of this group may access configuration and runtime data only in read-only mode. This group is primarily used for user accounts of Web publishing services, for example, the IIS (Internet Information Services) that is needed for operation of the SIMATIC PCS 7 Web server.

After the installation of SIMATIC PCS 7, follow these steps:

1. Create a project folder on the hard disk and create a folder share for it.
2. Assign only the minimum necessary share permissions to the project folder.
 - Configure "full access" only for the local groups "SIMATIC HMI" and "Administrators" in Windows Explorer.
3. Assign only the minimum necessary security settings (file system rights) to the project folder. - Add "full access" only for the local group "SIMATIC HMI" in Windows Explorer.

Note

For SIMATIC PCS 7, we recommend that you apply the principle of least privilege and refrain from using administrative user accounts, in particular when operating SIMATIC PCS 7.

7.3.4 SIMATIC NET

During installation of SIMATIC NET components via the SIMATIC PCS 7 setup program, the following local user group is added to the Windows group management:

- SIMATIC NET
When the "SIMATIC NET" user group is created, only the Windows user accounts that work with PCS 7, PCS 7 OS or Route Control projects must be members of this group.

The user account used during installation is added to the "SIMATIC HMI" group by default.

7.3.5 Siemens TIA Engineer

During installation of the engineering station (ES) via the SIMATIC PCS 7 setup program, the following local user group is added to the Windows group management:

- Siemens TIA Engineer
Only Windows user accounts that work with SIMATIC PCS 7 ES projects must be members of this group.

The user account used during the ES installation is added to the "Siemens TIA Engineer" group by default.

7.3.6 SIMATIC BATCH

For SIMATIC BATCH, the following new user group is created during installation using the SIMATIC PCS 7 setup program:

- SIMATIC BATCH
The members of this group have full access to the SIMATIC BATCH directory "sbdata". Only user accounts working with SIMATIC BATCH must be a member of this group.

The user account used during installation is added to the "SIMATIC BATCH" group by default.

The following approval is also created new at the time of installation:

- BATCH

The required approval authorization (full access to the user group "SIMATIC BATCH") is configured during the installation. The batch files are later created in these shares.

7.3.7 SIMATIC Route Control

For SIMATIC Route Control, the following user groups are created during installation via the SIMATIC PCS 7 Setup:

- RC_ENGINEER
- RC_MAINTENANCE
- RC_OPERATOR_L1
- RC_OPERATOR_L2
- RC_OPERATOR_L3

The user account used during installation is added to the "RC_MAINTENANCE" group by default.

The following share is also being configured:

- RC_LOAD

The share permissions and security settings are automatically issued during the installation. The settings are uniform for all five groups. This means access to the project does not depend on the group to which the logged on account is added. The RC data are later saved in these shares.

7.3.8 SIMATIC Management Console

For use of the SIMATIC Management Console, the following user groups are also created during installation using the SIMATIC PCS 7 setup program:

- **SIMATIC Management Administrators** (only present on the SIMATIC Management Console)
Members of this group have administrative access to the Management Console as well as all authorizations.
Enter the members of this group in the local Administrators group on the target computers. This gives the members of this group permission to make changes to the installed software.
- **SIMATIC Management Users**
Members of this group are given restricted access to the Management Console and "Read only" permission.
Enter users that are assigned to the "SIMATIC Management Administrators" user group on the Management Console computer and the other PCS 7 systems, in the "SIMATIC Management Users" user group as well.
- **Administrators**
All users of the Management Console must be users with administrative rights on the respective system, i.e. member of the local "Administrators" group. It makes no difference whether a local user or a computer-specific domain user is used.

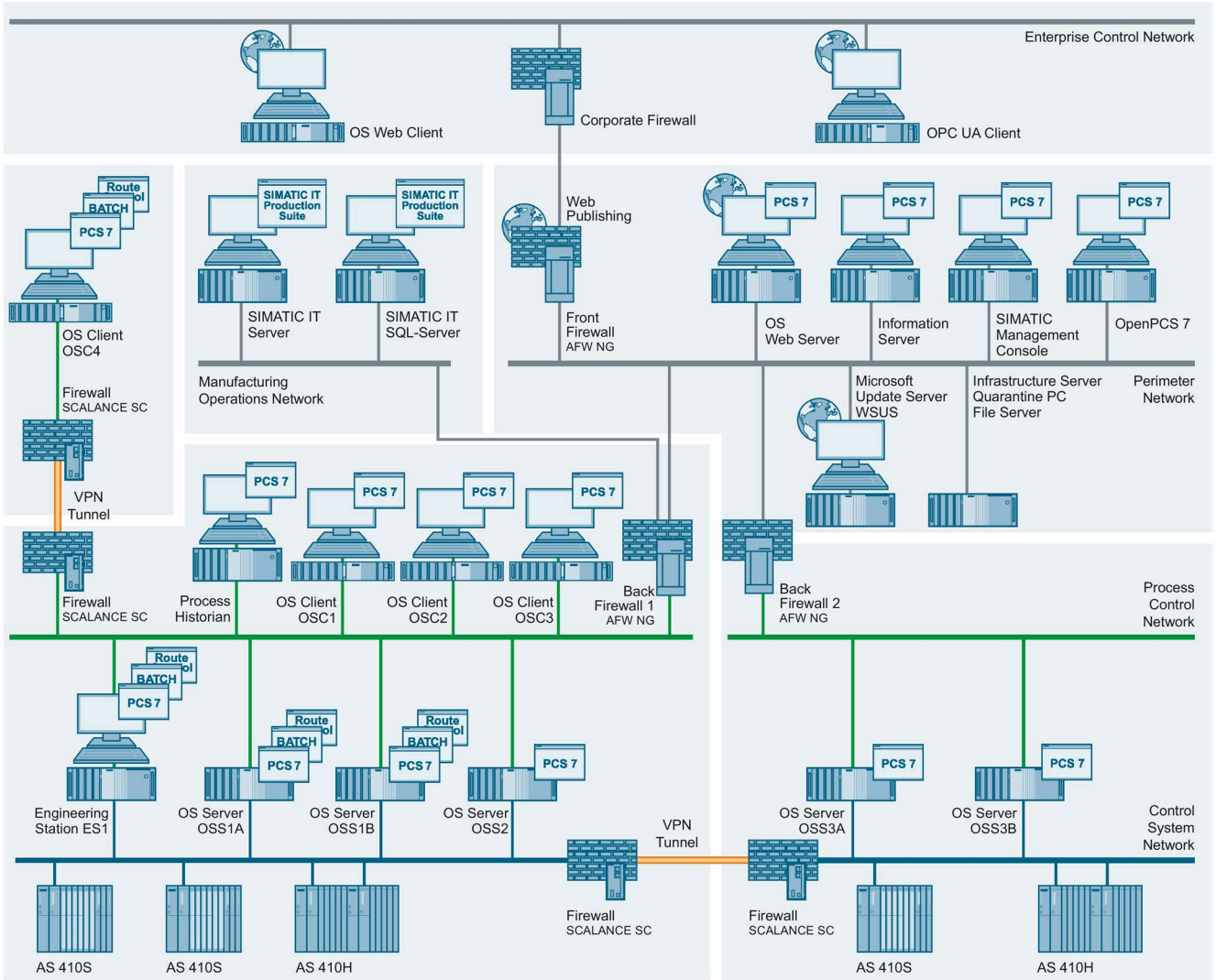
7.3.9 Logon_Administrator

During installation of SIMATIC PCS 7, using the SIMATIC PCS 7 setup program, the following local user group is added to the Windows group management if the "SIMATIC Logon" option was selected:

- **Logon_Administrator**
Only Windows users that want to configure SIMATIC Logon options must be a member of this group.

7.3.10 Example configuration

The following figure shows the example configuration:



7.3 Administration of computers and users

For the example configuration, the following users are created according to the above-mentioned recommendations in this section:

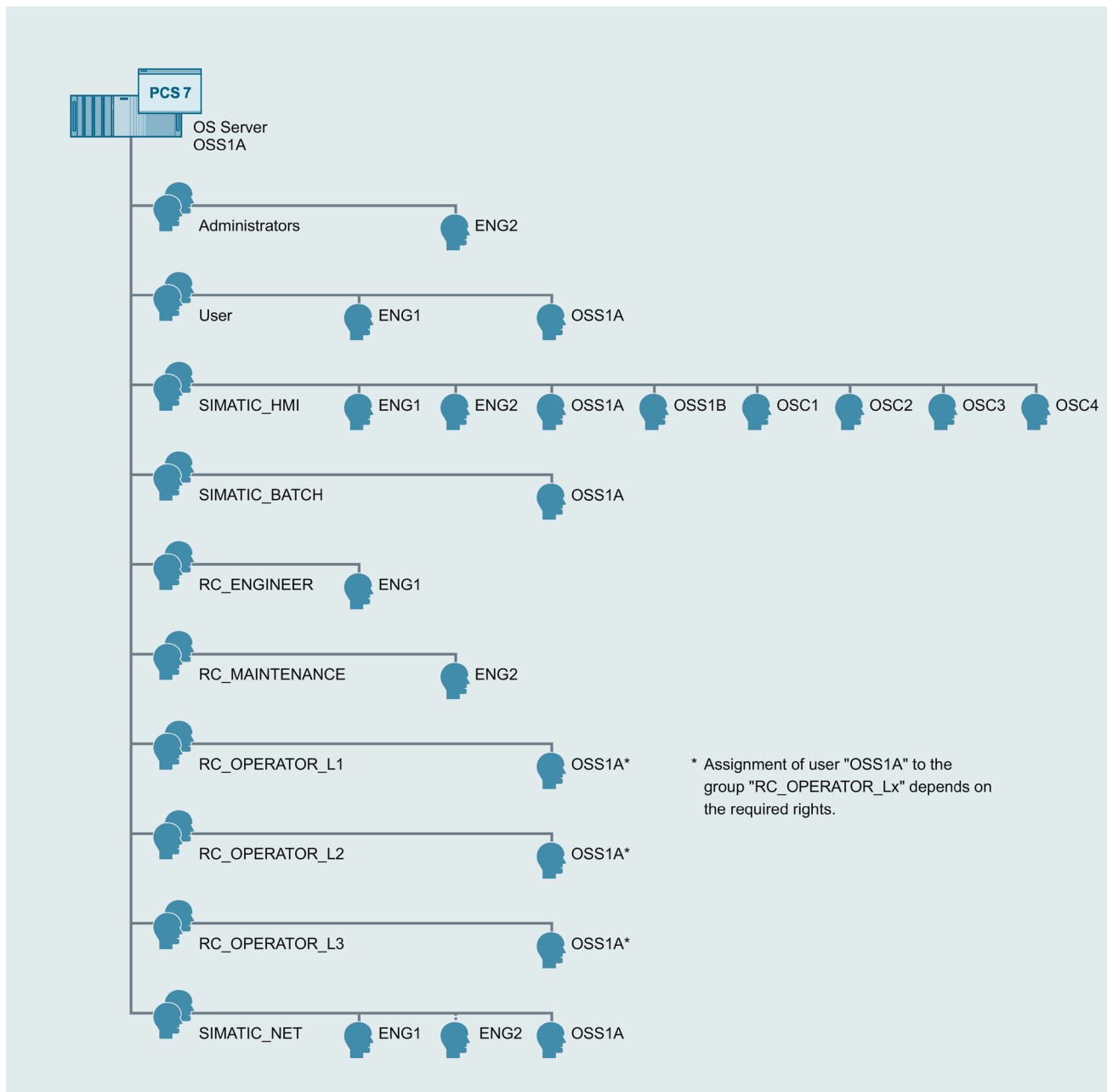
User	Description
ENG1	<p>PCS 7 Engineer 1</p> <ul style="list-style-type: none"> • Works on the engineering station (ES) with the SIMATIC Manager, HW Config, NetPro, CFC, SFC and WinCC • Loads the automation systems and the OS server from the ES • Also performs operations on the OS clients
ENG2	<p>PCS 7 Engineer 2</p> <p>In addition to ENG1, this user is the administrator of the system</p>
OSC1	<p>Local Windows user who is generally permanently logged on OS client "OSC1" (device-specific, "non-personalized").</p> <p>Logon to the operating system performed using Windows Autologon.</p>
OSC2	<p>Local Windows user who is generally permanently logged on OS client "OSC2" (device-specific, "non-personalized").</p> <p>Logon to the operating system performed using Windows Autologon.</p>
OSC3	<p>Local Windows user who is generally permanently logged on OS client "OSC3" (device-specific, "non-personalized").</p> <p>Logon to the operating system performed using Windows Autologon.</p>
OSC4	<p>Local Windows user who is generally permanently logged on OS client "OSC4" (device-specific, "non-personalized").</p> <p>Logon to the operating system performed using Windows Autologon.</p>
OSS1A	<p>Local Windows user who is generally permanently logged on OS server "OSS1A" (device-specific, "non-personalized").</p> <p>Logon to the operating system performed using Windows Autologon.</p>
OSS1B	<p>Local Windows user who is generally permanently logged on OS server "OSS1B" (device-specific, "non-personalized").</p> <p>Logon to the operating system performed using Windows Autologon.</p>
OSS2	<p>Local Windows user who is generally permanently logged on OS server "OSS2" (device-specific, "non-personalized").</p> <p>Logon to the operating system performed using Windows Autologon.</p>
OSS3A	<p>Local Windows user who is generally permanently logged on OS server "OSS3A" (device-specific, "non-personalized").</p> <p>Logon to the operating system performed using Windows Autologon.</p>
OSS3B	<p>Local Windows user who is generally permanently logged on OS server "OSS3B" (device-specific, "non-personalized").</p> <p>Logon to the operating system performed using Windows Autologon.</p>

The following table shows the different user groups to which the above-named users must be assigned:

Computer/ Local group	ES1	OSC1	OSC2	OSC3	OSC4	OSS1A	OSS1B	OSS2	OSS3A	OSS3B
Administrators	ENG2	ENG2	ENG2	ENG2	ENG2	ENG2	ENG2	ENG2	ENG2	ENG2
User	ENG1	OSC1 ENG1	OSC2 ENG1	OSC3 ENG1	OSC4 ENG1	OSS1A ENG1	OSS1B ENG1	OSS2 ENG1	OSS3A ENG1	OSS3B ENG1
SIMATIC HMI	ENG1 ENG2	ENG1 ENG2 OSC1 OSS1A OSS1B OSS2 OSS3A OSS3B	ENG1 ENG2 OSC2 OSS1A OSS1B OSS2 OSS3A OSS3B	ENG1 ENG2 OSC3 OSS1A OSS1B OSS2 OSS3A OSS3B	ENG1 ENG2 OSC4 OSS1A OSS1B OSS2 OSS3A OSS3B	ENG1 ENG2 OSC1 OSC2 OSC3 OSC4	ENG1 ENG2 OSC1 OSC2 OSC3 OSC4	ENG1 ENG2 OSC1 OSC2 OSC3 OSC4	ENG1 ENG2 OSC1 OSC2 OSC3 OSC4	ENG1 ENG2 OSC1 OSC2 OSC3 OSC4
SIMATIC BATCH ¹⁾	ENG1 ENG2	OSC1	OSC1	OSC3	OSC4	OSS1A	OSS1B	OSS2	OSS3A ¹⁾	OSS3B ¹⁾
RC_ENGINEER ²⁾ ENG1	ENG1	-	-	-	-	ENG1	ENG1	ENG1	ENG1	ENG1
RC_MAINTENANCE ENG1 ²⁾	ENG2	-	-	-	-	ENG2	ENG2	ENG2	ENG2	ENG2
RC_OPERATOR_L1 ³⁾	-	OSC1	OSC2	OSC3	OSC4	OSS1A	OSS1B	OSS2	OSS3A	OSS3B
RC_OPERATOR_L2 ³⁾	-	OSC1	OSC2	OSC3	OSC4	OSS1A	OSS1B	OSS2	OSS3A	OSS3B
RC_OPERATOR_L3 ³⁾	-	OSC1	OSC2	OSC3	OSC4	OSS1A	OSS1B	OSS2	OSS3A	OSS3B
SIMATIC NET	ENG1 ENG2	-	-	-	-	OSS1A ENG1 ENG2	OSS1B ENG1 ENG2	OSS2 ENG1 ENG2	OSS3A ENG1 ENG2	OSS3B ENG1 ENG2
Siemens TIA Engineer	ENG1 ENG2	-	-	-	-	-	-	-	-	-

¹⁾ Provided that SIMATIC BATCH is required/used in the example configuration.
²⁾ Provided that SIMATIC Route Control is required/used in the example configuration.
³⁾ Assignment of user OSC1 ... 4 to RC_OPERATOR_Lx depends on the required permission

The following figure shows an example of the local management of users and groups on the server "OSS1A":



Additional information

You can find additional information about computer and user management in the document "SIMATIC Process Control System PCS 7 Security Concept PCS 7 & WinCC (Basic)" (<https://support.industry.siemens.com/cs/ww/en/view/109780811>).

You can also find information on this in the manual "SIMATIC Process Control System PCS 7 PC Configuration" (<https://support.industry.siemens.com/cs/ww/en/view/109794377>).

You can find additional information on user rights for SIMATIC Route Control, especially regarding the assignment of users to the user groups RC_OPERATOR_L1/L2/L3, in the programming and operating manual "SIMATIC Process Control System PCS 7 SIMATIC Route Control" (<https://support.industry.siemens.com/cs/de/en/view/109794449>).

7.4 Password policies

Introduction

Source: https://www.bsi.bund.de/EN/Home/home_node.html (ORP.4. Identity and authorization management)

Poorly chosen passwords are still one of the most common deficiencies for security. Often, the user chooses character combinations that are too short or too simple.

Fixed rules must be defined for generating and handling passwords. The users of IT systems must be instructed in this regard. Thus, using weak passwords or handling them wrongly must be prevented. The following rules for password use must be followed:

- Passwords must be kept secret and only known to the user personally.
- At the most, passwords may be put down in writing for the purpose of depositing them securely. A distinction must be made here between physical storage, for example on paper, and digital storage, for example, through a password manager.
- In the case of physical storage, the password must be securely stored in a sealed envelope.
- Passwords must not be saved to programmable function keys of keyboards or mice.
- A password must be changed if it has become known to unauthorized persons or if there is any such doubt.
- Reuse of passwords that have already been used must be prohibited. If required, rules can be defined that passwords can be reused after a reasonable amount of time has passed.
- Passwords may only be entered unobserved.
- Pre-selected passwords and identifiers from the manufacturer upon delivery of IT systems, for example, must be replaced by individual passwords and, if possible, identifiers must be replaced as well.

To find passwords, for example, hackers use so-called brute-force attacks that automatically try a variety of possible character combinations or test entire dictionaries. To prevent such attacks, a password should meet certain quality requirements.

7.4 Password policies

This is why care should be taken in defining and implementing a password policy in the automation plant. Such a password policy should take the following points into consideration:

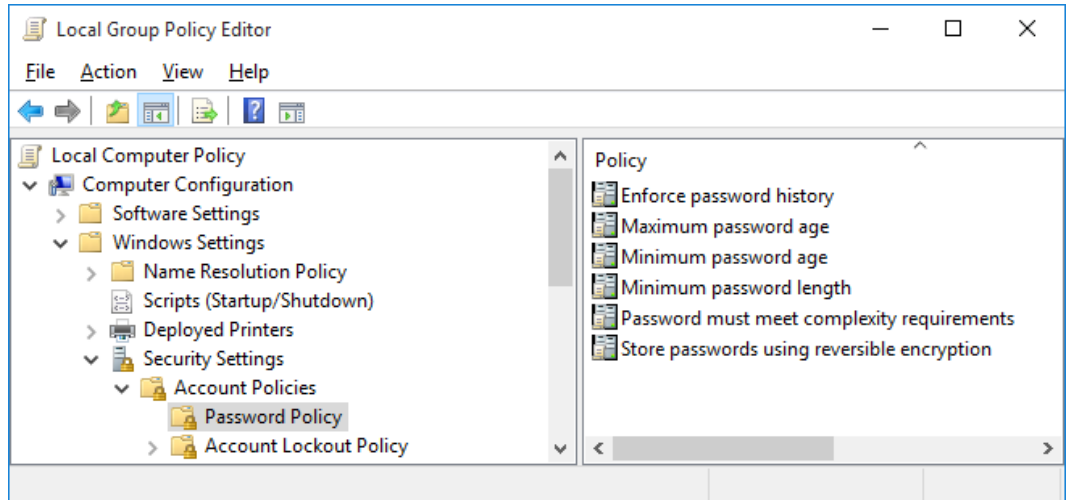
- A password must not be too easy to guess; therefore, it must not contain any personal or professional information of the user, such as the name, car license plate number or date of birth.
- Passwords may not be used multiple times. A different password must be used for every IT system or every application.
- For a good password, the length and types of characters like uppercase and lowercase letters, special characters and numbers must be chosen in a meaningful combination, depending on the process used:
for example, 20 – 25 characters in length and two character types used (less complex, longer password or pass-phrase),
for example 8 – 12 characters length and four character types used (complex, shorter passwords)
- The application use of passwords influences the requirements for the security of passwords.
- Password aging
Passwords must be changed at regular intervals (every 6 months at the latest).
- Password history
A new password must differ significantly from the previous password (by at least 3 characters).

Procedure

The following procedure is described using the example of a "Windows 10" operating system.

To implement the password policies, follow these steps:

1. Start the Group Policy Editor for the local group policies "gpedit.exe" in an administrative command prompt (these settings can be made centrally in a domain) and configure the following policy settings (Group Policy Object or GPO).
2. Select "Computer Configuration > Windows Settings > Security Settings > Account Policies > Password Policy" in the left navigation pane. The password policies are displayed.



3. Make the required settings for the following policies:

Policy	Purpose
Enforce password history	Prevents users from creating a new password that is the same as their current password or one recently used. The value "1", for example, means that only the last password is prevented as a new password. The value "5", for example, means that only the last five passwords are prevented as a new password.
Maximum password age	Specifies the maximum lifetime of passwords in days. After this number of days has expired, the user must change the password.
Minimum password age	Specifies after how many days a user can change their password at the earliest.
Minimum password length	Specifies the minimum number of characters that make up a password.
Password must meet complexity requirements	Requires that a password meets the following minimum requirements: <ul style="list-style-type: none"> • At least 6 characters. • It must consist of uppercase and lowercase letters, numbers and special characters. • It may not contain the user name.

Note

For device-specific user accounts, password changes are only permissible during a maintenance phase (SIMATIC PCS 7 runtime mode stopped), because these user accounts are used for authentication of the communication between SIMATIC PCS 7 systems, among other things. Password changes of the affected user accounts must be made simultaneously on all involved systems, otherwise proper operation cannot be ensured. We therefore recommend that you disable password aging for these user accounts.

7.5 Domain Controller

Introduction

For availability and redundancy reasons, configuration of an Active Directory (Windows domain) with at least two domain controllers within the SIMATIC PCS 7 security cell (terminal bus/PCN; in sample configuration cells 1 and 2) is recommended.

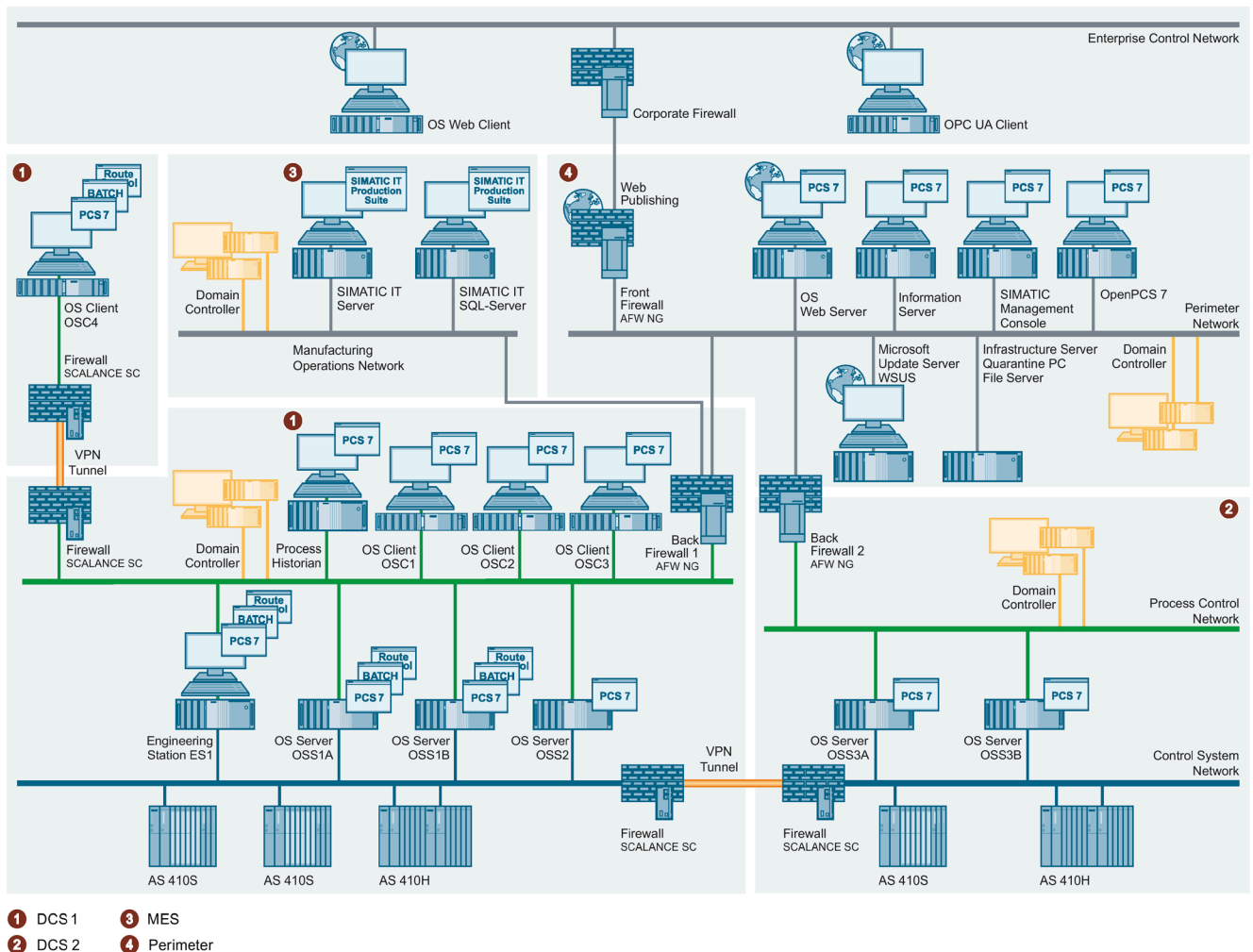
Note

An available and working domain infrastructure is necessary for correct and stable operation of SIMATIC PCS 7 systems in an Active Directory.

Instructions for the recommended design of a domain infrastructure can be found at Microsoft "Designing the Location Topology (<https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/designing-the-site-topology>)".

If there are multiple subnets/security cells/locations present in a system, depending on the requirement, at least one domain controller each must be provided there, if the availability of the Active Directory cannot be ensured through other measures (for example, by means of a corresponding network structure).

This changes the sample configuration as follows:



A redundant domain controller pair is implemented in each of the security cells DCS1, DCS2, MES and Perimeter for reasons of availability.

Preparations

A computer with the following operating system should be employed as a domain controller:

- Windows Server 2019

Note

The use of a SIMATIC PCS 7 computer (for example, of the PCS 7 OS server, PCS 7 ES station, etc.) as a domain controller is not permitted.

When a SIMATIC PCS 7-IPC bundle system is used as hardware for the domain controller, the A1 Image of a server bundle must be used for the operating system installation.

The installation and configuration of a computer as a domain controller is divided into the following steps:

1. Configuration of the computer name (this can no longer be changed after installation is complete)
2. Configuration of the network adapter (IP address, subnet, etc.)

Note

A domain controller should have only one active network adapter configured. Further information (keyword: Multihomed) can be found at Microsoft "Active Directory communication fails on multihomed domain controllers"

(<https://support.microsoft.com/en-us/kb/272294>).

If a redundant terminal bus (PCN) via PRP/SIMATIC NET SOFTNET-IE RNA is used, the domain controller must be connected to an RNA device (for example, RUGGEDCOM RSG909R). The use of SIMATIC NET SOFTNET-IE RNA is not approved for this.

3. Installation of Active Directory Domain Services
4. Installation and configuration of the DNS and WINS server
5. Configuration of users and user groups
6. If required, the configuration of group policies (GPO)

Procedure

The following points must be observed:

- Domain controllers should be fully installed and configured before starting the forest setup of SIMATIC PCS 7 (before adding the first SIMATIC PCS 7 system to the domain).
- The installation should be carried out with actual settings (for host name, IP address, subnet mask, etc.).
- The event logs on the domain controllers should be checked prior to adding the first SIMATIC PCS 7 computer to the new domain. If problems are detected, the errors should be resolved beforehand. The proper functioning of the Active Directory must be ensured.
- Systems should only be included in the domain after it has been ensured that all domain controllers, DNS servers and WINS servers have completely replicated (synchronized).

Note

If you install PCS 7 stations in a domain, be aware of the group policies or other restrictions that may hinder the installation. Consult the responsible Administrator as regards these settings the required approvals, and authorizations.

Computer name of the domain controller

To set the computer name, proceed as described in section 5.3.1, "Computer name (Page 27)".

Static IP address

The domain controllers must be provided with a static (fixed) IP address. To do so, proceed as described in section 5.2.4 "Example configuration: Setting of IP addresses and subnet mask (Page 24)".

The following table summarizes the addresses for the two domain controllers for the DCS1 security cell designated in the example before installation of the Active Directory Domain Services.

	Domain Controller 1 (DC1)	Domain Controller 2 (DC2)
IP address	192.168.2.125	92.168.2.126
Subnet mask	255.255.255.192	255.255.255.192
Standard gateway	192.168.2.65	192.168.2.65
FQDN	DC1.production1.enterprise.local	DC2.production1.enterprise.local

7.5.1 Installation and configuration of the first domain controller (DC1)

You can get information on how to install the Active Directory Domain Services (Windows domain) under Windows Server 2019, for example, under "Step by Step Guide: How to Setup Active Directory Domain Service on Windows Server 2019" (<https://msftwebcast.com/2019/03/step-by-step-guide-how-to-setup-active.html>).

If possible, install a new domain in a new forest without connection to other forests/domains (e.g. subdomains or trusts) to have full control over configuration and administration of this domain. This guarantees stable and high-availability operation for your SIMATIC PCS 7 system.

Note

The selected Fully-Qualified Domain Name (FQDN) can no longer be changed after installation of the AD DS role and should correspond to the desired domain name of the productive environment.

The FQDN must always consist of at least two name components that are separated by a dot. In this manual, the top-level domain (TLD) used is "local" (in this scenario, "production1.enterprise.local").

Note

When providing Active Directory Domain Services (AD DS), specify the highest value your environment supports for the domain and forest functional levels. In this way, you can use as many AD DS features as possible. The selection is based on the domain controllers with the oldest operating system versions in your domain/forest.

Further information on this can be found under "Forest Structure and Domain Functional Levels". (<https://docs.microsoft.com/en-de/windows-server/identity/ad-ds/active-directory-functional-levels>)

Note

The functional levels can be subsequently adapted in the Active Directory. However, these can only be upgraded. Information on this can be found under "Raise the Domain Functional Level" ([https://technet.microsoft.com/en-us/library/cc753104\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/cc753104(v=ws.11).aspx)) and "Raise the Forest Functional Level". ([https://technet.microsoft.com/en-us/library/cc730985\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/cc730985(v=ws.11).aspx))

Note

Select the "DNS server" option during installation of the AD DS to locally install the DNS server role. Among other things, this causes the "Preferred DNS Servers" setting in the local network adapter setting to be configured to the local host address 127.0.0.1.

The option "Obtain IPv6 Address Automatically" should be selected within the network configuration, under "Internet PROTOCOL Version 6 (TCP/IPv6) for the DNS server configuration."

7.5.1.1 Configuration of the DNS server

A central server-based name resolution is ensured through the Domain Name System (DNS). This is essential for operation of an Active Directory and its member systems. In this context, see section 5.3, "Name resolution (Page 27)".

Proper DNS operation requires both the Forward Lookup Zone and the Reverse Lookup Zone to be configured correctly. The Forward Lookup Zone resolves the computer name to an IP address. The Reverse Lookup Zone resolves an IP address to a computer name.

Forward Lookup Zone

The Forward Lookup Zone is created automatically during installation of the DNS server. Verify that the settings in the Server Manager are correct (here, using Windows Server 2019 as an example).

1. Click "Server Manager > Tools > DNS".
2. Open "DNS > '<ComputerName>' > Forward Lookup Zones" in the left navigation area.
3. Select the Forward Lookup Zone that you created by entering FQDN when you installed the DNS server (in this example: production1.enterprise.local) and select "Properties" from the shortcut menu (after a right-click).
4. In the "General" tab, select the option "secure only" under the menu command "Dynamic Updates".

The updates that do not conform to the Microsoft standard are classified as non-secure updates. This can sometimes happen during internal domain updates (for example, internal software, profile updates, etc.). That is why this option should be selected. Furthermore, the existing DNS zones must be AD-integrated, and the zone transmission should be disabled.

5. Check whether the "Name Server" tab contains the first domain controller "dc1.production1.enterprise.local" including its IP address. If not, manually add the system using "Add".
6. Click "OK".

Reverse Lookup Zone

A Reverse Lookup Zone is not created during the installation of the DNS server. It is recommended that this zone be created retroactively. To that end, proceed as follows:

1. Click "Server Manager > Tools > DNS".
2. Select "DNS > '<ComputerName>' > Reverse Lookup Zones" in the left navigation area.
3. Right-click the Reverse Lookup Zone and select the "New Zone" command from the shortcut menu.
The "New Zone Wizard" then opens. You can use it to create a new Reverse Lookup Zone.
4. Click "Next".
5. In the "Zone Type" dialog, select the "Primary zone" option and "Store the zone in Active Directory". Confirm the entry with "Next".
6. In the "Active Directory zone replication partition" select the option "On all DNS servers that are executed on domain controllers in this domain: '<FQDN of the domain>". Click "Next".
7. Select the "IPv4 Reverse Lookup Zone" option from the "Reverse Lookup Zone Name" dialog. Click "Next".
8. In the "Reverse Lookup Zone Name" dialog, select the "Network ID" option and enter an appropriate IP address of your subnet (192.168.2. in this example). Click "Next".
9. In the "Dynamic Updates" dialog, select the option "Allow Only Secure Dynamic Updates" (see Forward Lookup Zone). Click "Next".
10. Check the settings you have made and confirm the entries with "Finish".
The new Reverse Lookup Zone is created and displayed in the DNS Manager.
11. Check the newly created zone and check in the properties of the zone in the "Name Server" tab whether DC1 including its IP address is configured. If necessary, supplement this system by pressing the "Add..." button and entering the FQDN of the domain server ("dc1.production1.enterprise.local" in this example), if this is not the case, or resolve the IP address by pressing the "Edit..." – "Resolve" and "OK" buttons.
Exit the properties window by pressing "OK".

Additional settings and checking the DNS name resolution

The "nslookup" tool (Name Server Lookup) is available for checking whether the DNS name resolution is functioning correctly.

1. Open a command prompt window (cmd) and enter the command "nslookup".
The output ("Standard server: Unknown"; "Address: ::1") indicates that the server is trying to resolve the DNS name using the IPv6 protocol. Enter the "exit" command to exit "nslookup".
2. To change the DNS name resolution to the IPv4 protocol, open the properties of the Internet Protocol Version 6 (TCP/IPv6) in the network adapter settings.
3. In the properties dialog, select the "Obtain DNS server address automatically" option and confirm the entry with "OK".
4. Complete the configuration of the network adapter with "Close".
5. Under "Network connections", check whether the network adapter used has been assigned to the domain network. If this is not the case (e.g. "Unidentified Network"), disable and enable the respective adapter using the shortcut menu that opens with a right-click.
6. Switch to the command prompt and enter the command "nslookup" once again.
From the output of the standard server "localhost" and the IP address (127.0.0.1), you can recognize that the DNS name resolution is now using the IPv4 protocol.
When you enter the IP address of the first domain controller (192.168.2.125), the computer name (dc1.production1.enterprise.local) and the IP address are output.
When you enter the computer name as FQDN, the output is also the computer name and the associated IP address.
The function test of the DNS server on the first domain controller is thus completed successfully.
Quit 'nslookup' with input of the "exit" command.

7.5.2 Installation and configuration of an additional domain controller (DC2-DCn) in an existing domain

Check of network settings on the new future domain controllers

Prior to adding and installing an additional domain controller in the domain, the network adapter settings must be checked on this system.

To do so, change to the dialog in the network adapter settings in which the IP address and subnet mask are set. The IP addresses of the "Preferred DNS servers" are checked or set in this dialog.

In this case, the settings made in the following table for an additional new domain controller in security cell DCS1 must be made for the sample configuration:

	Domain Controller 2 (DC2)
IP address	192.168.2.126
Subnet mask	255.255.255.192
Standard gateway	192.168.2.65
Preferred DNS server	127.0.0.1
FQDN	DC2.production1.enterprise.local

Further procedure

There are two possibilities before the installation of an additional domain controller:

- The computer to be installed as an additional domain controller is not a member of the domain
- The computer to be installed as an additional domain controller is already a member of the domain

The installation differs slightly for these two possibilities.

If the computer that is intended as an additional domain controller is not yet a member of the domain, first add it as a member server in the domain. After restart, the system is a domain member and can now be upgraded to the domain controller.

The remaining procedure is then identical for both of the above-mentioned possibilities and is described below based on a Windows Server 2019 operating system.

1. Log onto the new domain controller to be installed as a domain administrator.
2. Open the Server Manager.
3. Go to "Manage" and use the function "add Roles and Features" to start the "add Roles and Features Wizard". Select the role "Active Directory Domain Services" (AD DS) (see "Installation and configuration of the first domain controller (DC1) (Page 131)").
4. After closing the wizard, use the notification function of the Server Manager similar to the first domain controller to start the configuration "Demote server to domain controller". The "Active Directory Domain Services Configuration Wizard" is started.

5. Select the option "Add a domain controller to an existing domain" and under "Domain" check the FQDN of the existing domain and the suggested user (Domain administrator) under "Logon information". Click "Next".
6. The remainder of the installation of the AD DS and the DNS server is the same as for the first domain controller (see Installation and configuration of the first domain controller (DC1) (Page 131)). Select "Any domain controller" under "Replication options".
7. In the DNS server zone settings, you have to open the "Name Servers" tab on all DCs to verify that the newly installed DCs with activated DNS role are present. If this is not the case, you have to add the missing DNS servers or resolve the IP addresses.

7.5.3 Check of network settings on the DCs

Once the domain controller installation is completed, the network settings must be checked on all domain controller systems.

To do this, change to the dialog in the network adapter settings in which the IP address and subnet mask are set. The IP addresses of the "Preferred DNS servers" are checked or set in this dialog. In this case, the settings made in the following table for the two domain controllers in security cell DCS1 must be made for the sample configuration:

Note

Under "Network connections", check whether the network adapter used has been assigned to the domain network. If this is not the case (for example, "Unidentified Network"), disable and enable the respective adapter using the shortcut menu which you can access with a right-click of the mouse.

	Domain Controller 1 (DC1)	Domain Controller 2 (DC2)
IPv4 address	192.168.2.125	192.168.2.126
Subnet mask	255.255.255.192	255.255.255.192
Standard gateway	192.168.2.65	192.168.2.65
Preferred DNS server	127.0.0.1	127.0.0.1
	192.168.2.126	192.168.2.125
IPv6 DNS setting	"Obtain DNS server address automatically"	"Obtain DNS server address automatically"
FQDN	DC1.production1.enterprise.local	DC2.production1.enterprise.local

7.5.4 WINS installation and configuration

The Windows Internet Name Service (WINS) server is used for the NetBIOS name resolution and is the Windows implementation of a NetBIOS Name Server (NBNS).

The NetBIOS name resolution is very important for operation of SIMATIC PCS 7 and can be implemented in a domain environment by installing WINS on the domain controllers.

7.5.4.1 WINS installation

1. Open the Server Manager.
2. Go to "Manage" and use the function "add Roles and Features" to start the "add Roles and Features Wizard". Select the "WINS Server" feature.
3. Click "Install".
4. The installation of the "WINS Server" feature starts.
5. Use the "Close" button to close the wizard once installation is complete.
This completes the installation of the WINS server.

7.5.4.2 Entering the WINS server in the IPv4 configuration

After installation, the WINS servers must be entered in the properties of the IPv4 configuration for all computers in the network, including the domain controller. To do this, proceed as follows:

1. Open the Properties dialog of the corresponding network adapter in the network connections.
2. Select the "Internet Protocol Version 4 (TCP/IPv4)" from the list and click the "Properties" button.
3. In the Properties dialog, click "Advanced..." to open the advanced TCP/IP settings.
4. Select the "WINS" tab in the dialog.
5. Click "Add...".
6. Add the IP addresses of the installed WINS servers, select the setting "Enable NetBIOS Over TCP/IP" and close all windows of the properties dialog.

7.5.4.3 Checking the configuration of the WINS server

1. To check the configuration of the WINS server, open a command prompt window (cmd) and enter the command "nbtstat -RR". Name release packages are sent to the WINS and the update is started.
2. Start the "WINS" Management Console under "Tools" in the Server Manager. The WINS Management console opens.
3. In the left pane, open the displayed function tree completely and right-click "Active Registrations". Select the "Show data records..." command from the shortcut menu.
4. Click "Start Search" to output all entries of the WINS server.
5. The result of the search is displayed in the WINS Management Console.

Note

With the recommended redundant WINS design on all participating WINS servers, configure the so-called "Push/Pull Replication" ([https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc727931\(v=ws.10\)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc727931(v=ws.10))).

It must be noted that on the WINS servers themselves, only the local system is entered as the WINS server in the network settings (<https://docs.microsoft.com/en-us/troubleshoot/windows-server/networking/setting-wins-server-options>).

7.5.5 Operations master roles (FSMO)

On the one hand, a large number of domain controllers can be used that allocate all domain-relevant data reciprocally using replication mechanisms (synchronization) and thus operate redundantly (as "multimasters"). On the other hand, every forest has operation master roles (FSMO - Flexible Single Master Operations) that should be distributed among individual domain controllers. Some of these roles are present only once in a forest, while others can be present multiple times.

A forest has five master roles and the so-called global catalog:

1. Schema master
The schema master is responsible for schema updates within the forest (e.g. user, computer or resources, as well as the attributes that can be assigned to individual objects). When the scheme is updated, it is replicated to the other domain controllers within the forest.
This role exists only once within the forest.
2. Domain naming master
The domain naming master is responsible for changes to the namespace within the forest. The holder (domain controller) of this master role is the system that can add and remove domains to and from the forest. In addition, the references to other forests are managed by this system.
This role exists only once per forest.

3. RID master

The RID master is responsible for managing RID pool requests from all domain controllers within a domain. It also implements the relocation of an object from one domain to another.

When a domain controller creates a new object, e.g. a user or group, the RID master assigns it a unique Security ID (SID). This SID consists of a domain SID (this is identical for all SIDs within the domain) and a relative ID (RID), which is unique for every generated object within the domain.

For this purpose, every domain controller reserves a pool of RIDs that allows it to generate a unique SID. If this RID pool is used up, it sends a request to the RID master, which answers by sending a new pool of unused RIDs.

This role exists only once per domain.

4. Infrastructure master

If an object references another object in another domain, this reference is represented by a GUID. This consists of an SID and the distinguished name (DN) of the referenced object.

The infrastructure master is responsible for updating the object SID and the DN in the cross-domain object references.

This role exists only once per domain.

5. Primary Domain Controller (PDC) emulator

The PDC is the system responsible for time synchronization within the forest (PDC at the root of the forest) and the domains (one PDC per domain). An accurate time is required for Kerberos authentication and for replication within the forest and domain; it is therefore a uniform and important basis for all systems. This time base is organized hierarchically within the domain.

The forest PDC should be synchronized with an external time source (for example, via Bürk Mobatime using DCF77 or GPS). The time synchronization of the other PDC role masters then follows the domain hierarchy.

In addition, the PDC master holds the PDC emulator role with the following functions:

- Password changes on other domain controllers are replicated first to the PDC.
- Authentication errors (e.g. wrong password) that occur on a domain controller are first forwarded to the PDC before an error message is output to the user.
- The PDC emulator also carries out all account blockings.
- The PDC emulator provides all functionalities of a Windows NT-based PDC.

This role exists once per domain.

6. Global catalog

The global catalog is an allocated data storage that allows searching through parts of all objects in all domains of a forest. The global catalog is stored on all domains that were configured as global catalog holders. It is allocated via replication. This accelerates the search for objects in a forest because no references to other domain controllers are needed.

Note**Global catalog and infrastructure master**

The global catalog service must not be run with the "Infrastructure master" role on a domain controller because this service can be disabled and serious replication errors can occur.

This malfunction is indicated by error messages 1419 in the event log.

The above-indicated limitation does not apply if all domain controllers in a domain have the "Global catalog" function enabled. This is the recommended configuration, which also increases the availability of domain-relevant data (e.g. for logon of users).

It is recommended that the five master roles be assigned to the two domain controllers (DC1 and DC2) as follows:

DC1	DC2
Schema master	Infrastructure master
Domain Naming Master	RID master
PDC emulator	Global catalog
Global catalog	

The following article describes how master roles can be distributed across the different domain controllers (with serviceable domain controllers, the roles should be transferred):

"Transfer or seize FSMO roles in Active Directory Domain Services"

(<https://docs.microsoft.com/en-us/troubleshoot/windows-server/identity/transfer-or-seize-fsmo-roles-in-ad-ds>).

The following article describes how to configure a domain controller as "global catalog": "Add or Remove the Global Catalog" ([https://technet.microsoft.com/en-us/library/cc755257\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/cc755257(v=ws.11).aspx)).

Note

The current assignment of FSMO server roles (operations master) can be displayed in a command prompt on a domain controller with the "netdom query fsmo" command.

You can determine which domain controllers are configured as "Global Catalog" in a "Site" with the administrative PowerShell commands described in the following article: "Finding the Domain Controllers or Global Catalog Servers in a Site" ([https://technet.microsoft.com/en-us/library/dd391944\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/dd391944(v=ws.10).aspx)).

7.5.6 Users and user groups

You must add users and groups that you create in the domain for operation of PCS 7 (domain users/groups) to the local SIMATIC user groups (SIMATIC HMI, SIMATIC HMI VIEWER, SIMATIC HMI CS) and the other groups, as described in section 7.3, "Administration of computers and users (Page 115)" to the SIMATIC PCS 7 systems.

Note

We recommend creating and using global domain groups. This can have a positive effect on the replication (Global Catalog, among other things) and when using SIMATIC Logon.

7.6 Operator authorizations – Rights management of the operator

The strategy of role-based access control includes restriction to minimally required rights and functions for users, operators, devices, network and software components.

7.6.1 SIMATIC Logon

Systems automated with process control systems have the following requirements concerning access to functions, data and system areas:

- User administration for granting access rights to avoid unauthorized or unwanted accesses to the system.
- Creating and archiving evidence of important or critical actions.

SIMATIC applications and system areas can be assigned individual, task-based permissions.

The user administration required for the purpose on local computers, in Windows workgroups and in Active Directory (Windows domains) is supported through the use of SIMATIC Logon.

In addition, the use of SIMATIC Logon in an Active Directory provides the benefits of high-availability and centralized administration of groups and users.

SIMATIC Logon supports the function of a "Default user". This user is automatically logged on at the start of the SIMATIC PCS 7 application or when a SIMATIC Logon user logs off. It is recommended that this user account be assigned only the minimum rights needed, e.g. rights for process monitoring or emergency operation.

7.6 Operator authorizations – Rights management of the operator

The following applications have a connection to the components of SIMATIC Logon:

- Automation License Manager (ALM)
- PCS 7 OS systems
- PCS 7 ES
- SIMATIC Batch Client
- SIMATIC Route Control
- SIMATIC Electronic Signature (optional)

You can find detailed information about SIMATIC Logon in the manual "SIMATIC Logon" (<https://support.industry.siemens.com/cs/ww/en/view/109793892>).

Also see the notes in the manual "SIMATIC Process Control System PCS 7 SIMATIC Logon Readme" (<https://support.industry.siemens.com/cs/ww/en/view/109793893>).

7.6.2 Access protection for projects/libraries on the engineering station

Introduction

It is recommended that projects and libraries on the engineering station be protected from unwanted access and that all accesses be logged.

This requires the use of SIMATIC Logon software. SIMATIC Logon allows the definition of user roles for the engineering system to which selected Windows users/groups are assigned.

The opening and editing of access-protected projects and libraries is then possible only for users that are assigned to one of the following user roles:

- Project administrator
- Project editor
- Any user who authenticates himself/herself using the project password

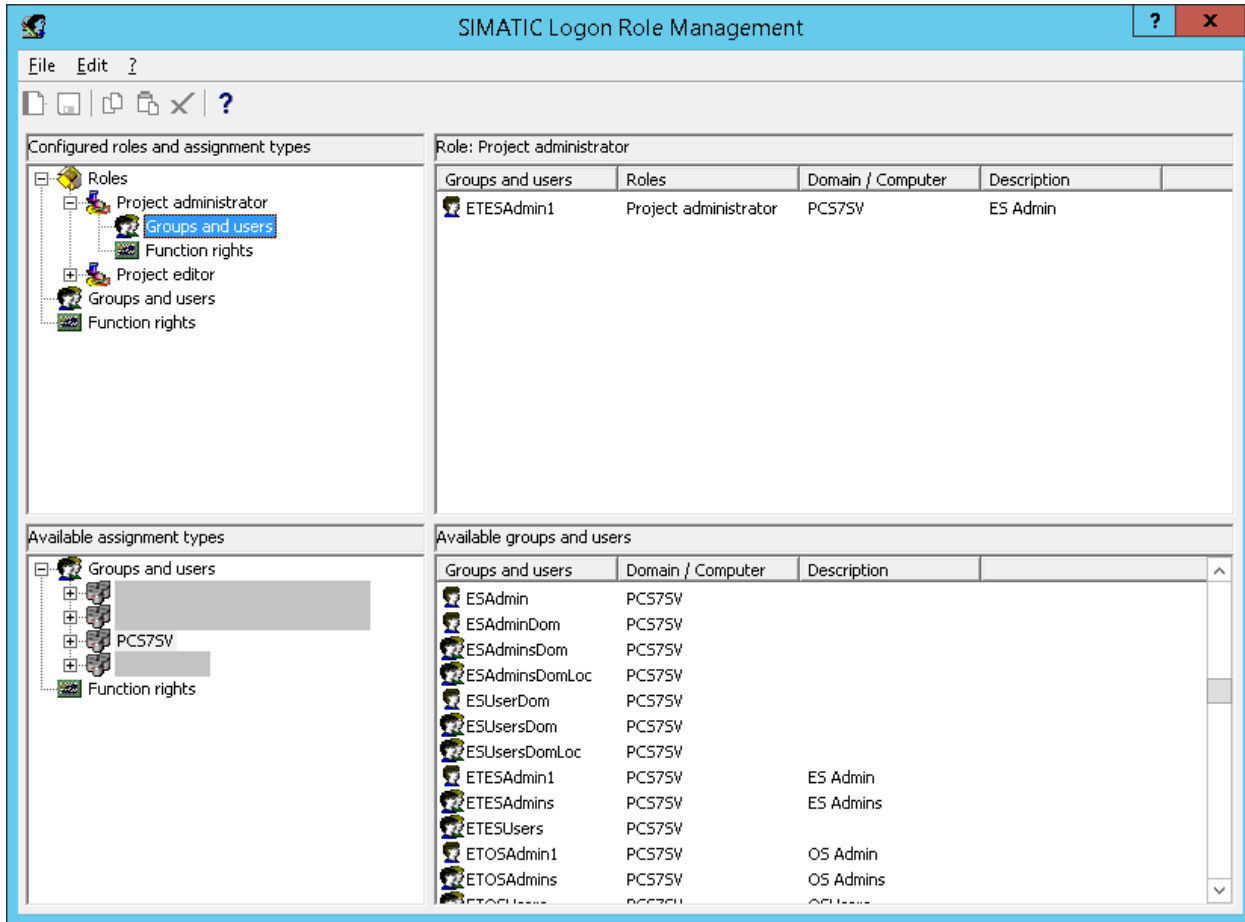
The user with the "Project administrator" role has the following rights:

- Specification of membership of users and groups of the "Project editor" role
- Specification of the project password
- Activation, deactivation and removal of access protection
- Activation, deactivation, display and removal of change logs

The user with the "Project editor" role has the following rights:

- Opening and editing of projects/libraries with access protection
- Display of change logs

The following figure shows the SIMATIC Logon Editor for role management:



Setting access protection

The following settings for access protection must be made for each project and library in the SIMATIC Manager. Synchronization is possible across an entire multiproject.

Network address range	Description	Can be executed with a user role
Enabling access protection (including defining a project password)	<ul style="list-style-type: none"> Activates access protection for a particular project or library. This project or library may only be opened and edited by Windows users who are assigned the roles of project editor or project administrator. Specifies the project password. A project password can be specified for each project/library. 	Project administrator
Deactivating Access Protection	Disables access protection for a particular project or library again.	Project administrator
Managing users	Specifies the project administrators and project editors	Project administrator
Synchronizing access protection in the multiproject	Specifies the project administrators and project editors globally for all projects and libraries in a multiproject.	Project administrator
Displaying the Change Log	Opens the change log	Project administrator Project editor
Removing Access Protection and Change Log	Removes the access protection and deletes the change log for a password-protected project or library.	Project administrator

Enabling access protection for projects/libraries

The following requirements must be met:

- SIMATIC Logon is installed.
- The "Project administrator" and "Project editor" user roles in SIMATIC Logon are automatically created during the SIMATIC PCS 7 installation.
- You are assigned the "Project administrator" role in SIMATIC Logon.
- You are logged on as "Project administrator".

The user currently logged on (e.g. "Project administrator") is displayed in the status bar of SIMATIC Manager.

Note

The project format is changed the first time access protection is activated. For this reason, you will get a message that the modified project can no longer be edited with older SIMATIC PCS 7 versions.

To enable access protection for projects/libraries and to change the password, follow these steps:

1. Select the project/library in the SIMATIC Manager.
2. Select the menu command "Options > Access Protection > Enable".
3. Enter the password and confirm it in the "Activate Access Protection" dialog.
4. Click "OK".
The selected project/library is now protected by a password and can only be opened for editing by authorized users.

To disable the access protection for projects/libraries, follow these steps:

1. Select the project/library in the SIMATIC Manager.
2. Select the menu command "Options > Access Protection > Disable".
3. Enter the password and confirm it in the "Deactivate Access Protection" dialog.
4. Click "OK".
The selected project or library is no longer protected by a password and can be opened by any user for editing.

Additional information

You can find additional information on this in the configuration manual "SIMATIC Process Control System PCS 7 Engineering System (<https://support.industry.siemens.com/cs/ww/en/view/109800500>)".

7.6.3 Change log

The change log documents the user, time, CPU, changes made, and the reason for the changes.

Requirement

The following requirements must be met:

- The SIMATIC Logon Service is installed.
- The access protection is activated.

Activating the change log

To activate the change log for a folder in the SIMATIC Manager, follow these steps:

1. In the component view of the SIMATIC Manager, select the folder for which you want to activate the change log.
2. Select the menu command "Options > Change log > Enable".
The change log for the selected folder is enabled.

The following is documented in the change log:

- Enabling/disabling/configuration of access protection and change log
- Opening/closing projects and libraries
- Downloading to the target system (system data)
- Selected operations for downloading and copying blocks
- Activities for changing the operating state
- CPU memory reset

7.6.4 ES log

The ES log documents the user, time, CPU, changes made, and the reason for the changes. If you activate the "ES log active" option, the actions for downloading and the current time stamps are logged in addition to the protected actions in CFC/SFC (objects of the chart folder).

Requirement

The following requirements must be met:

- The SIMATIC Logon Service is installed.
- The change log is activated.

Activating the ES log

To activate the ES log, follow these steps:

1. In the component view of the SIMATIC Manager, select the chart folder for which you want to activate the ES log.
2. Select the menu command "Edit > Object Properties".
The "Chart Folder Properties" dialog box opens.
3. Switch to the "Advanced" tab.
4. Select the "ES log active" option.
5. Click "OK".

The following is documented in the ES log:

- Every action is registered in chronological order in a main line followed by a line giving the reason and perhaps a log of the action itself (a download, for example). The most recent action appears in the first line.
- For the "Download entire program" action, the ES log is deleted from the log but archived as a file with a date identifier at the same time. The archiving action and the file name used (including the path) are recorded in the log.
- For the action "Start test mode", all subsequent actions resulting in a change (of value) in the CPU are logged. The logging includes the value and how it changed (address, old value, new value). Specifically, these are:
 - In the CFC
 - Assignment of parameters to I/Os
 - Activation/deactivation of forcing and force value changes
 - Activation/deactivation of runtime groups
 - In the SFC
 - Assignment of parameters to constants in steps
 - Assignment of parameters to constants in transitions
 - Assignment of parameters to constants in sequencer properties

7.6.5 Access protection for operator stations

Sufficient protection against unauthorized access to operator stations must be ensured. Two different use cases play a role here:

- The operator station must be protected against unauthorized access such as operator interventions or screen selection if nobody is logged onto this station.
This means that when the operator logs off from the station, either by manually running the corresponding function or removing the smart card, the station must be brought to a state that makes it impossible for unauthorized persons to use it.
- The operator station must be "locked" in such a way that it is impossible for an unauthorized user to exit the operator interface ("Runtime") and reach the desktop of the operating system.

Additional information

Additional information is available in the "SIMATIC Process Control System PCS 7; Operator Station" (<https://support.industry.siemens.com/cs/ww/en/view/109794374>) Configuration Manual.

7.7 Protection level concept

Using a protection level can protect the automation system (CPU) against unauthorized access. Three different protection levels in the CPU are available for this purpose:

Protection level 1

Depending on the CPU, this protection level can have different names.

For standard CPUs, protection level 1 is called "No protection". A password entry is not possible. Password protection can be set up with protection level 2 (CPU configuration via HW Config).

For F-CPU or H-CPU, protection level 1 is called "Access protection for F-CPU or Key switch position". By default, no security program can be loaded. Only after assigning a password and with the option "CPU contains security program" is it possible to load security modules in the CPU.

Protection level 2: Write protection

For protection level 2, only read access to the CPU is possible, regardless of the position of the key switch.

Protection level 3: Write/read protection

For protection level 3, neither read nor write access to the CPU is possible, regardless of the position of the switch.

Note**Protection against unauthorized access**

The use of protection level 3, "Write/read protection" to protect against unauthorized access to the automation system (CPU) is recommended.

Behavior of a password-protected CPU during operation

Before executing an online function, the reliability is checked and, if necessary, a password entry is requested.

Example: The module was configured with protection level 2, and you want to execute the "Control variable" function. Since this constitutes a write access, the configured password must be entered to execute this function.

Additional information

You can find additional information on the security level concept in the manual "SIMATIC Process Control System PCS 7 Engineering System (<https://support.industry.siemens.com/cs/ww/en/view/109800500>)" and in the manual "SIMATIC Process Control System PCS 7 CPU 410 Process Automation (<https://support.industry.siemens.com/cs/de/en/view/109748473>)".

Patch management

8.1 Overview

Microsoft usually publishes the latest updates on the second Tuesday of each month. Microsoft uses a number of different classifications for these updates "Description of the standard terminology that is used to describe Microsoft software updates" (<https://support.microsoft.com/en-us/help/824684/description-of-the-standard-terminology-that-is-used-to-describe-micro>).

Periodic installation of updates is required to ensure secure and stable operation of SIMATIC PCS 7.

In principle, these updates can be implemented in two ways:

- Windows Updates via the role Microsoft Windows Server Update Services (WSUS)
Provision of Windows updates for all computers of the control technology system from a separate, dedicated WSUS
- Manual update
Manual installation of the updates on all computers of the control technology system after downloading the updates from the Microsoft website

You can find information on the topic of "Patch Management" in the following documents:

- FAQ "Which Microsoft updates have been tested for compatibility with SIMATIC PCS 7?" (<https://support.industry.siemens.com/cs/ww/en/view/18490004>)"

Note

This is where you will find the latest information about the Microsoft updates and classifications tested in SIMATIC PCS 7. This information takes precedence over the specifications described in this document.

Note

Microsoft updates must be installed as quickly as possible after publication for infrastructure systems in the SIMATIC PCS 7 environment, such as domain controllers, quarantine stations and WSUS.

- FAQ "How can you find out which Microsoft Patches are installed on your PC?" (<https://support.industry.siemens.com/cs/ww/en/view/48844294>)"
- An overview of the installed Microsoft Patches is also available in the SIMATIC Management Console (SMMC) under "Inventory data - Installed software - Installed third-party software". You can find a detailed description of this in the manual "SIMATIC Process Control System PCS 7 SIMATIC Management Console" (<https://support.industry.siemens.com/cs/ww/en/view/109794443>).

You can find information on Microsoft updates and the WSUS on the following Web pages:

- Microsoft Security Advisories and Bulletins (<https://msrc.microsoft.com/update-guide>)
- Windows Server Update Services (WSUS) (<https://docs.microsoft.com/en-us/windows-server/administration/windows-server-update-services/get-started/windows-server-update-services-wsus>)

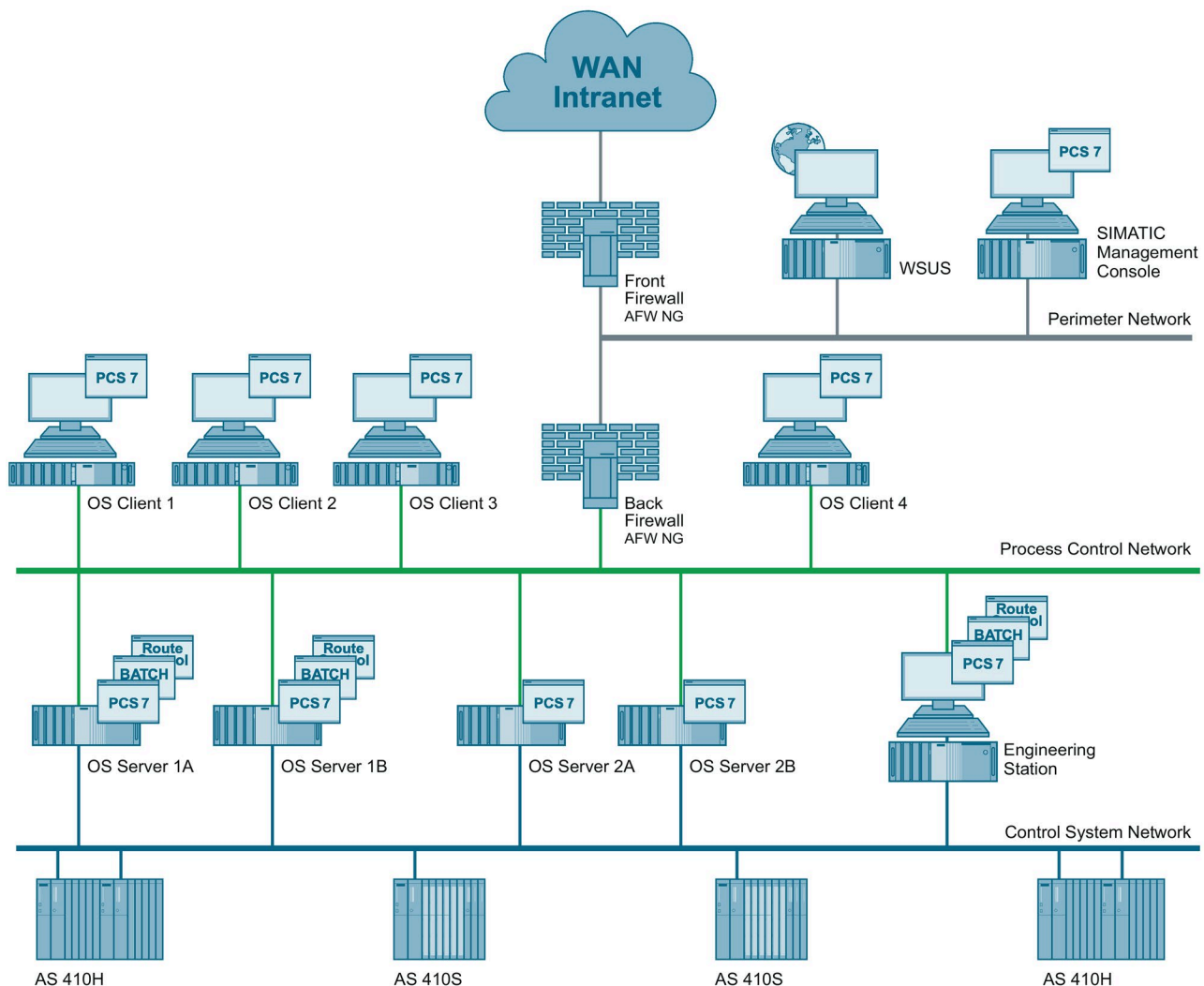
Support for implementing patch management in your system is available from the Industrial Security Services. You can find additional information and the corresponding contacts at the following address:

- Siemens Industrial Security Information: (<https://www.siemens.com/industrial-security>)

8.2 Windows Server Update Service (WSUS)

8.2.1 Integration of the WSUS server in the system

In accordance with the rules for dividing components into security cells, the WSUS server must be installed in a separate network (preferably in the Perimeter network / DMZ). All solutions relating to securing access points to the security cells, such as front-end/back-end firewall or three-homed firewall, can be used for the patch management or the WSUS server. During configuration of the firewall access rules for the back-end firewall or three-homed firewall, the protocols and ports needed by the WSUS for communication between the systems to be patched and the WSUS must be allowed.



8.2.2 Procedure for patch management with the WSUS

Requirement

A WSUS is installed and prepared for your SIMATIC PCS 7 system (basic configuration without synchronization).

Note

The WSUS server must be installed on the basis of the Windows Server 2019 operating system.

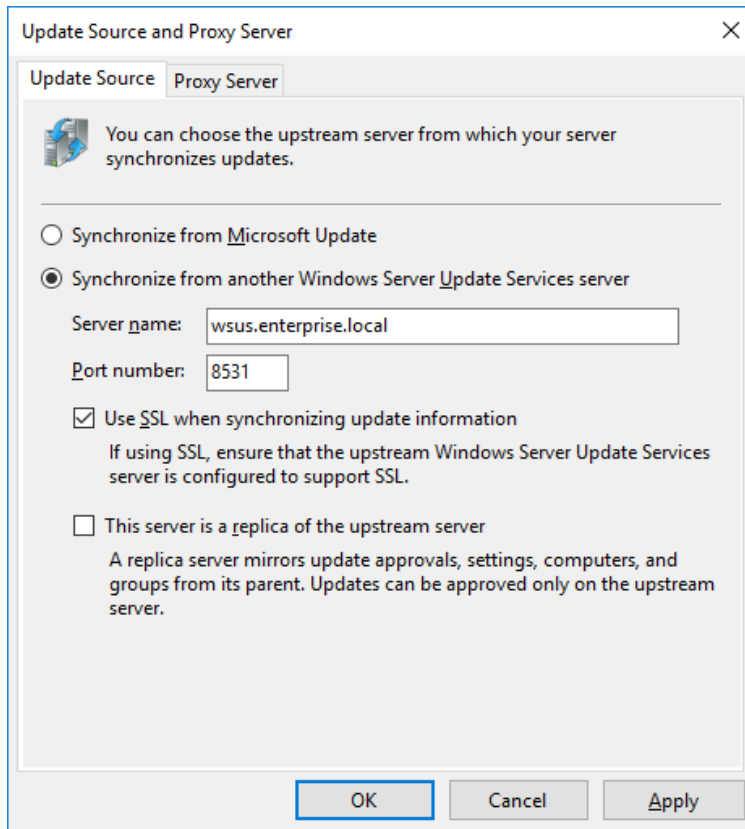
You can find additional information at the following links:

- "Deploy Windows Server Updates Services" (<https://docs.microsoft.com/en-us/windows-server/administration/windows-server-update-services/deploy/deploy-windows-server-update-services>)
 - "Updating Windows 10 in Corporate Licenses" (<https://technet.microsoft.com/itpro/windows/manage/introduction-to-windows-10-servicing>)
-

Update source

As an update source for the WSUS server of the SIMATIC PCS 7 system, either an existing WSUS in a higher-level external network, such as the corporate network, or Microsoft Update via the Internet can be set for synchronization. The decision not only affects the configuration of the firewall (front-end firewall or three-homed firewall), but also the configuration of the WSUS server itself.

The corresponding update source must be set in the WSUS configuration:

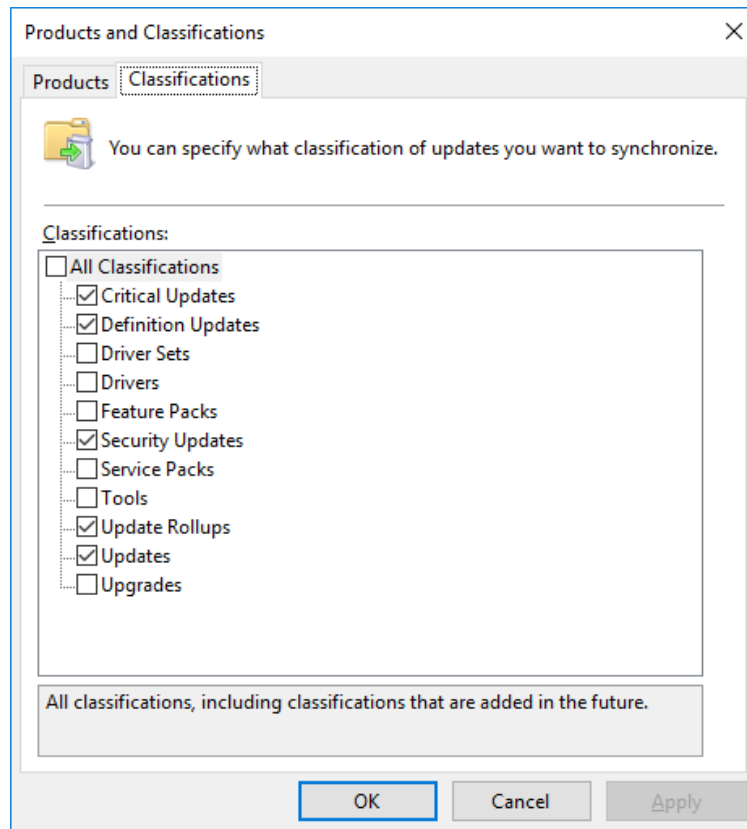


Configuring WSUS

To configure the WSUS, follow these steps:

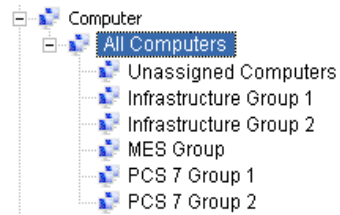
1. Open the WSUS Administration Console and click "Options".
2. On the "Products" tab of the "Products and Classifications" dialog, select all Microsoft products relevant to the system.

3. Select the classifications described in the FAQ above (see Note) in the "Products and Classifications" dialog. For example as shown here.

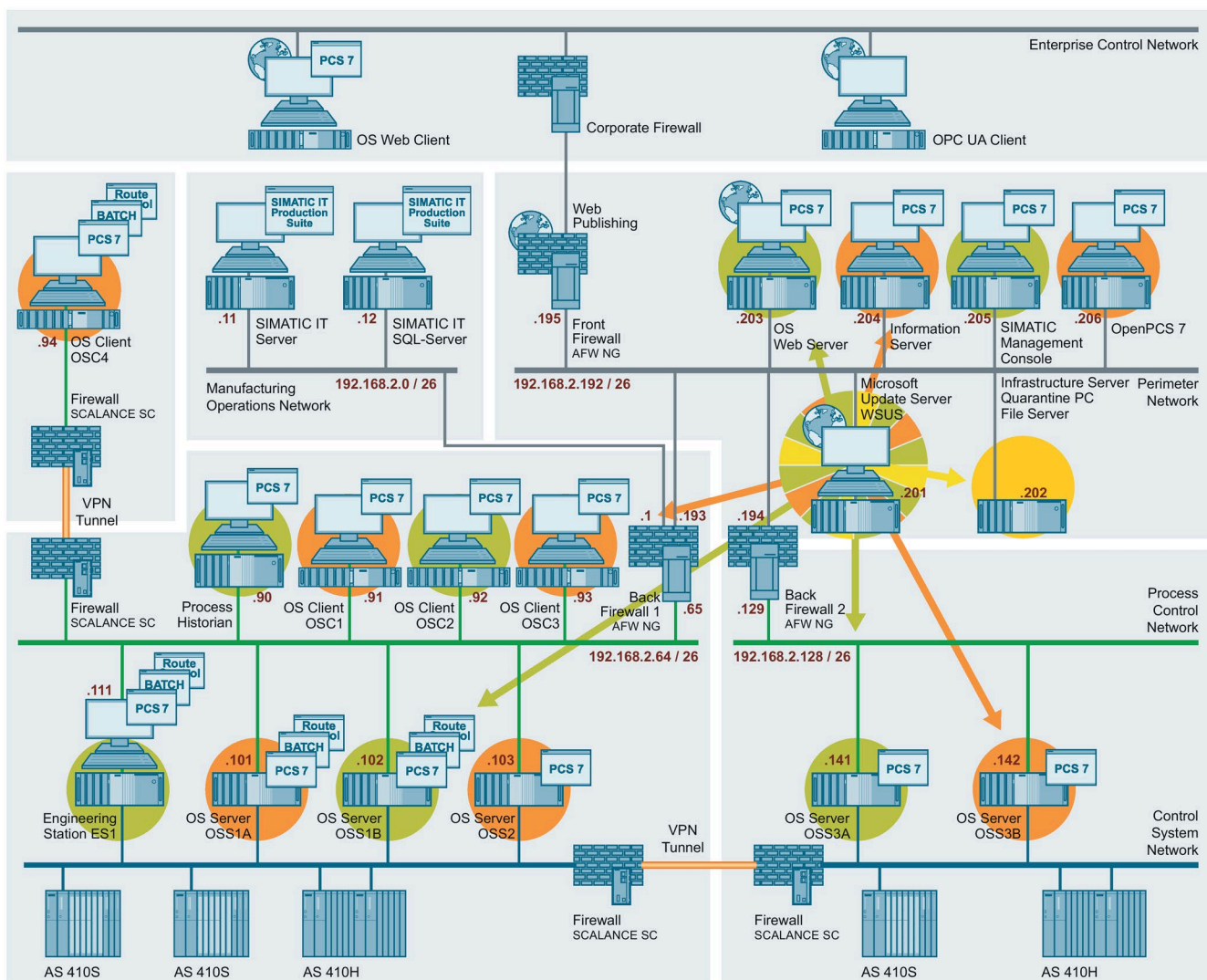


4. The configuration described in section 9.4 "Distribution of the virus signature files" must be observed. It allows prompt automatic installation of available virus signature file updates for Microsoft Defender AV.

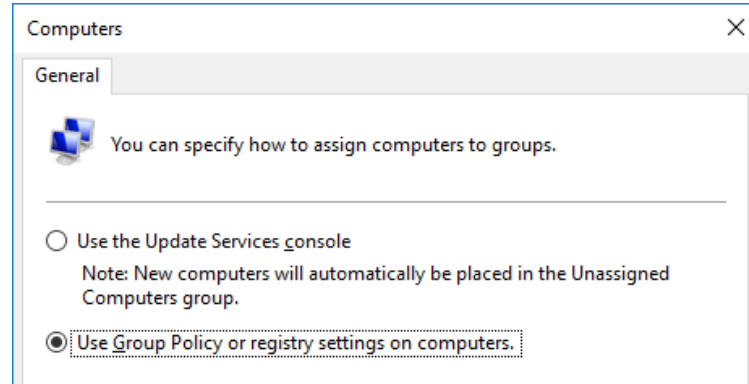
5. Create project-specific groups for the distribution of updates in the system according to the redundancy concept, and assign the individual SIMATIC PCS 7 systems, and any other systems to be patched, to these computer groups.



For example, the OS servers "OSS1A", "OSS2" and "OSS3A" and the OS clients "OSC1" and "OSC3" can be assigned to computer group "PCS 7 Group 1" and the OS servers "OSS1B" and "OSS3B" and the OS client "OSC2" can be assigned to computer group "PCS 7 Group 2".



The assignment of computers to the computer groups can be made in the Update Services Administration Console or it can be implemented via a group policy (GPO) (independent of whether computers are managed using Windows workgroups or Active Directory). The following option must be set accordingly.



6. Synchronize the WSUS with the update source.

Checking for updates

To check the updates tested under SIMATIC PCS 7, follow these steps:

1. Download the Excel table "Security_Patches_iec.xls" to your computer from the following FAQ:
"Which Microsoft updates have been tested for compatibility with SIMATIC PCS 7?" (<https://support.industry.siemens.com/cs/ww/en/view/18490004>)
2. Open the table and filter the "PassedProduct" column for all entries except "PCS7Vxy".
3. Check the "Comments" column to see whether these updates were replaced.

Enabling updates for installation and installing them

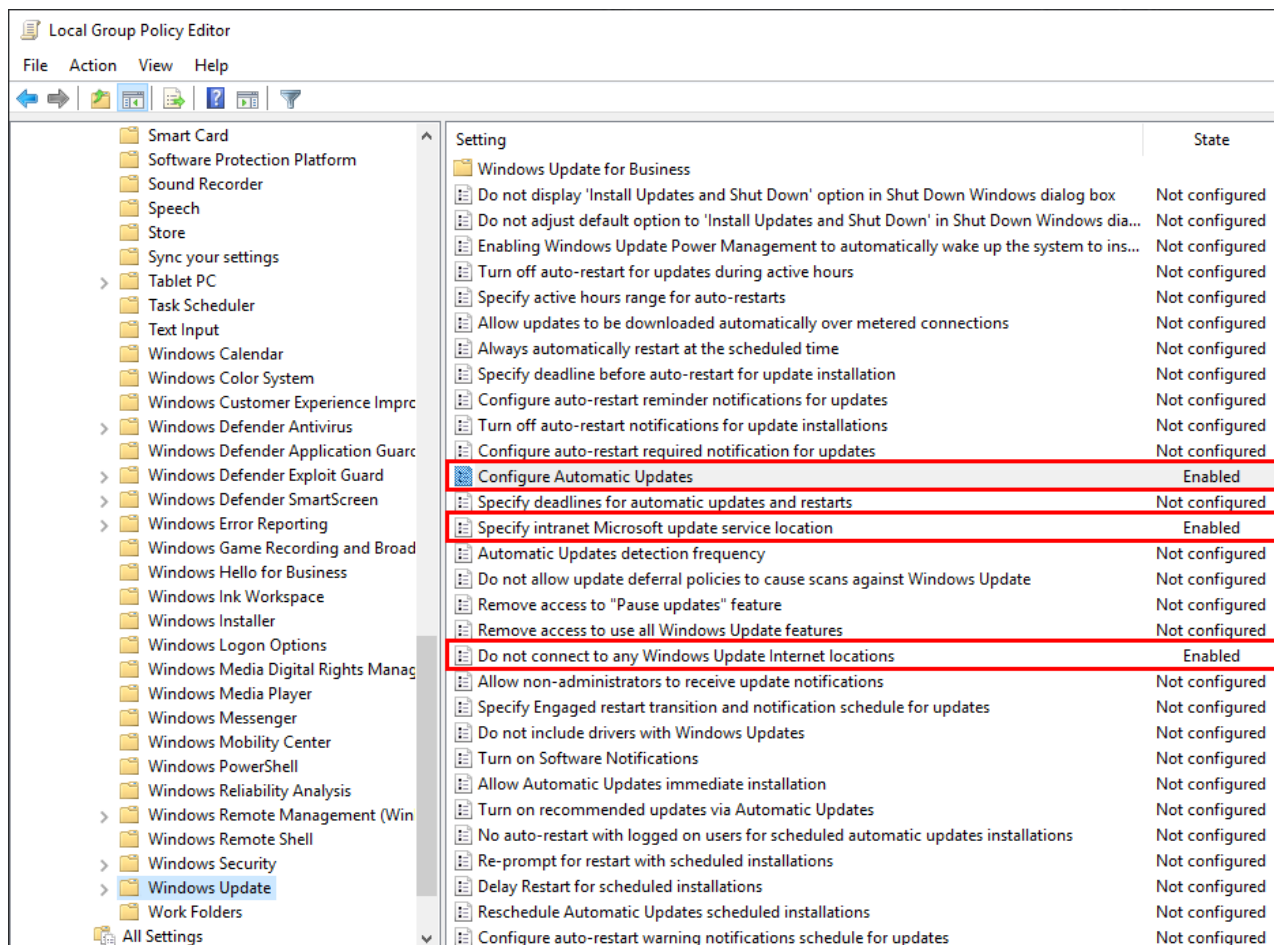
1. Select all available and not yet approved updates. Next, deselect only the updates that are incompatible with SIMATIC PCS 7 according to the Excel table above. Release the selected updates for installation in the created groups. Proceed group-by-group to ensure the availability and operability of your system.
2. Log on to the systems connected to the WSUS with an administrator account. The systems are configured accordingly to receive the updates from the WSUS (see section 8.2.3, Configuration of the group policies on the systems (Page 158))
To do so, use the function that can be accessed via "Notification icon > All settings > Update and Security" and initiate the search for available updates there.
3. Make sure that SIMATIC PCS 7 Runtime is stopped. Install all offered updates and restart the systems when prompted to do so. Check if additional updates are offered for installation after restarting the computer and install these as well.
4. If a used product appears in the "FailedProduct" column, reject the relevant update for affected systems.

8.2.3 Configuration of the group policies on the systems

In a Windows workgroup, the policies for the Windows Update service are set up using the editor for local group policies. In a Windows workgroup, these settings must be made separately on every computer.

If the computer is a member of an Active Directory (Windows domain), the group policy settings are made centrally and distributed to the systems according to the organizational unit assignment (OU).

The following figure shows the editor for local group policies in Windows 10 with the recommended settings for the Windows component "Windows Update":



The following group policies must be configured:

- Policy "Configure automatic updates". This policy must be activated. Then, via the additional configuration "Configure Automatic Updates" within this group policy, Option "3 – Automatic download, but notify before installation" must be set.

The screenshot shows the 'Configure Automatic Updates' dialog box. The 'Enabled' radio button is selected. The 'Options' section shows '3 - Auto download and notify for install' selected in the dropdown menu. The 'Help' section provides details about the policy settings.

Configure Automatic Updates

Previous Setting Next Setting

Not Configured Comment:

Enabled

Disabled

Supported on: Windows XP Professional Service Pack 1 or At least Windows 2000 Service Pack 3
Option 7 only supported on servers of at least Windows Server 2016 edition

Options: Help:

Configure automatic updating:
3 - Auto download and notify for install

The following settings are only required and applicable if 4 is selected.

Install during automatic maintenance

Scheduled install day: 0 - Every day

Scheduled install time: 03:00

If you have selected "4 – Auto download and schedule the install" for your scheduled install day and specified a schedule, you also have the option to limit updating to a weekly, bi-weekly or monthly occurrence, using the options below:

Every week

First week of the month

Second week of the month

Specifies whether this computer will receive security updates and other important downloads through the Windows automatic updating service.

Note: This policy does not apply to Windows RT.

This setting lets you specify whether automatic updates are enabled on this computer. If the service is enabled, you must select one of the four options in the Group Policy Setting:

2 = Notify before downloading and installing any updates.

When Windows finds updates that apply to this computer, users will be notified that updates are ready to be downloaded. After going to Windows Update, users can download and install any available updates.

3 = (Default setting) Download the updates automatically and notify when they are ready to be installed

Windows finds updates that apply to the computer and downloads them in the background (the user is not notified or interrupted during this process). When the downloads are complete, users will be notified that they are ready to install. After going

OK Cancel Apply

Note

To prevent possible notification banners of the operating system regarding available Microsoft updates which could disturb the plant operator during process operation, suitable settings can be made in WinCC within the configuration of the "Computer Properties" on the "Parameters" tab.

You can find additional details in the online help "WinCC Information System".

8.2 Windows Server Update Service (WSUS)

- Policy "Specify intranet Microsoft update service location" policy
The "Specify intranet Microsoft update service location" policy must be enabled.
The IP address or computer name of the WSUS server of the system must be specified in two text boxes in the Properties dialog of this policy. Depending on the configuration of the WSUS, a port number may also have to be added (typically 8530 (http) or 8531 (https), e.g. https://WSUS:8531).

The screenshot shows the 'Specify intranet Microsoft update service location' dialog box. The 'Enabled' radio button is selected. The 'Supported on' field is set to 'At least Windows XP Professional Service Pack 1 or Windows 2000 Service Pack 3, excluding Windows RT'. In the 'Options' section, the 'Set the intranet update service for detecting updates' field contains 'https://wsus:8531', and the 'Set the intranet statistics server' field contains 'https://wsus:8531'. The 'Proxy behavior' dropdown is set to 'Only use system proxy for detecting updates (default)'. The 'Help' section contains detailed instructions on how to configure the intranet update service and the alternate download server.

Specify intranet Microsoft update service location

Specify intranet Microsoft update service location Previous Setting Next Setting

Not Configured Comment:

Enabled

Disabled

Supported on: At least Windows XP Professional Service Pack 1 or Windows 2000 Service Pack 3, excluding Windows RT

Options:

Set the intranet update service for detecting updates:

Set the intranet statistics server:

Set the alternate download server:

(example: https://IntranetUpd01)

Download files with no Url in the metadata if alternate download server is set.

Do not enforce TLS certificate pinning for Windows Update client for detecting updates.

Select the proxy behavior for Windows Update client for detecting updates:

Only use system proxy for detecting updates (default)

Help:

Specifies an intranet server to host updates from Microsoft Update. You can then use this update service to automatically update computers on your network.

This setting lets you specify a server on your network to function as an internal update service. The Automatic Updates client will search this service for updates that apply to the computers on your network.

To use this setting, you must set two server name values: the server from which the Automatic Updates client detects and downloads updates, and the server to which updated workstations upload statistics. You can set both values to be the same server. An optional server name value can be specified to configure Windows Update Agent to download updates from an alternate download server instead of the intranet update service.

If the status is set to Enabled, the Automatic Updates client connects to the specified intranet Microsoft update service (or alternate download server), instead of Windows Update, to search for and download updates. Enabling this setting means that end users in your organization don't have to go through a firewall to get updates, and it gives you the opportunity to test updates before deploying them.

If the status is set to Disabled or Not Configured, and if Automatic Updates is not disabled by policy or user preference, the Automatic Updates client connects directly to the Windows Update site on the Internet.

The alternate download server configures the Windows Update Agent to download files from an alternative download server instead of the intranet update service.

The option to download files with missing Urls allows content to be downloaded from the Alternate Download Server when there are no download Urls for files in the update metadata. This option should only be used when the intranet update service does not provide download Urls in the update metadata for files which are present on the alternate download server.

Note: If the "Configure Automatic Updates" policy is disabled, then this policy has no effect.

OK Cancel Apply

- Policy "Do not connect to any Windows Update Internet locations"
The policy "Do not connect to any Windows Update Internet locations" must be activated.
- "Enable client-side targeting" policy (optional)
If it is required that the system be automatically assigned to a previously defined WSUS computer group, the "Enable client-side targeting" policy must be enabled.
The computer group to which the computer belongs must be specified in the Properties dialog of the policy.

Enable client-side targeting

Enable client-side targeting

Previous Setting Next Setting

Not Configured Comment:

Enabled

Disabled

Supported on: At least Windows XP Professional Service Pack 1 or Windows 2000 Service Pack 3, excluding Windows RT

Options:

Target group name for this computer

PCS 7 Group 1

Help:

Specifies the target group name or names that should be used to receive updates from an intranet Microsoft update service.

If the status is set to Enabled, the specified target group information is sent to the intranet Microsoft update service which uses it to determine which updates should be deployed to this computer.

If the intranet Microsoft update service supports multiple target groups this policy can specify multiple group names separated by semicolons. Otherwise, a single group must be specified.

If the status is set to Disabled or Not Configured, no target group information will be sent to the intranet Microsoft update service.

Note: This policy applies only when the intranet Microsoft update service this computer is directed to is configured to support client-side targeting. If the "Specify intranet Microsoft update service location" policy is disabled or not configured, this policy has no effect.

Note: This policy is not supported on Windows RT. Setting this

OK Cancel Apply

8.2.4 Firewall rules for operation of the WSUS

The following firewall rules apply to access of the WSUS server in the Perimeter network to computers in the PCN via the back-end firewall or three-homed firewall:

- Access rules between the WSUS server and a computer in the PCN

Name	Action	Protocols	From	To
PCN to Perimeter WSUS #1	Allow	Dependent on the configuration of the WSUS server: HTTPS TCP/8531 (The following configuration is not recommended: HTTP or TCP/8530)	IP address of client	IP address of WSUS server

The following access rules are required for access of the WSUS server in the Perimeter network to the external network for downloading security updates and critical updates via the front-end firewall or three-homed firewall:

- Access rules for firewall rule for updating via the Microsoft update server

Name	Action	Protocols	From	To
Allow WSUS access to MU (Microsoft Update Server)	Allow	HTTP HTTPS	IP address of WSUS server	Microsoft Update (MU) Sites (section 2.1.1): https://docs.microsoft.com/en-us/windows-server/administration/windows-server-update-services/deploy/2-configure-wsus

- Access rules for updating via a higher-level WSUS server

Name	Action	Protocols	From	To
Allow Windows Update access to upstream WSUS	Allow	Dependent on the configuration of the higher-level WSUS server: HTTPS TCP/8531 (The following configuration is not recommended: HTTP or TCP/8530)	IP address of WSUS server	IP address of higher-level WSUS server

See also

WSUS Configuration, sections 2.1.1 and 2.1.2, (English) (<https://docs.microsoft.com/en-us/windows-server/administration/windows-server-update-services/deploy/2-configure-wsus>)

8.2.5 Installing updates from the SIMATIC Management Console

The SIMATIC PCS 7 system-compliant installation of available Microsoft updates can also be carried out from the SIMATIC Management Console (SMMC).

The user should confirm the request to start the installation of updates on the SIMATIC PCS 7 system directly on the target system. The user can be given the option to postpone the installation of updates on the system several times through a corresponding configuration via the SMMC. If a user does not comply with this request, the installation of updates takes place automatically after a configurable period.

You can find a detailed description of this and the relevant configuration options in the manual "SIMATIC Process Control System PCS 7 SIMATIC Management Console (<https://support.industry.siemens.com/cs/ww/en/view/109794443>)".

8.3 Manual update

For manual updates, the required updates of the systems must first be downloaded from the Microsoft Update Catalog (<https://www.catalog.update.microsoft.com>) to any computer. In doing so, you must ensure that you use the appropriate operating system version of the updates.

After the download and transfer of the updates to the target systems, the updates must be separately installed. For an OS server or OS client, process control (SIMATIC PCS 7 Runtime) must be stopped before the installation.

Run the setup program and follow the instructions on the screen. A restart may be required after the installation.

Note

The manual approach is not recommended for the following reasons:

- Updates required for the systems may not be completely taken into account.
 - A potential security risk may be created for the system if the updates are installed from a removable data storage medium.
 - The process may be time-consuming and prone to errors
 - Reporting over patched and unpatched systems may require even more time
-

Note

The procedure described above for the installation of updates does not apply to Microsoft Service Packs, the use of which still requires an explicit release. If the updates require a later version of the Microsoft software, read the SIMATIC PCS 7 Readme (<https://support.industry.siemens.com/cs/ww/en/view/109780270>)(online) or use the Compatibility Tool (<http://www.siemens.com/kompatool>) in advance to ensure that these later software versions or service packs have been approved for SIMATIC PCS 7.

8.4 SIMATIC PCS 7 Updates

Updates for SIMATIC PCS 7 components should be installed and administered from the SIMATIC Management Console (SMMC).

The current software/hardware version of every component can be determined via the SMMC to identify the required updates.

You can find additional information on inventory and software installation in the documentation of the SMMC

(<https://support.industry.siemens.com/cs/de/en/view/109794443>).

Note

An optional integrity check of the files to be installed can take place during the installation of PCS 7 software components from the SIMATIC Management Console.

You can find a detailed description of this in the manual "SIMATIC Process Control System PCS 7 SIMATIC Management Console

(<https://support.industry.siemens.com/cs/ww/en/view/109794443>)".

Note

To stay informed about security-relevant product updates, subscribe to the Siemens Industrial Security RSS Feed / Newsletter on the website of Siemens ProductCERT and Siemens CERT

(<https://www.siemens.com/cert>).

Protection against malware using virus scanners

9.1 Overview

This section focuses on protecting the automation system or the computers of the automation system against malicious software. Malicious software and malicious programs (malware) refers to computer programs that were developed to execute undesirable and possible damaging functions. The following types are differentiated:

- Computer virus
- Computer worm
- Trojan horse
- Other potentially dangerous programs, for example:
 - Backdoor
 - Ransomware
 - Spyware
 - Adware
 - Scareware
 - Grayware

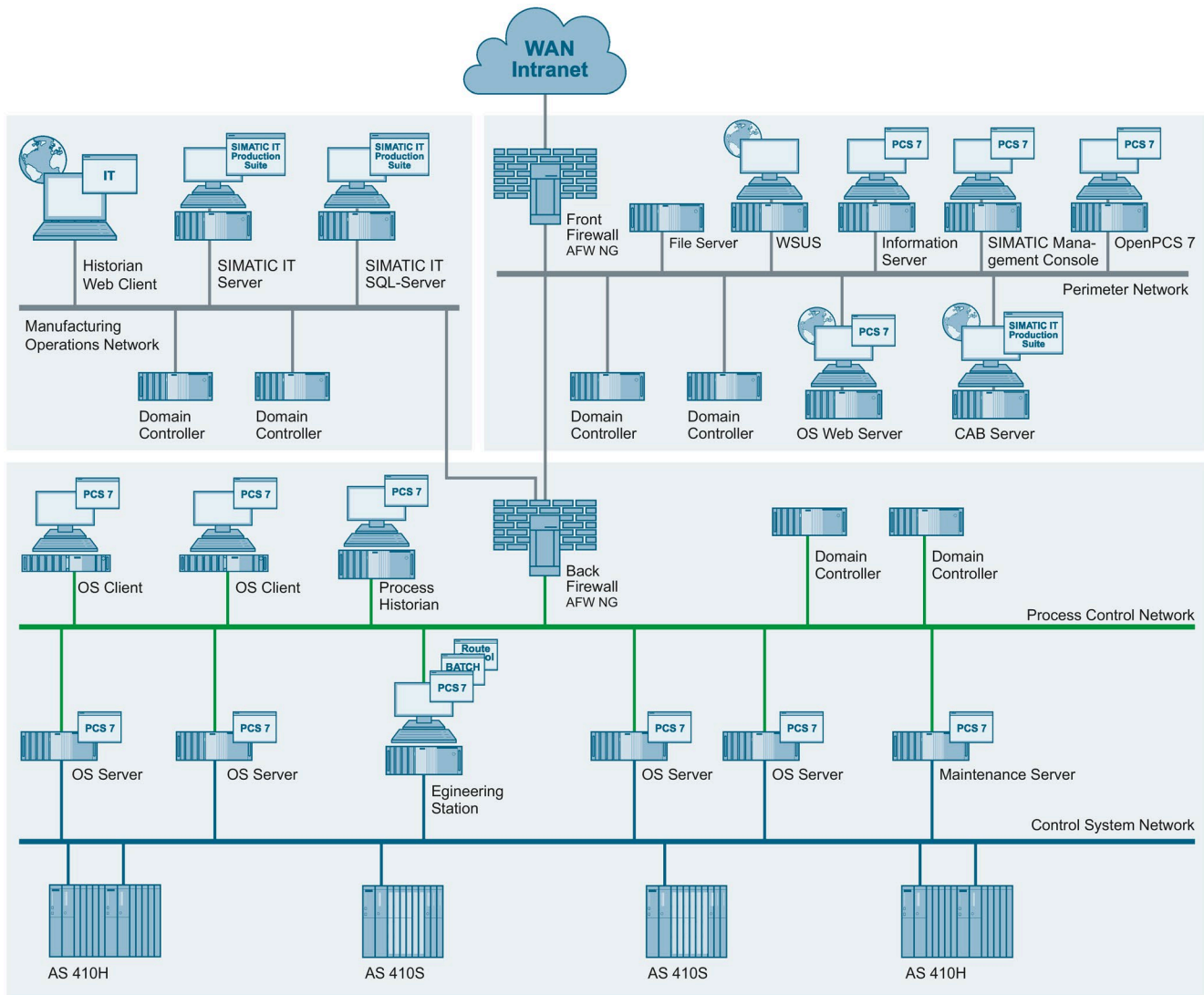
A virus scanner or antivirus program is a software that detects, blocks and, if necessary, removes malware.

The use of a virus scanner on the computers of an automation plant must not interfere with the process mode of a plant. The following two examples illustrate the problems that arise in automation through the use of virus scanners:

- Even when infected with malware, a computer may not be switched off by a virus scanner if this would lead to a loss of control of the production system (e.g. for an OS server).
- A project file "infected" by malware (e.g. a database archive) may not be automatically moved to quarantine or deleted.

9.1 Overview

The following virus scanner architecture is recommended for implementing this requirement:



From SIMATIC PCS 7 V9.1, only the Microsoft Defender Antivirus (AV) will be tested for compatibility as a virus scanner. There is no central virus scan server for this product.

This virus scanner gets its current virus signature files (virus patterns) from the WSUS in the Perimeter Network / DMZ. Therefore, it must be configured accordingly, so that it makes available, on the one hand, current virus patterns, and on the other, updates for the Microsoft Defender AV itself as well.

The virus pattern updates are selected through the classification "Definition updates", and the updates for the virus scanner via the product selection "Microsoft Defender" and processed accordingly by the WSUS.

More information on this can be found using the link "Use WSUS to deploy definition updates to computers that are running Windows Defender" (<https://docs.microsoft.com/en-us/troubleshoot/mem/configmgr/deploy-definition-updates-using-wsus>).

Also located in the Perimeter network is the SIMATIC Management Console. For the administered SIMATIC PCS 7 systems, it acts as the central event reporting center for Microsoft Defender AV events (for example, reporting a malware attack) and can display current Defender signature versions.

You can find more information on this in the manual "SIMATIC Process Control System PCS 7 SIMATIC Management Console" (<https://support.industry.siemens.com/cs/de/en/view/109794443>).

9.2 Update source

The update source for the Microsoft Defender Antivirus is a WSUS that should be located in the Perimeter Network / DMZ. It can be configured in such a way that it downloads the required updates either via a WSUS in a higher-level external network, for example, the corporate network (so-called upstream server), or directly from Microsoft from its Windows Update server on the Internet.

The decision not only affects the configuration of the firewall (front-end firewall or three-homed firewall), but also the configuration of the WSUS.

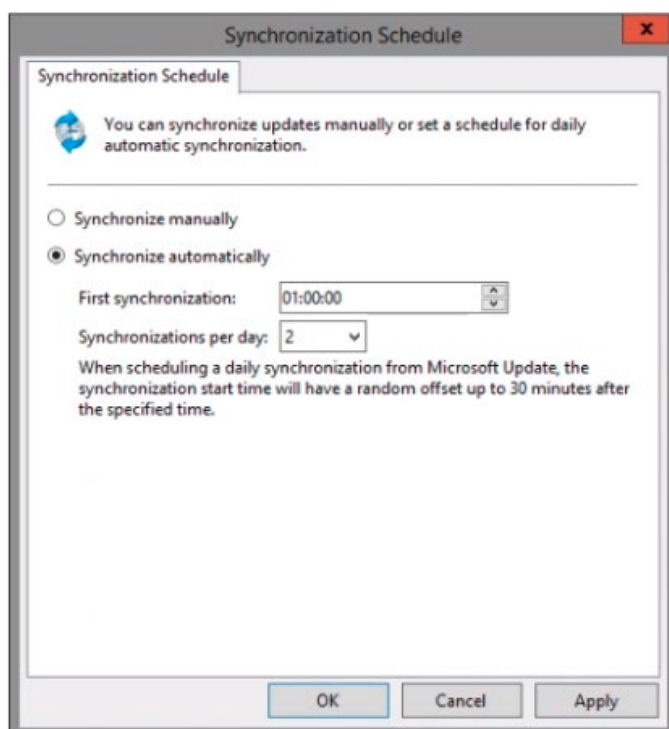
9.3 Firewall rules

For the required firewall rules, see section 8.2.4, Firewall rules for operation of the WSUS (Page 162).

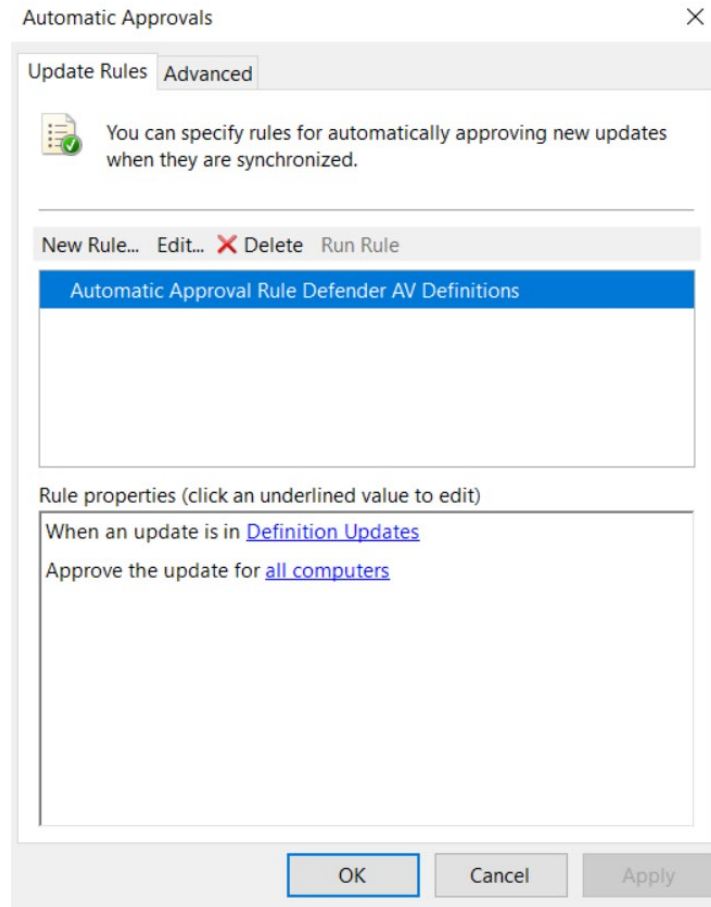
9.4 Distribution of virus signature files

For the distribution of the virus signature files from the WSUS to the Microsoft Defender AV clients, the following settings are recommended on the WSUS.


To provide the latest virus signature files to the systems at any time, the automatic synchronization cycle ("Synchronization Schedule") should be configured as follows with the options of the WSUS:



For the distribution of the Microsoft Defender AV virus signature files from the WSUS to the Microsoft Defender AV clients, configuring an automatic approval rule of "Definition Updates" is recommended.



Edit Rule ×

 Select which updates to approve and the groups for which to approve them.

Step 1: Select properties

When an update is in a specific classification

When an update is in a specific product

Set a deadline for the approval

Step 2: Edit the properties (click an underlined value)

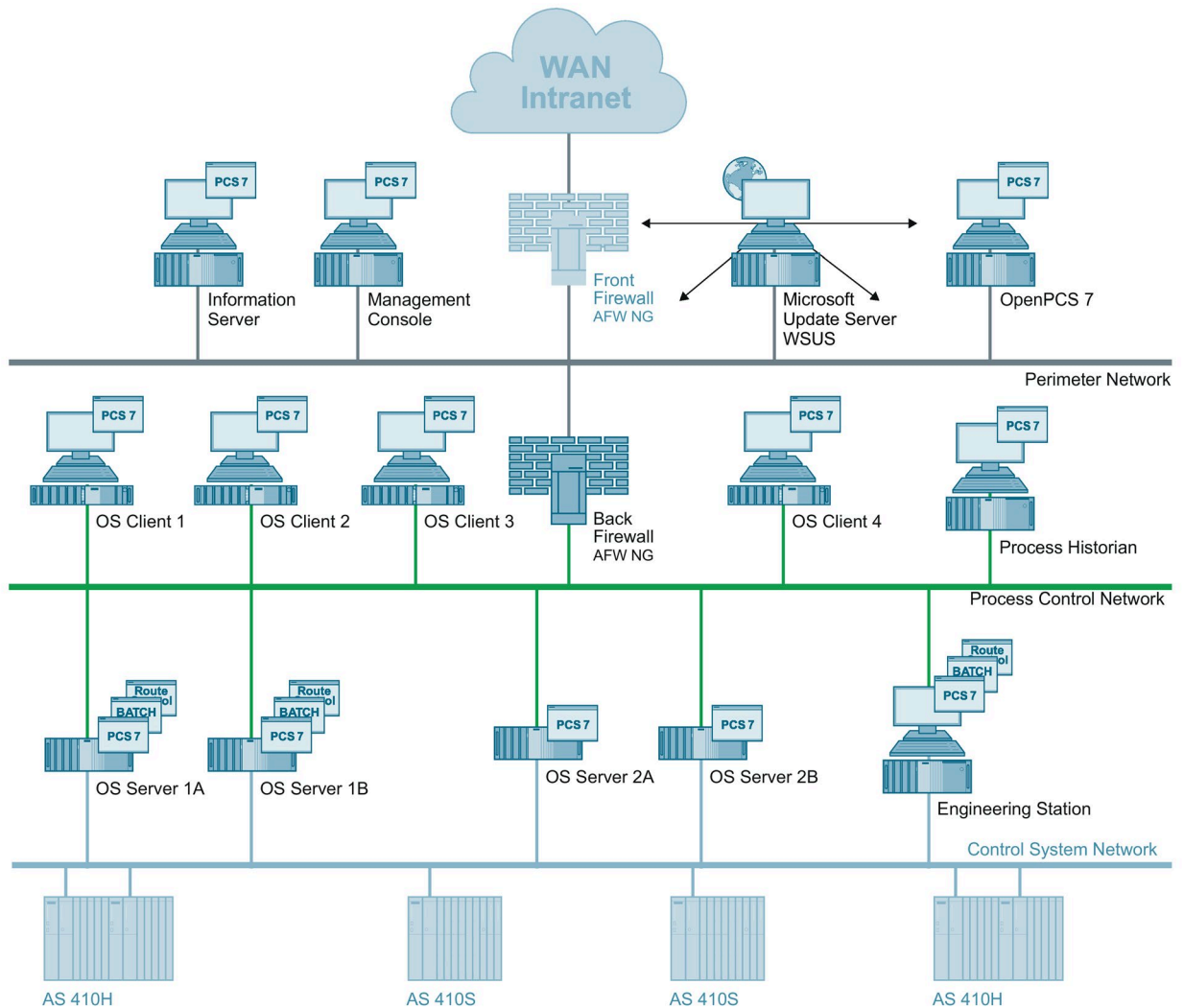
When an update is in Definition Updates

Approve the update for all computers

Step 3: Specify a name

Automatic Approval Rule Defender AV Definitions

Thus, the distribution of the virus signatures to the clients can be depicted as shown in the example:



Additional information

You can find more information about the topic "Protection against malware using virus scanners" in the following documents:

- Manual "SIMATIC Process Control System PCS 7 Managing Virus Scanners (<https://support.industry.siemens.com/cs/ww/de/view/109760461>)"
- FAQ "What is the compatibility of SIMATIC PCS 7? (<http://www.siemens.com/kompatool>)"

9.5 Further settings for the Microsoft Defender AV

The Microsoft Windows Defender AV is to be further configured using the following Group Policy settings (Group Policy > Computer Configuration > Administrative Templates > Windows Components > Microsoft Defender Antivirus):

Path	Setting	Recommended setting	Additional description of the policies
Root	Configuring the collaborative behavior of local administrators for lists	Disabled	Prevent or allow users to locally modify policy settings (https://github.com/MicrosoftDocs/microsoft-365-docs/blob/public/microsoft-365/security/defender-endpoint/configure-local-policy-overrides-microsoft-defender-antivirus.md)
Updating the security information	Determining the sequence of the sources for downloading updates of the security information	Enabled The sequence of sources must be defined as follows: InternalDefinitionUpdateServer MicrosoftUpdateServer Meaning: 1 "Internal Definition Update Server" corresponds to the WSUS 2. Microsoft Update Server	Manage Microsoft Defender Antivirus protection and security intelligence updates (https://github.com/MicrosoftDocs/microsoft-365-docs/blob/public/microsoft-365/security/defender-endpoint/manage-protection-updates-microsoft-defender-antivirus.md)
Reports	Disable extended notifications	Enabled	Configure the notifications that appear on endpoints (https://github.com/MicrosoftDocs/microsoft-365-docs/blob/public/microsoft-365/security/defender-endpoint/configure-notifications-microsoft-defender-antivirus.md)
Client interface	Suppress all notifications	Enabled	Configure the notifications that appear on endpoints (https://github.com/MicrosoftDocs/microsoft-365-docs/blob/public/microsoft-365/security/defender-endpoint/configure-notifications-microsoft-defender-antivirus.md)
Client interface	Suppresses restart notifications	Enabled	Configure the notifications that appear on endpoints (https://github.com/MicrosoftDocs/microsoft-365-docs/blob/public/microsoft-365/security/defender-endpoint/configure-notifications-microsoft-defender-antivirus.md)

Path	Setting	Recommended setting	Additional description of the policies
MAPS	Entry to Microsoft MAPS	Disabled	Enable cloud-delivered protection (https://github.com/MicrosoftDocs/microsoft-365-docs/blob/public/microsoft-365/security/defender-endpoint/enable-cloud-protection-microsoft-defender-antivirus.md)
Scan	Allow users to pause scans	Disabled	Prevent users from seeing or interacting with the Microsoft Defender Antivirus user interface (not supported by Windows 10) (https://github.com/MicrosoftDocs/microsoft-365-docs/blob/public/microsoft-365/security/defender-endpoint/prevent-end-user-interaction-microsoft-defender-antivirus.md)
Scan	Scanning exchangeable data media	Enabled	Configure scanning options in Microsoft Defender Antivirus (https://github.com/MicrosoftDocs/microsoft-365-docs/blob/public/microsoft-365/security/defender-endpoint/configure-advanced-scan-types-microsoft-defender-antivirus.md)

9.6 Procedure after malware infection

A generally applicable procedure cannot be recommended for a malware infection. If such an infection occurs, the procedure for removing or cleaning the affected components must be planned individually.

In principle, a complete re-installation (operating system and application software) of the infected components is recommended. An existing, up-to-date hard disk image (system backup) that is free of malware can also be used for this purpose.

Before loading an image, you should first check to determine whether the image itself or its storage location is infected. An image of an infected storage location should not be used because it cannot be excluded that the image has also been manipulated.

The following points affect the cleaning procedure and should be included in the considerations and planning:

- Status of the plant documentation (including the network topology, addresses, accounts, etc.)
- Cleaning during ongoing operation or during a maintenance period
- Continuous or batch process
- Redundancy concept
- Type of malware
- Number of infected computers
- Infection route

Procedure

Note

Note that the procedure described here is an example list of possible steps that may be performed for cleaning a plant. This list does not claim to be complete. Each of the steps listed must be planned in detail and implemented accordingly.

The procedure after a malware infection may include the following steps:

- Setup/installation/implementation of the required additional infrastructure for the cleaning, for example:
 - A separate quarantine network
 - A secure file server with up-to-date virus scanner for distributing data
 - Internet access using a separate workstation with up-to-date virus scanner

- Listing of all network nodes and their tasks
Backup of all the current data (engineering data, archives, backups, etc.) for each node.
- Import, scan, cleaning and storage of the current data for each network node on the file server
- Planning the required redundancies (when cleaning during ongoing operation)
- Identification of standby components; creation of an image; analysis and examination of the image with the goal of identifying the malware as well as its dissemination mechanism (forensics)
- Reinstallation of the component either from the system backup (if this is available and does not pose an infection threat) or via an original data medium (operating system recovery DVD and automation components)
- Recommissioning of the cleaned, reinstalled components in the quarantine network as the new master
- Transfer of "clean" data (engineering data, archives, backups, etc.) from the file server to the cleaned, reinstalled component in the quarantine network
- Review and adaptation of the security concept of the system
- Review and adaptation of the security concept in the "Quarantine" network
- Step-by-step "reconfiguration" of the system in the "Quarantine" network with cleaned, reinstalled components
- Expansion of the "Quarantine" network for the new automation network with the adapted measures of the security concept
- Step-by-step implementation of the measures from the security concept in the "Quarantine" network

Additional information

You can obtain support in implementing malware protection in the form of a virus scanner from the Industrial Security Services. You can find additional information and the corresponding contacts on the Siemens Industrial Security website (<https://www.siemens.com/industrial-security>).

Backing up and restoring data

In order to clean the automation system and restore its smooth and trouble-free operation as quickly as possible after a security incident, such as a malware infection, (see section 9.5, "Procedure following a virus infection" (Page 174)) or a storage medium failure (hard disk crash), regular creation of backups is essential.

Two types of backups are differentiated here:

- Backup of engineering data (project backup)
- Backup of the system and any existing data partitions
A system backup backs up the system partition. This means that the following data are backed up:
 - Hardware-specific files (e.g. drivers)
 - Windows operating system files and settings
 - Installed programs and their configurations

Project data or project-specific data (e.g. configuration overviews) are backed up on data partitions (partitions or other hard disks).

10.1 Backup strategy

The backup strategy must be planned according to the type of defense-in-depth (see section 4.2 "Concept of "defense in depth" (Page 12)") organizationally for both the project backup and for the system backups. The following points must be taken into account in this regard:

- Scope of backups (for project backup and system backup)
- Frequency for creating backups (for project backup and system backup)
- Complete, differential or incremental backup
- Storage or storage location of backups
- Archiving cycle of the backups

10.1.1 Scope of the backups

Project backup

The project backup includes the entire project data. This means all data that belongs to a SIMATIC PCS 7 project. These data and the SIMATIC PCS 7 project (multiproject including all the individual projects it contains) can be archived as a ZIP file that contains all configuration data using the SIMATIC Manager.

Note

The steps for creating a project backup and the procedure in the SIMATIC Manager is available in the manual "SIMATIC Process Control System PCS 7 Compendium Part A - Configuration Guidelines".

System backup

The system backup contains all system data for a specific system component, for example, an OS server, an OS client or an engineering station. These system data include:

- The operating system, that is, all data of the operating system
- All installed programs, for example SIMATIC Manager and WinCC
- All required device-specific drivers, for example, for graphics, network
- Configuration of all these programs and drivers

All these data are usually located on the system partition (C: \). A system backup therefore involves backing up the entire system partition (C: \).

Additional partitions or hard disks (e.g. drive D:\) must be taken into account for a complete computer backup.

10.1.2 Interval for creating backups

Specifying the backup interval determines when a specific backup must be created. The interval here depends on the type of backup. A project needs to be backed up more often (with higher frequency) than a system in practice.

Project backup

The project backup contains the configuration data and for this reason becomes outdated if a configuration change has been made. The cycle for creating a project backup therefore depends on the frequency of changes and should be defined accordingly (e.g. after changes in the configuration).

Note

Use the product-specific archiving functions of the PCS 7 system (see section 10.3 (Page 179)).

System backup

The system backup contains the system data of a system component. These data are generally only very rarely changed during operation. One possible scenario for a change would be the installation of an additional program or a new driver. However, these are administrative activities that are not generally performed on a daily basis. For this reason, the frequency for system backup depends on such administrative interventions in a system component.

Patch management represents a special situation. If a new update such as a security update, a critical update or an application hotfix is installed on a system component, for example, an up-to-date system backup must be taken for this system component.

Note

For SIMATIC PCS 7 system backups during runtime, the add-on product "SIDS Backup & Restore" has been approved for IPC computers and tested for compatibility under SIVaaS. "SIMATIC DCS / SCADA Infrastructure" (<https://support.industry.siemens.com/cs/ww/en/sc/4784>).

For "Offline backups" without activated runtime and when the operating system is stopped, the product "SIMATIC IPC Image & Partition Creator" (<https://mall.industry.siemens.com/mall/en/WW/Catalog/Products/10046686?activeTab=productinformation>) is available for SIMATIC IPC computers.

You can find general information on how to protect systems against data loss in the application example: "SIMATIC IPC – Protection from data loss". (<https://support.industry.siemens.com/cs/ww/en/view/109738084>)

10.2 Storage location of backups

Project and system backups must be stored in a secure location. The criteria for "secure" locations must be determined in each case by the operator within the context of its organizational security (IT Security Management Plan, Disaster Recovery Plan). The following points should be taken into account in this regard:

- Buildings
- Fire zones or fire areas
- Redundancy (multiple availability of backups in different locations)

Note

Backups must never be stored in the vicinity of the backed up systems. They must always be stored at a separate secure location that is accessible only to a selected group of responsible administrators/personnel. This ensures the security, confidentiality and availability of the backups.

10.3 Archiving

Backups, especially project backups should be archived. The specifications for archiving backups must be determined individually by the operator within the context of the organizational security (IT Security Management Plan, Disaster Recovery Plan).

Note

You can find information about the topic "Backing up and restoring data" in the following documents:

- Manual "SIMATIC PCS 7; Service Support and Diagnostics" (<https://support.industry.siemens.com/cs/de/en/view/109794378>), section 3.2 "Data backup"
 - Manual "SIMATIC Process Control System PCS 7 Compendium Part D – Operation and Maintenance" (www.siemens.de/industry/onlinesupport/pcs7)
-

10.4 Restoration

Restoring systems is more critical than the creation of backups. This process has to be tested and reproduced to guarantee fast availability of the plant systems in case of emergency and minimize downtimes. Systems must only be restored by trusted personnel. Here are some examples of the kind of topics that have to be taken into account when restoring a system:

- Where are the latest backups stored?
- What type of backup is required for restoration (complete, differential or incremental backup)?

10.4 Restoration

- Who has access to the backups?
- Who has permission to restore backups on which systems?
- When may backups be restored?
- Who clarifies the integrity and absence of malware in the backups that are to be restored?
- Is the handling of the backup software for the system restoration known?

Disposal of systems and components

Source and further notes: BSI - CON.6: Delete and destroy

(https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium_Einzel_PDFs/03_CON_Konzepte_und_Vorgehensweisen/CON_6_Loeschen_und_Vernichten_Edition_2_020.html)

Equipment or materials (e.g. printer paper, disks, streamer tapes, magnetic tapes, hard disks, CD-ROM, DVDs, USB sticks, flash drives or cards as well as special toner cartridges, carbon paper and carbon ribbons) are no longer needed at some time and must be discarded because they are defective. If these contain data of a sensitive nature, they must be disposed of so that no conclusions can be drawn from the previously saved data. For functioning data storage media, the data should be physically deleted. Non-functional data storage media or data storage media that can only be used once, such as files or CD-ROMs as well as DVDs, must be destroyed mechanically.

The type of disposal for material worthy of protection is to be regulated in a special security policy.

If sensitive material is collected prior to its disposal, it must be kept under lock and key and protected from unauthorized access.

Procedure in SIMATIC PCS 7 systems

Additional measures during decommissioning or replacement of modules and systems must be taken into account in SIMATIC PCS 7 systems. The corresponding product documentation has to be observed (e.g. resetting modules to the factory state) or third-party applications must be used.

The measures are divided into two steps (the list is by no means exhaustive):

1. Decommissioning / replacement of hardware components in the SIMATIC PCS 7 system
 - SCALANCE components must be reset to the factory state
 - CPU components must be reset to the factory state and the flash memory must be deleted

Note

The reset to the factory state is described in the S7-400 CPU manuals:

- Manual "SIMATIC PCS 7 Process Control System CPU 410 Process Automation" (section 9.8) (<https://support.industry.siemens.com/cs/ww/en/view/109801828>)
- Manual "SIMATIC S7-400 Automation Systems S7-400 CPU Data" (section 3.4) (<https://support.industry.siemens.com/cs/ww/en/view/53385241>)

The following steps must only be executed when disposing of S7-400 CPUs.

The internal flash memory of S7-400 CPUs must be erased as follows:

- For AS 410-5H / AS 410E:
Press the Reset button for more than five seconds while the CPU is in STOP. You can release it when the RUN and STOP LED are flashing at the same time. The flash memory is completely erased when the CPU indicates that it is in STOP (STOP LED lit permanently).
- For S7-400 CPUs:
With the CPU in STOP, pull and plugin the memory card quickly for four times. Now wait until the top LED starts flashing. This completes the deletion of the flash memory. The memory card must then be handed over for secure disposal.

-
- PC hard disks, USB media, CDs, DVDs and other media must be completely erased or handed over for secure disposal (e.g. shredder)
 - Complete systems (e.g. IPC computers) must be handed over for secure disposal
2. Disposed components must be removed from the configuration of SIMATIC PCS 7 system configuration
 - Pre-shared Keys (PSKs) (e.g. SIMATIC Shell, SIMATIC Management Console) of the PCS 7 systems in the plant must be changed, if necessary (e.g. during a maintenance phase).
 - Certificates must be revoked (e.g. for OPC UA, PCS 7 Web servers) This may also affect third-party systems.
 - CP 1628 / CP443-1 ADV: Decommissioned CP modules must be removed from the configuration (VPN group). This step also removes their certificates.
 - It must be ensured that domain controllers that have been put out of service, or are faulty and have been removed, are completely removed from the existing domain configuration.

Remote access

12.1 Remote maintenance based on the Remote Services platform

Introduction

Optimal proactive, secure and system-specific support for the automation system from remote locations: This is the idea behind the Remote Services platform. Thanks to its modular design, Remote Services can be optimally adapted to actual requirements. Not only is the remote infrastructure provided in the framework of the offered modules, but support and maintenance are included as well. Because the remote services are based on the common Remote Services Platform (cRSP) from Siemens, plant operators work on a secure, high-performance, and high-availability platform for remote access to their SIMATIC automation systems.

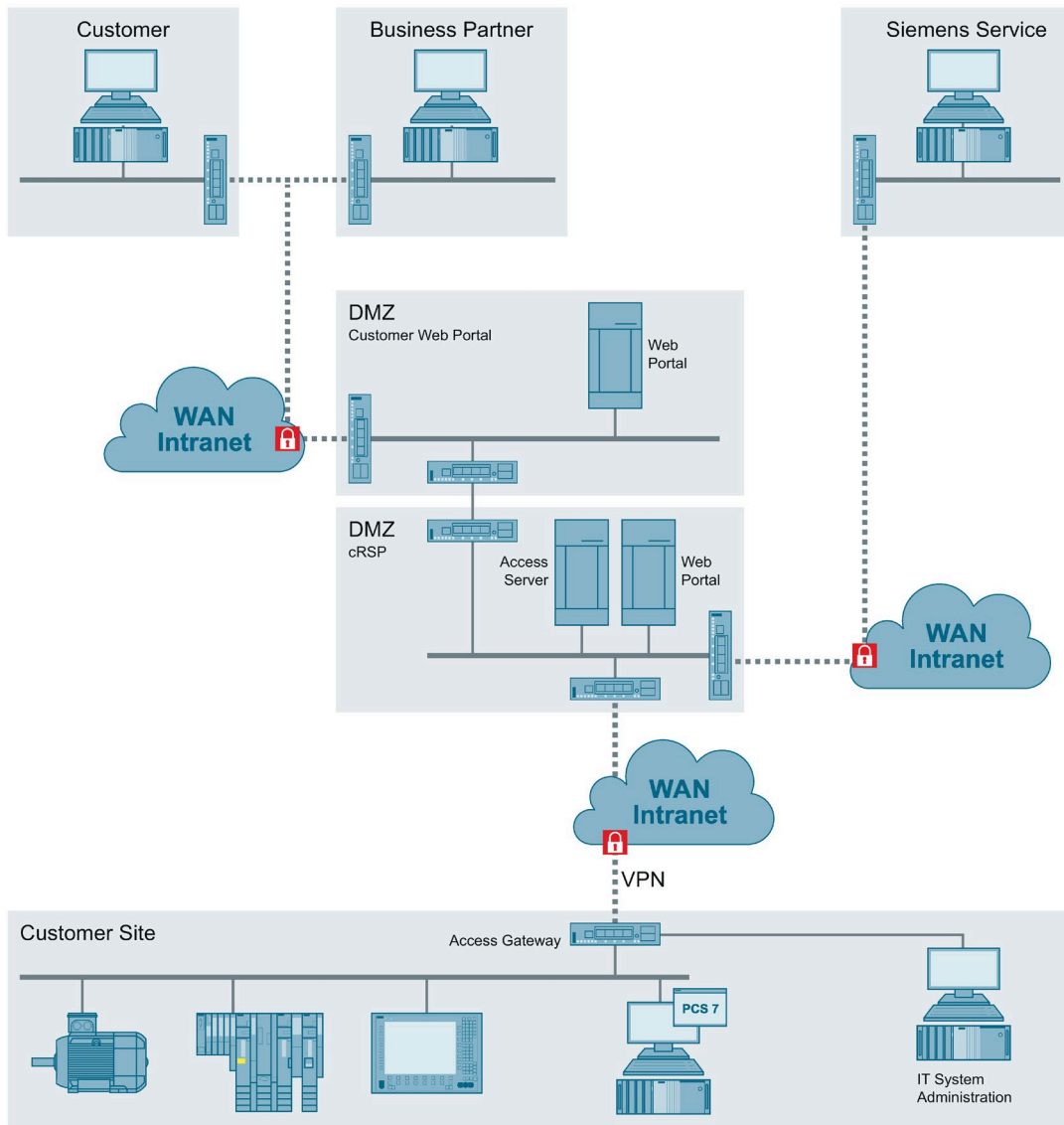
Properties and architecture of the Remote Services platform

The SIMATIC Remote Services platform provides the following properties and functions:

- Tiered security and access concept
- Collaboration & Customer Web Portal
- Central monitoring, logging and reporting
- E-mail notification
- Transparent access at any time
- Secure authentication
- Encrypted communication using SSL and VPN

The following figure shows the architecture of the Remote Services platform:

12.1 Remote maintenance based on the Remote Services platform



You can find more information on the Remote Services platform on the "Remote Services for Process Automation" (<https://support.industry.siemens.com/cs/ww/en/sc/2281>) website.

12.2 Creating a remote service concept

For secure remote maintenance, you first need to identify the key components for remote access and make them available. Most security gaps occur due to the lack of a concept and lack of access because of time and cost pressure, thereby resulting in potential economic damage.

The following questions should be considered:

- What equipment do I need to provide services?
- Where is this equipment located?
- How can I obtain this equipment?
- What tools (STEP 7, WinCC, SDT, File Transfer, RDP, etc.) do I need?

The service case should also be taken into consideration to minimize potential problems in providing the service in advance:

- For example, will the equipment be needed by several people at the same time?
- Is the service activity non-reacting?
- Who issues authorization for the remote connection, who is the proxy?

Once these questions are answered, these points are entered in the configuration of the SIMATIC Remote Service platform by the platform administration and thus represent a functional remote service access that is also set up in accordance with the principle of minimalism. The service providers now have the systems and tools available, which they need to render the services.

Because the remote service means increased risk for customers as well as for service providers, this cooperation is maintained and secured in a service contract.

12.3 Connection to the Remote Services platform

The Remote Services platform is available as a central infrastructure. Various access solutions are available for systems/plants for which remote access should be provided.

- SRS "DSL/UMTS access" (Internet access via ADSL/SDSL modem)
- SRS "Customer access" (The required tunnel connection is terminated in the IT infrastructure of the customer)
- SRS "SSL client access" (provide SSL VPN client software)

12.4 Implementation of your own remote access solution

If you are implementing your own remote access solution, the multi-tiered security concept must be taken into account. Such solutions must always be designed on a project-specific basis and according to the state of the art.

Ideas for a possible design can be found in the document "SIMATIC Process Control System PCS 7; Support and Remote Dialup"

(<https://support.industry.siemens.com/cs/ww/en/view/38621092>).

A possible product for setting up a secure remote connection under separate management and for support purposes only is SINEMA Remote Connect (SINEMA RC)

(<https://new.siemens.com/global/en/products/automation/industrial-communication/industrial-remote-communication/remote-networks/sinema-remote-connect-access-service.html>).

Note

Follow the instructions given in the documentation "SIMATIC Process Control System PCS 7 Readme V9.1" (<https://support.industry.siemens.com/cs/ww/en/view/109780270>) for "Remote Service and Remote Operation", section 3.4.14 and 3.4.15.

Definitions and Abbreviations

The following table shows the abbreviations used in this document:

Abbreviation/acronym	Explanation
AD	Active Directory: Directory service of Microsoft (Windows domain)
AFW NG	Automation Firewall Next Generation
CSN	Control System Network (plant bus)
DC	Domain Controller
DMZ	Demilitarized Zone
DNS	Domain Name System
DSRM	Directory Services Restore Mode
ECN	Enterprise Control Network
ERP	Enterprise Resource Planning
ES	PCS 7 Engineering Station
FSMO	Flexible Single Master Operations
GC	Global Catalog
IANA	Internet Assigned Numbers Authority
MES	Manufacturing Execution System
MON	Manufacturing Operations Network
MS	Microsoft
OS Client	PCS 7 Operator Station; client design
OS server	PCS 7 Operator Station; server design
PDC	Primary Domain Controller, Emulator role (FSMO)
PCN	Process Control Network (terminal bus)
PCN1	Production cell 1
PCN2	Production cell 2
PCS 7	Process Control System from SIEMENS AG
PN	Perimeter Network
RID	Relative ID
SCT	Security Configuration Tool
WINS	Windows Internet Name Service
WSUS	Windows Server Update Services

Service and support

Industry Online Support

Do you have questions or need assistance?

Using the Industry Online Support, you have round-the-clock access to expertise spanning the entire range of service and support, as well as to our services.

Industry Online Support is the central address for information about our products, solutions and services.

Product information, manuals, downloads, FAQs and application examples – all information can be accessed with just a few mouse clicks: <https://support.industry.siemens.com/>.

Industry Online Support app

The "Siemens Industry Online Support" app provides you with optimal support even when you are on the go. The app is available for Apple iOS, Android and Windows Phone:

<https://support.industry.siemens.com/cs/ww/en/sc/2067>

Technical Forum

Exchange your experience and know-how about our products or systems or benefit from the knowledge of others.

Have discussions on special products or general topics, discover new ideas and inspiration and help yourself and others on the Technical Forum

(<http://www.siemens.com/automation/forum>) – free of charge, outside office hours and at the weekend.

Technical Support

The Siemens Industry Technical Support offers you fast and competent support for any technical queries you may have with a number of tailor-made solutions – ranging from basic support to individual support contracts.

Send your queries to Technical Support using the following web form:

www.siemens.com/industry/supportrequest.

Range of services

Our range of services includes the following:

- Product training courses
- Plant data services
- Spare parts services
- Repair services
- On-site and maintenance services
- Retrofitting and modernization services
- Service programs and contracts

You can find detailed information on our range of services in the service catalog:

<https://support.industry.siemens.com/cs/sc>.

Contact partner

If you have any questions or need support, please contact your local representative, who will put you in contact with the responsible service center. You can find your contact partner in the contact database: www.siemens.com/yourcontact.