SIEMENS

SIMATIC

Process Control System PCS 7 Compendium Part F - Industrial Security (V8.2)

Configuration Manual

Valid for PCS 7 V8.2

10/2016

A5E38164581-AA

Legal information

Warning notice system

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

⚠DANGER

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

⚠WARNING

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

⚠CAUTION

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

NOTICE

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

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

Qualified Personnel

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

Proper use of Siemens products

Note the following:

⚠WARNING

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

Trademarks

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

Disclaimer of Liability

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

Siemens AG
Division Digital Factory
Postfach 48 48
90026 NÜRNBERG
GERMANY

A5E38164581-AA
℗ 10/2016 Subject to change

Table of contents

Security information 1

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. For more information about industrial security, please visit http://www.siemens.com/industrialsecurity.

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends 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 at http://www.siemens.com/industrialsecurity.

Preface 2

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.

The compendium directly reflects the recommended method for configuration, 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.

The compendium is divided into the following parts:

- Configuration guidelines including checklist
- Process safety including two checklists
- Technical functions with SFC types
- Operation and maintenance including checklist
- Hardware installation including checklist
- Industrial Security

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.

This manual serves as a compendium and supplements 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.

The compendium directly reflects the recommended method for configuration, which is based on 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.

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 V8.2.

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

Full PCS 7 documentation is available to you free of charge and in multiple languages in PDF format at www.siemens.com/pcs7-documentation.

What's new? 3

The existing contents were updated for SIMATIC PCS 7 V8.2. Changes and additions were made in the following sections in particular:

- Security strategies
  - Concept of "defense in depth" > section "Division into security cells" (Page 12)
- Network security
  - Name resolution > Computer name > Specifications for the computer name (Page 26)
  - Name resolution > Host name resolution with the Hosts file (Page 31)
  - Access points to the security cells > Example configuration: Access rules (Page 36)
  - Secure communication between security cells > Data exchange between OS and AS stations (new) (Page 65)
- System hardening
  - Installation of the operating system > Setting data protection and telemetry data in Windows 10 (new) (Page 76)
  - Installation of the operating system > Additional hardening measures to be configured manually (new) (Page 82)
  - Whitelisting > Central administration of McAfee Application Control (Page 116)
  - Time synchronization of the plant (new) (Page 119)
  - Handling of digital signatures for applications (new) (Page 119)
- User administration and operator authorizations
  - Administration of computers and users (Page 123)
  - Domain controller > Installation and configuration of an additional domain controller (DC2-DCn) in an existing domain (Page 156)
  - Domain controller > Check of network settings on the DCs (Page 157)
  - Domain controller > Operation master roles (FSMO) (new) (Page 167)

Security strategies 4

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

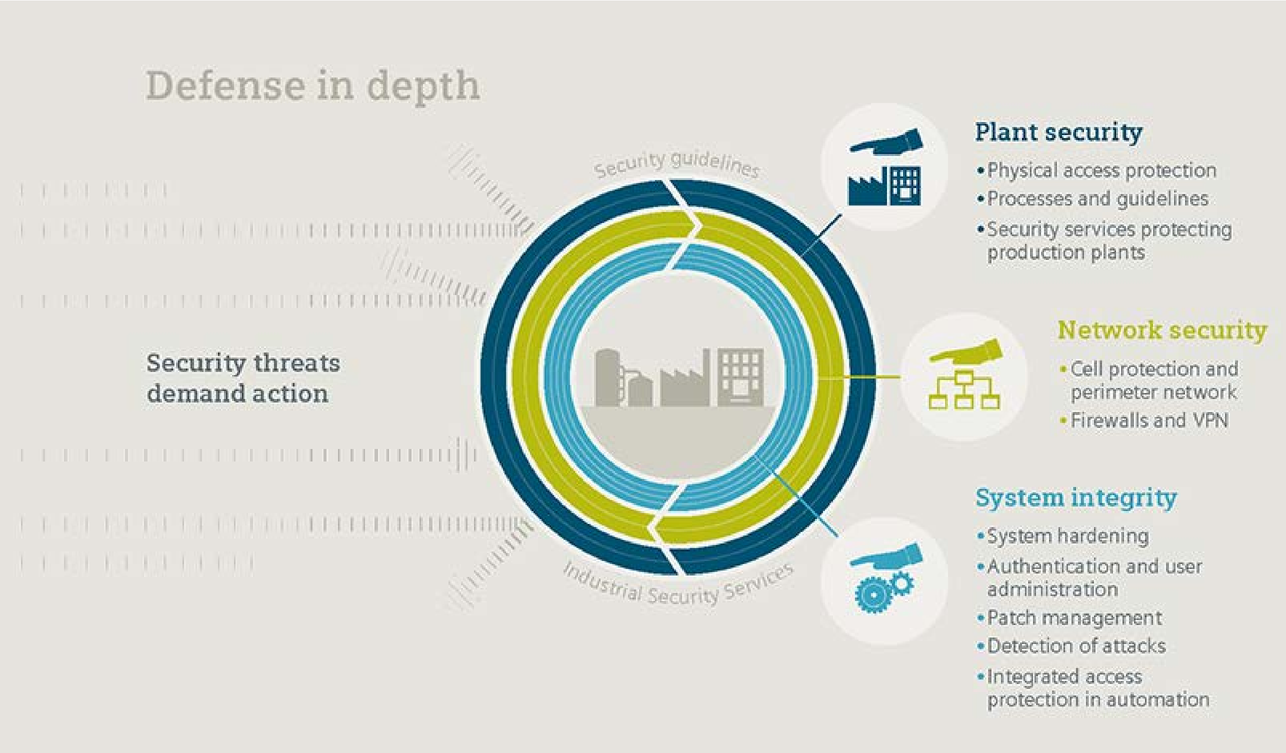
- Division into security cells
  A comprehensively secured network architecture subdivides the control network into different task levels.
  Perimeter zone techniques should be employed for this. This means that systems set up in the perimeter network (DMZ) are shielded by one or more firewalls (front-end 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 PPTP (Point To Point Tunneling Protocol), L2TP (Layer Two Tunneling Protocol) and IPSec (IPSecurity) 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) or SSL (Secure Sockets Layer) 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

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


Defense in depth
Security threats demand action
Security guidelines
Industrial Security Services
Plant security
•Physical access protection
•Processes and guidelines
•Security services protecting production plants
Network security
•Cell protection and perimeter network
•Firewalls and VPN
System integrity
•System hardening
•Authentication and user administration
•Patch management
•Detection of attacks
•Integrated access protection in automation

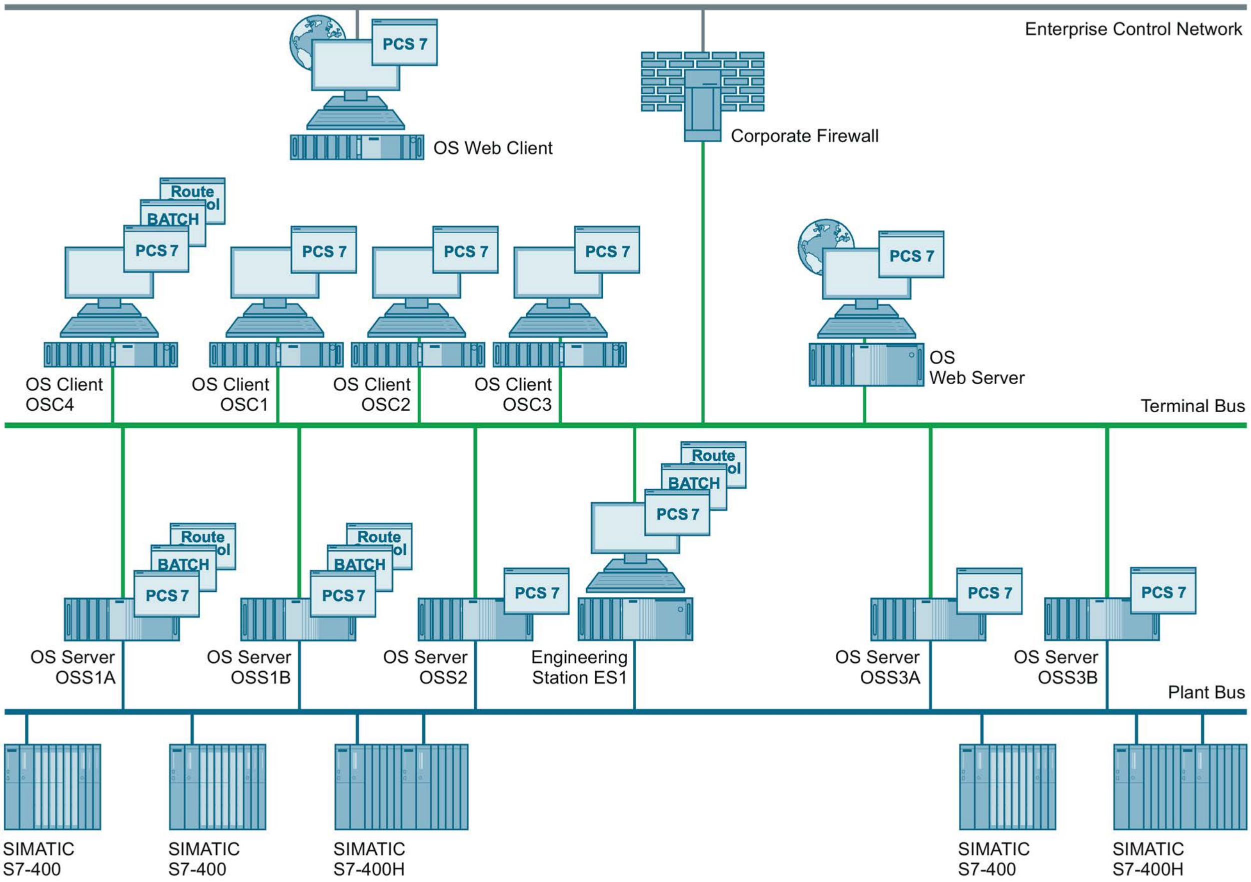
4.3 Example configuration

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 above 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 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 with the corporate network which, in turn, provides Internet access. An engineering station is available for configuring the overall plant.

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

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/60119725)"

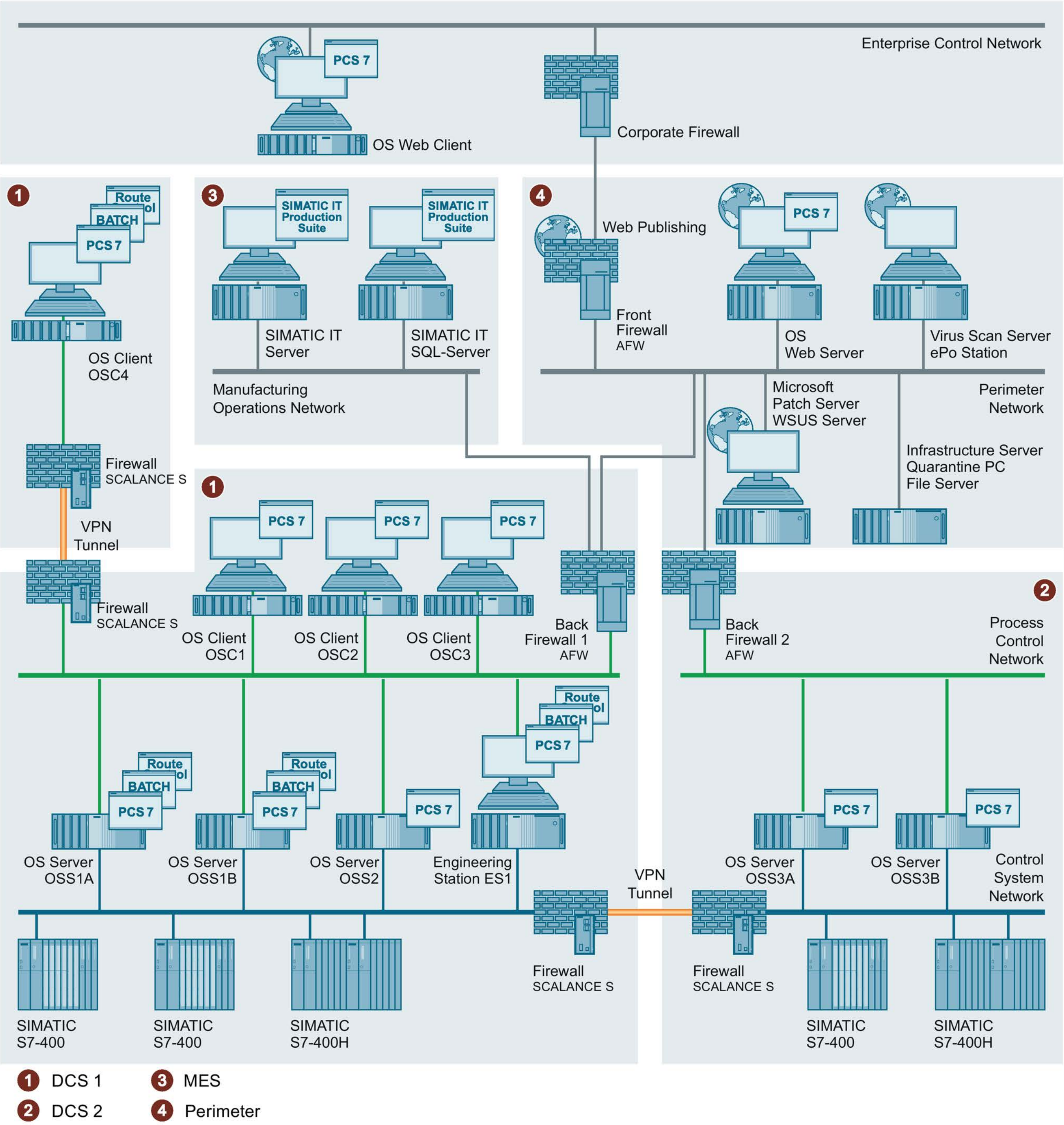
Example configuration: Division into security cells

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. 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	141.84.65.2	1000 1101	0101 0100	0110 0101	0000 0010
Subnet mask	255.255.255.0	1111 1111	1111 1111	1111 1111	0000 0000
Network	141.84.65.0	1000 1101	0101 0100	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	224 = 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	220 = 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	216 = 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-PSN, 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))

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 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

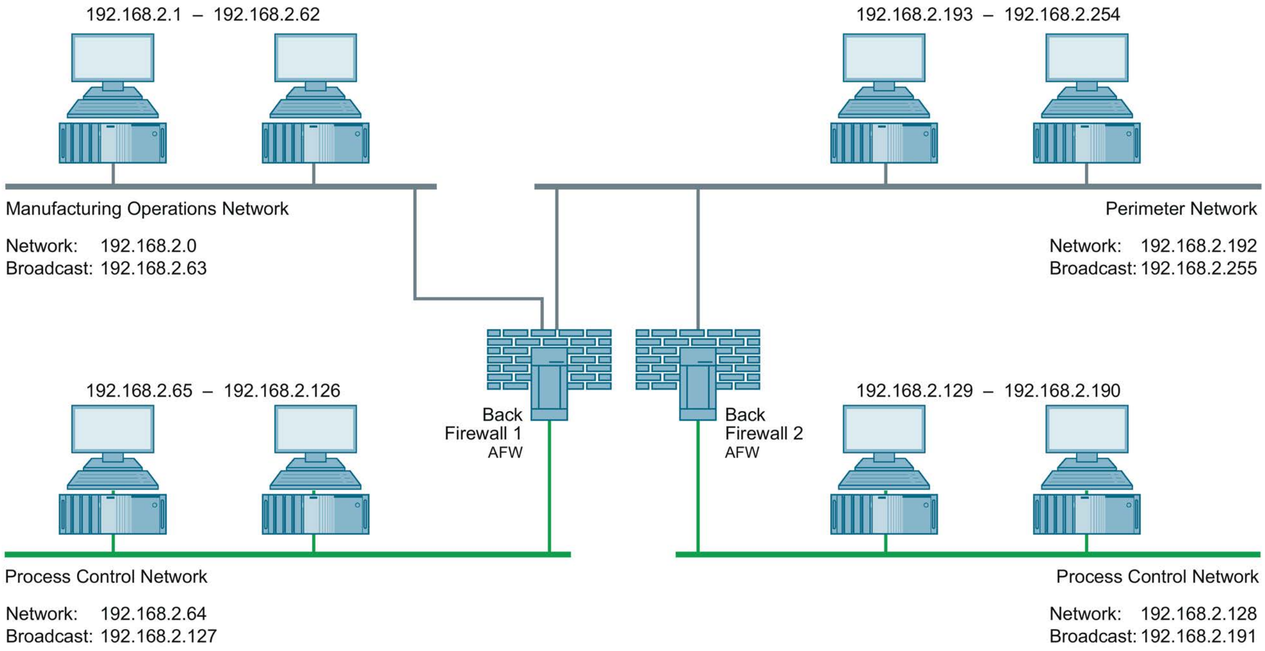
- Network 3: Process Control Network 2 (IP addresses of PCN2 (Unit B), 192.168.2.128/26)

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 routing 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.

5.2.4 Example configuration: Setting of IP addresses and subnet mask

Procedure

The following procedure is described using the example of the "Windows 7" operating system.

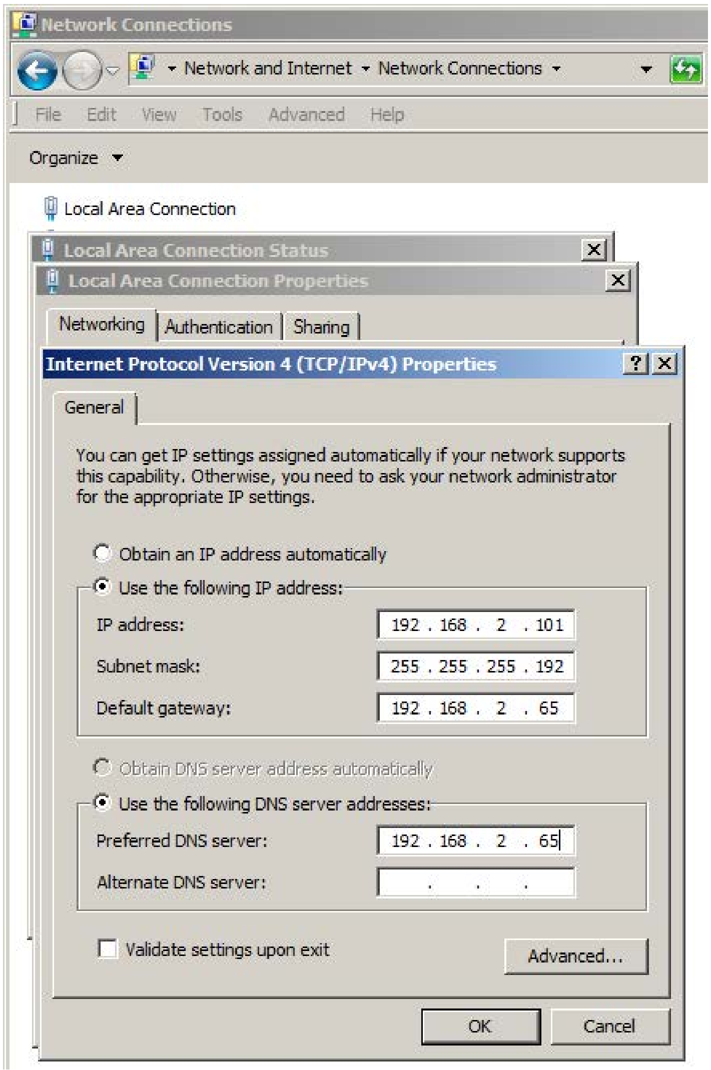
To set the IP address, subnet mask and default gateway, follow these steps:

1. Open the Network and Sharing Center with the command "Start > Control Panel > Network and Sharing Center".
   The "Network and Sharing Center" dialog box opens.
2. In the left navigation pane of the dialog, click on "Change adapter settings".
   The "Network Connections" dialog box opens.
3. Open the status display of the corresponding network connection (Process Control Network 1 or 2, Perimeter Network or Manufacturing Operations Network) by double-clicking on the icon.
   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. 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.



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 2 . 101

Subnet mask: 255 . 255 . 255 . 192

Default gateway: 192 . 168 . 2 . 65

○ Obtain DNS server address automatically

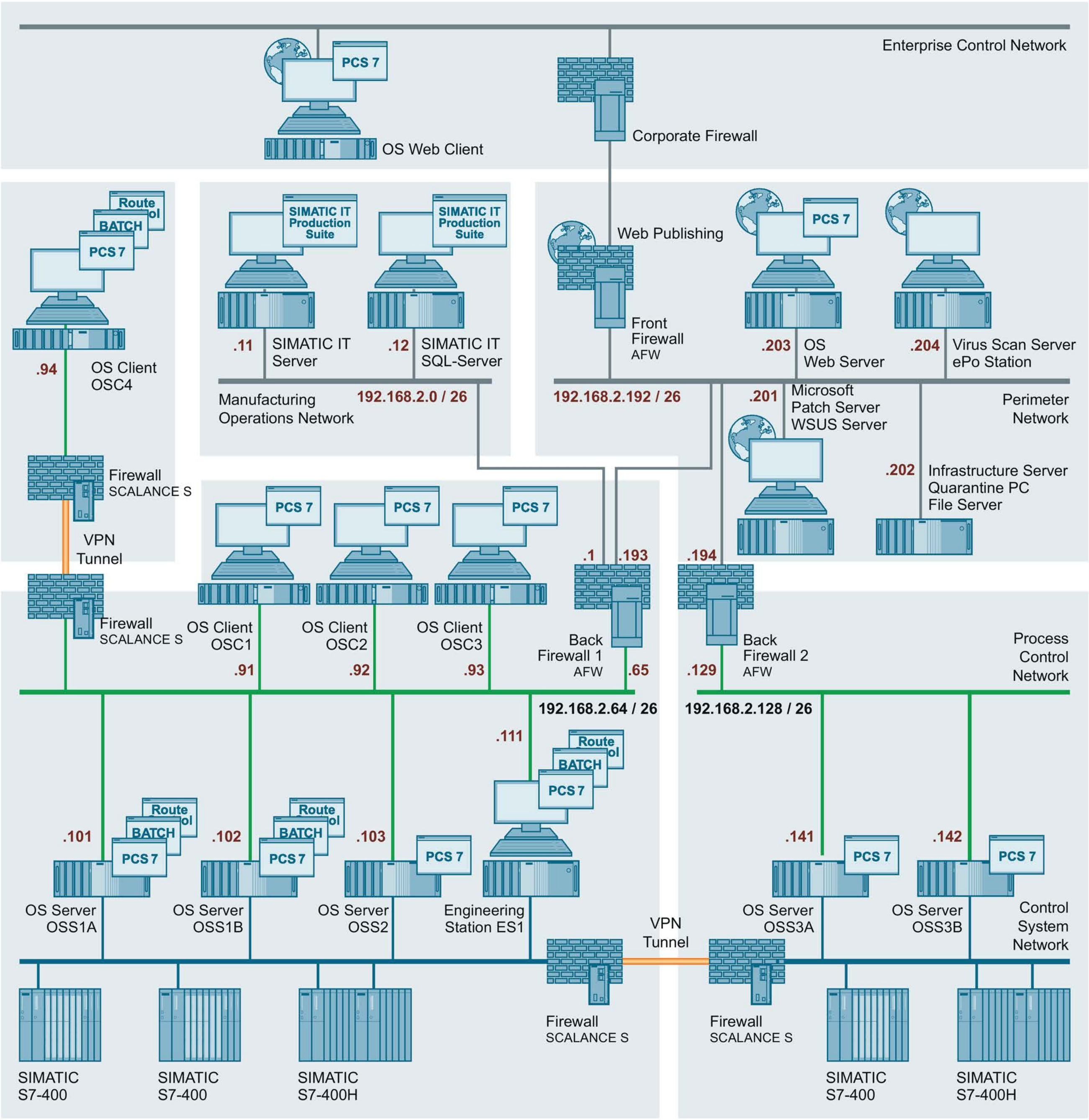
● Use the following DNS server addresses:

Preferred DNS server: 192 . 168 . 2 . 65

Alternate DNS server: . . .

□ Validate settings upon exit

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 uniquely identified within a network by the computer name. This is the prerequisite for communication with the computer. The name has to be uniquely associated with the computer. This ensures that a computer can be reliably located. Accidental assignment of a computer name to more than one computer can lead to unpredictable 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 has a maximum of 15 characters (limited by the operating system).

Note

You can learn about the rules for assigning the computer name in the installation manual "SIMATIC Process Control System PCS 7 PC Configuration" (https://support.industry.siemens.com/cs/ww/en/view/109485951).

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" (http://support.microsoft.com/kb/909264/en)

You can find more naming conventions in the following documents:

- Manual "SIMATIC Process Control System PCS 7 Engineering System" (https://support.industry.siemens.com/cs/ww/en/view/109485969) section "Rules for naming in the PH"
- WinCC Information System online help "Working with projects > Appendix > Invalid characters"
  The "Projects.chm" file can be found in the installation folder of the SIMATIC product series of Siemens AG

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 Process Control System PCS 7 PC Configuration"
(https://support.industry.siemens.com/cs/ww/en/view/109485951)
(section 5.3.3 - "Changing the computer name").

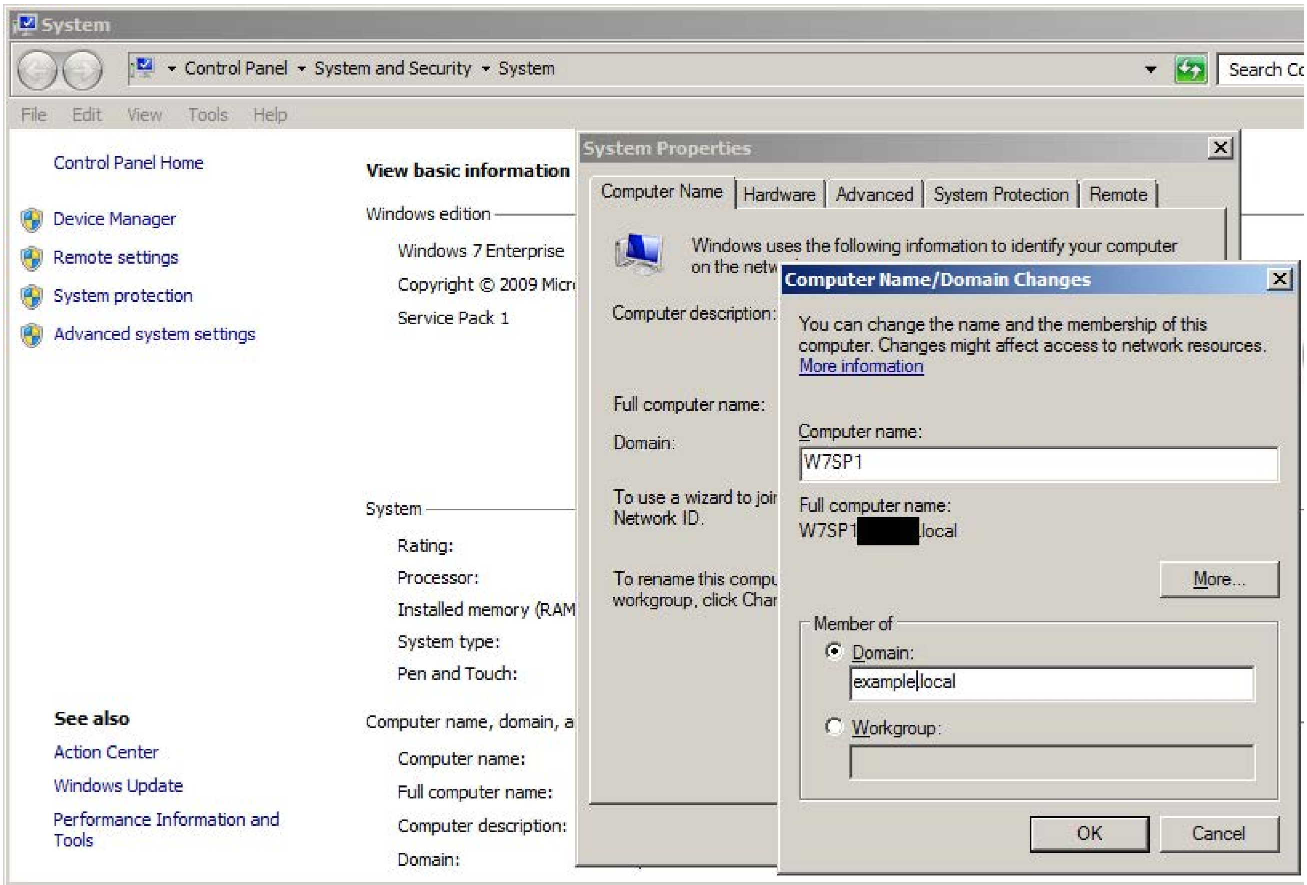
Procedure

The following procedure is described using the example of the "Windows 7" operating system.

To change the computer name, follow these steps:

1. Select the command "Start > Control Panel > System".
   The "System" dialog opens.
2. Click the "Change settings" link in the "Settings for computer name, domain and workgroup" 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.
3. Click "Change" in the "Computer name" tab.
   The "Computer Name/Domain Changes" dialog box opens.

4. In the "Computer name" box, enter the name of the computer.



Windows uses the following information to identify your computer on the netw

Computer description:

Full computer name:

Domain:

To use a wizard to joi Network ID.

To rename this compu workgroup, click Char

Computer Name/Domain Changes

You can change the name and the membership of this computer. Changes might affect access to network resources. More information

Computer name: W7SP1

Full computer name: W7SP1[redacted]local

More...

Member of

● Domain: example.local

○ Workgroup:

OK Cancel

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:
  131.107.7.29 OSSRV01
- 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"

To resolve NetBIOS names of NetBIOS applications that are executed on local computers or remote computers, NetBT usually utilizes a NetBIOS name server (NBNS). 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 WINS 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: 131.107.7.29 OSSRV01
- 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 "%systemroot%\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.

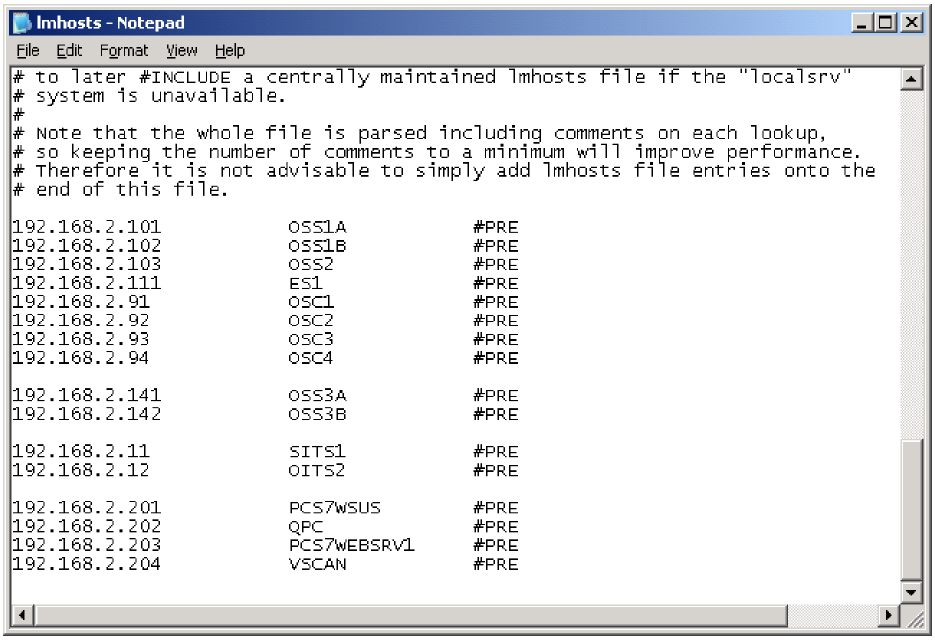
5.3.10 Example configuration: Name resolution

The example configuration was divided into four or five 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.

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.



```
# to later #INCLUDE a centrally maintained lmhosts file if the "localsrv"
# system is unavailable.
#
# 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
192.168.2.91            OSC1            #PRE
192.168.2.92            OSC2            #PRE
192.168.2.93            OSC3            #PRE
192.168.2.94            OSC4            #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           VSCAN           #PRE
```

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. Copy the file from the computer where you have created it to all other computers in the plant.
6. Add the entries made in the "lmhosts" file to the "hosts" file.

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

Decentralized 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 apply to an automation system, which is why use of a DCHP server is not recommended in this example.

Note

If a DHCP server is used in a 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/60119725).

5.5.2 Automation Firewall V2

To implement the different solutions for access points according to the PCS 7 & WinCC security concept (front-end/back-end firewall, three-homed firewall or access point firewall), Automation Firewall V2 is available as a SIMATIC PCS 7 add-on.

Automation Firewall 2 is based on the Windows firewall solution of Microsoft and additional tools for configuration and securing (e.g. intrusion detection). An optimized rule base can be created with the help of a wizard and the integrated SecureGUARD appliance management.

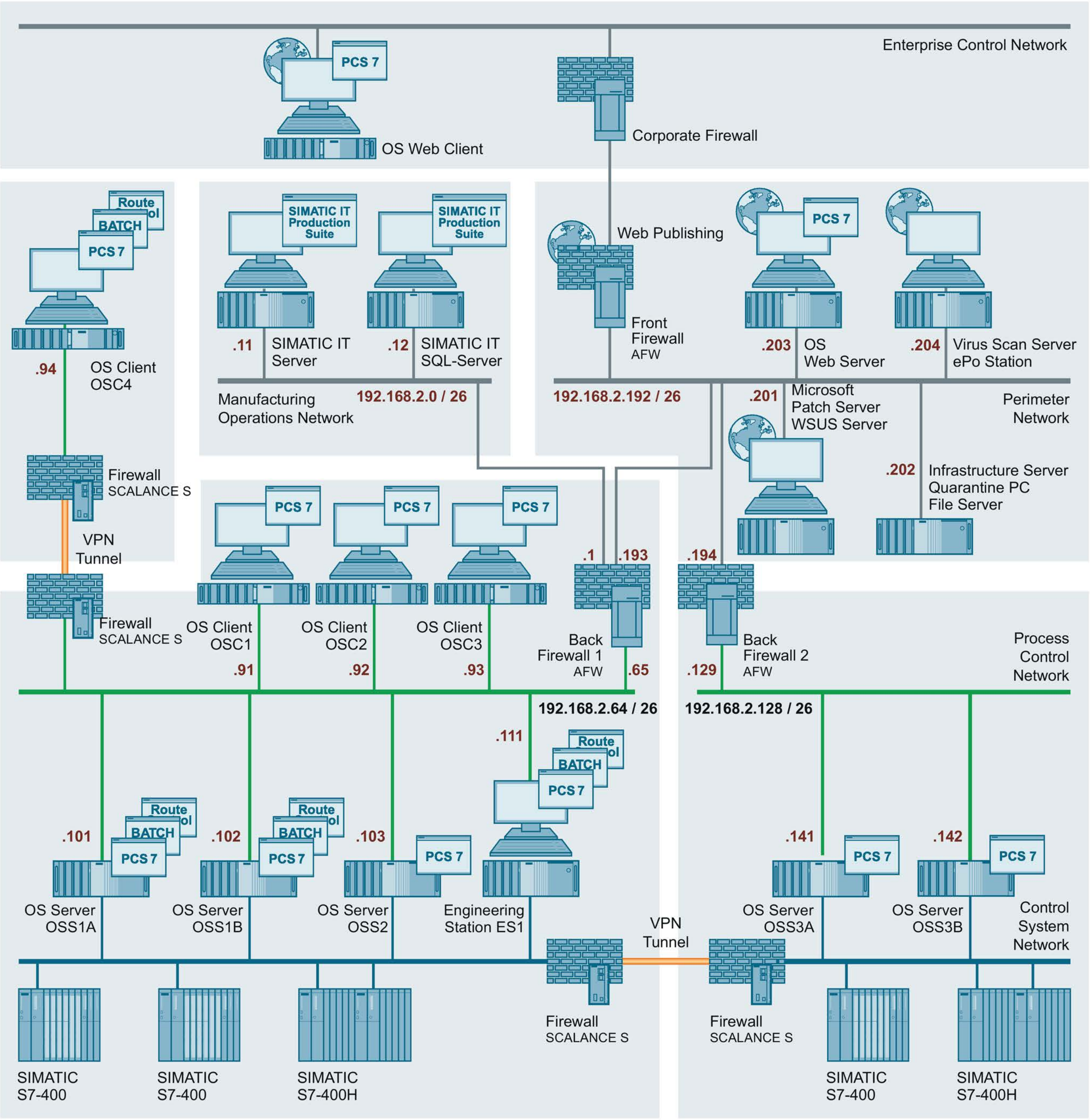
Note

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 V2 in the PCS 7 Add-on catalog. You can download this catalog from the SIMATIC PCS 7 website (https://w3.siemens.com/mcms/process-control-systems/en/simatic-pcs-7/Pages/simatic-pcs-7.aspx).

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).



To ensure unrestricted operation of the plant, a data exchange between the different security cells is required. 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	• Distribution of Windows updates (security patches and critical patches) via PCS7WSUS to all computers within 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 QPC / File Server
Perimeter	DCS2	Back-end firewall 2	• Distribution of Windows updates (security patches and critical patches) via PCS7WSUS 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
Perimeter	MON	Back-end firewall 1	• Distribution of Windows updates (security patches and critical patches) via PCS7WSUS to all computers within 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	• Communication between OSS3A/B in PCN2 and the OS clients in PCN1 • Communication between OSS3A/B in PCN2 and the ES1 in PCN1

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 virus scan server to PCN1 #1 The virus scanner firewall rules must be configured dependent on the utilized virus scanner product, its version and installation. See footnote [2]	Allow	Diverse manufacturer-specific protocols and ports[2]	[Virus Scan Server] [192.168.2.204]	[All] [192.168.2.64/26]
PCN 1 to Perimeter Virus Scan Server #1 The virus scanner firewall rules must be configured dependent on the utilized virus scanner product, its version and installation. See footnote [2]	Allow	Diverse manufacturer-specific protocols and ports[2]	[All] [192.168.2.64/26]	[Virus Scan Server] [192.168.2.204]
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] [OS Server] [192.168.2.103]	[OS Web Server] [192.168.2.203]

Name	Action	Protocols	From	To
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] [OS Server] [192.168.2.103]
Bidirectional Ping between Perimeter and PCN1 #1	Allow	ICMP/Ping	Perimeter PCN1	Perimeter PCN1
PCN1 ES to Perimeter QPC[3]	Allow	TCP/139 TCP/445[3]	[ES] [192.168.2.111]	[QPC] [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 PCS 7 security policy.
   Starting in PCS 7 V8.1, it is possible to activate the encrypted communication in the SIMATIC Shell. The configured port must then be opened in the back-end firewall with the TCP/UDP protocols.
   In addition, if IPSec is not used, the bidirectional communication for Windows data transfer (use of drive shares) and ICMP/Ping between the PCS 7 systems involved must be enabled.
   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 offer advantages when a firewall with IDS functionality (Intrusion Detection System) is used (e.g. Automation Firewall), because it enables a detailed check of the data traffic.
   Configuration of these rules is thus dependent on the requirements of the project, the firewall options and the anticipated risks.
2. To ensure the functionality of the virus scan servers and clients, product- and installation-dependent ports must be opened on the back-end firewall. Additional information on the released virus scan products and their utilized ports can be found on the web sites of the virus scanner manufacturers:
   - Trend Micro (https://esupport.trendmicro.com/solution/en-us/1054836.aspx)
   - Symantec (http://www.symantec.com/docs/TECH163787)
   - Intel Security (McAfee) (https://kc.mcafee.com/corporate/index?page=content&id=KB66797)

   It is additionally recommended that ports TCP/139 and TCP/445 from PCN1 to the virus scan server in the Perimeter be opened to allow client installation packages to be downloaded from the virus scan management systems.
3. Alternatively, an FTP server can be set up on the QPC system (see 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 Virus Scan Server to PCN2 #1 The virus scanner firewall rules must be configured dependent on the utilized virus scanner product, its version and installation. See footnote [2]	Allow	Diverse manufacturer-specific protocols and ports[2]	[Virus Scan Server] [192.168.2.204]	[All] [192.168.2.128/26]
PCN2 to Perimeter Virus Scan Server #1 The virus scanner firewall rules must be configured dependent on the utilized virus scanner product, its version and installation. See footnote [2]	Allow	Diverse manufacturer-specific protocols and ports[2]	[All] [192.168.2.128/26]	[Virus Scan Server] [192.168.2.204]
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 PCS 7 security policy.
Starting in PCS 7 V8.1, it is possible to activate the encrypted communication in the SIMATIC Shell. The configured port must then be opened in the back-end firewall with the TCP/UDP protocols.
In addition, if IPSec is not used, the bidirectional communication for Windows data transfer (use of drive shares) and ICMP/Ping between the PCS 7 systems involved must be enabled.
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 offer advantages when a firewall with IDS functionality (Intrusion Detection System) is used (e.g. Automation Firewall), because it enables a detailed check of the data traffic.
Configuration of these rules is thus dependent on the requirements of the project, the firewall options and the anticipated risks.

[2] To ensure the functionality of the virus scan servers and clients, product- and installation-dependent ports must be opened on the back-end firewall. Additional information on the released virus scan products and their utilized ports can be found on the web sites of the virus scanner manufacturers:

- Trend Micro (https://esupport.trendmicro.com/solution/en-us/1054836.aspx)
- Symantec (http://www.symantec.com/docs/TECH163787)
- Intel Security (McAfee) (https://kc.mcafee.com/corporate/index?page=content&id=KB66797)

It is additionally recommended that ports TCP/139 and TCP/445 from PCN1 to the virus scan server in the Perimeter be opened to allow client installation packages to be downloaded from the virus scan management systems.

[3] Alternatively, an FTP server can be set up on the QPC system (see section "Quarantine station as data exchange point" for more information).

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 PCS 7 security policy. Starting in PCS 7 V8.1, it is possible to activate the encrypted communication in the SIMATIC Shell. The configured port must then be opened in the back-end firewall with the TCP/UDP protocols. In addition, if IPSec is not used, the bidirectional communication for Windows data transfer (use of drive shares) and ICMP/Ping between the PCS 7 systems involved must be enabled. 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 offer advantages when a firewall with IDS functionality (Intrusion Detection System) is used (e.g. Automation Firewall), because it enables a detailed check of the data traffic. 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]

Name	Action	Protocols	From	To
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]
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]

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 PCS 7 security policy.
   Starting in PCS 7 V8.1, it is possible to activate the encrypted communication in the SIMATIC Shell. The configured port must then be opened in the back-end firewall with the TCP/UDP protocols.
   In addition, if IPSec is not used, the bidirectional communication for Windows data transfer (use of drive shares) and ICMP/Ping between the PCS 7 systems involved must be enabled.
   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 offer advantages when a firewall with IDS functionality (Intrusion Detection System) is used (e.g. Automation Firewall), because it enables a detailed check of the data traffic.
   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

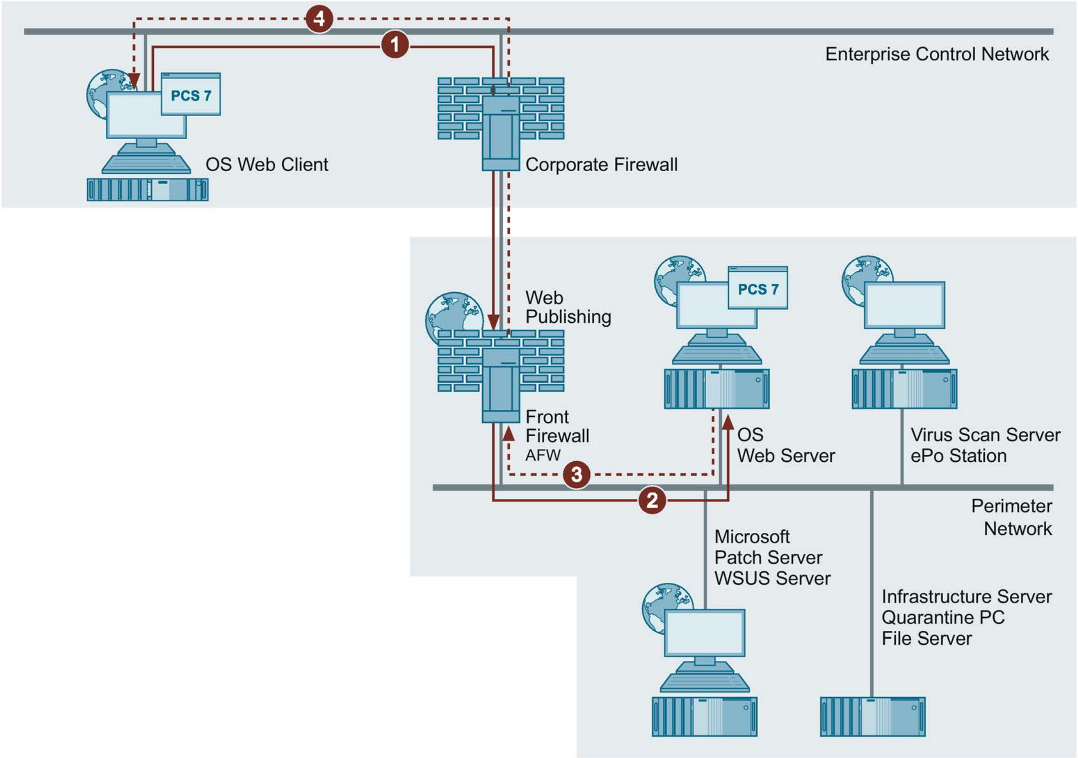
Setup of an Active Directory (Windows domain) is recommended from a security perspective. In this case, other protocols and ports may need to be configured on the firewalls to enable communication between the domain controllers as well as communication of domain members with the domain controllers.

You can find additional information under the following link: https://technet.microsoft.com/en-us/library/8daead2d-35c1-4b58-b123-d32a26b1f1dd.

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

For access to a Web server in the Perimeter network by Web clients from an external network, the Web server must be published across the front-end firewall. The technique of Web publishing, which is supported by Automation Firewall V2 and is used here, offers better security than the outdated technique of Web tunneling or Web forwarding. The opening of port 80 or 443 and the resulting passing through of communication through the front-end firewall directly to the Web server, as practiced in the obsolete method, should no longer be used.

In Web publishing (see following figure), the Web client does not directly access the Web server from the external network. Instead, it directs its query to Automation Firewall V2 (1). Automation Firewall V2 forwards the verified query to the Web server (2), and receives the requested information in return (3). It then forwards this information to the Web client (4).


4
1
Enterprise Control Network
PCS 7
OS Web Client
Corporate Firewall
Web Publishing
PCS 7
Front Firewall AFW
OS Web Server
Virus Scan Server ePo Station
3
2
Perimeter Network
Microsoft Patch Server WSUS Server
Infrastructure Server Quarantine PC File Server

Only HTTPS should be allowed between the Web client in the external network and Automation Firewall V2 (AFW2). In this way, the authenticity of AFW2 can be guaranteed via a server certificate and communication between Web client and firewall can be encrypted, thereby protecting it against manipulation and sniffing. For access of AFW2 to the web server, either HTTP or HTTPs can be used, depending on the required security level.

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/ww/en/view/109485959).

5.5.5 Example configuration: Web publishing of 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 Web client, the Web server must be published on the back-end firewall 1.

Since this functionality is not implemented in the Industrial Wizard, you must manually create the publishing rule in back-end firewall 1 using the Automation Firewall V2 management console.

5.5.6 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 Open Source IDS/IPS functionality from Suricata used in Automation Firewall V2 is a high-performance IDS/IPS solution that is designed to detect and prevent attacks on operating systems, networks and applications. Suricata is based on signatures that are periodically updated and can be downloaded manually or automatically.

The IDS/IPS of Automation Firewall V2 provides protection from known attacks with a low-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.

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:

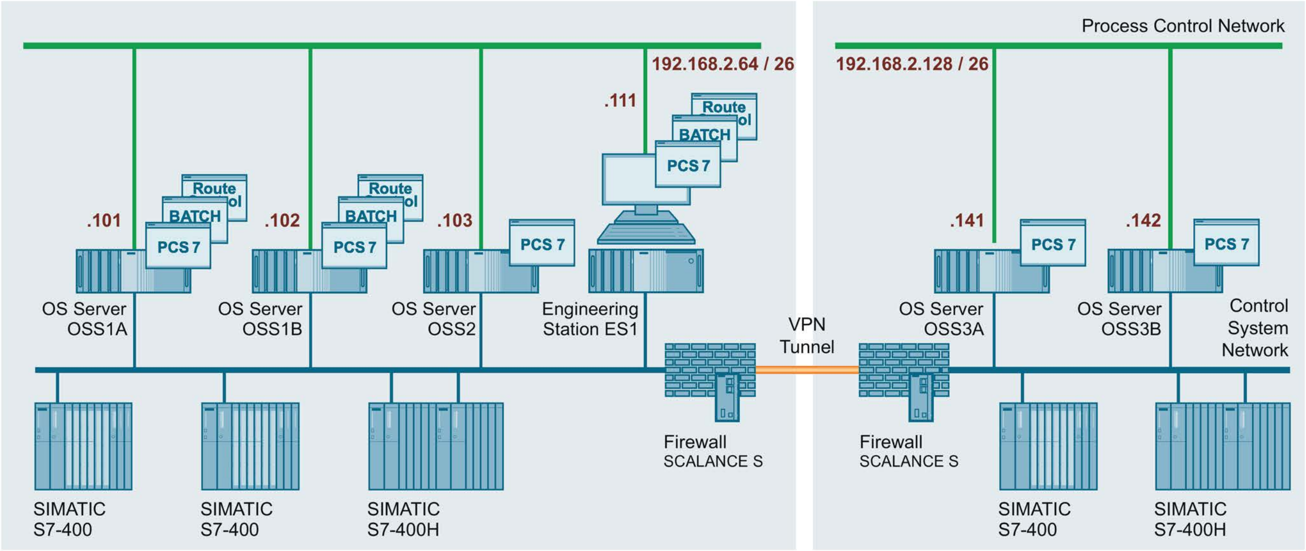
- Data exchange on the CSN level
  Data exchange between automation systems in different security cells
- Data exchange on the PCN level
  Data exchange for operating and monitoring with remote OS clients, which means OS clients located in other security cells than the corresponding OS server(s).

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 (IPSec). This communication can be established using two SCALANCE S security modules.

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



SCALANCE S modules allow the tunneling of communication via the IPSec protocol (tunnel mode of IPSec). 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.

This gives the data exchange of the devices via the IPSec tunnels in the VPN the following properties:

- 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

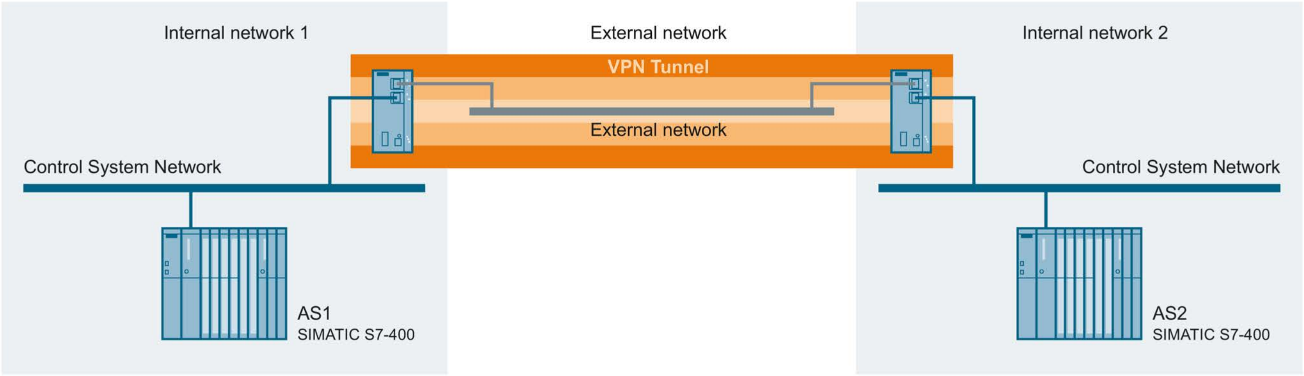
You can find additional information on SCALANCE S in the manual "SIMATIC NET Industrial Ethernet Security Basics and application" (https://support.industry.siemens.com/cs/ww/en/view/67437017).

5.6.1.2 Establishing secure communication between security cells with SCALANCE S

Introduction

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

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



The internal (secure) network is connected to SCALANCE S at Port 2 ("Internal Network" Port; Port 2 = green). The internal network contains one network node each, which is represented by an automation system.

- AS 1: Represents a node of the CSN in security cell 1 (internal network 1)
- AS 2: Represents a node of the CSN in security cell 2 (internal network 2)
- SCALANCE S Module 1: SCALANCE S module for security cell 1
- SCALANCE S Module 2: SCALANCE S module for security cell 2

The public, external network ("insecure network") is connected to the "External Network" Port (Port 1 = red) of the SCALANCE S module.

The engineering station is used for configuration. To do so, the "Security Configuration Tool" must be installed on the ES.

Overview of configuration steps

1. Setting up SCALANCE S modules and networks
2. Configuring IP settings of automation systems
3. Creating project and security modules
4. Configuring the VPN group
5. Downloading configuration to the SCALANCE S modules
6. Test

Setting up SCALANCE S modules and networks

To set up the SCALANCE S and the network connections, follow these steps:

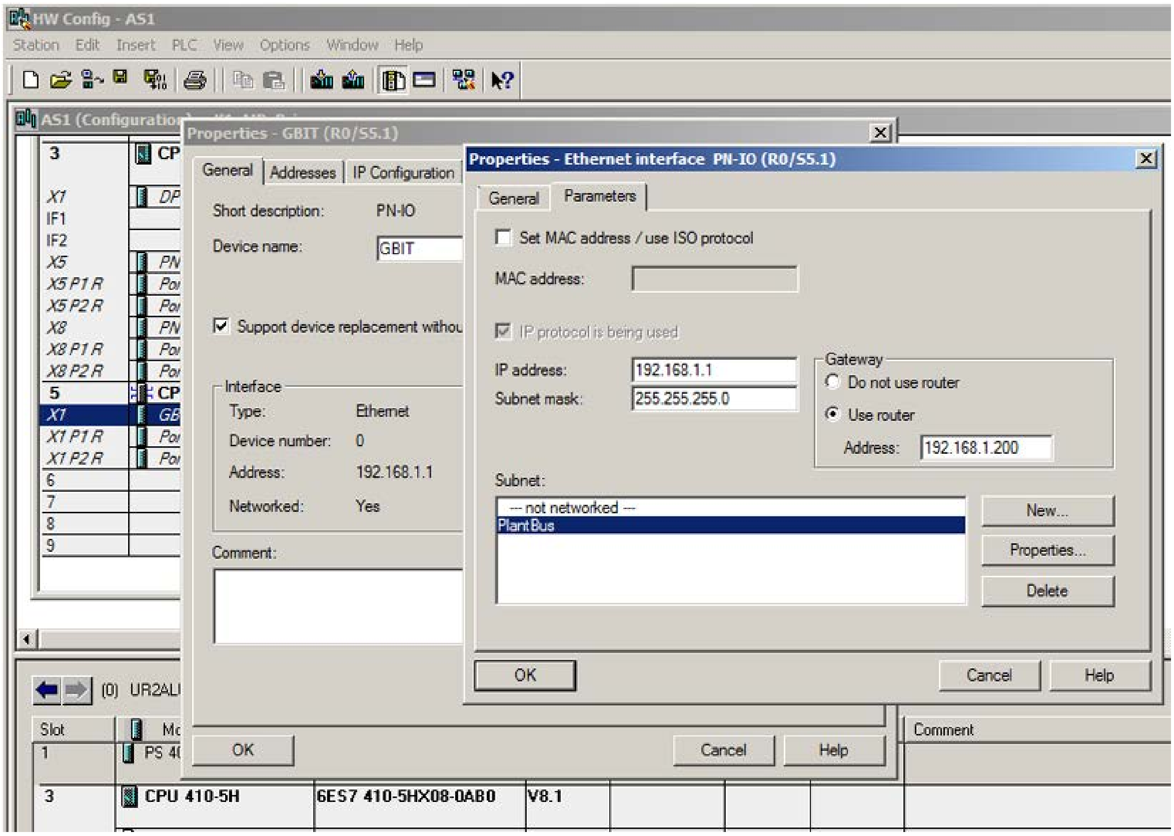
1. Start up the SCALANCE S according to the operating instructions.
2. Establish the physical network connections by connecting the network cables to the corresponding ports (RJ45 sockets):
   - Connect Control System Network 1 with Port 2 of Module 1 and Control System Network 2 with Port 2 of Module 2.
   - Connect Port 1 of Module 1 and Port 1 of Module 2 with a network switch and establish the "external" network.
   - Switch on the participating components.

Configuring IP settings of automation systems

Set up the following IPv4 address settings for the automation systems:

Automation system	IPv4 address	Subnet mask	Standard gateway
AS 1	192.168.1.1	255.255.255.0	192.168.1.200
AS 2	192.168.2.1	255.255.255.0	192.168.2.200

The following figure shows an example of how the IPv4 address of the automation system is set:



HW Config - AS1

Properties - GBIT (R0/S5.1)

Short description: PN-IO
Device name: GBIT
☑ Support device replacement withou

Interface
Type: Ethernet
Device number: 0
Address: 192.168.1.1
Networked: Yes

Comment:

Properties - Ethernet interface PN-IO (R0/S5.1)

□ Set MAC address / use ISO protocol
MAC address:
☑ IP protocol is being used
IP address: 192.168.1.1
Subnet mask: 255.255.255.0

Gateway
○ Do not use router
● Use router
Address: 192.168.1.200

Subnet:
--- not networked ---
PlantBus

Slot	Module	Order number	Firmware
1	PS 4(		
3	CPU 410-5H	6ES7 410-5HX08-0AB0	V8.1

Creating project and security modules

The SCALANCE S modules are configured with the "Security Configuration Tool".

To create the project and the modules for the example configuration, follow these steps:

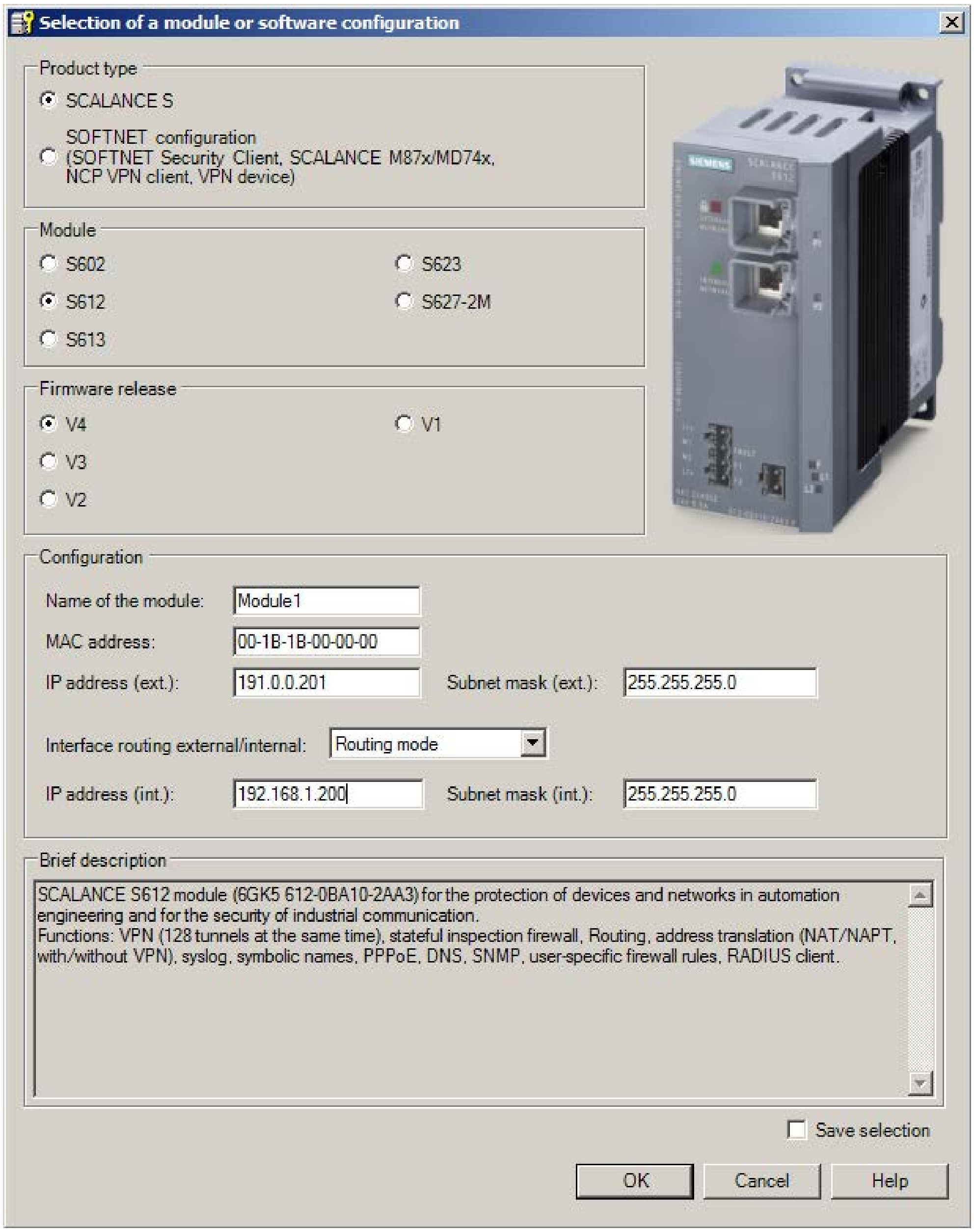
1. Start the "Security Configuration Tool" software.
2. Create a new project with the command "Project > New".
3. Create a new user with user name and associated password.
   The user is automatically assigned the "Administrator" role. Confirm the entries with "OK".
   A new project is created. The "Selection of a module or software configuration" dialog opens.
4. Select the following options in the "Product type", "Module" and "Firmware release" areas:
   - Product type: SCALANCE S
   - Module: S612 (or corresponding to the selected module)
   - Firmware release: V4
5. In the "Configuration" area, enter the MAC address in the specified format.

Note

The MAC address is printed on the front of the SCALANCE S module.

6. In the "Configuration" area, enter the external IP address (191.0.0.201) and the external subnet mask (255.255.0.0) in the specified format and confirm your entries with "OK".
7. In the "Interface routing external/internal" area, select the entry "Routing mode" from the drop-down list.

8. Enter the internal IP address 192.168.1.200 and the internal subnet mask 255.255.255.0 in the specified format and confirm the dialog with "OK".



Selection of a module or software configuration

Product type

● SCALANCE S

○ SOFTNET configuration (SOFTNET Security Client, SCALANCE M87x/MD74x, NCP VPN client, VPN device)

Module

○ S602 ○ S623

● S612 ○ S627-2M

○ S613

Firmware release

● V4 ○ V1

○ V3

○ V2

Configuration

Name of the module: Module1

MAC address: 00-1B-1B-00-00-00

IP address (ext.): 191.0.0.201 Subnet mask (ext.): 255.255.255.0

Interface routing external/internal: Routing mode

IP address (int.): 192.168.1.200 Subnet mask (int.): 255.255.255.0

Brief description

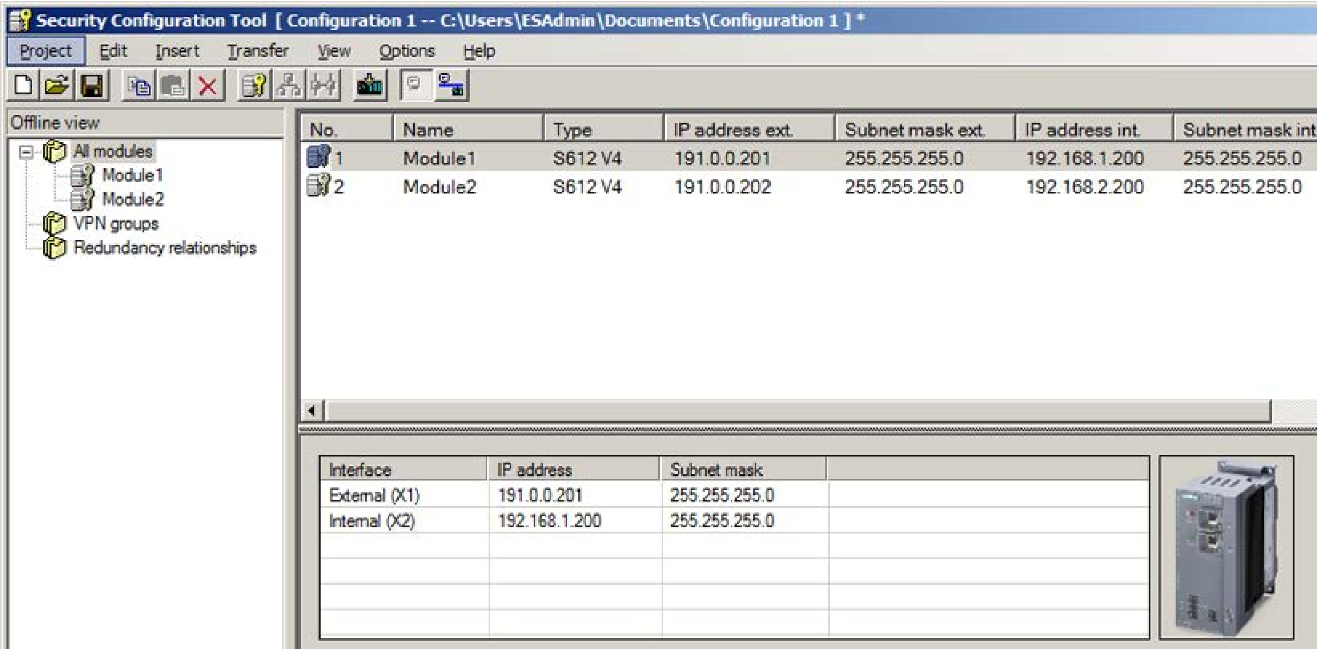
SCALANCE S612 module (6GK5 612-0BA10-2AA3) for the protection of devices and networks in automation engineering and for the security of industrial communication.
Functions: VPN (128 tunnels at the same time), stateful inspection firewall, Routing, address translation (NAT/NAPT, with/without VPN), syslog, symbolic names, PPPoE, DNS, SNMP, user-specific firewall rules, RADIUS client.

□ Save selection

9. Select the "Insert > Module" menu command.
   The "Selection of a module or software configuration" dialog opens.

10. Repeat the steps for the second security module. In doing so, assign the following address parameters to the security module:

    - IP address (ext.): 191.0.0.202
    - Subnet mask (ext.): 255.255.0.0
    - Interface routing external/internal: Routing mode
    - IP address (int.): 192.168.2.200
    - Subnet mask (int.): 255.255.255.0



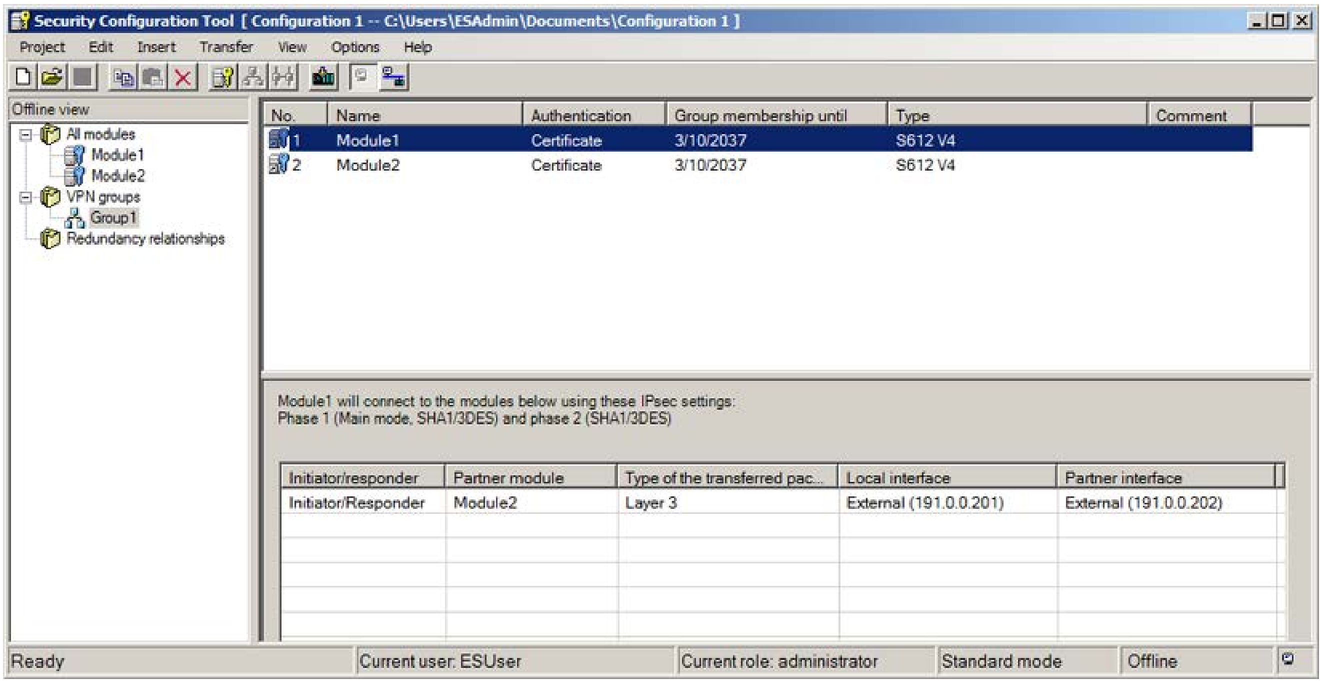
No.	Name	Type	IP address ext.	Subnet mask ext.	IP address int.	Subnet mask int
1	Module1	S612 V4	191.0.0.201	255.255.255.0	192.168.1.200	255.255.255.0
2	Module2	S612 V4	191.0.0.202	255.255.255.0	192.168.2.200	255.255.255.0

Interface	IP address	Subnet mask
External (X1)	191.0.0.201	255.255.255.0
Internal (X2)	192.168.1.200	255.255.255.0

Configuring the VPN group

Two security modules can establish an IPSec tunnel for secure communication when they are assigned to the same group in the project. To configure a tunnel connection, follow these steps:

1. In the Security Configuration Tool, select the entry "VPN groups" and select the "Insert > Group" command in the shortcut menu.
   A VPN group is created. The VPN group automatically receives the name "Group1".



No.	Name	Authentication	Group membership until	Type	Comment
1	Module1	Certificate	3/10/2037	S612 V4	
2	Module2	Certificate	3/10/2037	S612 V4	

Module1 will connect to the modules below using these IPsec settings:
Phase 1 (Main mode, SHA1/3DES) and phase 2 (SHA1/3DES)

Initiator/responder	Partner module	Type of the transferred pac...	Local interface	Partner interface
Initiator/Responder	Module2	Layer 3	External (191.0.0.201)	External (191.0.0.202)

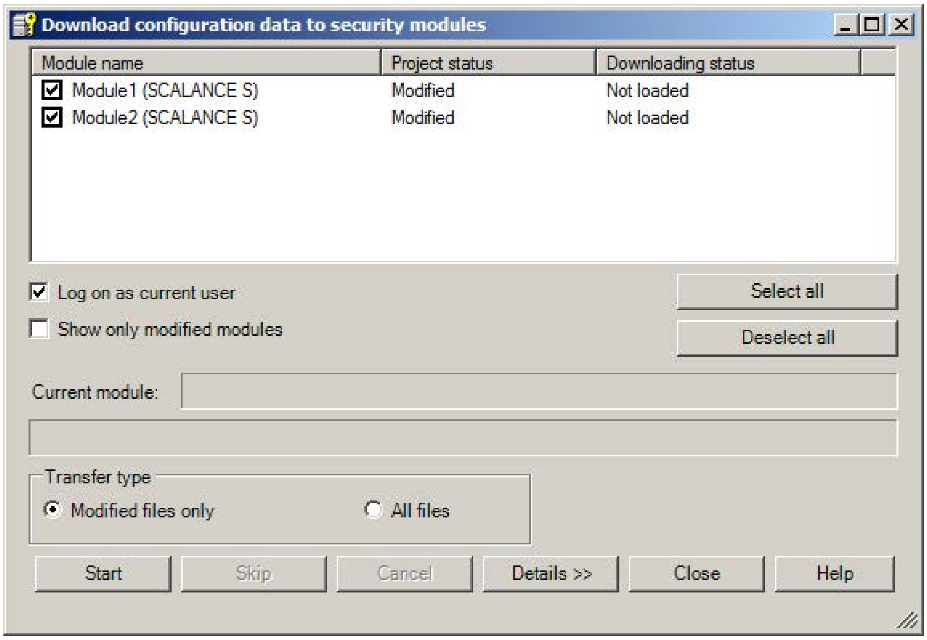
Ready | Current user: ESUser | Current role: administrator | Standard mode | Offline

2. Select the entry "All modules" in the navigation window.
3. Select the first security module in the content area and drag it to the VPN group "Group1" in the navigation window.
   The security module is assigned to this VPN group. The color of the key icon changes from gray to blue.
4. Select the second security module in the content area and drag it to the VPN group "Group1" in the navigation window.
   The second security module is also assigned to this VPN group.
5. Save the project with "Project > Save".
   This concludes the configuration of the tunnel connection.

Downloading configuration to the SCALANCE S modules

To download the created configuration to the SCALANCE S modules, follow these steps:

1. Select the command "Transfer > To all modules…".
   The "Download configuration data to security modules" dialog opens.



Download configuration data to security modules

Module name	Project status	Downloading status
☑ Module1 (SCALANCE S)	Modified	Not loaded
☑ Module2 (SCALANCE S)	Modified	Not loaded

☑ Log on as current user

□ Show only modified modules

Current module:

Transfer type: ● Modified files only ○ All files

2. Select the command "To all modules ..." in the "Transfer" menu.
3. Select both security module with "Select all".
4. Start the download process with "Start".
   If the download process takes place without any errors, the security modules are restarted automatically and the new configuration is activated.

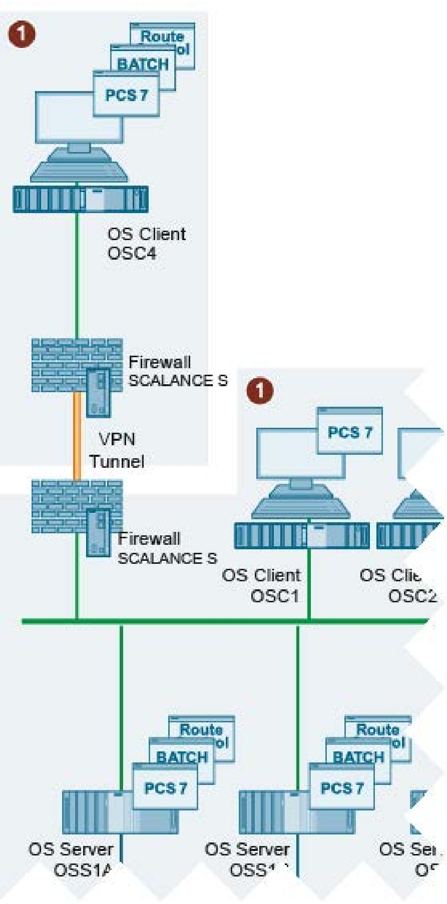
Note

You can find more information about configurations and possible uses of SIMATIC security products in theFAQ (https://support.industry.siemens.com/cs/ww/en/view/67329379) or in the Siemens Industry Online Support Portal (https://support.industry.siemens.com/cs).

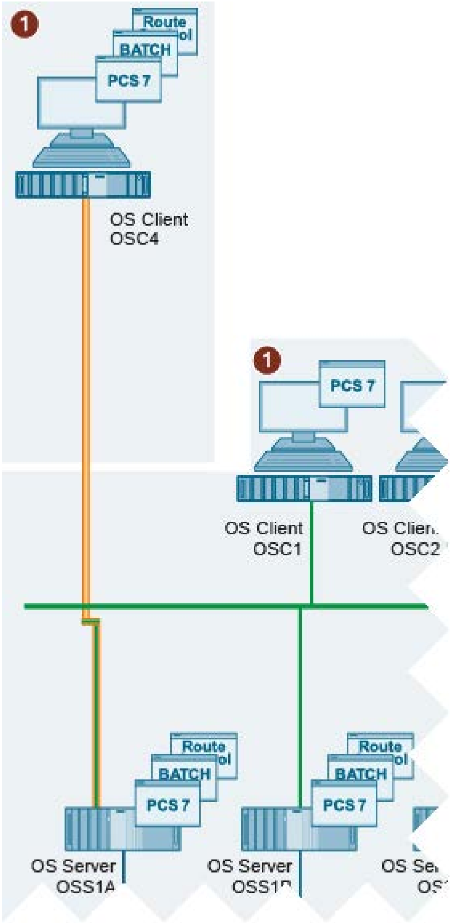
5.6.2 Data exchange for operating and monitoring with remote OS clients

The data exchange between PCS 7 OS stations (PCS 7 OS servers and PCS 7 OS client(s)) located in different security cells (possibly spatially separated, i.e. in different buildings) should be encrypted. Such encrypted communications can, on the one hand, be established by means of two SCALANCE S 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.

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 S 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 variant 1, the end point is always the SCALANCE S security module. With variant 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 variant, the entire communication is encrypted by the encrypted tunnel that exists between the SCALANCE S security modules. In variant 2, only the 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 connections for which an identical common Pre Shared Key (PSK) has been specified will be established between computers. Only these systems can communicate with one another. The Windows "Security Support Provider Interface" (SSPI) is used for communication. This interface allows authenticated and encrypted communication between the participating PCS 7 OS systems.

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

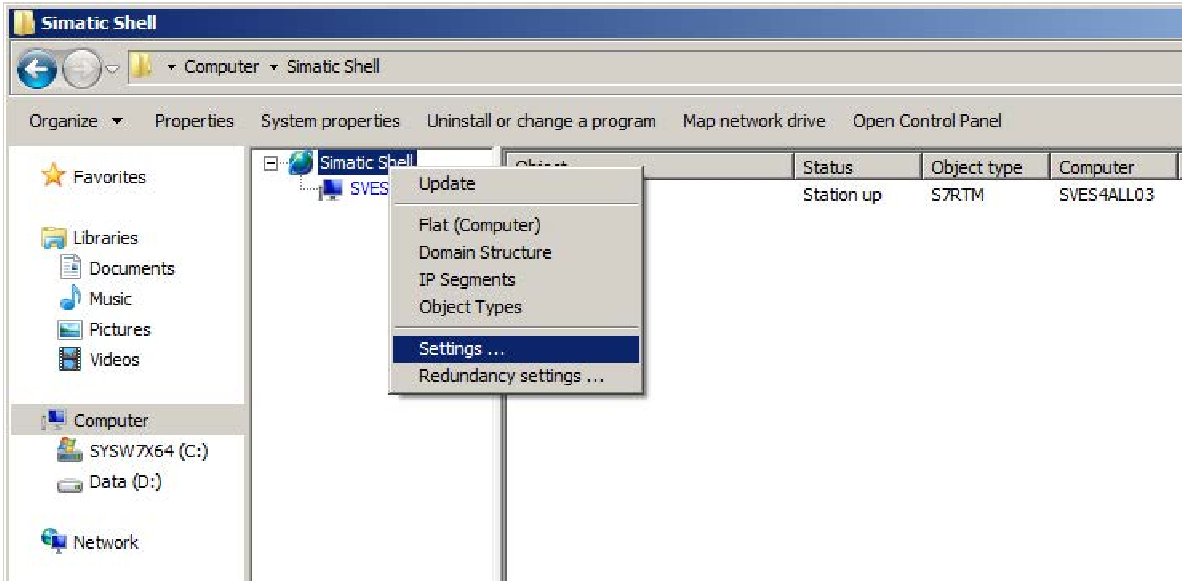
Note

Encrypted communication can be configured on the PC stations containing the SIMATIC Shell:

- Operator Station (OS server/client)
- Engineering station
- PCS 7 Web server
- PCS 7 Web client
- Open PCS 7
- SIMATIC Route Control
- SIMATIC BATCH

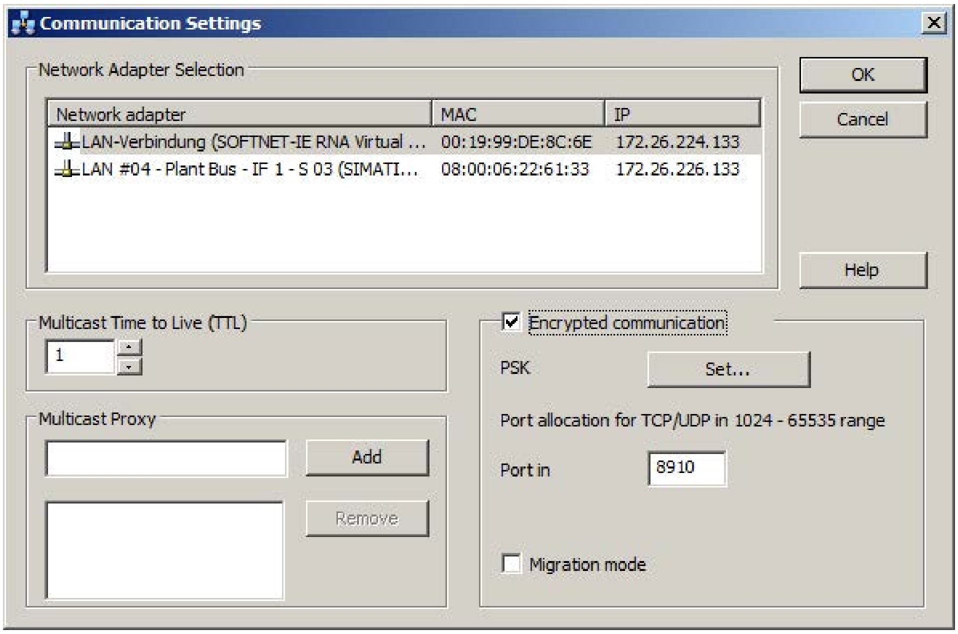
Encrypted communication is configured using the SIMATIC Shell. Proceed as follows:

1. Select the SIMATIC Shell in the Windows Explorer.
2. Open the shortcut menu and select the "Settings" command.



The "Communication Settings" dialog opens.

3. Enable the "Encrypted communication" option.


Communication Settings
Network Adapter Selection
OK
Cancel
Help
Multicast Time to Live (TTL)
Multicast Proxy
Add
Remove
PSK
Set...
Port allocation for TCP/UDP in 1024 - 65535 range

Network adapter	MAC	IP
LAN-Verbindung (SOFTNET-IE RNA Virtual ...	00:19:99:DE:8C:6E	172.26.224.133
LAN #04 - Plant Bus - IF 1 - S 03 (SIMATI...	08:00:06:22:61:33	172.26.226.133

Multicast Time to Live (TTL): 1

☑ Encrypted communication

Port in: 8910

□ Migration mode

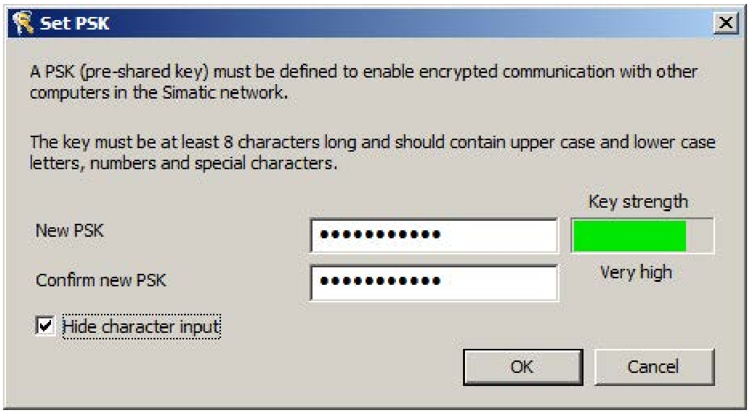
The "Set PSK" dialog box opens.

4. Specify a PSK and click "OK".
   The PSK must be at least 8 characters long and include uppercase/lowercase letters as well as numbers and special characters. The key strength is displayed next to the text box.

   The PSK must be identical on all PCS 7 systems involved because PCS 7 communication between these systems is not possible otherwise.

   Note

   If one computer in the system is compromised, the PSK must be changed on all other computers.



Set PSK

A PSK (pre-shared key) must be defined to enable encrypted communication with other computers in the Simatic network.

The key must be at least 8 characters long and should contain upper case and lower case letters, numbers and special characters.

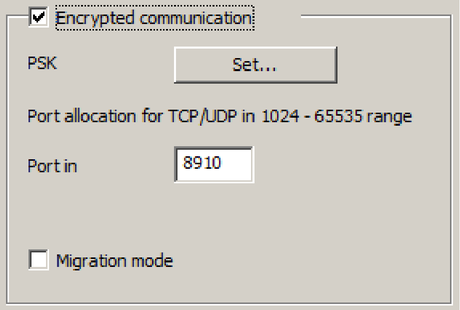
New PSK: ●●●●●●●●●●●●

Confirm new PSK: ●●●●●●●●●●●●

Key strength: 🟩 Very high

☑ Hide character input

5. In the "Encrypted communication" area, you can set a TCP/UDP port for communication in the range of 1024 to 65535.
   If port 8910 (default value) is set, for example, then TCP port 8910 and UDP port 8910 are used exclusively for the PCS 7-specific communication on this station. The ICMP protocol will continue to be used.
   The migration mode is relevant for an upgrade scenario if the settings for encrypted communication are to be changed during operation of the plant.



☑ Encrypted communication

PSK: Set...

Port allocation for TCP/UDP in 1024 - 65535 range

Port in: 8910

☐ Migration mode

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" (https://support.industry.siemens.com/cs/ww/en/view/109485951) manual.

Note

Using SIMATIC NET Softnet IE-RNA in connection with WinCC Secure Communication

In PCS 7 V8.2, you must adapt the "MTU Size" when using SIMATIC NET Softnet IE-RNA and encrypted communication (WinCC Secure Communication) (see "PCS 7 Readme (https://support.industry.siemens.com/cs/ww/en/view/109478781)", 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 or engineering data) to certain computers within the automation system or from computers of the automation system to 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 96)"). 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 patches, etc.) must be used and configured more 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 V2 is used as the back-end firewall, the quarantine station (configured as FTPS server) can be published at the back-end firewall for the DCS1 and DCS2 security cells (see Web publishing of the PCS 7 Web server at the front-end firewall). For this purpose, a corresponding publishing rule for the FTPS server must be created via Destination NAT that forwards requests on the "external" network interface (in this case, DCS 1 and DCS 2) to the FTPS server in the perimeter.

The publication or configuration on the front-end firewall is carried out in the same way.

Name	Action	Traffic	From	To	Networks
Publish FTPS server	Allow Publish	FTPS server	Anywhere	IP address of quarantine station	PCN1/2, ECN

This publication of the FTPS server (quarantine station) achieves greater security compared to port forwarding only.

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

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

Name	Action	Protocols	From	To
ECN computer to perimeter Q-PC	Allow	FTPS	IP address of the computer in the office network	IP address of the Q-PC 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 Q-PC	Forward	FTPS	IP address of the computer in the office network	IP address of the Q-PC 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 … to Perimeter Q-PC	Allow	FTPS	IP address of the computer in PCNx (e.g. ES1)	IP address of the Q-PC in the Perimeter network

Note

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

)

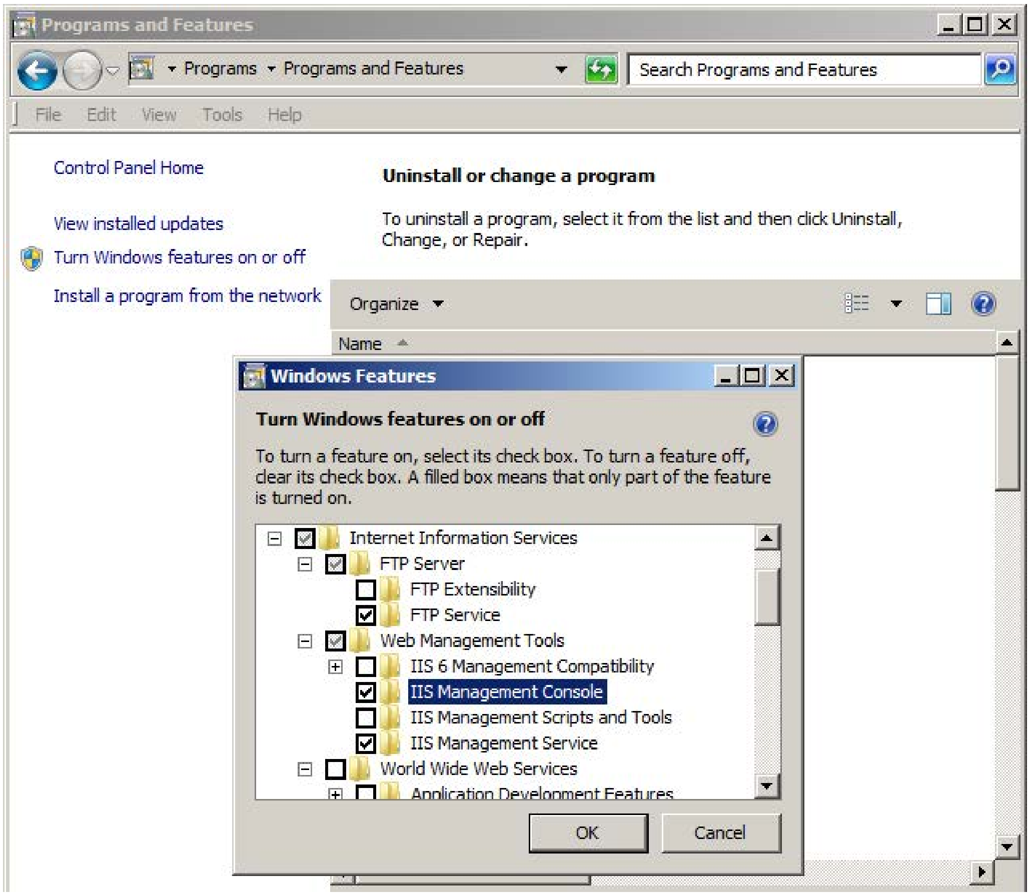
5.6.3.2 FTPS server configuration

The procedure is described using the example of a "Windows 7" operating system.

Enabling FTP Service

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

1. In the Windows Start menu, select the command "Start > Control Panel > Programs and Features".
   The "Uninstall or change a program" dialog opens.
2. Click the "Turn Windows features on or off" entry in the navigation pane.
   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 opens.
3. Enable the "FTP Service" feature in the area "Internet Information Services > FTP Server".
4. Enable the "IIS Management Console" and "IIS Admin Service" features in the "Web Management Tools" area.


Programs and Features
Programs ▸ Programs and Features
Search Programs and Features
File
Edit
View
Tools
Help
Control Panel Home
View installed updates
Turn Windows features on or off
Install a program from the network
Organize
Name
Windows Features
OK
Cancel

Uninstall or change a program

To uninstall a program, select it from the list and then click Uninstall, Change, or Repair.

Turn Windows features on or off

To turn a feature on, select its check box. To turn a feature off, clear its check box. A filled box means that only part of the feature is turned on.

- ☑ Internet Information Services
  - ☑ FTP Server
    - □ FTP Extensibility
    - ☑ FTP Service
  - ☑ Web Management Tools
    - □ IIS 6 Management Compatibility
    - ☑ IIS Management Console
    - □ IIS Management Scripts and Tools
    - ☑ IIS Management Service
  - □ World Wide Web Services
    - □ Application Development Features

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

Staring FTP Service

To launch the Microsoft FTP Service, follow these steps:

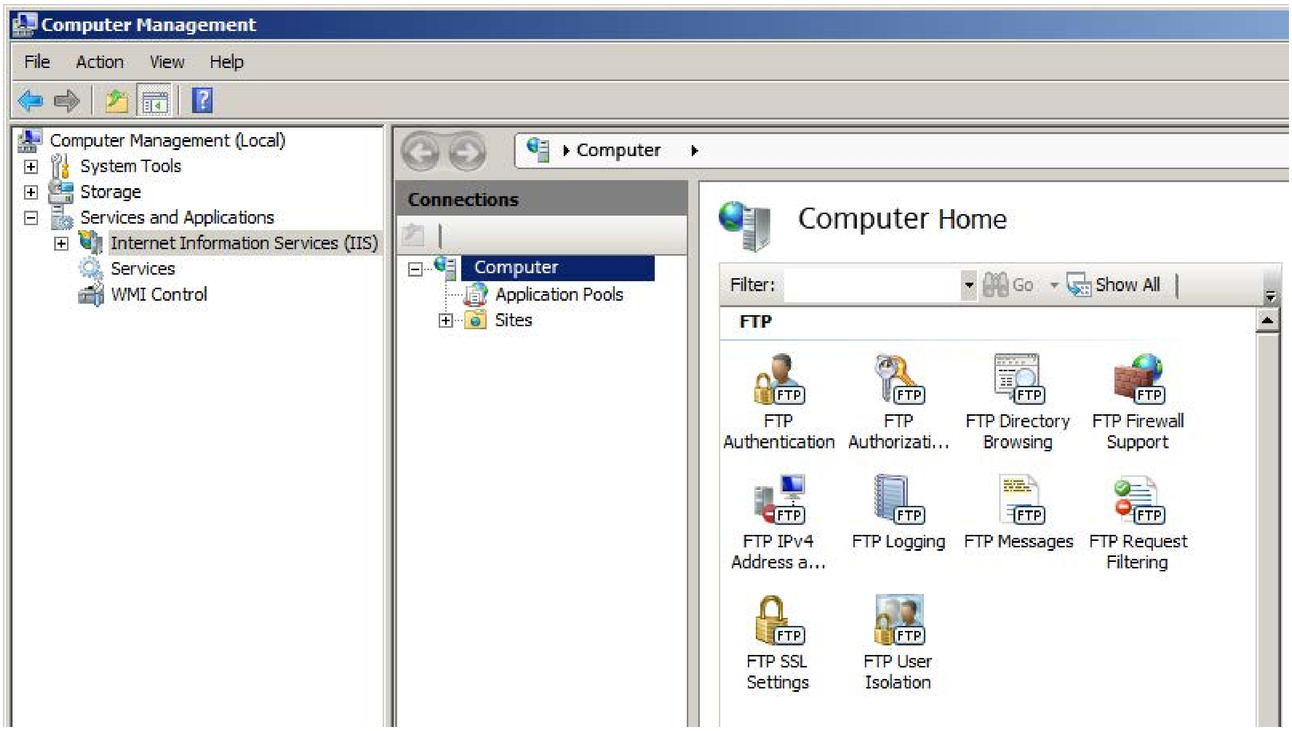
1. Right-click on "Computer" and select the shortcut menu command "Manage".
   Enter the administrator password, if required. If you are already logged on as an administrator, confirm the execution of the application. The "Computer Management" dialog opens.
2. In the navigation pane, select "Services 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: Started

   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

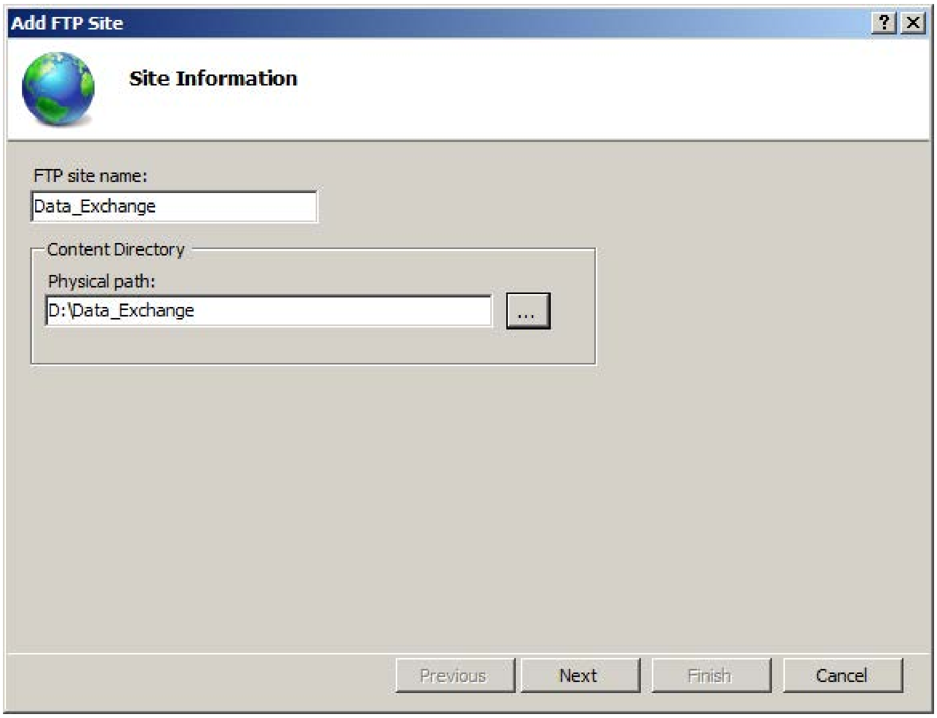
To configure the FTP server, follows these steps:

1. In the Windows Start menu, right-click on "Computer" and select the shortcut menu command "Manage".
   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).
4. Right-click on the "Sites" icon. Select the "Add FTP Site" command from the shortcut menu.
   The "Add FTP Site" dialog opens.

5. 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).



Add FTP Site

Site Information

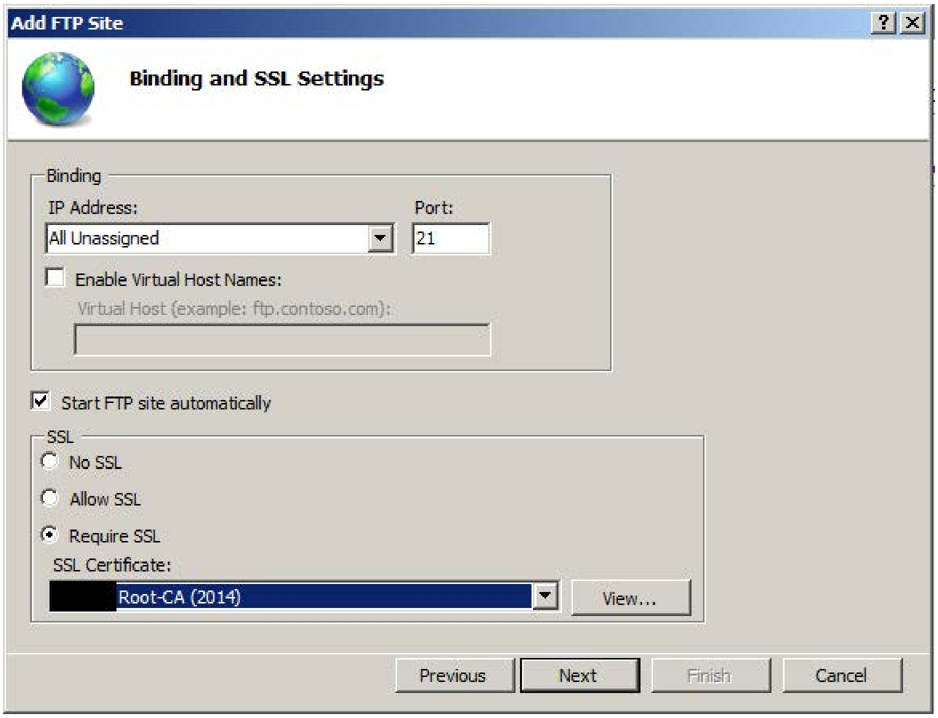
FTP site name: Data_Exchange

Content Directory

Physical path: D:\Data_Exchange

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

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.



Add FTP Site

Binding and SSL Settings

Binding

IP Address: All Unassigned

Port: 21

☐ Enable Virtual Host Names:

Virtual Host (example: ftp.contoso.com):

☑ Start FTP site automatically

SSL

○ No SSL

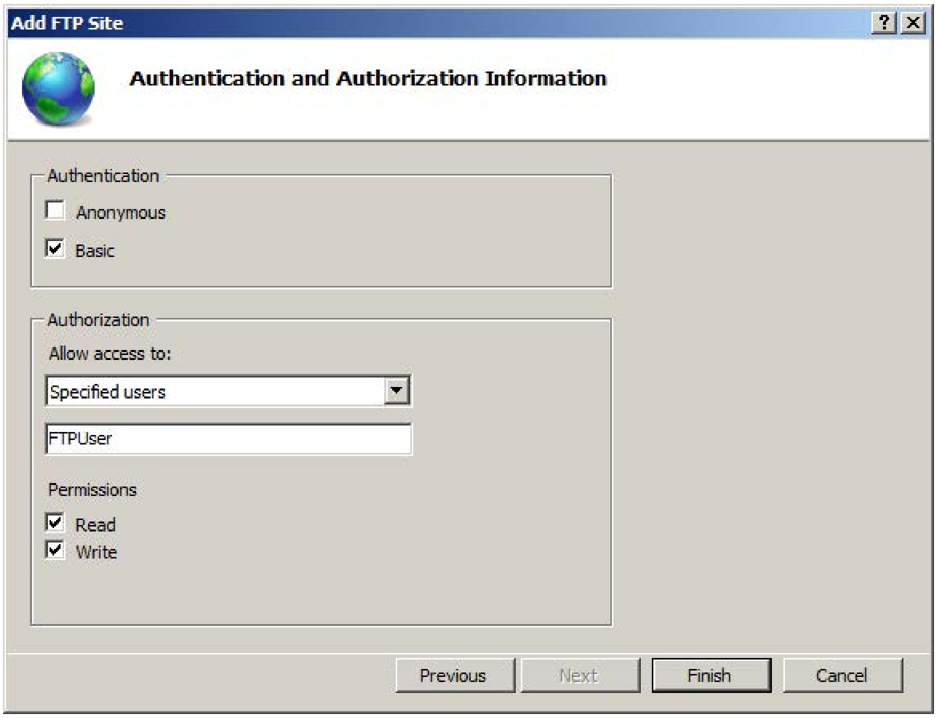
○ Allow SSL

● Require SSL

SSL Certificate: [redacted] Root-CA (2014)

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

9. Make the following settings in the "Authentication and Authorization Information" dialog:
   - "Authentication" area: Clear the "Anonymous" check box.
   - "Authorization > Access allowed for" area: Select the entry "Specific 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".



Add FTP Site

Authentication and Authorization Information

Authentication

□ Anonymous

☑ Basic

Authorization

Allow access to:

Specified users

FTPUser

Permissions

☑ Read

☑ Write

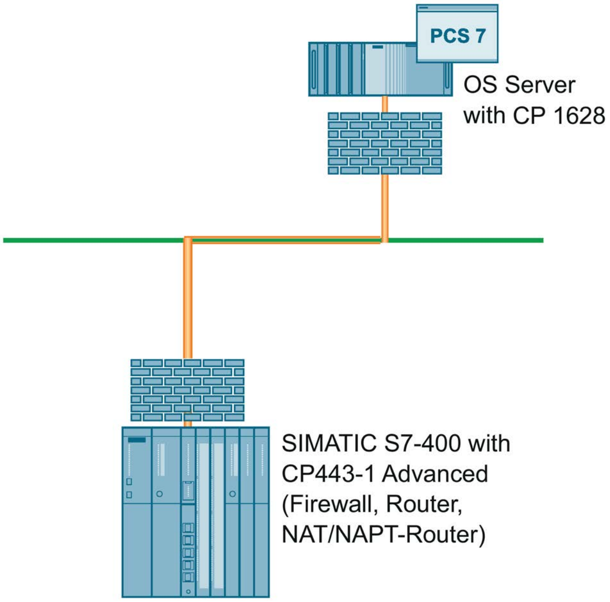
10. Click "Finish" to complete the configuration.

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 regularly supplied with the current Windows Security and critical updates. The WSUS server, which is also located in the Perimeter network, can serve as the update source. In addition, a current virus scanner must be installed on the quarantine station. The station receives current virus definitions via the virus scan server, 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 Data exchange between OS and AS stations

In addition to the scenarios in which encrypted data exchange of systems in different security cells is described, the communication between PCS 7 OS stations and the automation systems (AS) on the plant bus (PCN) can also be encrypted 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 Adv. (in the AS rack).



Note

The operation of H-connections (S7-400H high availability system) within a VPN tunnel is not supported by the CP 443-1 Advanced.

Note

You will 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/109477614)
(sections 1.2, 1.3, 1.9 and 1.10).

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 when configuring 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 in the following manuals:

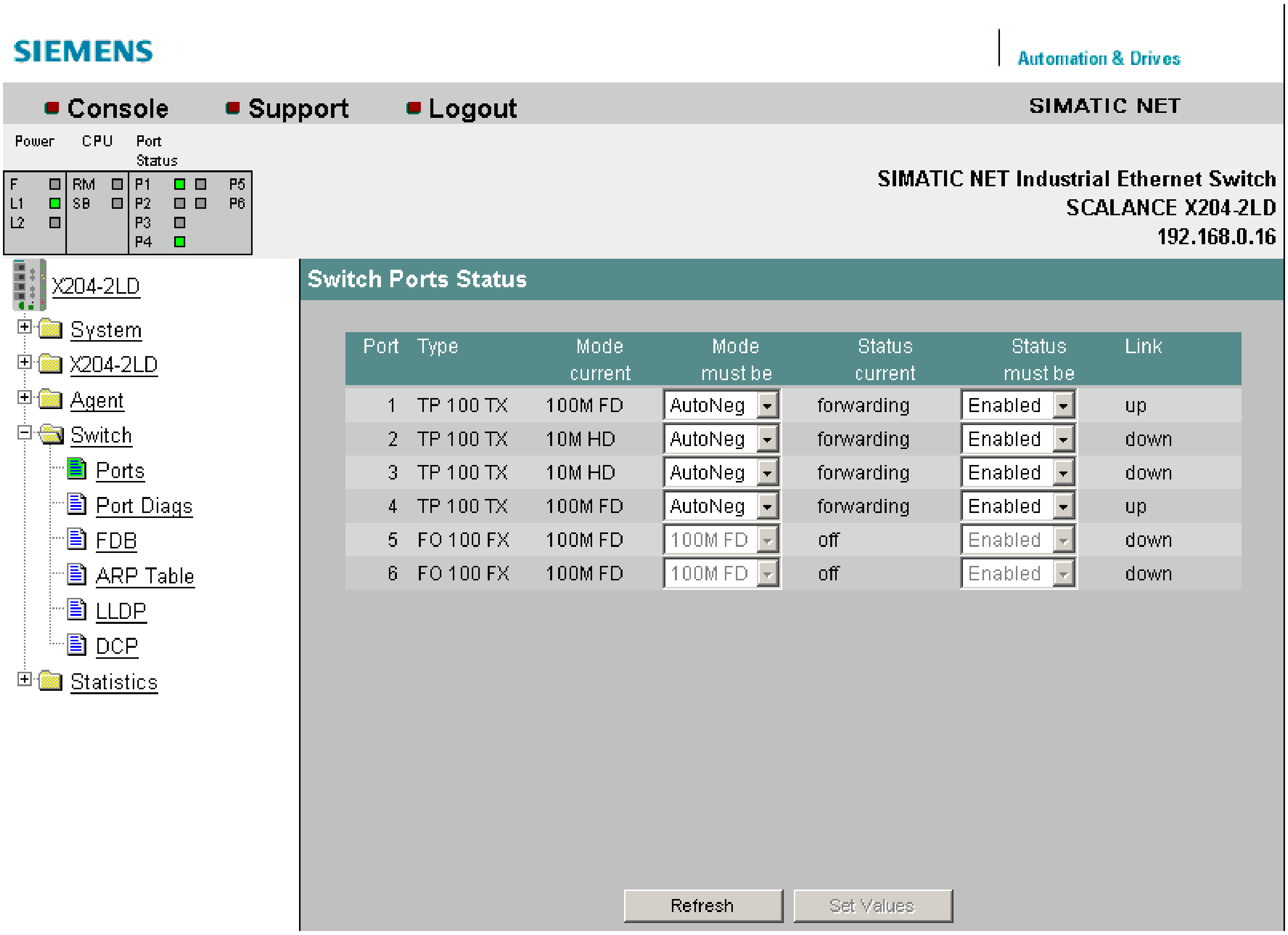
- SIMATIC NET Industrial Ethernet Switches SCALANCE X-300 / X-400 Configuration Manual (https://support.industry.siemens.com/cs/ww/en/view/109485773)
- SIMATIC NET Industrial Ethernet Switches SCALANCE X-200 Configuration Manual (https://support.industry.siemens.com/cs/ww/en/view/109482789)

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 Web (https://www.siemens.com/industrial-security).

Inquiries can also be emailed directly to "industrialsecurity.i@siemens.com".

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. To do this, open the "Switch Ports" WBM menu on SCALANCE X switches and disable the ports that are not required in this mask.



SIMATIC NET Industrial Ethernet Switch
SCALANCE X204-2LD
192.168.0.16

Switch Ports Status

Port	Type	Mode current	Mode must be	Status current	Status must be	Link
1	TP 100 TX	100M FD	AutoNeg	forwarding	Enabled	up
2	TP 100 TX	10M HD	AutoNeg	forwarding	Enabled	down
3	TP 100 TX	10M HD	AutoNeg	forwarding	Enabled	down
4	TP 100 TX	100M FD	AutoNeg	forwarding	Enabled	up
5	FO 100 FX	100M FD	100M FD	off	Enabled	down
6	FO 100 FX	100M FD	100M FD	off	Enabled	down

This dialog provides information about the current status of the port. In addition, various port settings can be performed:

- Port: Shows the port number.
- Type: Shows the type of port.
- Mode: Shows the transmission rate (10 or 100 Mbps) and the transfer procedure (full-duplex or half-duplex).
- Negotiation: Indicates whether autonegotiation is enabled (preferred setting) or disabled.
- Status: Indicates the current status of the port.
- Link: Indicates the connection status to the network.

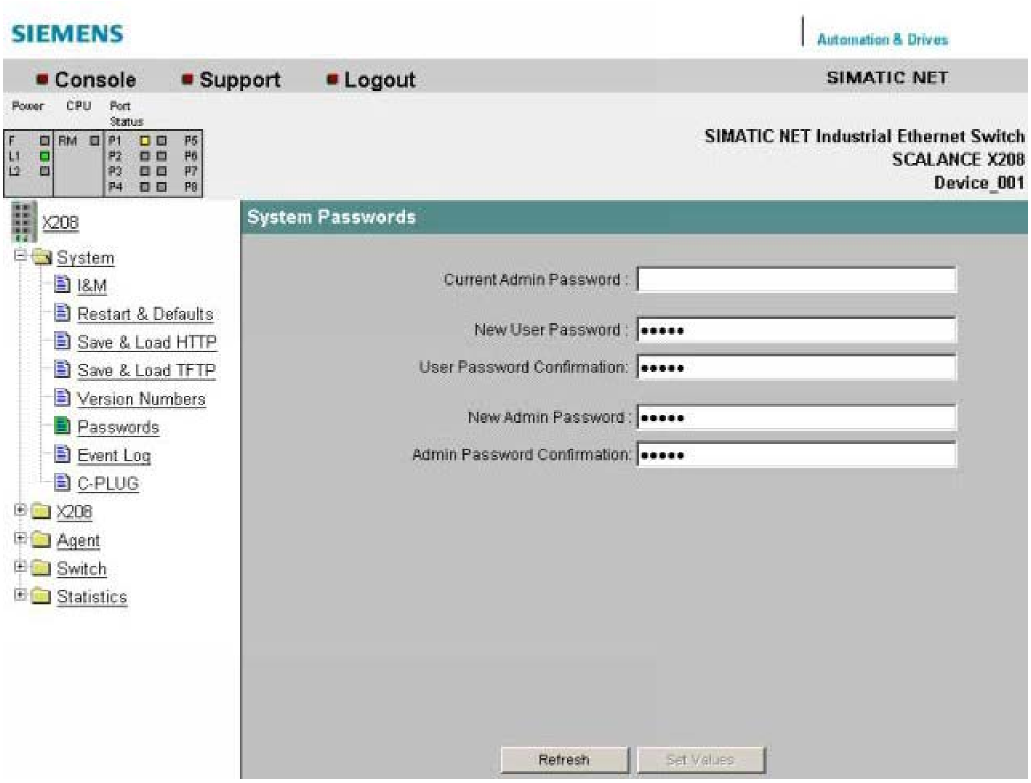
If a port is not used, the status of this port should be set to "Disabled".

5.7.2 System password for the switch configuration

Change the passwords for the "Admin" and "User" in the "System Passwords" WBM menu on SCALANCE X switches. The following passwords are preset in the factory state:

- "User" user: user
- "Admin" user: admin

You need to log on as the administrator to change the passwords. Click the "Set Value" button to confirm your changes.



Current Admin Password :
New User Password : •••••
User Password Confirmation: •••••
New Admin Password : •••••
Admin Password Confirmation: •••••

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.

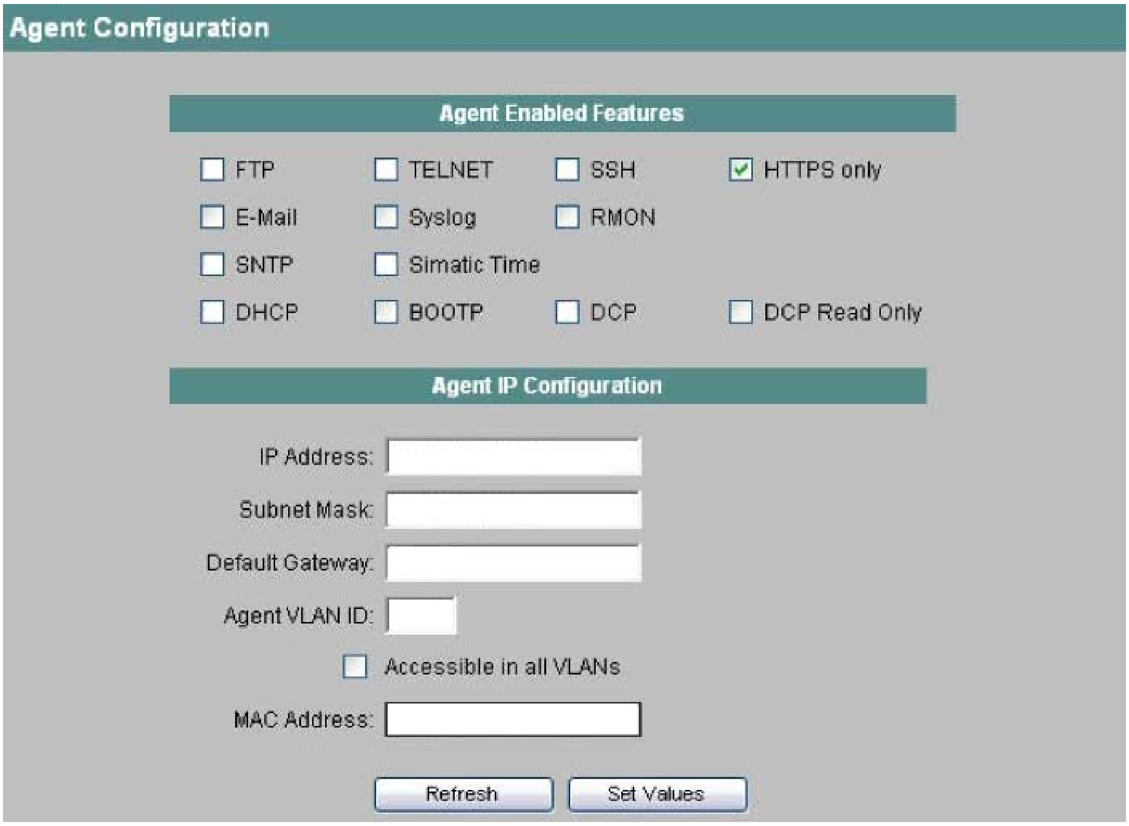
Note

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.

Use of static IP addresses

Note that a static IP address is used with a subnet mask for this setting. For more on this, see section "Managing networks and network services" (Page 34), subsection "DHCP (Dynamic Host Configuration Protocol)".



Agent Configuration

Agent Enabled Features

□ FTP	□ TELNET	□ SSH	☑ HTTPS only
□ E-Mail	□ Syslog	□ RMON	
□ SNTP	□ Simatic Time		
□ DHCP	□ BOOTP	□ DCP	□ DCP Read Only

Agent IP Configuration

IP Address:

Subnet Mask:

Default Gateway:

Agent VLAN ID:

□ Accessible in all VLANs

MAC Address:

System hardening 6

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:

- PCS 7 Readme (https://support.industry.siemens.com/cs/ww/en/view/109478781)
- Manual "SIMATIC Process Control System PCS 7 PC Configuration" (https://support.industry.siemens.com/cs/ww/en/view/109485951)

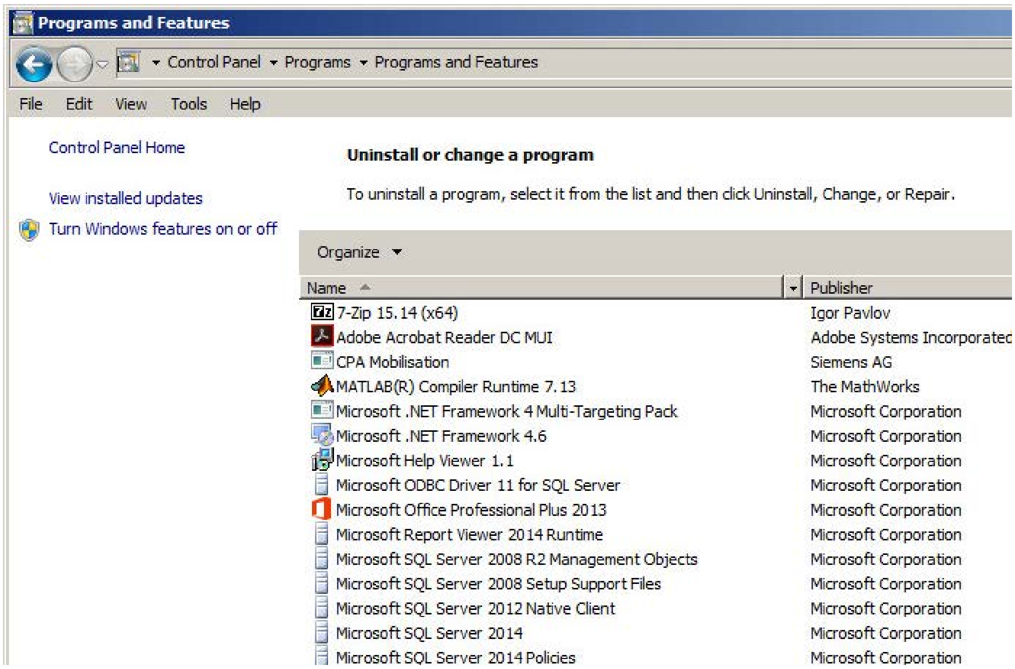
For a SIMATIC PCS 7 computer that fulfills a specific function in an automation system (OS server, OS client, engineering station), certain programs that were installed during installation of the operating system are not required for operation. These programs should be removed. In most cases, this involves "Windows components", such as Games, Calculator, Notepad, WordPad, Paint, etc.

6.2.1 Removing Windows components

The following procedure is described using the example of the "Windows 7" operating system.

To remove unneeded Windows components, follow these steps:

1. In the Windows Start menu, select the command "Start > Control Panel > Programs and Features".
   The "Uninstall or change a program" dialog opens.

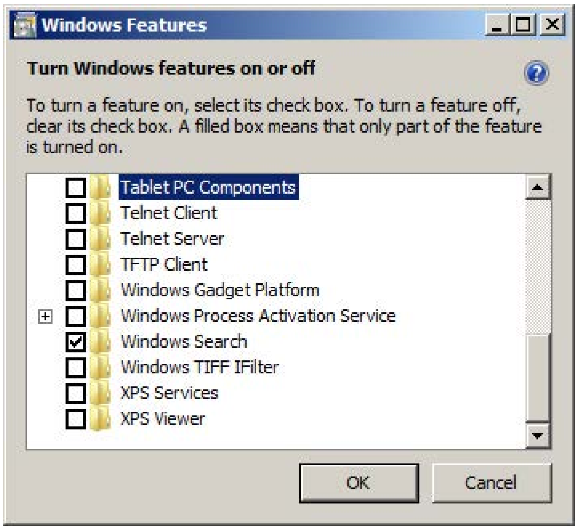

Programs and Features
Control Panel ▸ Programs ▸ Programs and Features
File Edit View Tools Help
Control Panel Home
View installed updates
Turn Windows features on or off
Organize ▾

Uninstall or change a program

To uninstall a program, select it from the list and then click Uninstall, Change, or Repair.

Name	Publisher
7-Zip 15.14 (x64)	Igor Pavlov
Adobe Acrobat Reader DC MUI	Adobe Systems Incorporated
CPA Mobilisation	Siemens AG
MATLAB(R) Compiler Runtime 7.13	The MathWorks
Microsoft .NET Framework 4 Multi-Targeting Pack	Microsoft Corporation
Microsoft .NET Framework 4.6	Microsoft Corporation
Microsoft Help Viewer 1.1	Microsoft Corporation
Microsoft ODBC Driver 11 for SQL Server	Microsoft Corporation
Microsoft Office Professional Plus 2013	Microsoft Corporation
Microsoft Report Viewer 2014 Runtime	Microsoft Corporation
Microsoft SQL Server 2008 R2 Management Objects	Microsoft Corporation
Microsoft SQL Server 2008 Setup Support Files	Microsoft Corporation
Microsoft SQL Server 2012 Native Client	Microsoft Corporation
Microsoft SQL Server 2014	Microsoft Corporation
Microsoft SQL Server 2014 Policies	Microsoft Corporation

2. Click the "Turn Windows features on or off" entry in the navigation pane.
   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 opens.



Windows Features

Turn Windows features on or off

To turn a feature on, select its check box. To turn a feature off, clear its check box. A filled box means that only part of the feature is turned on.

- ☐ Tablet PC Components
- ☐ Telnet Client
- ☐ Telnet Server
- ☐ TFTP Client
- ☐ Windows Gadget Platform
- ⊞ ☐ Windows Process Activation Service
- ☑ Windows Search
- ☐ Windows TIFF IFilter
- ☐ XPS Services
- ☐ XPS Viewer

3. Disable the unused components.
4. Confirm the changes with "OK".

6.2.2 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.

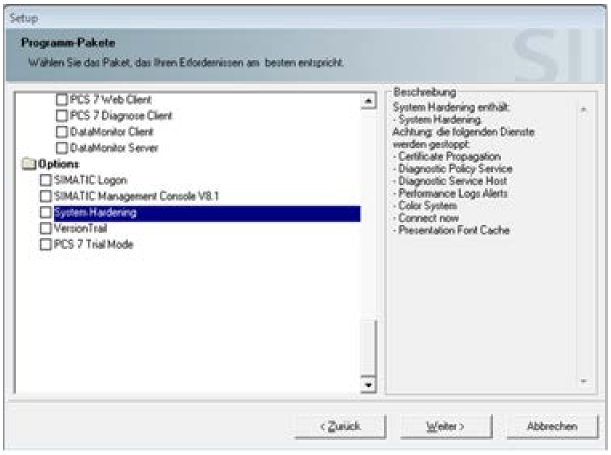
The following services can be disabled for all operating systems supported by PCS 7 V8.2:

- Certificate distribution
- Diagnostic Policy Service
- Diagnostic Service Host
- Windows Color System
- Windows Connect Now - Config Registrar
- Performance Logs and Alerts
- Windows Presentation Foundation Font Cache

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

Note

This functionality is available starting in PCS 7 V8.1 and cannot be used on older PCS 7 versions.



Setup

Programm-Pakete

Wählen Sie das Paket, das Ihren Erfordernissen am besten entspricht.

□ PCS 7 Web Client
□ PCS 7 Diagnose Client
□ DataMonitor Client
□ DataMonitor Server
Options
□ SIMATIC Logon
□ SIMATIC Management Console V8.1
□ System Hardening
□ VersionTrail
□ PCS 7 Trial Mode

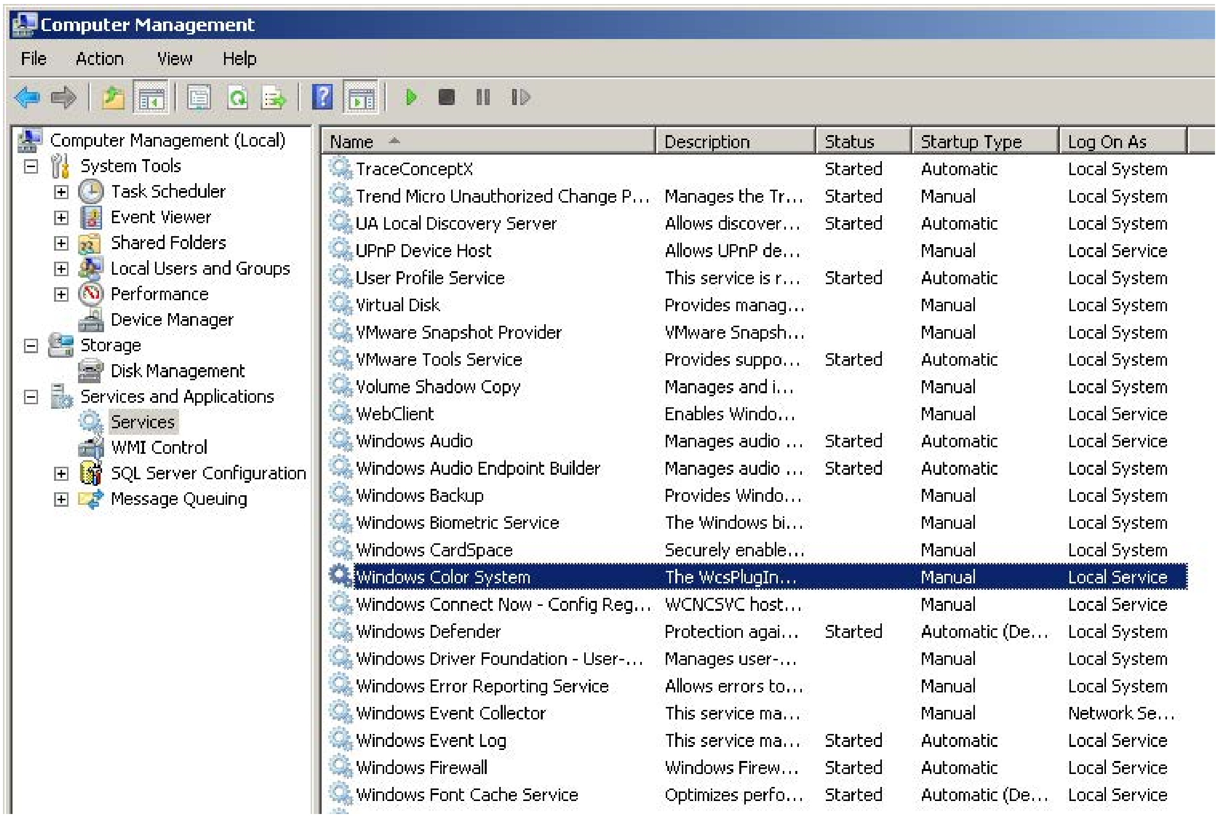
Beschreibung

System Hardening enthält:
- System Hardening
Achtung: die folgenden Dienste werden gestoppt:
- Certificate Propagation
- Diagnostic Policy Service
- Diagnostic Service Host
- Performance Logs Alerts
- Color System
- Connect now
- Presentation Font Cache

Procedure

To disable the above-mentioned services manually, follow these steps:

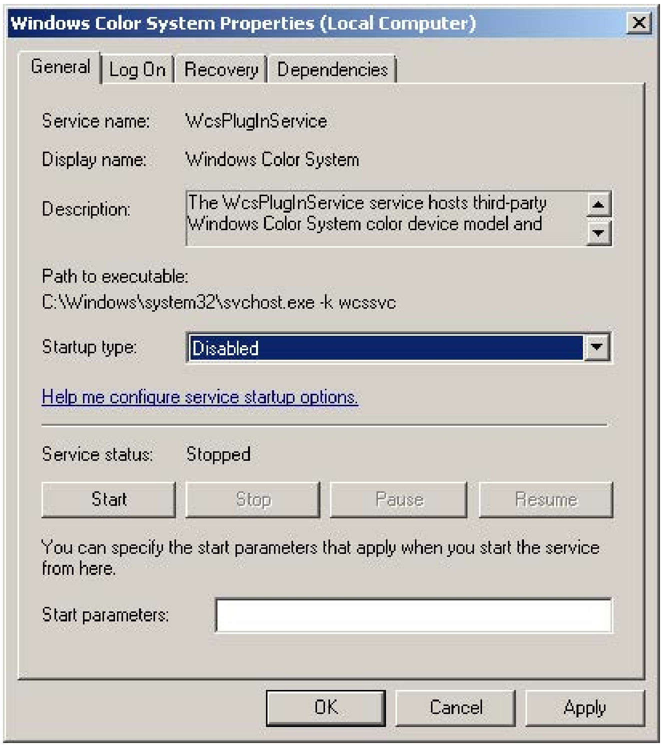
1. In the Windows Start menu, right-click on "Computer" and select the shortcut menu command "Manage".
   Enter the administrator password, if required. If you are already logged on as an administrator, confirm the execution of the application.
   The "Computer Management" dialog opens.
2. In the navigation 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 how the service is started, "Manual", "Automatic", "Automatic (Delayed Start)" or "Disabled" (service cannot be started).



Name	Description	Status	Startup Type	Log On As
TraceConceptX		Started	Automatic	Local System
Trend Micro Unauthorized Change P...	Manages the Tr...	Started	Manual	Local System
UA Local Discovery Server	Allows discover...	Started	Automatic	Local System
UPnP Device Host	Allows UPnP de...		Manual	Local Service
User Profile Service	This service is r...	Started	Automatic	Local System
Virtual Disk	Provides manag...		Manual	Local System
VMware Snapshot Provider	VMware Snapsh...		Manual	Local System
VMware Tools Service	Provides suppo...	Started	Automatic	Local System
Volume Shadow Copy	Manages and i...		Manual	Local System
WebClient	Enables Windo...		Manual	Local Service
Windows Audio	Manages audio ...	Started	Automatic	Local Service
Windows Audio Endpoint Builder	Manages audio ...	Started	Automatic	Local System
Windows Backup	Provides Windo...		Manual	Local System
Windows Biometric Service	The Windows bi...		Manual	Local System
Windows CardSpace	Securely enable...		Manual	Local System
Windows Color System	The WcsPlugIn...		Manual	Local Service
Windows Connect Now - Config Reg...	WCNCSVC host...		Manual	Local Service
Windows Defender	Protection agai...	Started	Automatic (De...	Local System
Windows Driver Foundation - User-...	Manages user-...		Manual	Local System
Windows Error Reporting Service	Allows errors to...		Manual	Local System
Windows Event Collector	This service ma...		Manual	Network Se...
Windows Event Log	This service ma...	Started	Automatic	Local Service
Windows Firewall	Windows Firew...	Started	Automatic	Local Service
Windows Font Cache Service	Optimizes perfo...	Started	Automatic (De...	Local Service

3. In the right area, select the service to be disabled, and open the properties dialog of the service by double-clicking on it.

4. Click "Stop" to stop the service.
5. Select "Disabled" as the startup type and confirm your changes with "OK".



Windows Color System Properties (Local Computer)

Service name: WcsPlugInService

Display name: Windows Color System

Description: The WcsPlugInService service hosts third-party Windows Color System color device model and

Path to executable:
C:\Windows\system32\svchost.exe -k wcssvc

Startup type: Disabled

Help me configure service startup options.

Service status: Stopped

You can specify the start parameters that apply when you start the service from here.

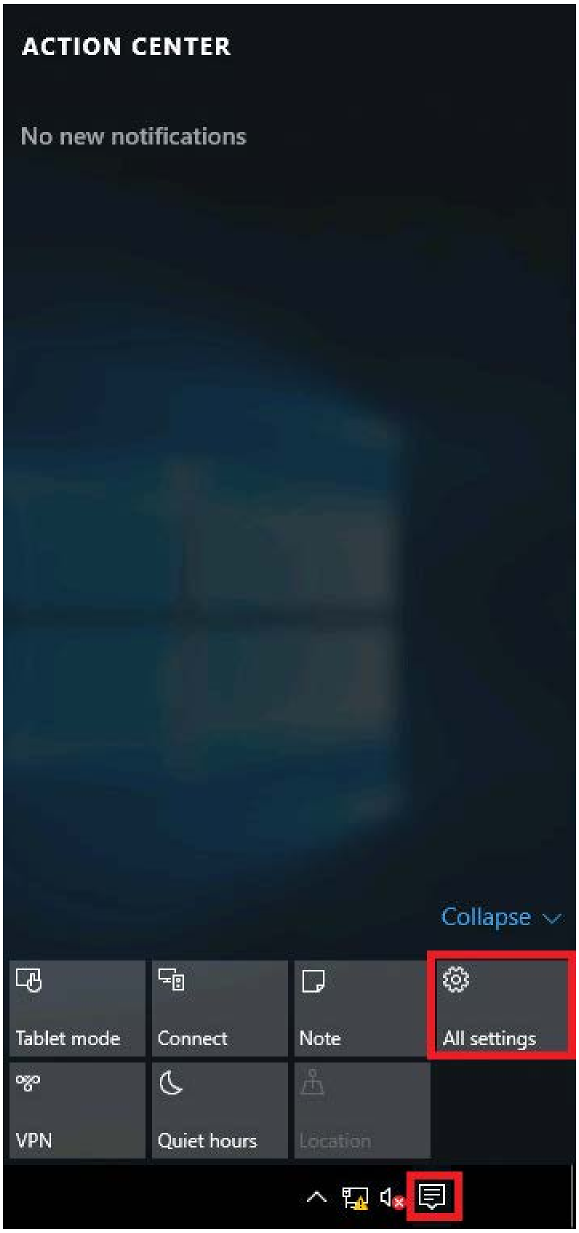
Start parameters:

6.2.3 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, follow these steps:

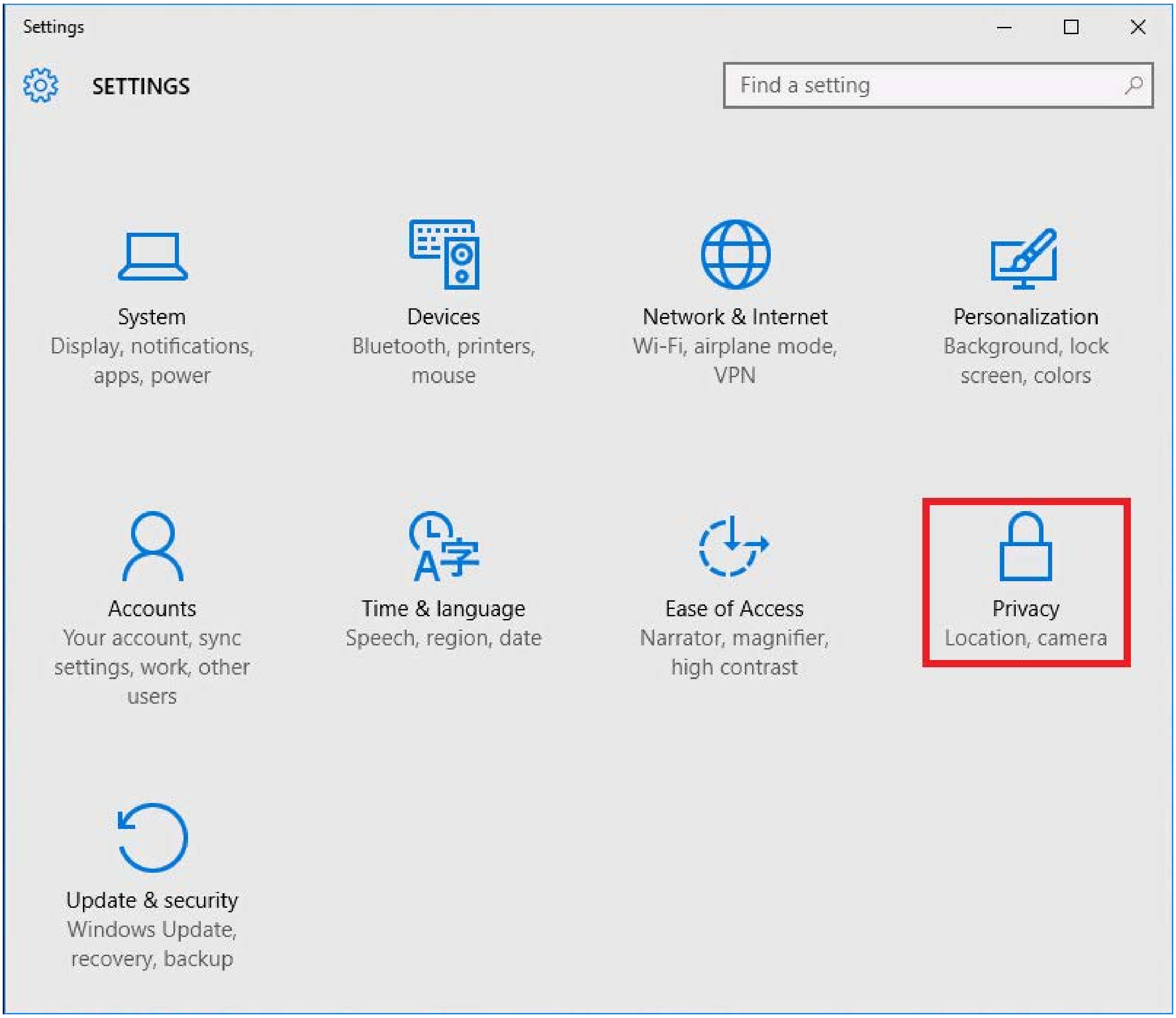
1. Select the "Notifications" icon in the Windows taskbar.
   The "ACTION CENTER" opens.
2. Select the "All settings" option.



ACTION CENTER

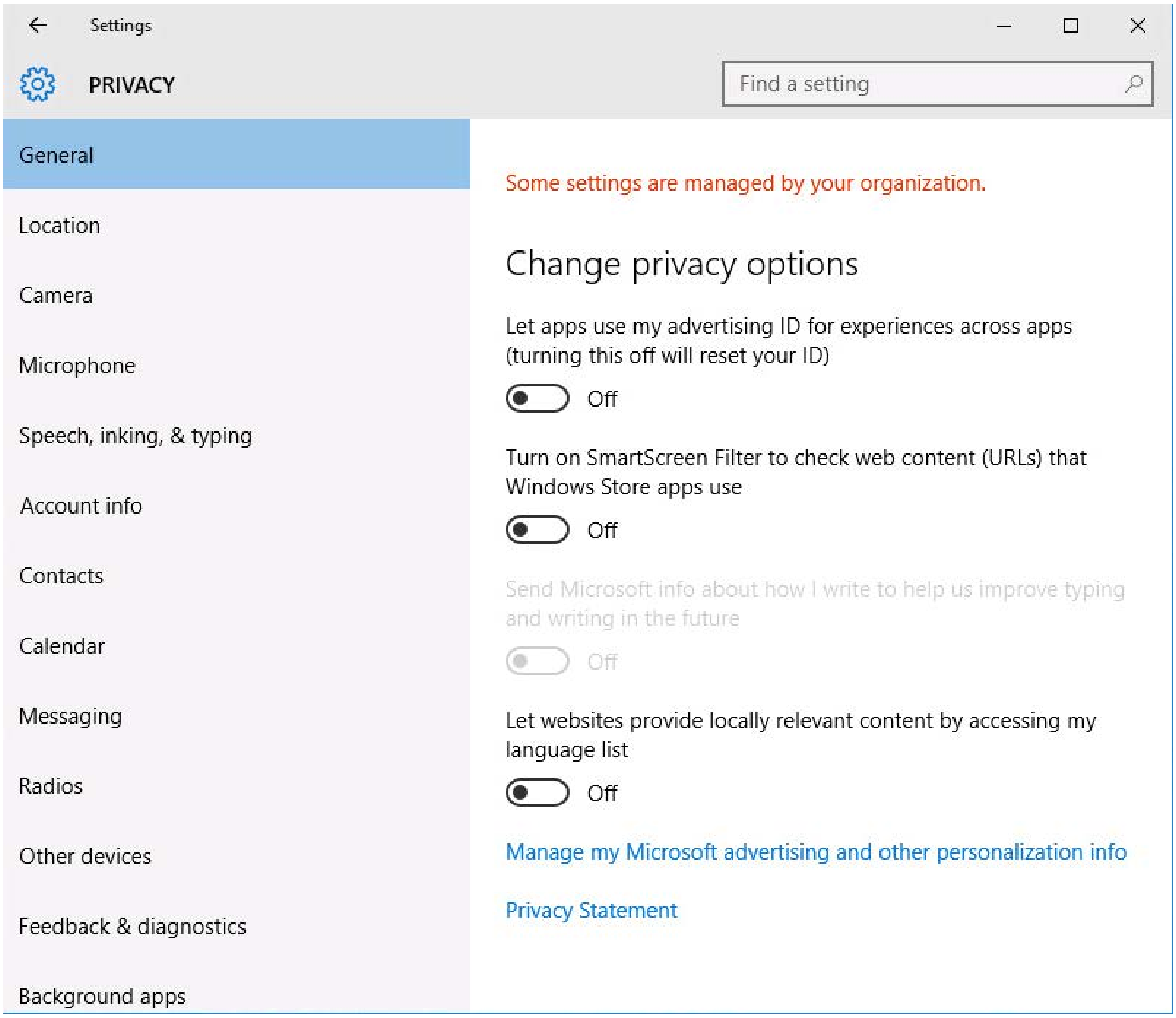
No new notifications

3. In the "Settings" navigation area, click the "Privacy – Location, Camera" entry.


Settings
SETTINGS
Find a setting
System
Display, notifications, apps, power
Devices
Bluetooth, printers, mouse
Network & Internet
Wi-Fi, airplane mode, VPN
Personalization
Background, lock screen, colors
Accounts
Your account, sync settings, work, other users
Time & language
Speech, region, date
Ease of Access
Narrator, magnifier, high contrast
Privacy
Location, camera
Update & security
Windows Update, recovery, backup

The privacy settings are displayed.

4. Go step by step through the privacy settings and disable them if this is possible.



Some settings are managed by your organization.

Change privacy options

Let apps use my advertising ID for experiences across apps (turning this off will reset your ID)

Off

Turn on SmartScreen Filter to check web content (URLs) that Windows Store apps use

Off

Send Microsoft info about how I write to help us improve typing and writing in the future

Off

Let websites provide locally relevant content by accessing my language list

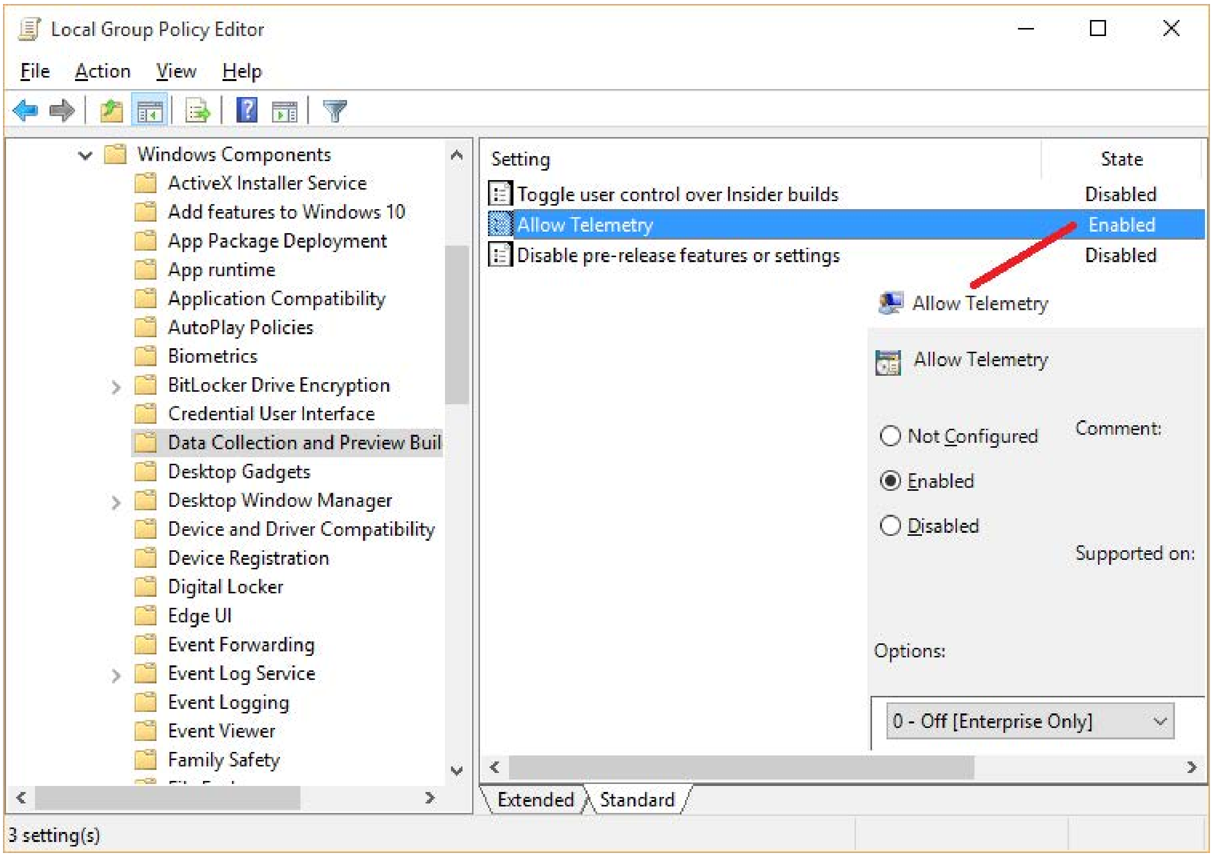
Off

Manage my Microsoft advertising and other personalization info

Privacy Statement

5. Close the "Settings" window.

Additional Windows 10 functions can be disabled 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). Data protection can be improved using the policy setting "Computer Configuration > Policies > Administrative Templates > Windows Components > Data Collection and Preview Builds".



Setting	State
Toggle user control over Insider builds	Disabled
Allow Telemetry	Enabled
Disable pre-release features or settings	Disabled

Allow Telemetry

Allow Telemetry

○ Not Configured
● Enabled
○ Disabled

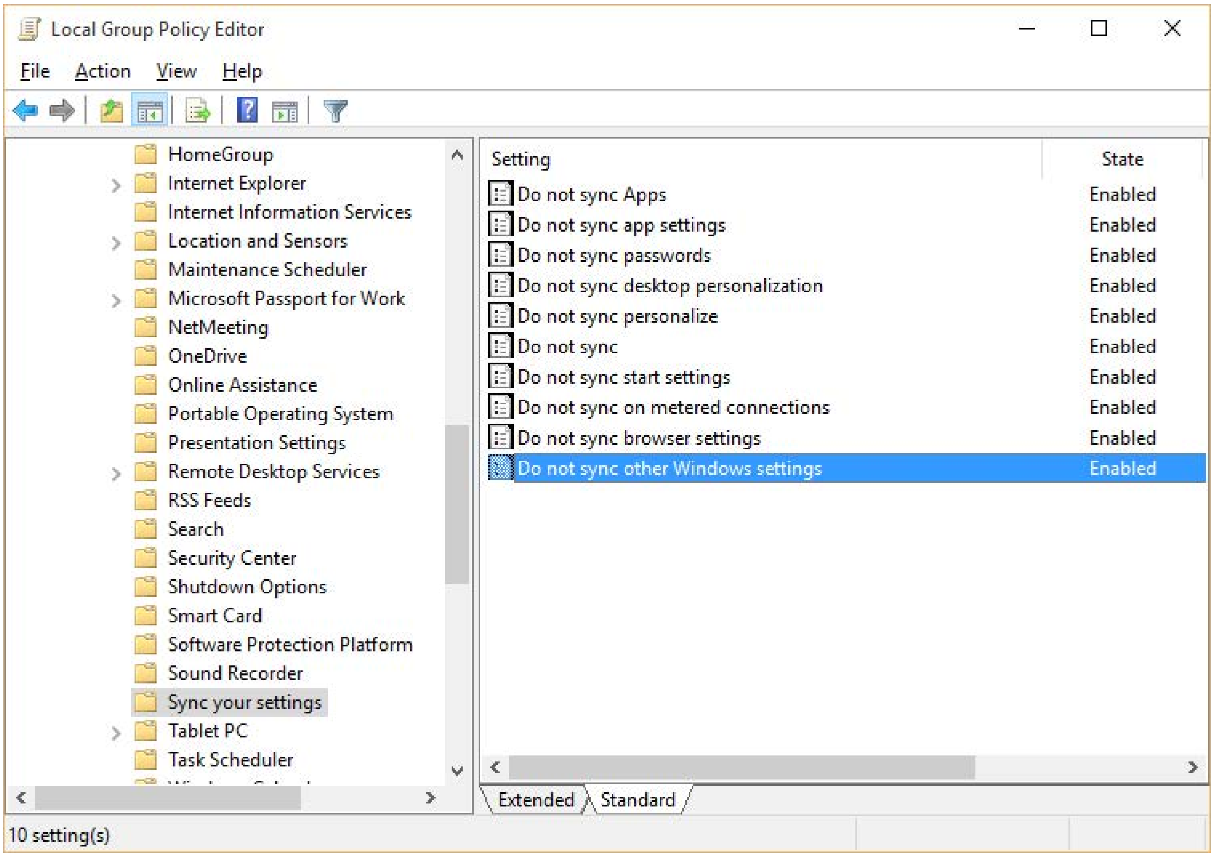
Comment:

Supported on:

Options:

0 - Off [Enterprise Only]

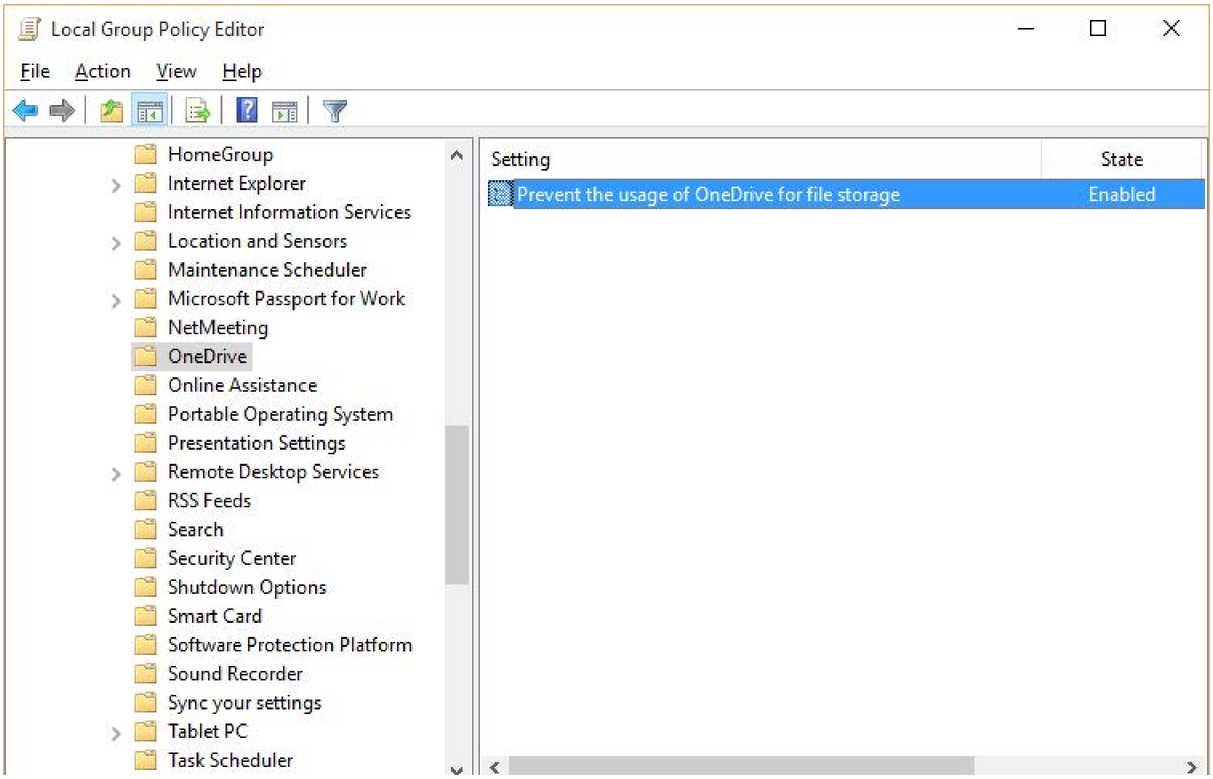
A group policy can be used to prevent users from synchronizing the settings of their computers with other computers. The corresponding policy setting can be found under "Computer Configuration > Policies > Administrative Templates > Windows Components > Synchronize Setting".



Setting	State
Do not sync Apps	Enabled
Do not sync app settings	Enabled
Do not sync passwords	Enabled
Do not sync desktop personalization	Enabled
Do not sync personalize	Enabled
Do not sync	Enabled
Do not sync start settings	Enabled
Do not sync on metered connections	Enabled
Do not sync browser settings	Enabled
Do not sync other Windows settings	Enabled

10 setting(s)

The policy setting "Computer Configuration > Policies > Administrative Templates > Windows Components > OneDrive" can be used to prevent the use of the OneDrive cloud memory.



Setting	State
Prevent the usage of OneDrive for file storage	Enabled

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://support.microsoft.com/en-us/help/12456/windows-10-privacy).

Note

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

- PCS 7 Readme (https://support.industry.siemens.com/cs/ww/en/view/109478781)
- Manual "SIMATIC Process Control System PCS 7 PC Configuration" (https://support.industry.siemens.com/cs/ww/en/view/109485951)

6.2.4 Additional hardening measures to be configured manually

Restriction of encryption and hash techniques

For Windows to only use current encryption and hash techniques, the older techniques must be disabled in the Windows Registry. These include all SSL versions and TLS versions before Version 1.2.
You can find information on disabling these techniques on the Microsoft website (https://technet.microsoft.com/en-us/en-en/library/dn786418(v=ws.11).aspx#BKMK_SchannelTR_TLS11) under "Schannel SSP registry entries" (SSL 2.0, SSL 3.0, TLS 1.0, TLS 1.1 and Hashes).

Note

If a HW RAID controller from Adaptec is used in the system, note that older cipher suites such as TLS_RSA_WITH_AES_256_CBC_SHA or TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA must be allowed for access to the Adaptec maxview Web server. These are to be activated only on computers on which access to Maxview is explicitly needed.

Additional information on the settings can be found on the following website: https://support.microsoft.com/en-en/kb/245030.

Parameter assignment of the ALM as license server

The Automation License Manager (ALM) is assigned as the license server by default. This is only needed when the computer is to be connected as a remote license computer (e.g. during commissioning of the system so that a central server on which licenses are stored is available).

If centrally managed floating licenses are not used for PCS 7 systems during operation, it is recommended that the ALM license server be disabled. PCS 7 systems (e.g. ES, OS Server, OS Client) should not be used as the license server. For this reason, the interface used on these systems can be disabled.

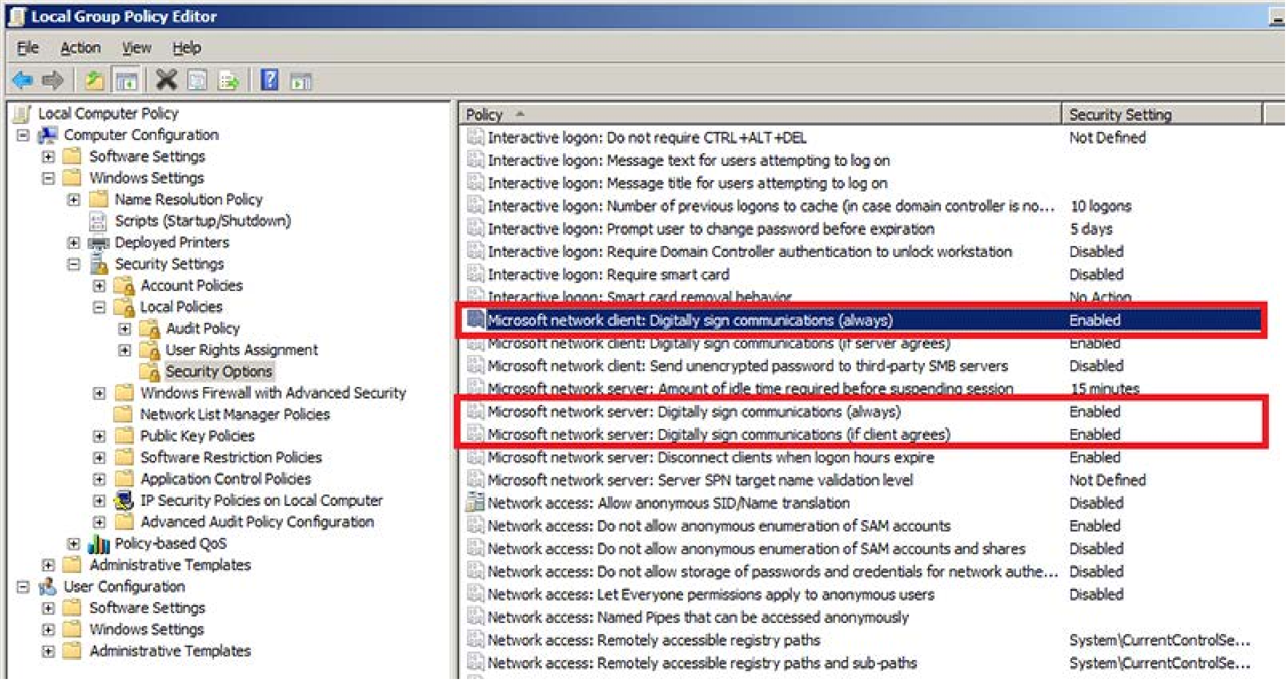
SMB signing

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.

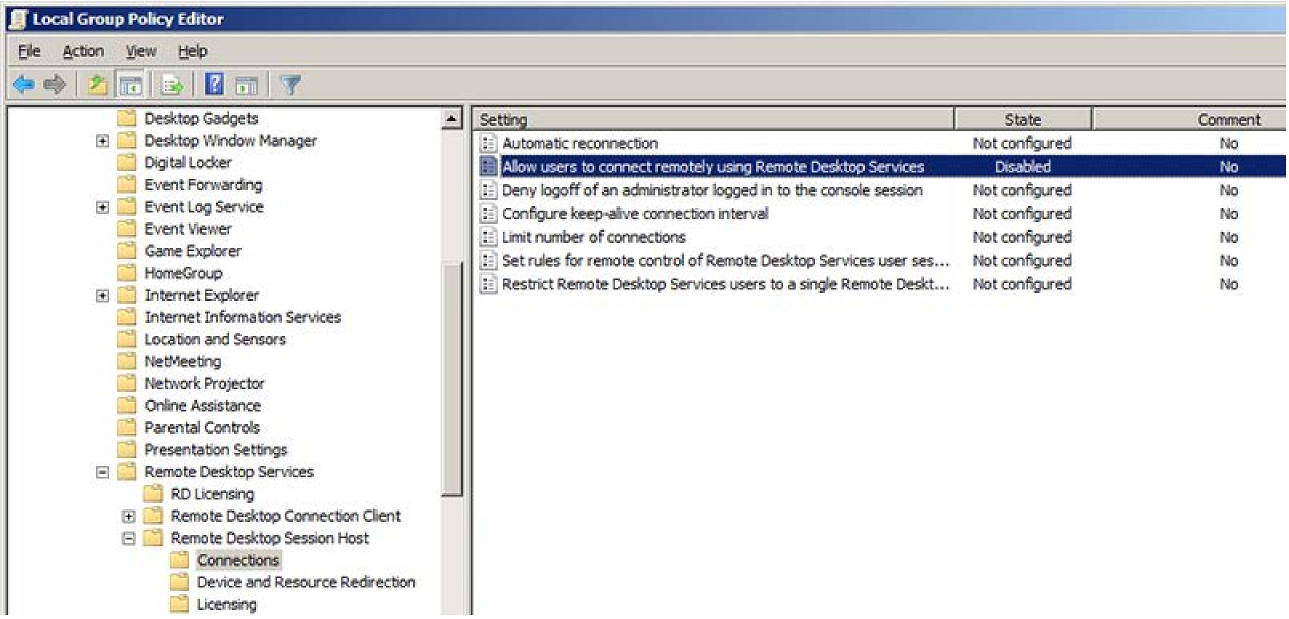


Policy	Security Setting
Interactive logon: Do not require CTRL+ALT+DEL	Not Defined
Interactive logon: Message text for users attempting to log on	
Interactive logon: Message title for users attempting to log on	
Interactive logon: Number of previous logons to cache (in case domain controller is no...	10 logons
Interactive logon: Prompt user to change password before expiration	5 days
Interactive logon: Require Domain Controller authentication to unlock workstation	Disabled
Interactive logon: Require smart card	Disabled
Interactive logon: Smart card removal behavior	No Action
Microsoft network client: Digitally sign communications (always)	Enabled
Microsoft network client: Digitally sign communications (if server agrees)	Enabled
Microsoft network client: Send unencrypted password to third-party SMB servers	Disabled
Microsoft network server: Amount of idle time required before suspending session	15 minutes
Microsoft network server: Digitally sign communications (always)	Enabled
Microsoft network server: Digitally sign communications (if client agrees)	Enabled
Microsoft network server: Disconnect clients when logon hours expire	Enabled
Microsoft network server: Server SPN target name validation level	Not Defined
Network access: Allow anonymous SID/Name translation	Disabled
Network access: Do not allow anonymous enumeration of SAM accounts	Enabled
Network access: Do not allow anonymous enumeration of SAM accounts and shares	Disabled
Network access: Do not allow storage of passwords and credentials for network authe...	Disabled
Network access: Let Everyone permissions apply to anonymous users	Disabled
Network access: Named Pipes that can be accessed anonymously	
Network access: Remotely accessible registry paths	System\CurrentControlSe...
Network access: Remotely accessible registry paths and sub-paths	System\CurrentControlSe...

Remote Desktop Security setting

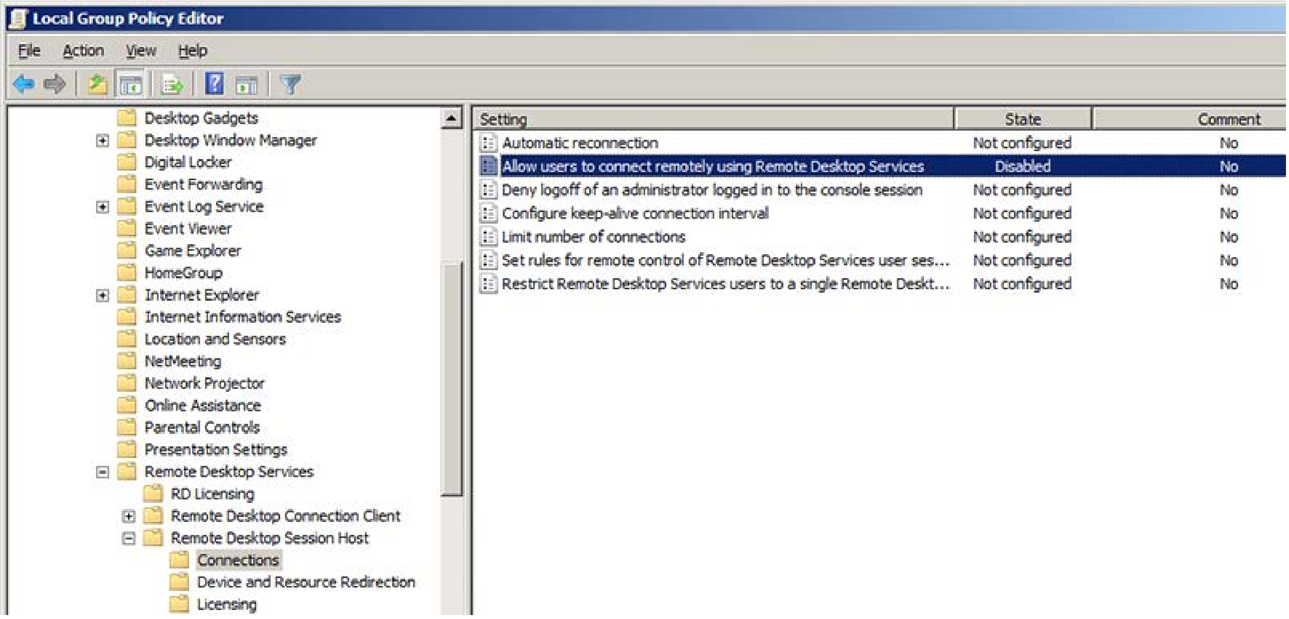
If required, e.g. when an OS client is accessed via the Remote Desktop Protocol (RDP), an additional security measure should be taken. To do so, start the Group Policy Editor for the local group policies "gpedit.exe" in an administrative command prompt (this setting can be made centrally in a domain)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



Setting	State	Comment
Automatic reconnection	Not configured	No
Allow users to connect remotely using Remote Desktop Services	Disabled	No
Deny logoff of an administrator logged in to the console session	Not configured	No
Configure keep-alive connection interval	Not configured	No
Limit number of connections	Not configured	No
Set rules for remote control of Remote Desktop Services user ses...	Not configured	No
Restrict Remote Desktop Services users to a single Remote Deskt...	Not configured	No

On all 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.



Setting	State	Comment
Automatic reconnection	Not configured	No
Allow users to connect remotely using Remote Desktop Services	Disabled	No
Deny logoff of an administrator logged in to the console session	Not configured	No
Configure keep-alive connection interval	Not configured	No
Limit number of connections	Not configured	No
Set rules for remote control of Remote Desktop Services user ses...	Not configured	No
Restrict Remote Desktop Services users to a single Remote Deskt...	Not configured	No

6.3 Security Controller

The Security Controller (available starting with PCS 7 V8.0) is a program that makes application-specific security settings on the system. The Security Controller (SC) is integrated by default in SIMATIC PCS 7 and SIMATIC WinCC.

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

The communication to non-configured devices or to other subnets, as well as the use of 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) or changing the group membership of users, be aware that the local firewall configuration or the local group memberships must be adapted and the Security Controller must be restarted.

The Security Controller makes the following settings automatically:

- Windows firewall exceptions
- DCOM settings
- Registry settings
- Group settings (User Management – SIMATIC Logon)
- File and/or directory authorizations

These settings are made depending on the installation (PCS 7 OS server, PCS 7 OS client, ES) and the following software packages:

- Automation License Manager
- File and Printer Sharing
- SIMATIC Batch
- SIMATIC Communication Services
- SIMATIC Logon
- SIMATIC Management Console
- SIMATIC NET PC Software
- SIMATIC PC Diagnosis Application
- SIMATIC PCS 7 Engineering System
- SIMATIC Route Control
- SIMATIC SFC Visualization (SFV)
- SIMATIC STEP 7 components
- SIMATIC WinCC
- SIMATIC WinCC OPC
- SIMATIC WinCC User Archive
- SQL Server (SQL Server version depends on the SIMATIC PCS 7 version)

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/109485951).

6.4 Windows Firewall

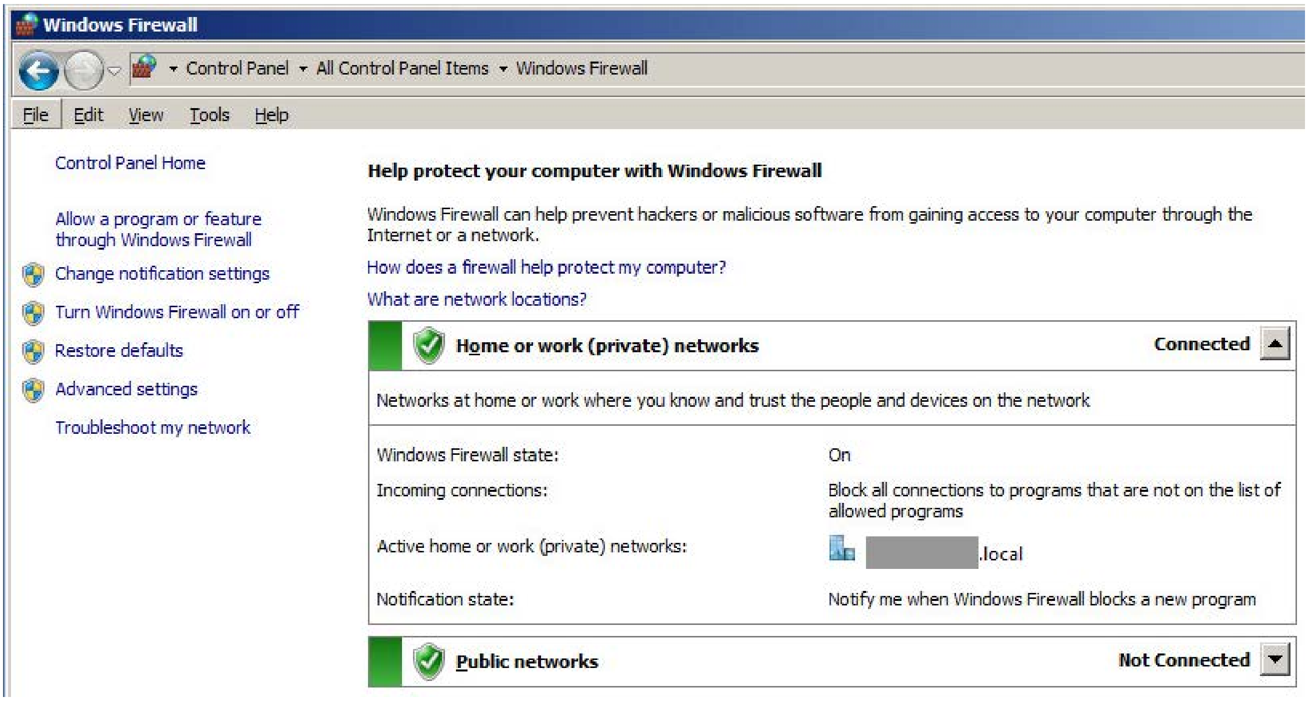
As described in the "Security Controller" (Page 86) section, the "Security Controller" program makes settings on the local Windows Firewall. With respect to the sample configuration in which communication of PCS 7 computers between various subnets must be guaranteed, additional manual adjustments to the Windows Firewall must be made after running the program.

Example configuration: Windows Firewall

The following procedure is described using the example of the "Windows 7" 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. Select the command "Start > Control Panel > System and Security > Windows Firewall": The "Windows Firewall" dialog opens.


Windows Firewall
Control Panel ▸ All Control Panel Items ▸ Windows Firewall
File
Edit
View
Tools
Help
Control Panel Home
Allow a program or feature through Windows Firewall
Change notification settings
Turn Windows Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network

Help protect your computer with Windows Firewall

Windows Firewall can help prevent hackers or malicious software from gaining access to your computer through the Internet or a network.

How does a firewall help protect my computer?

What are network locations?

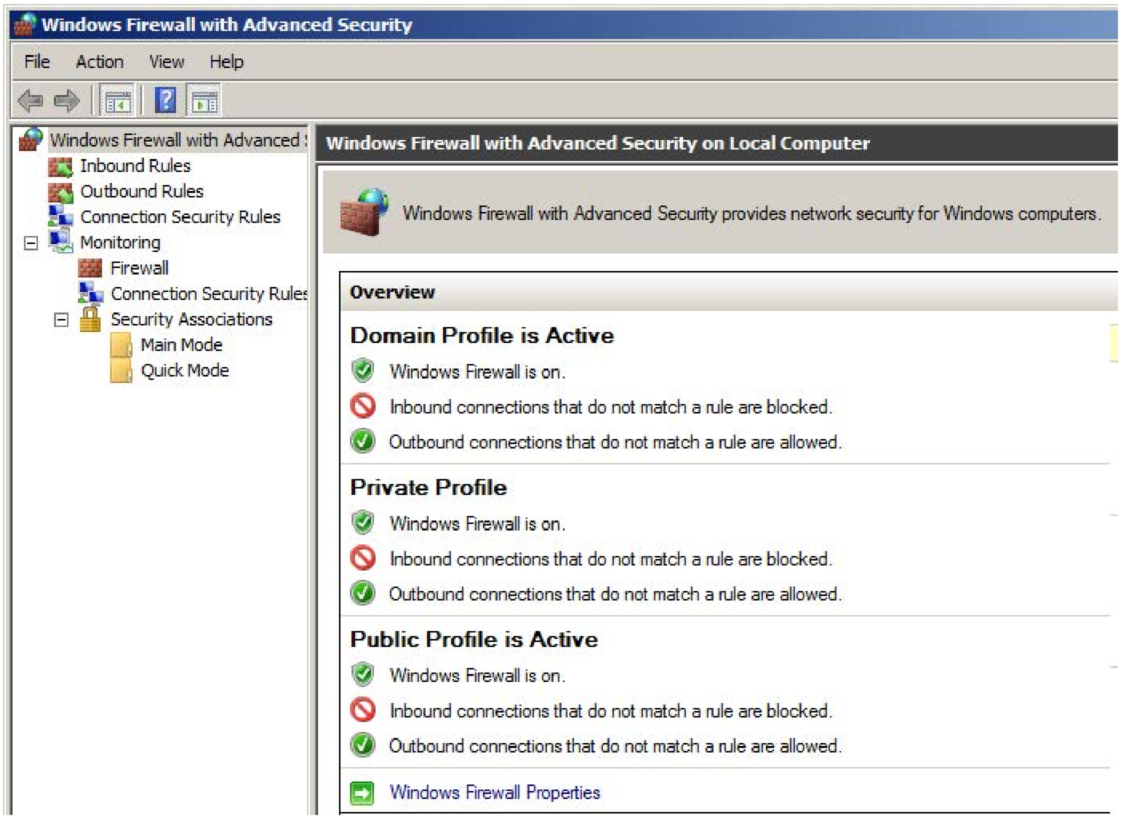
Home or work (private) networks **Connected**

Networks at home or work where you know and trust the people and devices on the network

Windows Firewall state:	On
Incoming connections:	Block all connections to programs that are not on the list of allowed programs
Active home or work (private) networks:	[redacted].local
Notification state:	Notify me when Windows Firewall blocks a new program

Public networks **Not Connected**

2. Click "Advanced Settings" in the left navigation pane.
   Enter the administrator password, if required. If you are already logged on as an administrator, confirm the execution of the application.
   The "Windows Firewall" dialog box opens.


Windows Firewall with Advanced Security
File
Action
View
Help
Windows Firewall with Advanced S
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Firewall
Connection Security Rules
Security Associations
Main Mode
Quick Mode
Windows Firewall with Advanced Security on Local Computer

Windows Firewall with Advanced Security provides network security for Windows computers.

Overview

Domain Profile is Active

✓ Windows Firewall is on.

🚫 Inbound connections that do not match a rule are blocked.

✓ Outbound connections that do not match a rule are allowed.

Private Profile

✓ Windows Firewall is on.

🚫 Inbound connections that do not match a rule are blocked.

✓ Outbound connections that do not match a rule are allowed.

Public Profile is Active

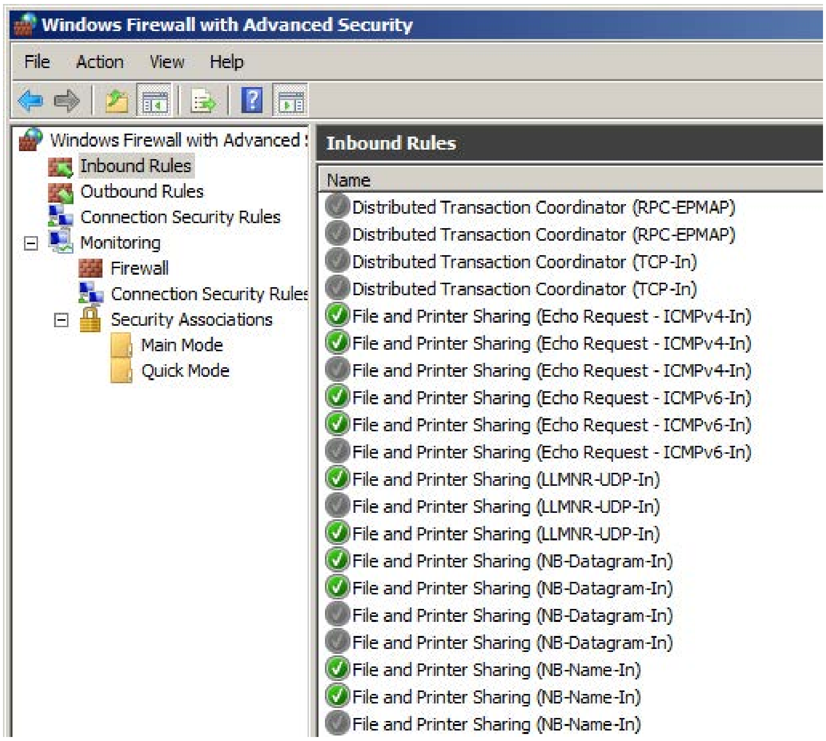
✓ Windows Firewall is on.

🚫 Inbound connections that do not match a rule are blocked.

✓ Outbound connections that do not match a rule are allowed.

Windows Firewall Properties

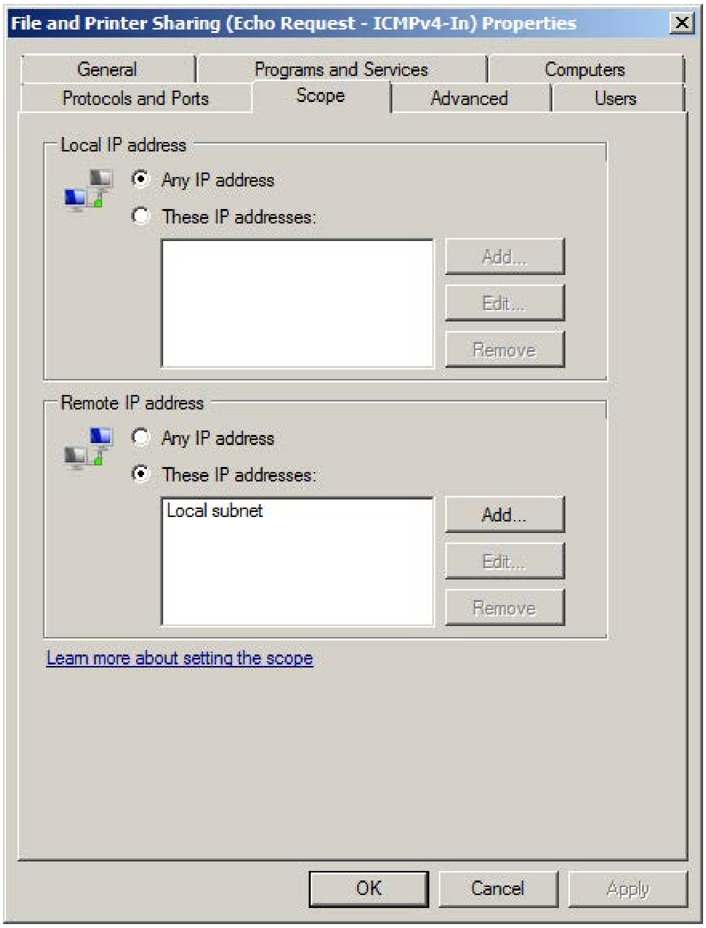
3. Click "Inbound Rules" in the left navigation pane.
   The "Inbound Rules" are displayed.


Windows Firewall with Advanced Security
File
Action
View
Help
Windows Firewall with Advanced S
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Firewall
Connection Security Rules
Security Associations
Main Mode
Quick Mode
Inbound Rules
Name

Name
Distributed Transaction Coordinator (RPC-EPMAP)
Distributed Transaction Coordinator (RPC-EPMAP)
Distributed Transaction Coordinator (TCP-In)
Distributed Transaction Coordinator (TCP-In)
✓ File and Printer Sharing (Echo Request - ICMPv4-In)
✓ File and Printer Sharing (Echo Request - ICMPv4-In)
File and Printer Sharing (Echo Request - ICMPv4-In)
✓ File and Printer Sharing (Echo Request - ICMPv6-In)
✓ File and Printer Sharing (Echo Request - ICMPv6-In)
File and Printer Sharing (Echo Request - ICMPv6-In)
✓ File and Printer Sharing (LLMNR-UDP-In)
File and Printer Sharing (LLMNR-UDP-In)
✓ File and Printer Sharing (LLMNR-UDP-In)
✓ File and Printer Sharing (NB-Datagram-In)
✓ File and Printer Sharing (NB-Datagram-In)
File and Printer Sharing (NB-Datagram-In)
File and Printer Sharing (NB-Datagram-In)
✓ File and Printer Sharing (NB-Name-In)
✓ File and Printer Sharing (NB-Name-In)
File and Printer Sharing (NB-Name-In)

4. Open the properties of an active file and printer sharing rule with a double-click.
   The properties dialog of this rule opens.

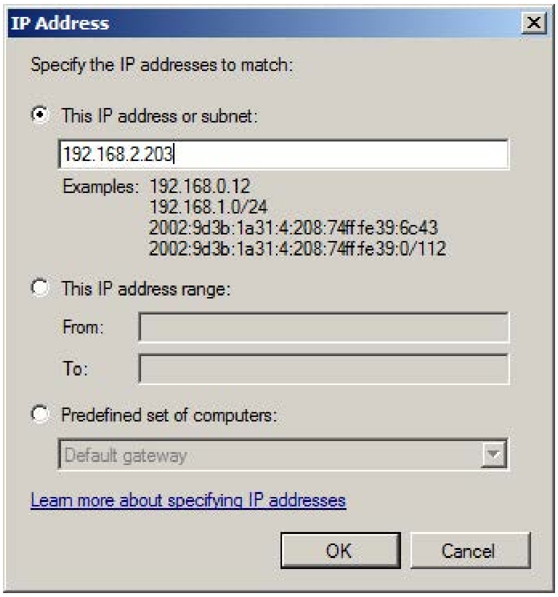
5. Open the "Scope" tab.
   The "Remote IP address" area shows the IP address range for which this firewall rule is valid and, for example, does not block the inbound communication.
   In the case of the figure below, the communication is allowed only with computers in the "Local subnet". Communication of computers in a different subnet is thus blocked.


File and Printer Sharing (Echo Request - ICMPv4-In) Properties

Local IP address
● Any IP address
○ These IP addresses:

Remote IP address
○ Any IP address
● These IP addresses:
Local subnet

6. 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.



IP Address

Specify the IP addresses to match:

● This IP address or subnet:

192.168.2.203

Examples: 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

○ This IP address range:

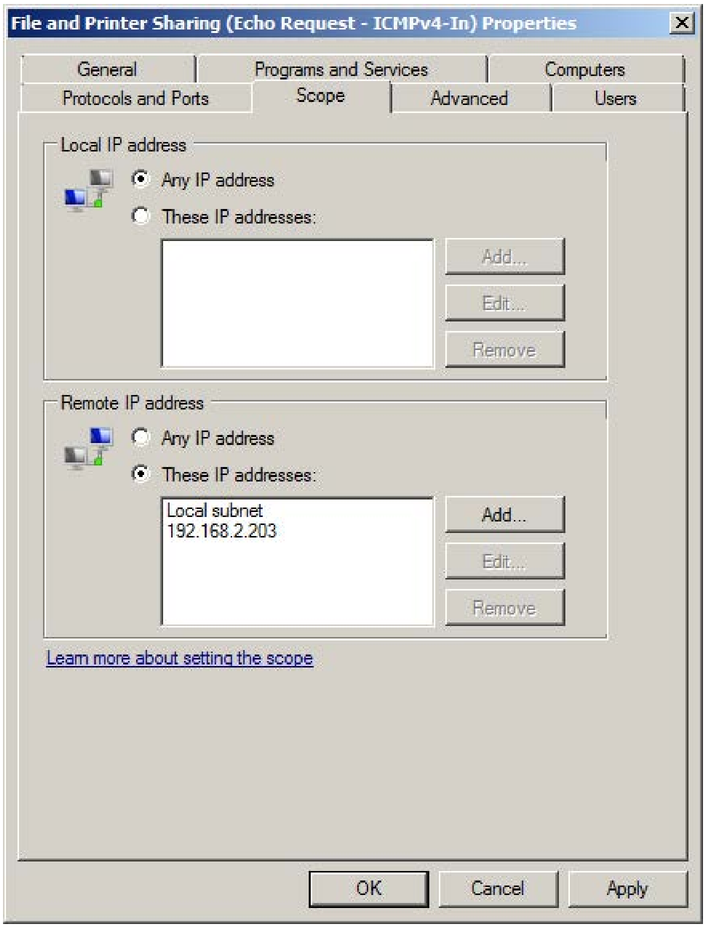
From:

To:

○ Predefined set of computers:

Default gateway

7. 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.



File and Printer Sharing (Echo Request - ICMPv4-In) Properties

Local IP address

● Any IP address

○ These IP addresses:

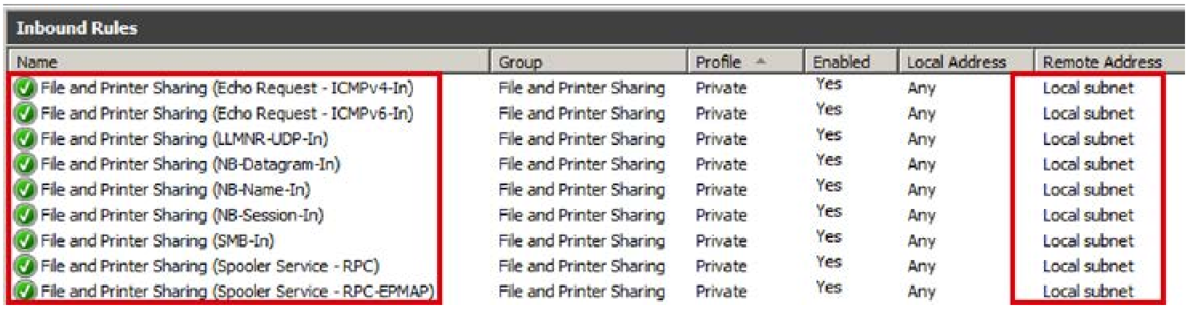
Remote IP address

○ Any IP address

● These IP addresses:

Local subnet
192.168.2.203

8. Confirm the change with "OK".
9. Adapt all inbound and outbound rules marked in the following figure accordingly. All inbound rules of the "SIMATIC …" group must also be adapted.



Inbound Rules

Name	Group	Profile	Enabled	Local Address	Remote Address
File and Printer Sharing (Echo Request - ICMPv4-In)	File and Printer Sharing	Private	Yes	Any	Local subnet
File and Printer Sharing (Echo Request - ICMPv6-In)	File and Printer Sharing	Private	Yes	Any	Local subnet
File and Printer Sharing (LLMNR-UDP-In)	File and Printer Sharing	Private	Yes	Any	Local subnet
File and Printer Sharing (NB-Datagram-In)	File and Printer Sharing	Private	Yes	Any	Local subnet
File and Printer Sharing (NB-Name-In)	File and Printer Sharing	Private	Yes	Any	Local subnet
File and Printer Sharing (NB-Session-In)	File and Printer Sharing	Private	Yes	Any	Local subnet
File and Printer Sharing (SMB-In)	File and Printer Sharing	Private	Yes	Any	Local subnet
File and Printer Sharing (Spooler Service - RPC)	File and Printer Sharing	Private	Yes	Any	Local subnet
File and Printer Sharing (Spooler Service - RPC-EPMAP)	File and Printer Sharing	Private	Yes	Any	Local subnet

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 that the first boot attempt is from the 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 CDs or USBs.
- 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/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/baust/b05/b05014.html

There are a multitude of different variants of mobile data media, including diskettes, removable disks, CDs/DVDs, USB hard disks and also Flash memories such as 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

Source:
https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04200.html?nn=6604968

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 BIOS settings for disabling USB ports (see section "BIOS settings (Page 95)"), unwanted access can also be restricted using Windows settings. By disabling/restricting the USB ports via the BIOS or Windows settings, it is ensured that unauthorized use of USB storage media is prevented.

Restricting access to USB storage media using Windows

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

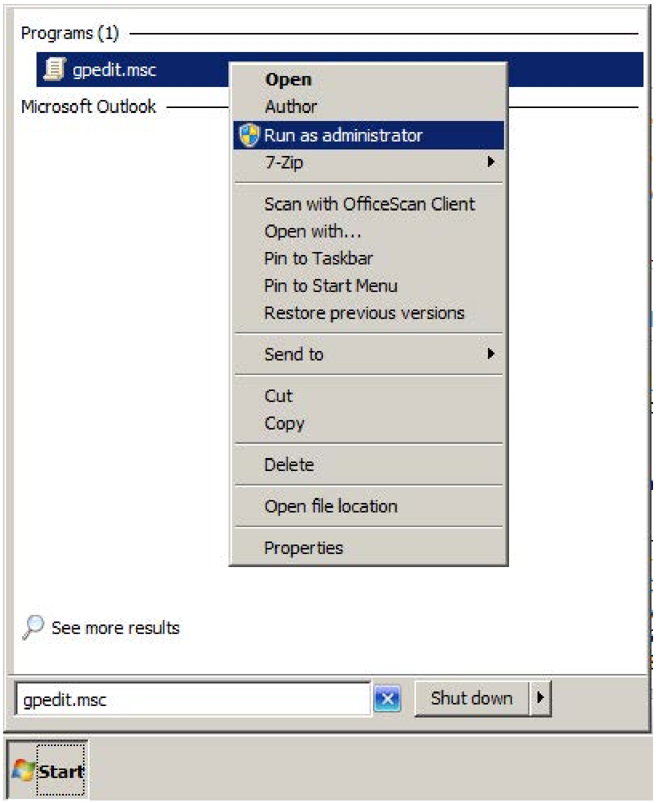
- Blocking access to USB storage media using group policy
- Regulating the use of USB storage media using a group policy
- Disabling the Autoplay function using group policy
- Disabling the Autorun functions using group policy

6.6.1 Blocking access to all USB storage media

You can completely block access to all removable storage media on Windows with the following group policy settings.

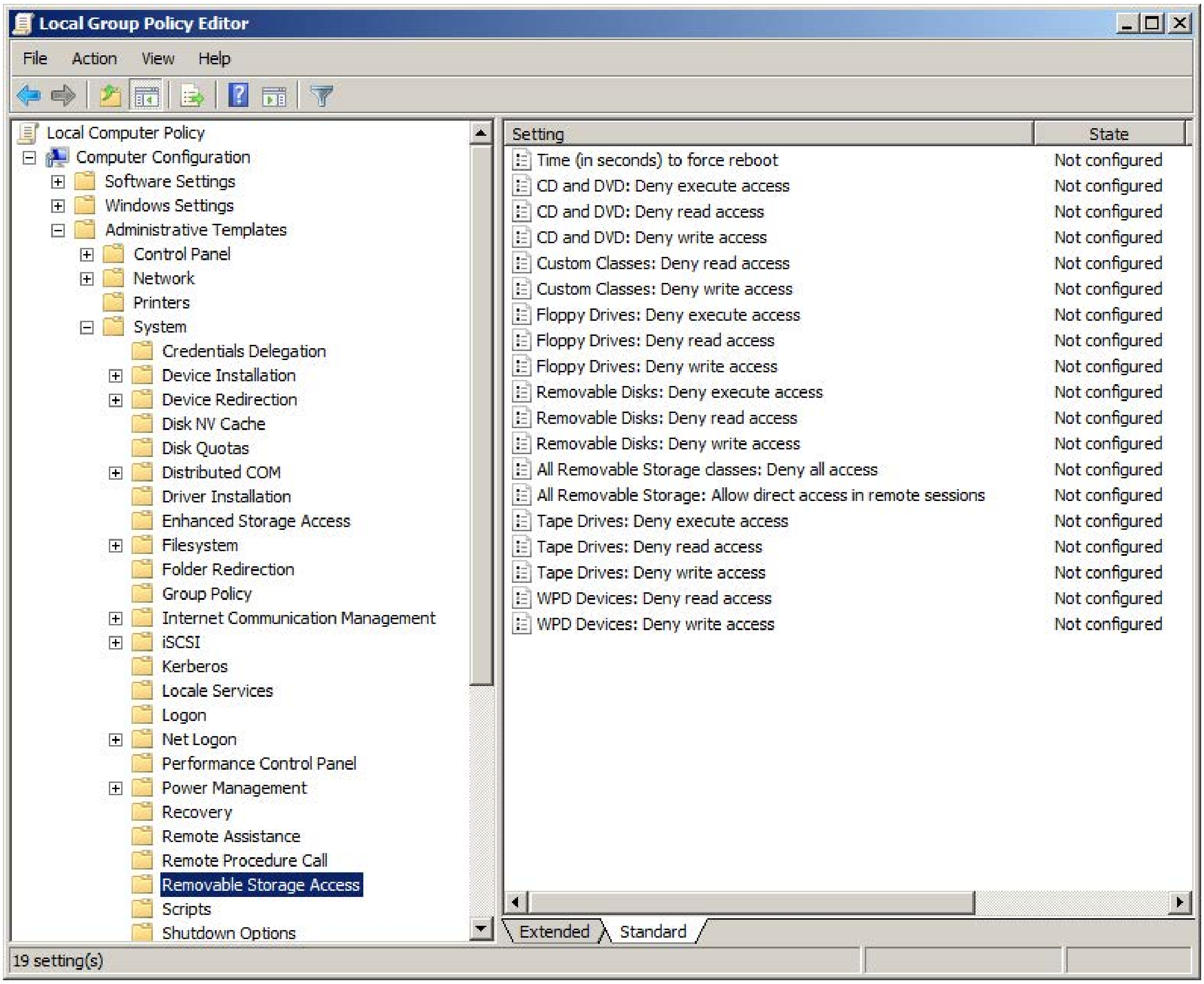
Procedure

1. Click "Start" and enter the string "gpedit.msc" in the "Search" box.
2. Start the Group Policy Editor as an administrator.
 To perform the configuration described in the following, the Group Policy Editor must be run with administrator rights.
 Enter the administrator password, if required.



The group policy editor opens.

3. Select the folder "Computer Configuration > Administrative Templates > System> Removable Storage Access".

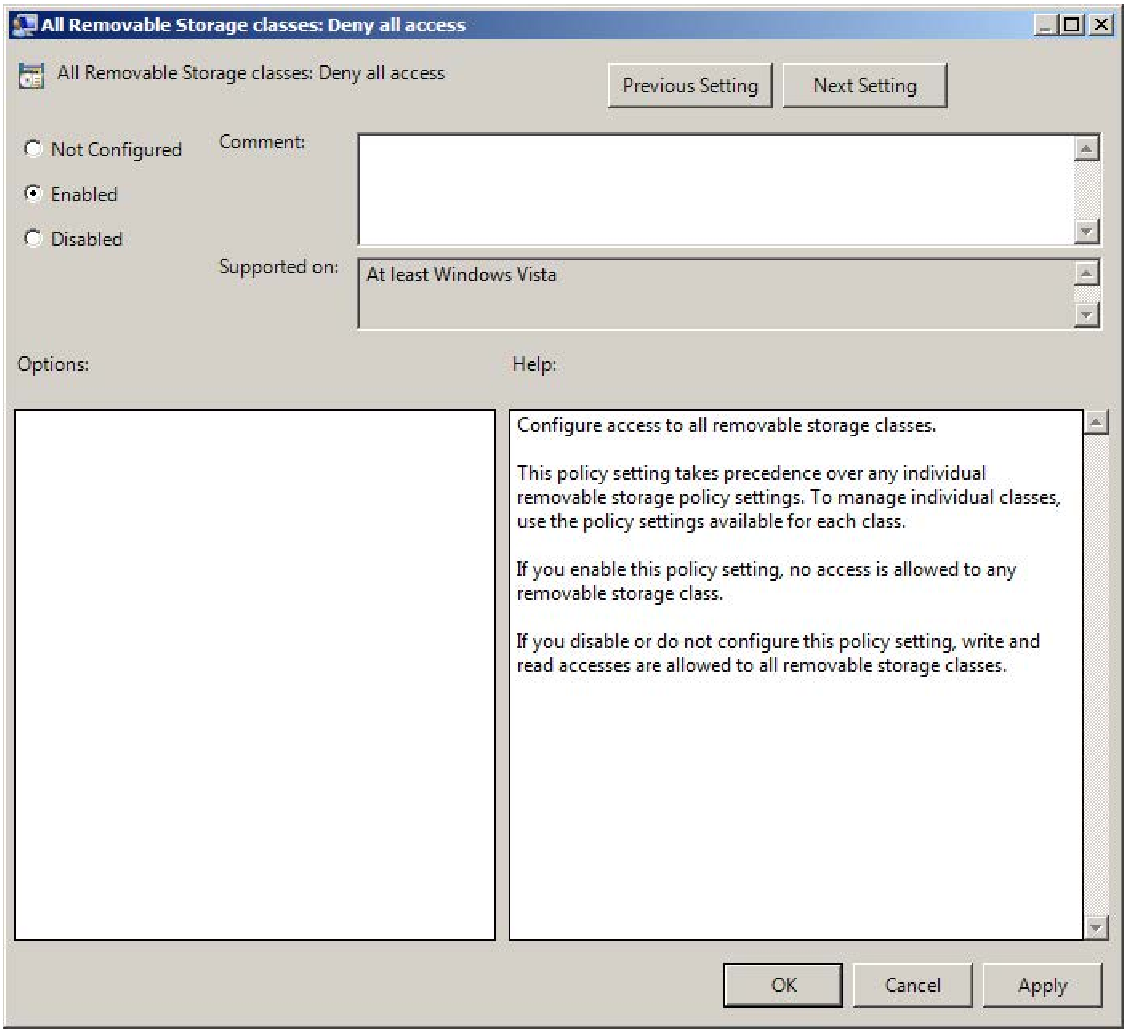


Setting	State
Time (in seconds) to force reboot	Not configured
CD and DVD: Deny execute access	Not configured
CD and DVD: Deny read access	Not configured
CD and DVD: Deny write access	Not configured
Custom Classes: Deny read access	Not configured
Custom Classes: Deny write access	Not configured
Floppy Drives: Deny execute access	Not configured
Floppy Drives: Deny read access	Not configured
Floppy Drives: Deny write access	Not configured
Removable Disks: Deny execute access	Not configured
Removable Disks: Deny read access	Not configured
Removable Disks: Deny write access	Not configured
All Removable Storage classes: Deny all access	Not configured
All Removable Storage: Allow direct access in remote sessions	Not configured
Tape Drives: Deny execute access	Not configured
Tape Drives: Deny read access	Not configured
Tape Drives: Deny write access	Not configured
WPD Devices: Deny read access	Not configured
WPD Devices: Deny write access	Not configured

19 setting(s)

4. Double-click the group policy "All Removable Storage classes: Deny all access". The Group Policy properties dialog opens.

5. Select "Enabled" and confirm your changes with "OK".



All Removable Storage classes: Deny all access

○ Not Configured
● Enabled
○ Disabled

Supported on: At least Windows Vista

Help:

Configure access to all removable storage classes.

This policy setting takes precedence over any individual removable storage policy settings. To manage individual classes, use the policy settings available for each class.

If you enable this policy setting, no access is allowed to any removable storage class.

If you disable or do not configure this policy setting, write and read accesses are allowed to all removable storage classes.

6. Reboot the computer.

Note

In a Windows domain, access to removable storage media can also be blocked using a central domain group policy for all computers in the domain.

6.6.2 Regulating the use of USB storage media

Before using a USB storage medium on a computer, the medium 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:

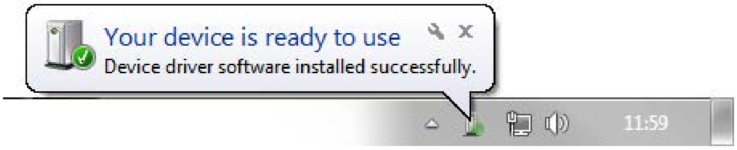
- The installation of explicitly defined devices by the user can be allowed (positive list)
- The installation of explicitly defined devices by the user can be disallowed (negative list)
- Read and write access to mobile data media, such as USB sticks, USB HDDs, diskettes, CD/DVD burners, can be configured.

Determining the hardware ID of a device

In order to influence the installation of a device using group policies as described in the above-mentioned situations, you need to know the hardware ID of the device.

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

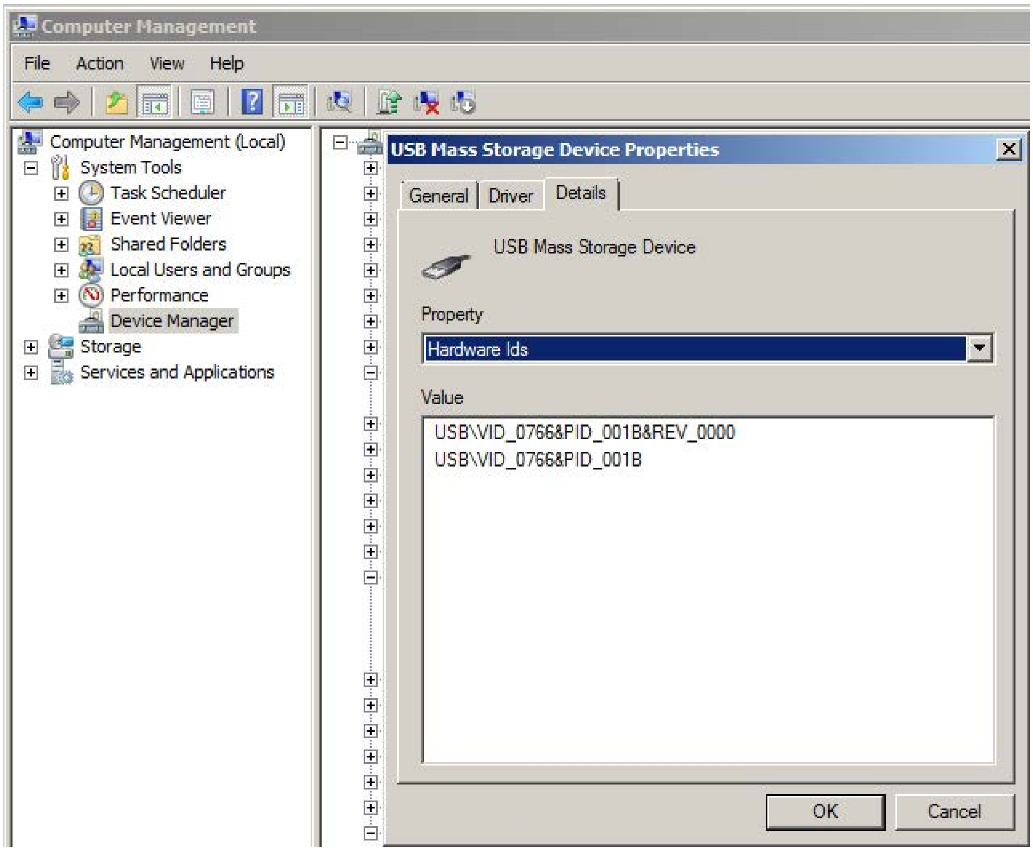
1. Connect the device with a Windows PC and wait until the installation of the corresponding driver finishes.
   Successful installation is indicated with the message "Your device is ready to use".



Your device is ready to use
Device driver software installed successfully.

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 "Hardware IDs" from the drop-down list to display the hardware IDs of the device. You need the hardware IDs to configure the respective group policies.



Property: Hardware Ids

Value:
```
USB\VID_0766&PID_001B&REV_0000
USB\VID_0766&PID_001B
```

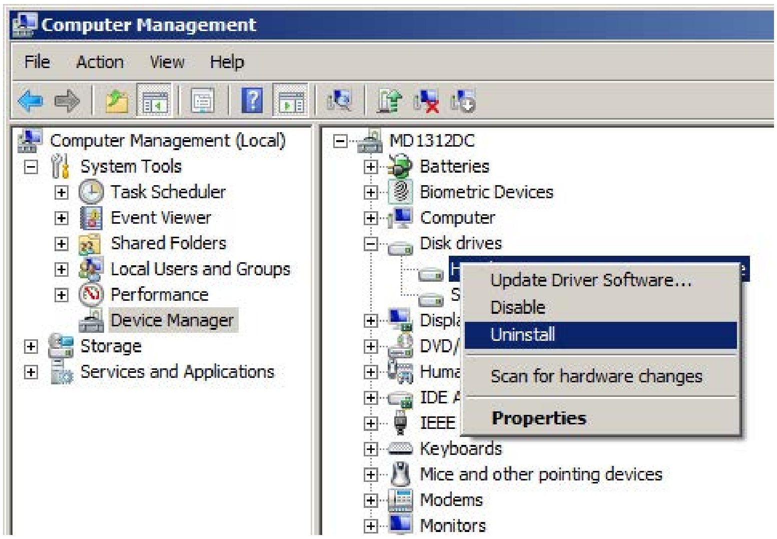
5. Select "Compatible IDs" from the drop-down list to display the compatible IDs of the device.
   You need the compatible IDs to configure the respective group policies.

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.



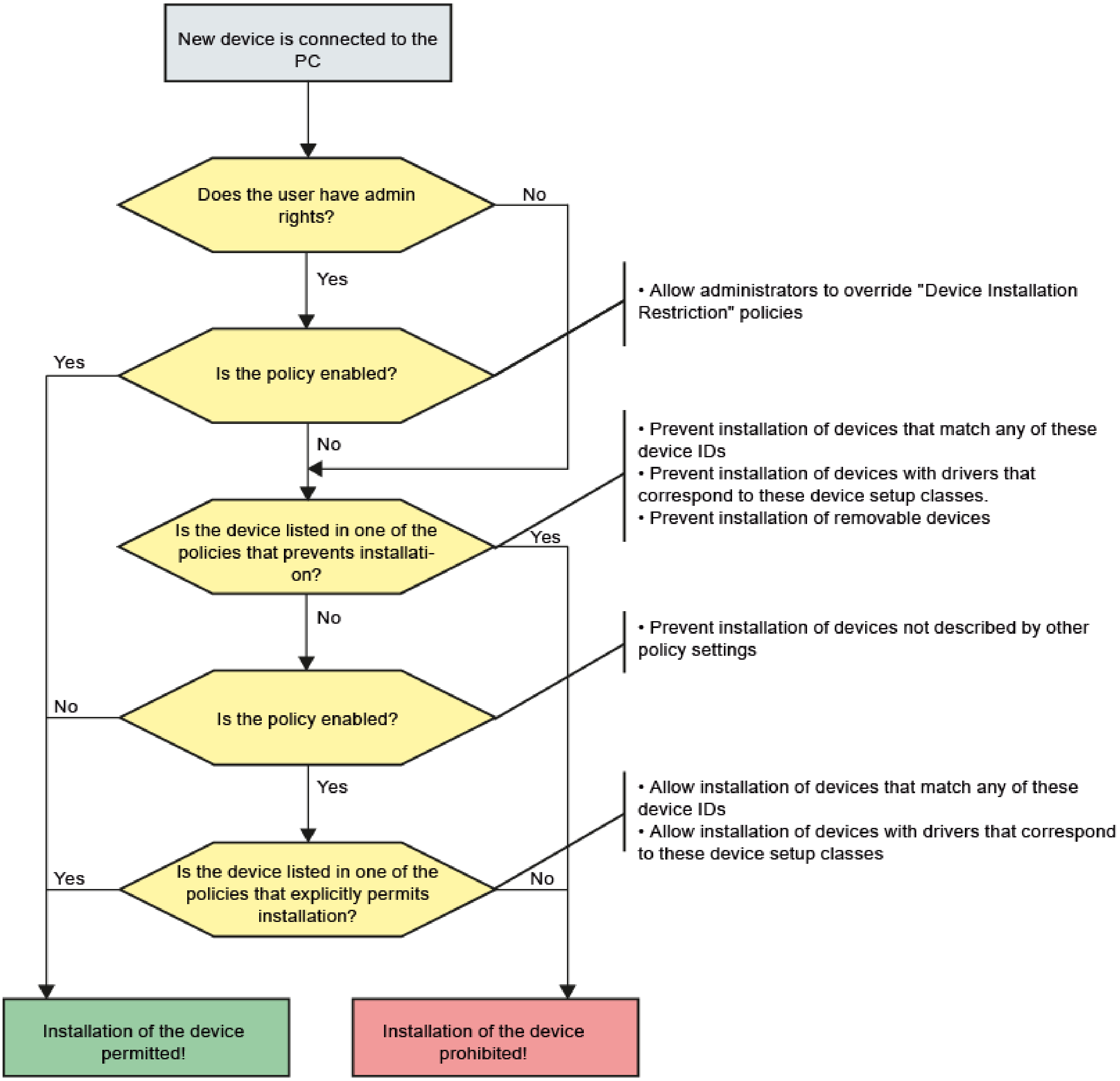
2. Click "OK" in the final dialog.

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:


New device is connected to the PC
Does the user have admin rights?
No
Yes
• Allow administrators to override "Device Installation Restriction" policies
Yes
Is the policy enabled?
No
• Prevent installation of devices that match any of these device IDs
• Prevent installation of devices with drivers that correspond to these device setup classes.
• Prevent installation of removable devices
Is the device listed in one of the policies that prevents installati-on?
Yes
No
• Prevent installation of devices not described by other policy settings
No
Is the policy enabled?
Yes
• Allow installation of devices that match any of these device IDs
• Allow installation of devices with drivers that correspond to these device setup classes
Yes
Is the device listed in one of the policies that explicitly permits installation?
No
Installation of the device permitted!
Installation of the device prohibited!

If you want to allow only certain 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 needed for this.)

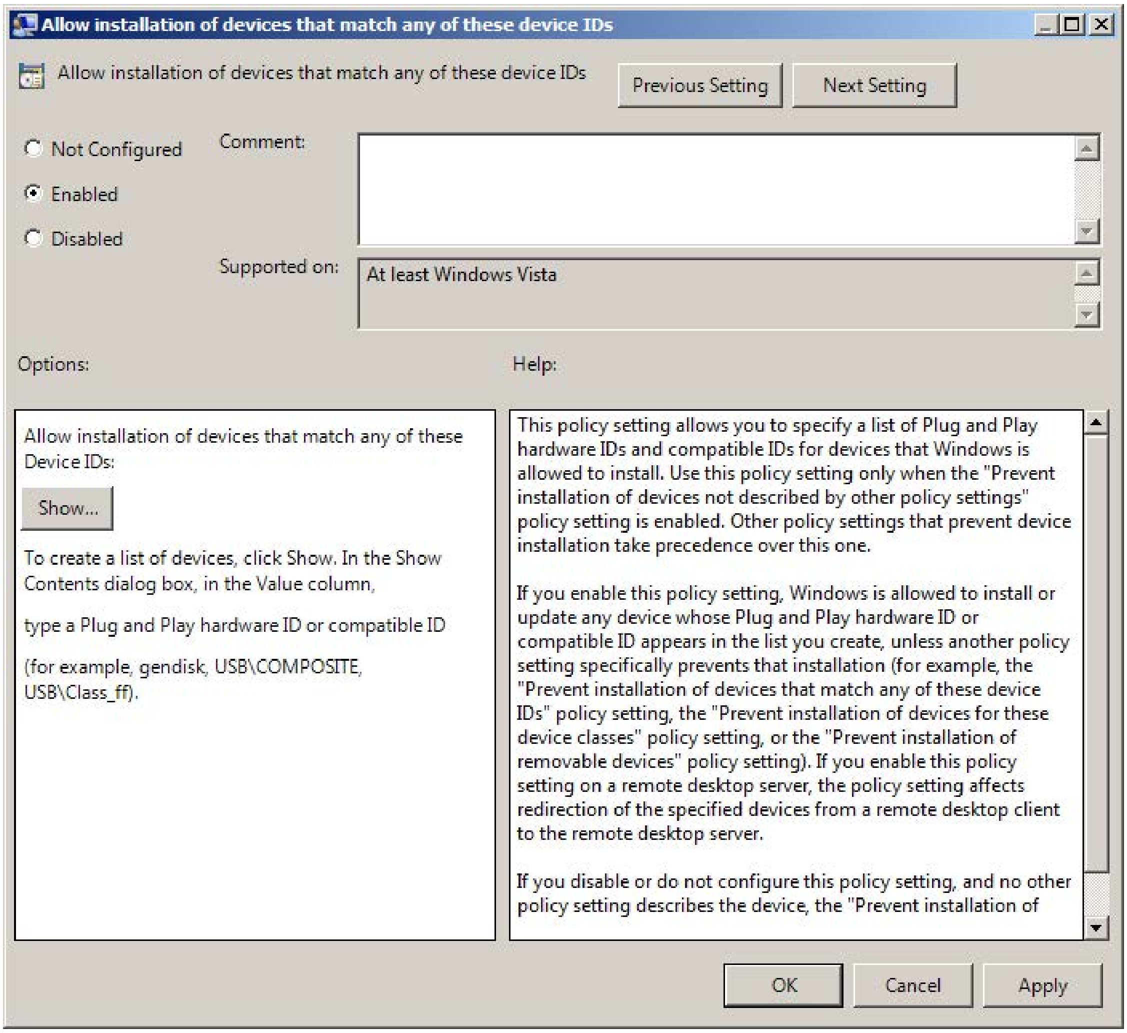
1. Ensure that all devices involved are uninstalled in the Device Manager.
2. Open the Group Policy Editor and navigate to the folder "Computer Configuration > Administrative Templates > System > Device Installation > Device Installation Restrictions".
   The group policies are displayed in the right 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 using the "Enabled" option and confirm the setting by pressing "OK".
   The installation of all devices on the computer is prohibited.

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.



Allow installation of devices that match any of these device IDs

Allow installation of devices that match any of these device IDs

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: At least Windows Vista

Options:

Allow installation of devices that match any of these Device IDs:

To create a list of devices, click Show. In the Show Contents dialog box, in the Value column,

type a Plug and Play hardware ID or compatible ID

(for example, gendisk, USB\COMPOSITE, USB\Class_ff).

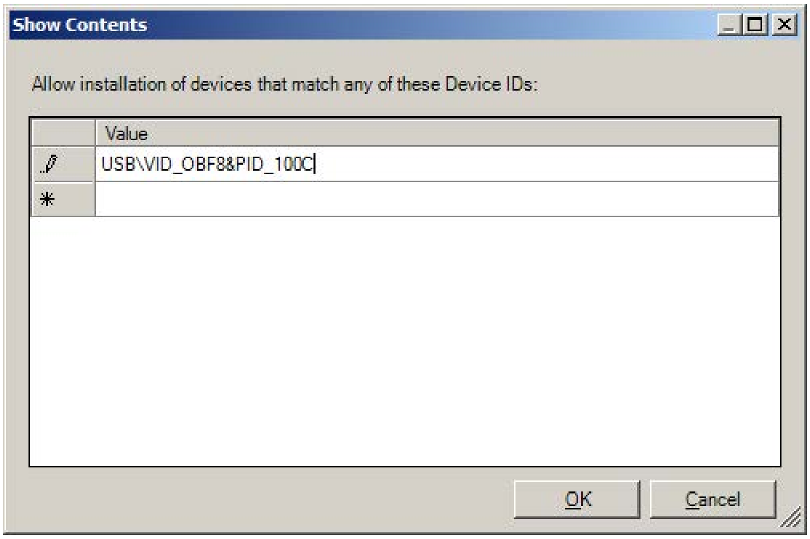
Help:

This policy setting allows you to specify a list of Plug and Play hardware IDs and compatible IDs for devices that Windows is allowed to install. Use this policy setting only when the "Prevent installation of devices not described by other policy settings" policy setting is enabled. Other policy settings that prevent device installation take precedence over this one.

If you enable this policy setting, Windows is allowed to install or update any device whose Plug and Play hardware ID or compatible ID appears in the list you create, unless another policy setting specifically prevents that installation (for example, the "Prevent installation of devices that match any of these device IDs" policy setting, the "Prevent installation of devices for these device classes" policy setting, or the "Prevent installation of removable devices" policy setting). If you enable this policy setting on a remote desktop server, the policy setting affects redirection of the specified devices from a remote desktop client to the remote desktop server.

If you disable or do not configure this policy setting, and no other policy setting describes the device, the "Prevent installation of

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.


Show Contents
Allow installation of devices that match any of these Device IDs:
Value
OK
Cancel

USB\VID_OBF8&PID_100C

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 ID of the device using the Device Manager.
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.

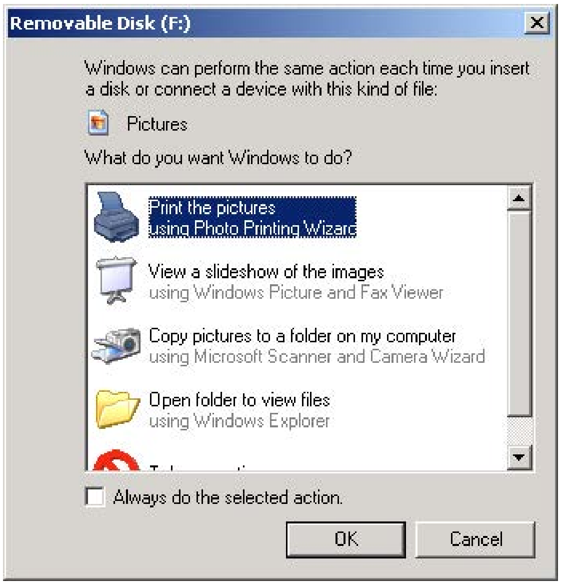
6.6.3 Disabling AutoRun / AutoPlay for external drives and storage media

Source: http://support.microsoft.com/kb/967715/en

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.



Removable Disk (F:)

Windows can perform the same action each time you insert a disk or connect a device with this kind of file:

Pictures

What do you want Windows to do?

Print the pictures
using Photo Printing Wizard
View a slideshow of the images
using Windows Picture and Fax Viewer
Copy pictures to a folder on my computer
using Microsoft Scanner and Camera Wizard
Open folder to view files
using Windows Explorer
□ Always do the selected action.
OK
Cancel

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

Note

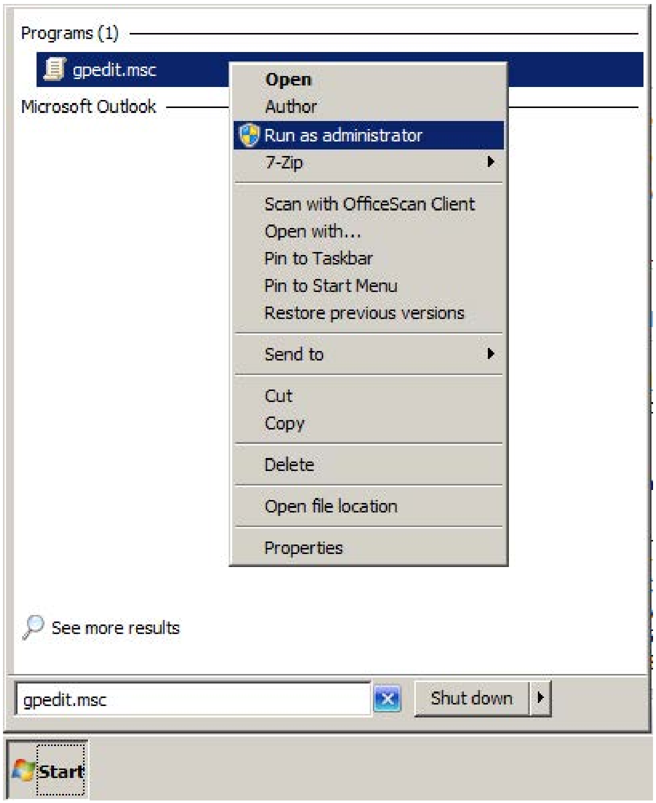
Malware, such as a Trojan horse, can be started via the AutoRun and AutoPlay functions.

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:

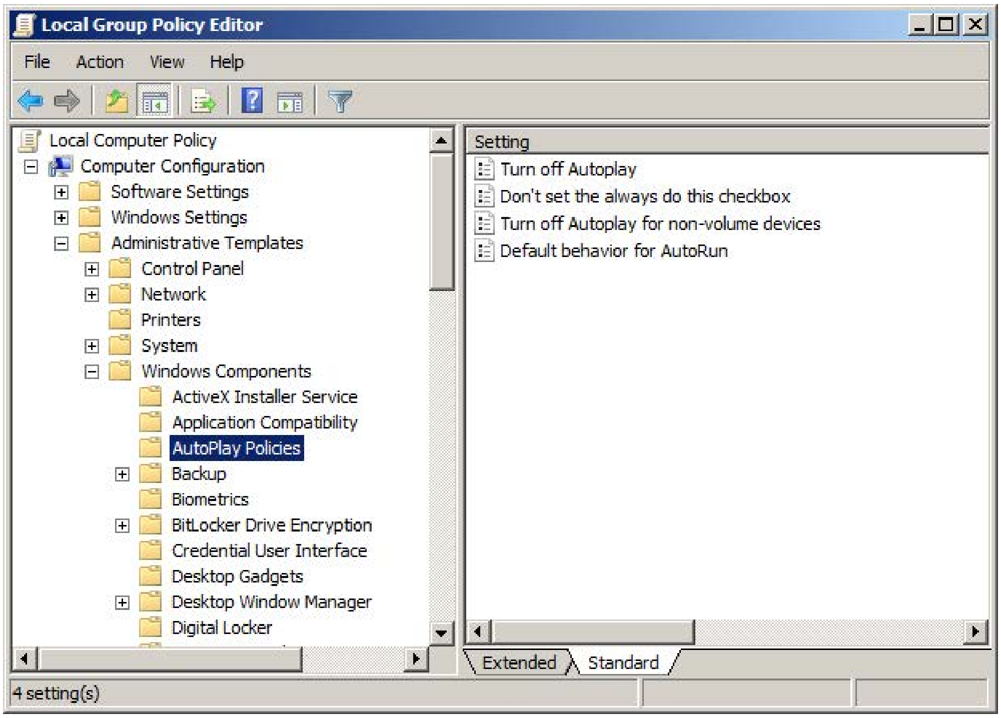
1. Click "Start" and enter the string "gpedit.msc" in the "Search" box.
2. Start the Group Policy Editor as an administrator.
   To perform the configuration described below, the Group Policy Editor must be run with administrator rights.
   Enter the administrator password, if necessary.



The group policy editor opens.

3. 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.



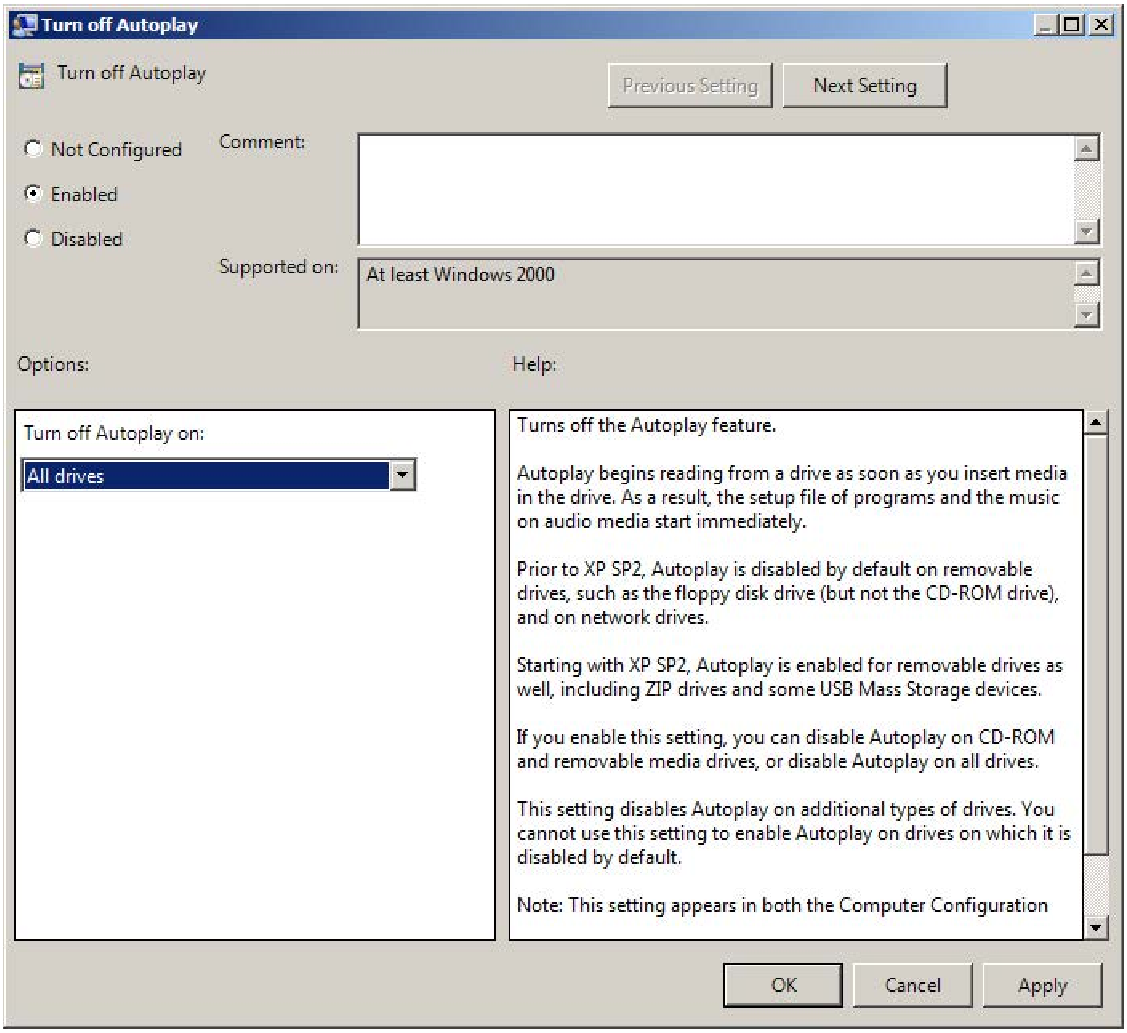
Turn off Autoplay
Don't set the always do this checkbox
Turn off Autoplay for non-volume devices
Default behavior for AutoRun

4 setting(s)

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

5. Select the "Enabled" option.

6. In the "Turn off Autoplay on:" area, select the "All drives" option.



○ Not Configured
● Enabled
○ Disabled

Supported on: At least Windows 2000

Options:

Turn off Autoplay on: All drives

Help:

Turns off the Autoplay feature.

Autoplay begins reading from a drive as soon as you insert media in the drive. As a result, the setup file of programs and the music on audio media start immediately.

Prior to XP SP2, Autoplay is disabled by default on removable drives, such as the floppy disk drive (but not the CD-ROM drive), and on network drives.

Starting with XP SP2, Autoplay is enabled for removable drives as well, including ZIP drives and some USB Mass Storage devices.

If you enable this setting, you can disable Autoplay on CD-ROM and removable media drives, or disable Autoplay on all drives.

This setting disables Autoplay on additional types of drives. You cannot use this setting to enable Autoplay on drives on which it is disabled by default.

Note: This setting appears in both the Computer Configuration

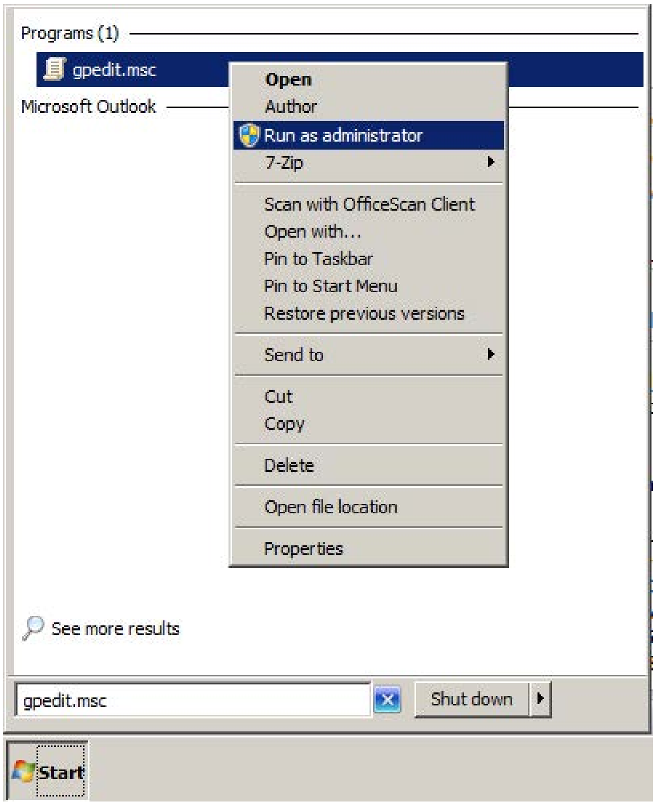
7. Confirm the settings with "OK".
8. Reboot the computer.

6.6.3.2 Disabling all AutoRun functions using a group policy

Procedure

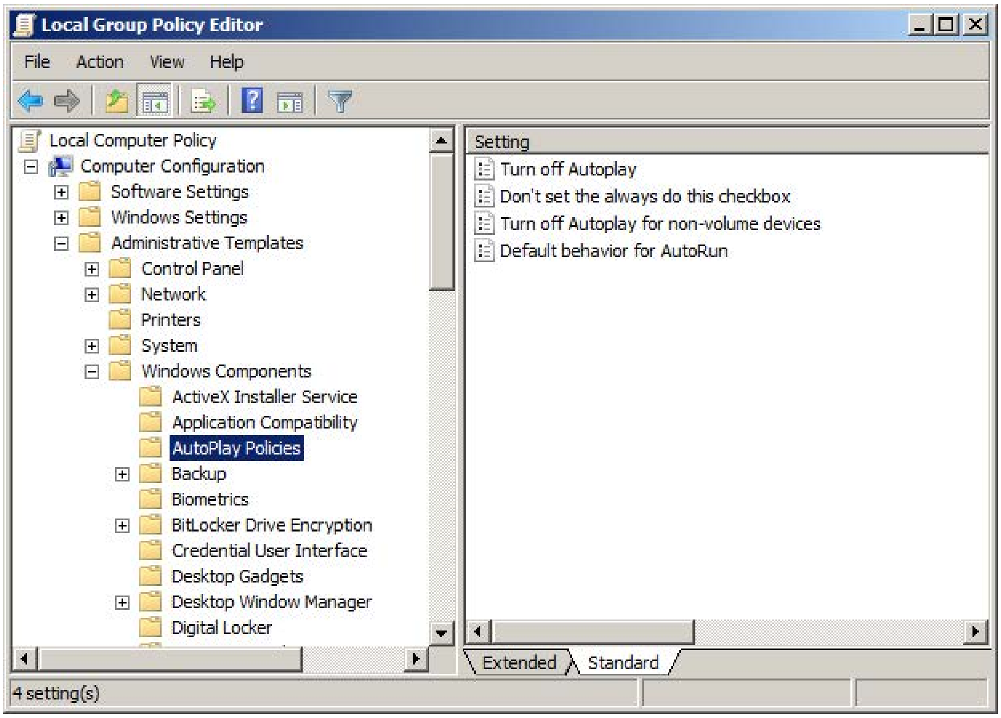
To disable the AutoRun function in Windows via a group policy, follow these steps:

1. Click "Start" and enter the string "gpedit.msc" in the "Search" box.
2. Start the Group Policy Editor as an administrator.
   To perform the configuration described below, the Group Policy Editor must be run with administrator rights.
   Enter the administrator password, if necessary.



3. 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.

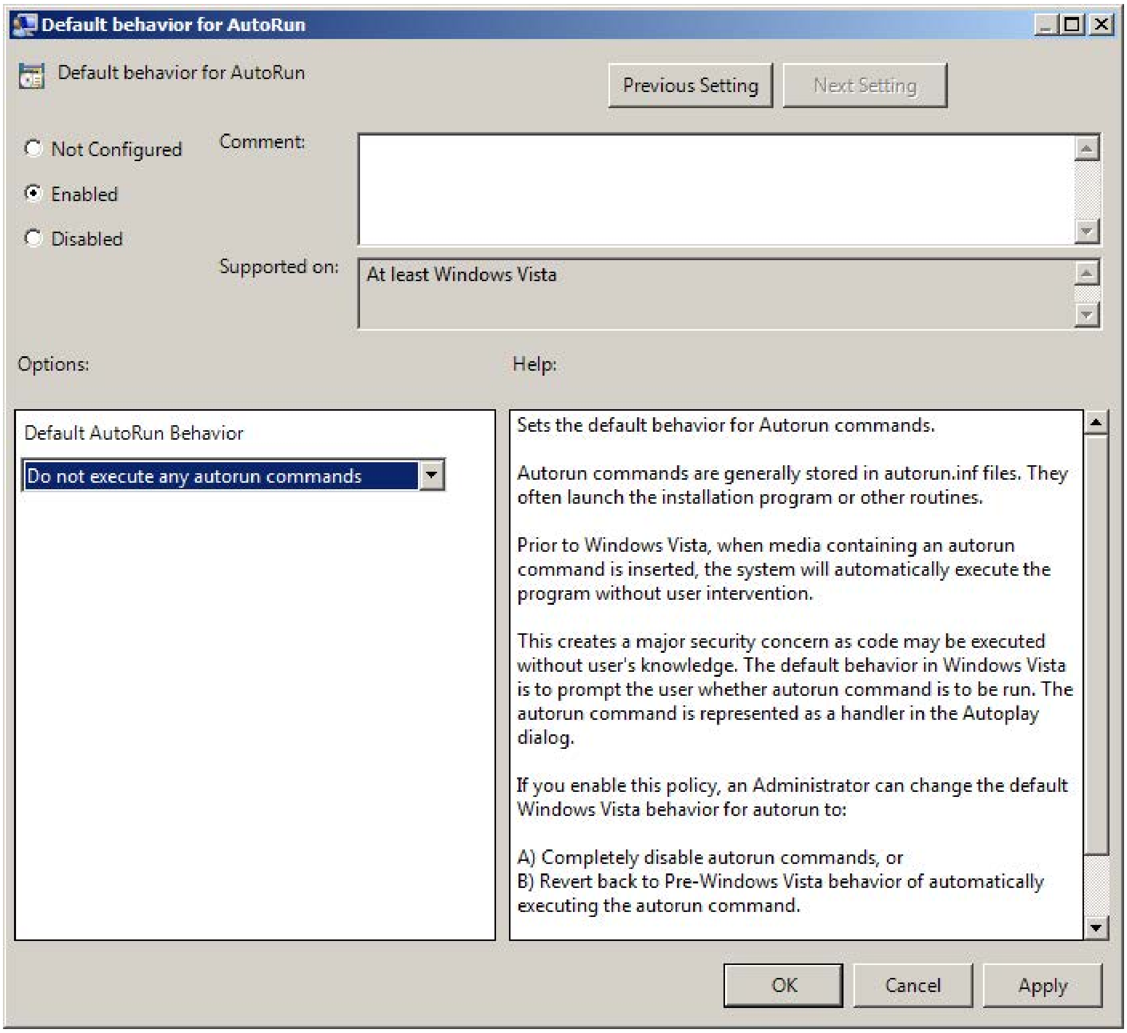


Setting
Turn off Autoplay
Don't set the always do this checkbox
Turn off Autoplay for non-volume devices
Default behavior for AutoRun

4 setting(s)

4. Double-click the group policy "Default Autorun Behavior".
   The properties dialog of the group policy opens.
5. Select the "Enabled" option.

6. From the drop-down list in the "Default Autorun Behavior" area, select the "Do not execute any autorun commands" option.



Default behavior for AutoRun

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: At least Windows Vista

Options:

Default AutoRun Behavior: Do not execute any autorun commands

Help:

Sets the default behavior for Autorun commands.

Autorun commands are generally stored in autorun.inf files. They often launch the installation program or other routines.

Prior to Windows Vista, when media containing an autorun command is inserted, the system will automatically execute the program without user intervention.

This creates a major security concern as code may be executed without user's knowledge. The default behavior in Windows Vista is to prompt the user whether autorun command is to be run. The autorun command is represented as a handler in the Autoplay dialog.

If you enable this policy, an Administrator can change the default Windows Vista behavior for autorun to:

A) Completely disable autorun commands, or
B) Revert back to Pre-Windows Vista behavior of automatically executing the autorun command.

7. Confirm the settings with "OK".
8. 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, the computer must first be "solidified". This means that all connected local drives are scanned for executable files. The duration of this procedure depends on the data volume and computing power and may take several hours. This takes approx. 20-30 minutes for a PCS 7 OS server installation and medium-sized projects with the current hardware.
- 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, etc.). All executable files (exe, com, dll, bat, etc.) found during the scan are now protected against changes (renaming, deletion, etc.) and the whitelisting mechanism is activated. As a result, other files that are newly copied to the system cannot be executed.

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 under (https://support.industry.siemens.com/cs/ww/en/view/64847781).

You can find a description of the recommended procedure and configuration with McAfee Application Control under (https://support.industry.siemens.com/cs/ww/en/view/88653385).

You can find the McAfee Knowledge Center with current documentation on McAfee products at https://support.mcafee.com/ServicePortal/faces/knowledgecenter.

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 be configured and controlled using bat files or 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 offers many network management and network monitoring features, some free of charge.

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 (e.g. WSUS, virus scan server), McAfee ePO can also be installed on this computer.

Note

McAfee ePO must not be installed on an automation device or a domain controller.

6.8 Hardening of devices by Industrial Security Services

In addition to the system hardening possibilities described above, there are additional possibilities 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 additional information and the corresponding contacts at https://www.siemens.com/industrial-security.

Inquiries can also be emailed directly to "industrialsecurity.i@siemens.com".

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.

Additional information

Detailed information about the possible protection levels of the S7-400 CPUs and the know-how protection of blocks can be found in the following entries

- Manual "SIMATIC S7-400H Fault-tolerant Systems (https://support.industry.siemens.com/cs/ww/en/view/82478488)"
- 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 S7-400 - Industrial Ethernet CPs

In addition to an integrated Web server, Industrial Ethernet CPs (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 no asset management is 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 operation of H-connections (S7-400H high availability system) within a VPN tunnel is not supported by the CP 443-1 Advanced.

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/109738462)
- SIMATIC NET Industrial Ethernet Security Security Basics and Application (https://support.industry.siemens.com/cs/ww/en/view/109738463)

6.11 Time synchronization of system

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

The time source (e.g. SICLOCK) should be located in the system security cell.

Additional information

You can find additional information on the configuration of time synchronization in PCS 7 systems in the "SIMATIC PCS 7 Process Control System Time Synchronization" (https://support.industry.siemens.com/cs/ww/en/view/109485963) manual.

6.12 Handling of digital signatures for applications

In 2014, Microsoft introduced a mechanism in Windows that is used to check the digital signatures of binary files that are signed with the Windows Authenticode Signature Format. This change is contained in the Security Bulletin MS13-098. As soon as it is enabled, 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.

To increase the system integrity, the update described in the Security Bulletin should be installed.

Additional information

Information on setting up this function can be found using the following link
(Security Bulletin MS13-098): https://technet.microsoft.com/library/security/2915720.
Note the description of enabling the function under "Test the Improvement to Authenticode Signature Verification".

You can find information on measures for preventing possible delays 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).

User Administration and Operator Permissions 7

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 receives the permissions required for his/her role, e.g. as operator/configuring engineer of a unit.

7.2 Windows workgroup or Windows domain

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

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

When Windows workgroups are used, the computers and users/groups are administered in a decentralized manner and locally on each individual computer. Within a Windows domain (Active Directory), centralized administration of computers and 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 a Windows domain (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:

- 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

A redundant DHCP server can be configured based on Windows Server 2012 (or newer). The use of a DHCP server under PCS 7 requires the configuration of static IP address assignment for the 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)
  - 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 a Windows domain, 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 two different user accounts and thus related authorizations:

- User accounts that are used for logging onto the operating system and starting the applications.
- User accounts that are used for logon of operators on the user interface ("PCS 7 Runtime").

Note

It is recommended that the two user accounts be defined and handled separately.

In addition, the option exists to consolidate the two user accounts and to use only one user account for accessing a 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).

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.

The user accounts that are logged onto 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.

Note

A user only has to belong to the administrators group for configuration of the computer and installation of PCS 7.

Administrative rights are not needed for operation of 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.

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

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.

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 who is carrying out the installation and the local administrator are automatically added to this group. Other users must be manually added to this group by an administrator.
- 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 used as a matter of priority for the user accounts of Web publishing services, e.g. the IIS (Internet Information Services) that is needed for operation of the WinCC Web navigator.

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

After installation of PCS 7, follow these steps:

1. Create a project folder on the hard disk and create a folder share for it.
2. Assign the necessary share authorizations and security settings (file system rights) to the share folder. The following options are available for this:
   - Using the SIMATIC Tool "SIMATICRights.exe", which is located in the "Additional_Products" folder on the PCS 7 Installation DVD 2.
   - Manually using Windows Explorer
     In this case, use "full access" for the "SIMATIC HMI" group.
3. Assign the same rights to the "Administrators" group.

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, all Windows users that work with PCS 7, PCS 7 OS or Route Control projects must be a member 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
  All Windows users that work with PCS 7 ES projects must be a member 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 directories "sbdata" and "sbdata_backup". All 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 shares are created:

- BATCH

The administration of share permissions occurs during installation. Add the "SIMATIC BATCH" user group with full access permission in the security settings for shares (NTFS permissions). 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 unrestricted access to the Management Console as well as all authorizations.
  Enter the members of this group in the 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

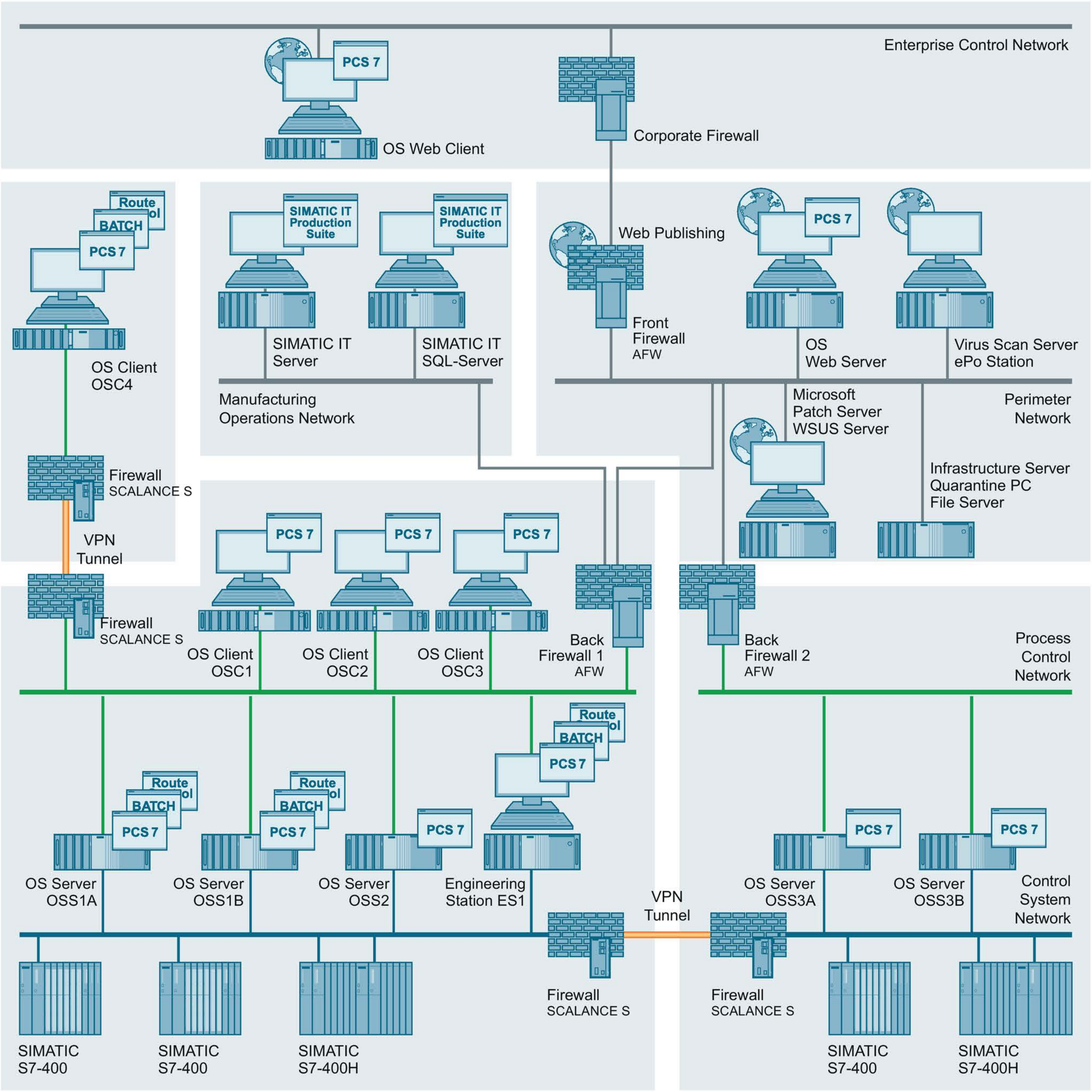
During installation of PCS 7 using the SIMATIC PCS 7 setup program, the following local user group is added to the Windows group management if the "SIMATIC Logon" option was selected:

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

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

7.3.10 Example configuration

The following figure shows the example configuration:



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

User	Description
ENG1	PCS 7 Engineer 1 • 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	PCS 7 Engineer 2 In addition to ENG1, this user is the administrator of the system
OSC1	Local Windows user who is generally permanently logged on OS client "OSC1" (device-specific, "non-personalized"). Logon to the operating system performed using Windows Autologon.
OSC2	Local Windows user who is generally permanently logged on OS client "OSC2" (device-specific, "non-personalized"). Logon to the operating system performed using Windows Autologon.
OSC3	Local Windows user who is generally permanently logged on OS client "OSC3" (device-specific, "non-personalized"). Logon to the operating system performed using Windows Autologon.
OSC4	Local Windows user who is generally permanently logged on OS client "OSC4" (device-specific, "non-personalized"). Logon to the operating system performed using Windows Autologon.
OSS1A	Local Windows user who is generally permanently logged on OS server "OSS1A" (device-specific, "non-personalized"). Logon to the operating system performed using Windows Autologon.
OSS1B	Local Windows user who is generally permanently logged on OS server "OSS1B" (device-specific, "non-personalized"). Logon to the operating system performed using Windows Autologon.
OSS2	Local Windows user who is generally permanently logged on OS server "OSS2" (device-specific, "non-personalized"). Logon to the operating system performed using Windows Autologon.
OSS3A	Local Windows user who is generally permanently logged on OS server "OSS3A" (device-specific, "non-personalized"). Logon to the operating system performed using Windows Autologon.
OSS3B	Local Windows user who is generally permanently logged on OS server "OSS3B" (device-specific, "non-personalized"). Logon to the operating system performed using Windows Autologon.

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

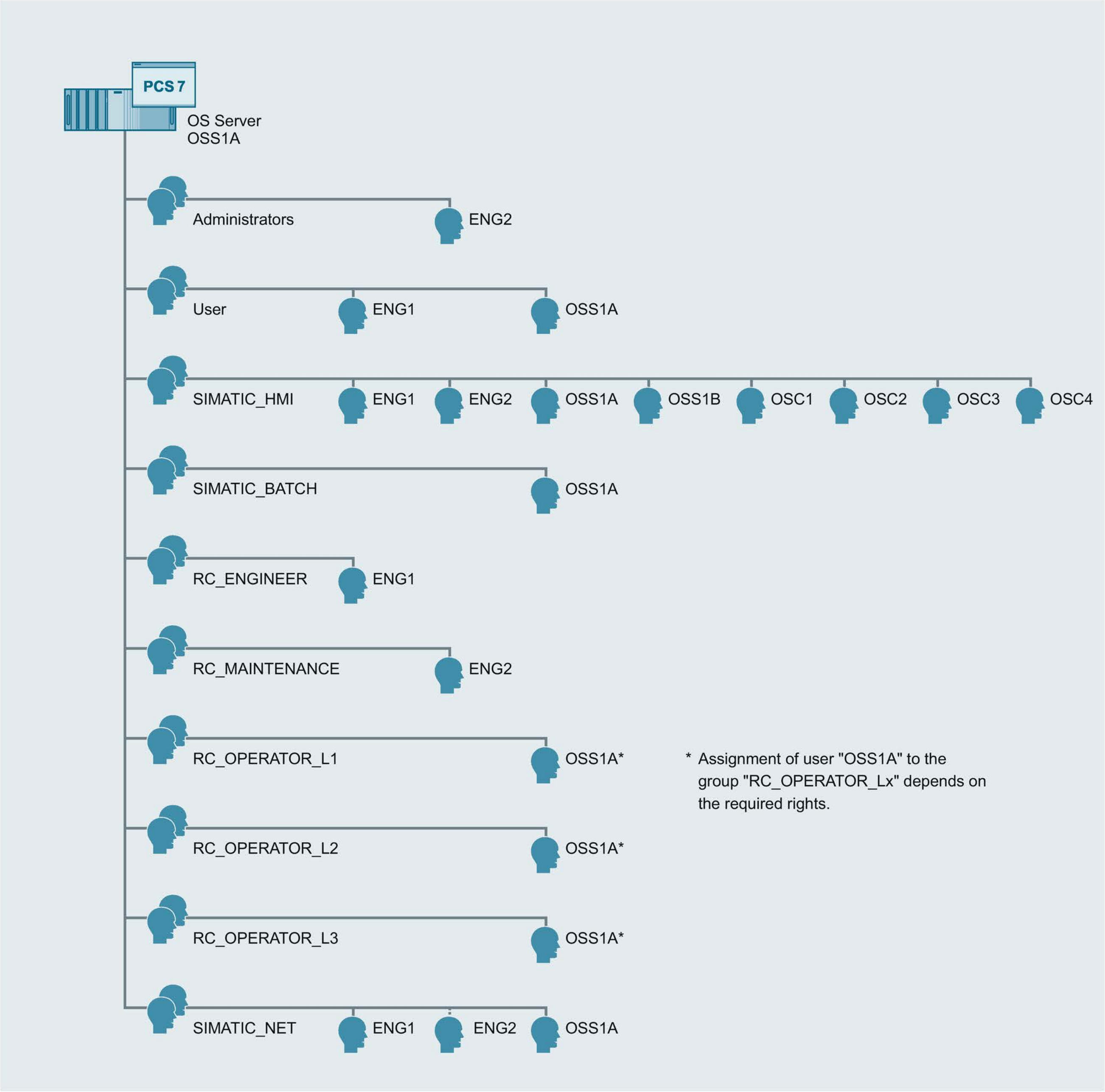
Computer/ Local group	ES1	OSC1	OSC2	OSC3	OSC4	OSS1A	OSS1B	OSS2	OSS3A	OSS3B
Administrators	ENG2	ENG2	ENG2	ENG2	ENG2	ENG2	ENG2	ENG2	ENG2	ENG2
User	ENG1	OSC1 ENG1	OSC2 ENG1	OSC3 ENG1	OSC4 ENG1	OSS1A ENG1	OSS1B ENG1	OSS2 ENG1	OSS3A ENG1	OSS3B ENG1
SIMATIC HMI	ENG1 ENG2	ENG1 ENG2 OSC1 OSS1A OSS1B OSS2 OSS3A 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 OSS1A OSS1B OSC1 OSC2 OSC3 OSC4	ENG1 ENG2 OSS1B OSS1A OSC1 OSC2 OSC3 OSC4	ENG1 ENG2 OSS2 OSC1 OSC2 OSC3 OSC4	ENG1 ENG2 OSS3A OSS3B OSC1 OSC2 OSC3 OSC4	ENG1 ENG2 OSS3B OSS3A OSC1 OSC2 OSC3 OSC4
SIMATIC BATCH[1)]	ENG1 ENG2	OSC1	OSC1	OSC3	OSC4	OSS1A	OSS1B	OSS2	OSS3A[1)]	OSS3B[1)]
RC_ENGINEERENG1[2)]	ENG1	-	-	-	-	ENG1	ENG1	ENG1	ENG1	ENG1
RC_MAINTENANCEENG1[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":



* Assignment of user "OSS1A" to the group "RC_OPERATOR_Lx" depends on the required rights.

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/60119725).

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/109485951)".

You can find addition information on user rights for SIMATIC Route Control, especially regarding the assignment of users to the user groups RC_OPERATOR_L1/L"/L3, in the programming and operating manual "SIMATIC Process Control System PCS 7 SIMATIC Route Control (https://support.industry.siemens.com/cs/ww/en/view/109738713)".

7.4 Password policies

Introduction

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

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.

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.

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:

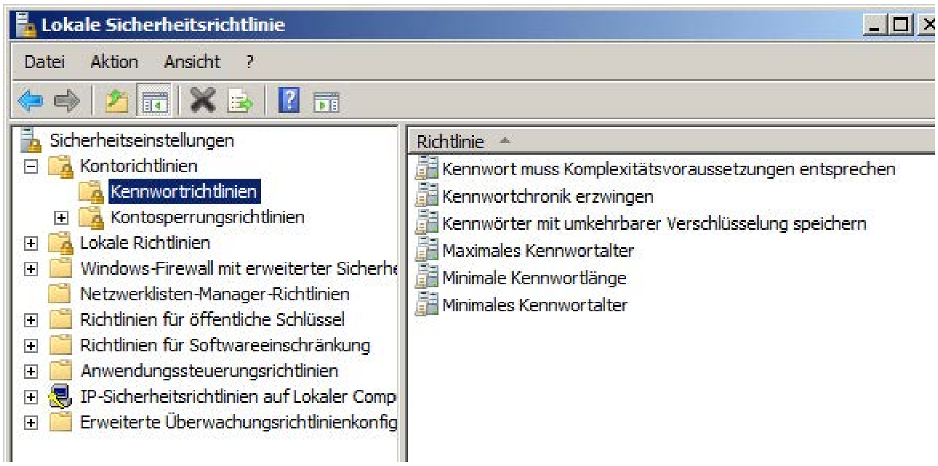
- Password aging
  Passwords must be changed at regular intervals (every 6 months at the latest).
- Minimum complexity
  A password must meet minimum complexity standards, i.e. it should meet the following requirements:
  - Minimum length of 8 characters
  - At least 2 alphanumeric characters (upper/lower case letters), at least 1 number and special character
- 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 the "Windows 7" operating system.

To implement the password policies, follow these steps:

1. Open the Windows Start menu and type "secpol.msc" in the search box.
   The "secpol.msc" application is displayed in the results.
2. Click on the "secpol.msc" application in the results.
   Enter the administrator password, if required. If you are already logged on as an administrator, confirm the execution of the application.
   The "Local Security Policy" dialog opens.
3. Select "Account Policies> Password Policy" in the left navigation pane of the "Local Security Policy" dialog.
   The password rules are displayed.



- Sicherheitseinstellungen
  - Kontorichtlinien
    - Kennwortrichtlinien
    - Kontosperrungsrichtlinien
  - Lokale Richtlinien
  - Windows-Firewall mit erweiterter Sicherhe
  - Netzwerklisten-Manager-Richtlinien
  - Richtlinien für öffentliche Schlüssel
  - Richtlinien für Softwareeinschränkung
  - Anwendungssteuerungsrichtlinien
  - IP-Sicherheitsrichtlinien auf Lokaler Comp
  - Erweiterte Überwachungsrichtlinienkonfig

Richtlinie

- Kennwort muss Komplexitätsvoraussetzungen entsprechen
- Kennwortchronik erzwingen
- Kennwörter mit umkehrbarer Verschlüsselung speichern
- Maximales Kennwortalter
- Minimale Kennwortlänge
- Minimales Kennwortalter

4. Make the required settings for the following policies:

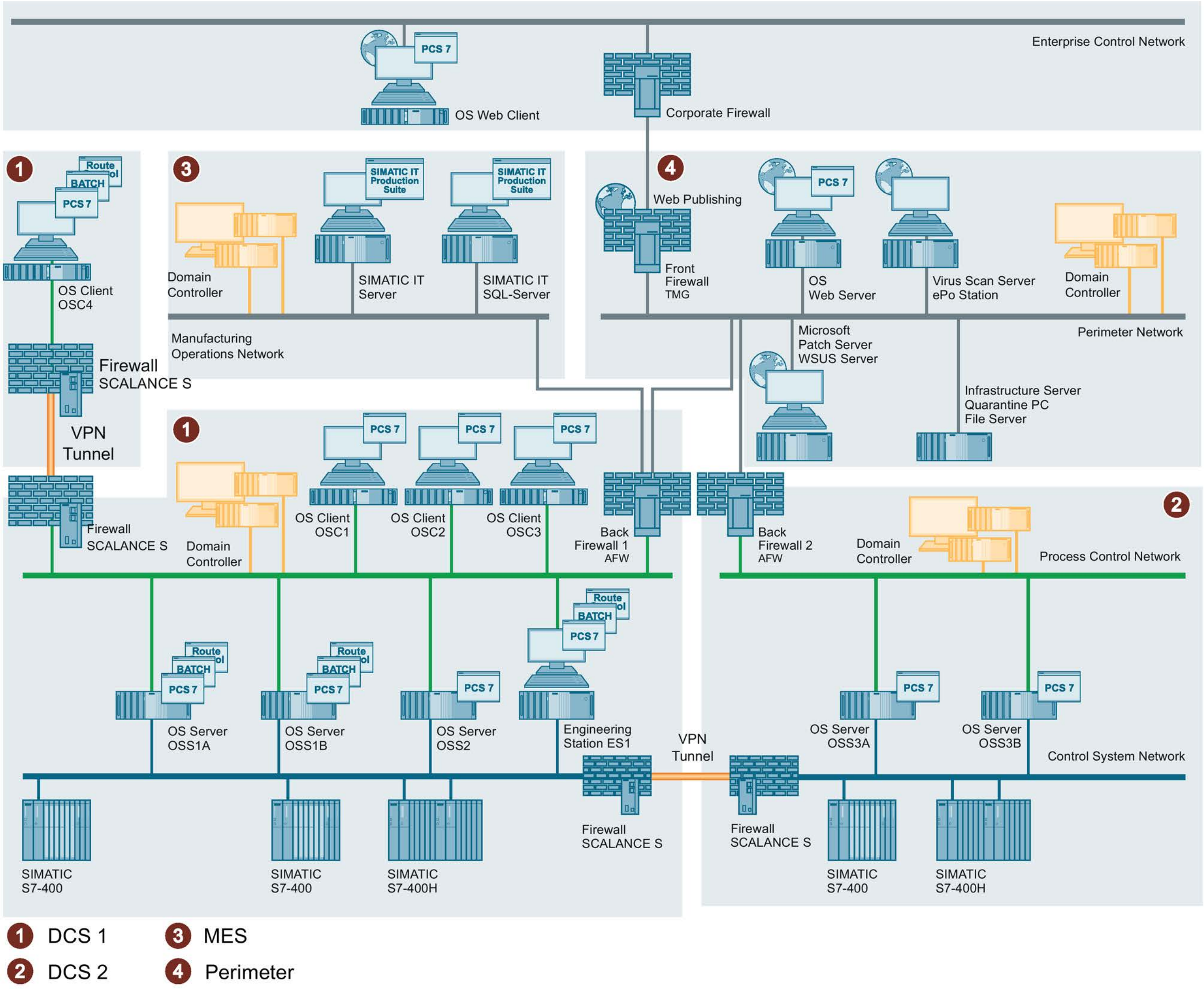
Policy	Purpose
Enforce password history	Prevents users from creating a new password that is the same as their current password or one recently used. The value "1", for example, means that only the last password is prevented as a new password. The value "5", for example, means that only the last five 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: • At least 6 characters. • It must consist of uppercase and lowercase letters, numbers and special characters. • It may not contain the user name.

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 PCS 7 security cell (terminal bus/PCN; in sample configuration cells 1 and 2) is recommended. If multiple subnets/security cells are present, at least one domain controller must also be provided there, depending on requirements.

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.

Preparations

A computer with one of the following operating systems can be used as a domain controller:

- Windows Server 2008 R2 SP1 (Standard Edition)
- Windows Server 2012 R2 Update (Standard Edition)

Note

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

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 https://support.microsoft.com/en-us/kb/272294.

The so-called teaming of network adapters should be avoided.

If a redundant terminal bus (PCN) via PRP/SIMATIC NET SOFTNET-IE RNA is used, the domain controller must be connected to a SCALANCE X204RNA. 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

Note

When an IPC bundle system is used as hardware for the domain controller, the A1 Image (Restore DVD) of a server bundle must be used for the operating system installation.

Procedure

The following points must be observed:

- Domain controllers should be fully installed and configured before starting the overall setup of PCS 7 (before adding the first PCS 7 system to the domain).
- The installation should be carried out with actual settings (for host name, IP address, subnet mask, etc.).
- The first computer should not be added until 24 hours after installation and configuration of the domain to allow all domain controllers to fully synchronize. The event logs on the domain controllers should be checked prior to adding the first PCS 7 computer to the new domain. If problems are detected, the errors should be resolved beforehand.

Computer name of the domain controller

To set the computer name, proceed as described in the section "Computer name (Page 26)".

Static IP address

The domain controllers must be provided with a static (fixed) IP address. Follow the procedure described in the section "Example configuration: Setting of IP addresses and subnet mask (Page 23)".

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)

There are different ways to start installation of a server. The procedure described in this section is recommended.

Note

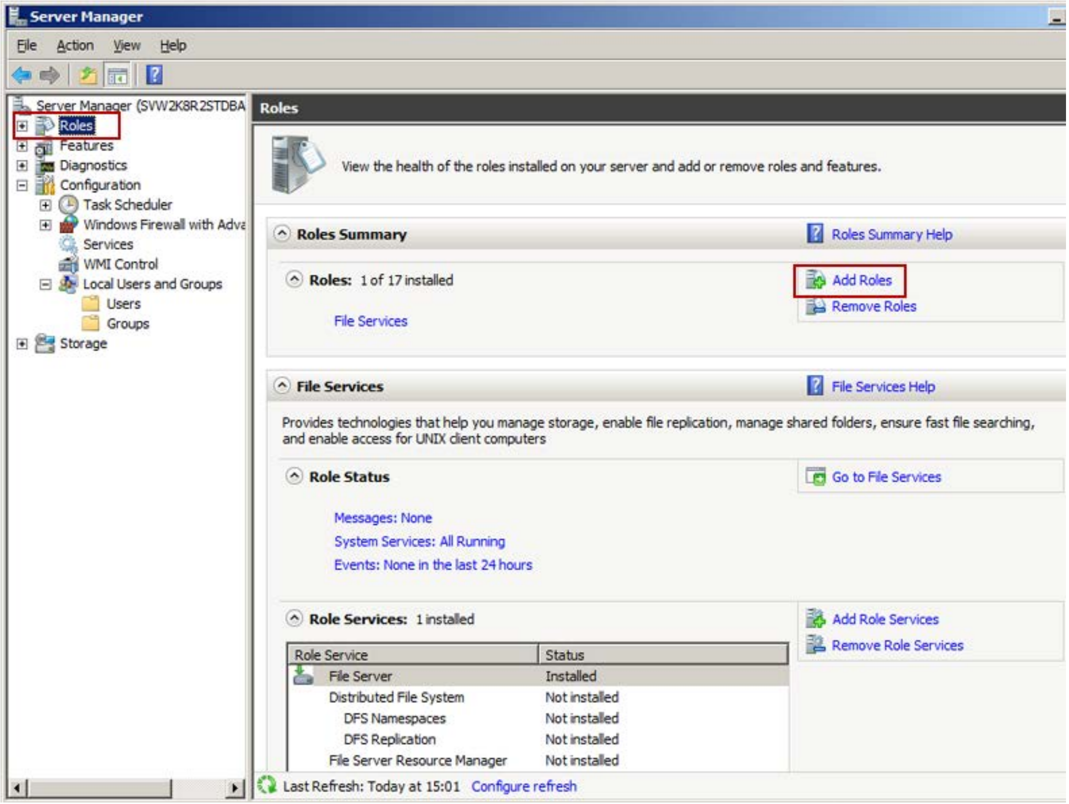
The procedure is described using the Windows Server 2008 R2 operating system and English language setting as an example. It sets up a new domain in a new forest.

You can find information about Windows Server 2012 R2 at https://technet.microsoft.com/en-US/library/hh472162.aspx#BKMK_GUI.

7.5.1.1 Installing the "Active Directory Domain Services" role

Procedure

1. Logon to the system as a local administrator and
   click "Start > Administrative Tools > Server Manager".
   The Server Manager opens.
2. In the navigation window, select "Roles" and click the "Add Roles" button to add a new role.



View the health of the roles installed on your server and add or remove roles and features.

Roles: 1 of 17 installed

File Services

File Services

Provides technologies that help you manage storage, enable file replication, manage shared folders, ensure fast file searching, and enable access for UNIX client computers

Role Status

Messages: None
System Services: All Running
Events: None in the last 24 hours

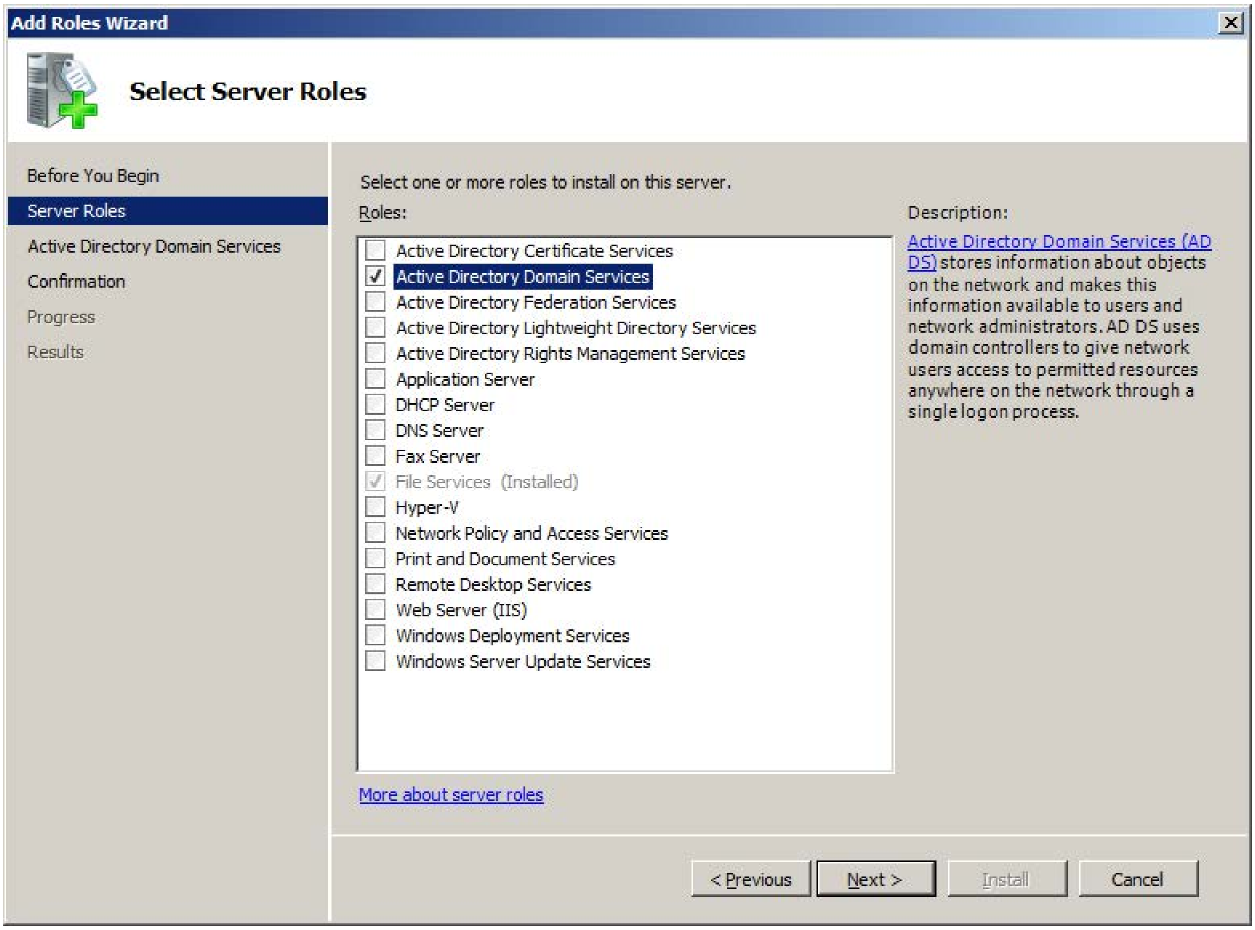
Role Services: 1 installed

Role Service	Status
File Server	Installed
Distributed File System	Not installed
DFS Namespaces	Not installed
DFS Replication	Not installed
File Server Resource Manager	Not installed

Last Refresh: Today at 15:01

The "Add Roles" wizard opens.

3. Click "Next" in the first dialog.
4. In the "Select Server Roles" dialog, select the "Active Directory Domain Services" option (AD DS) and click "Next".



Select one or more roles to install on this server.

Roles:

- □ Active Directory Certificate Services
- ☑ Active Directory Domain Services
- □ Active Directory Federation Services
- □ Active Directory Lightweight Directory Services
- □ Active Directory Rights Management Services
- □ Application Server
- □ DHCP Server
- □ DNS Server
- □ Fax Server
- ☑ File Services (Installed)
- □ Hyper-V
- □ Network Policy and Access Services
- □ Print and Document Services
- □ Remote Desktop Services
- □ Web Server (IIS)
- □ Windows Deployment Services
- □ Windows Server Update Services

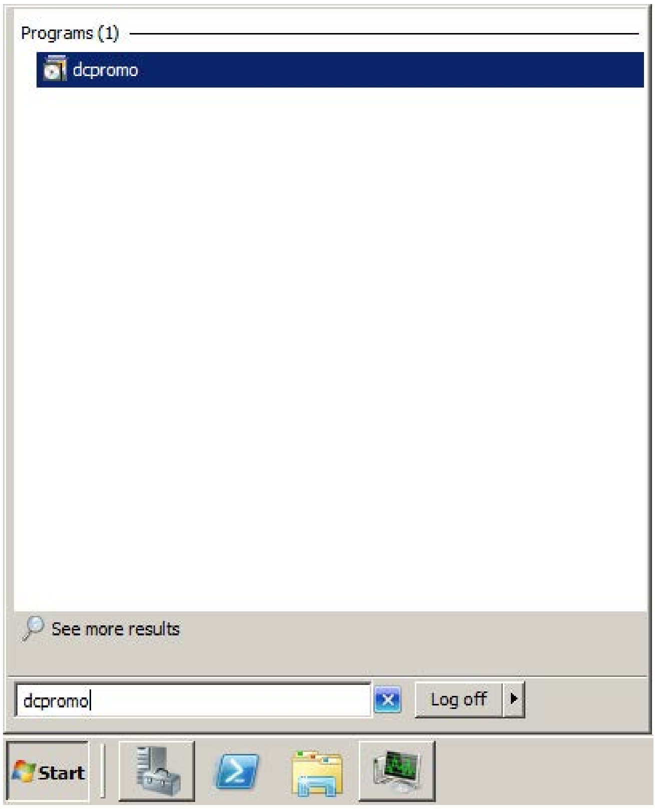
Description:

Active Directory Domain Services (AD DS) stores information about objects on the network and makes this information available to users and network administrators. AD DS uses domain controllers to give network users access to permitted resources anywhere on the network through a single logon process.

5. Use the "Next" button to navigate through other settings of the wizard. No special settings have to be made for PCS 7. The default settings can be used.
6. Click "Install" to install the role.

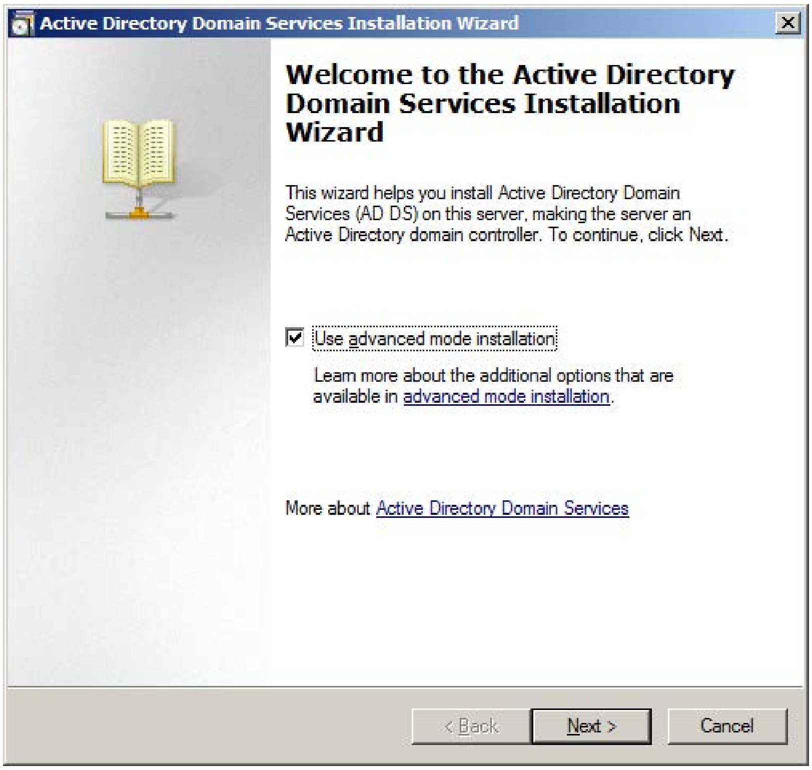
Installing and configuring Active Directory Domain Services

1. Click Start and enter the program name "dcpromo" in the "Search programs and files" text box. Confirm your entry with the Return key.



The "Active Directory Domain Services Installation Wizard" starts.

2. Select the "Use advanced mode installation" option and click "Next".



Active Directory Domain Services Installation Wizard

Welcome to the Active Directory Domain Services Installation Wizard

This wizard helps you install Active Directory Domain Services (AD DS) on this server, making the server an Active Directory domain controller. To continue, click Next.

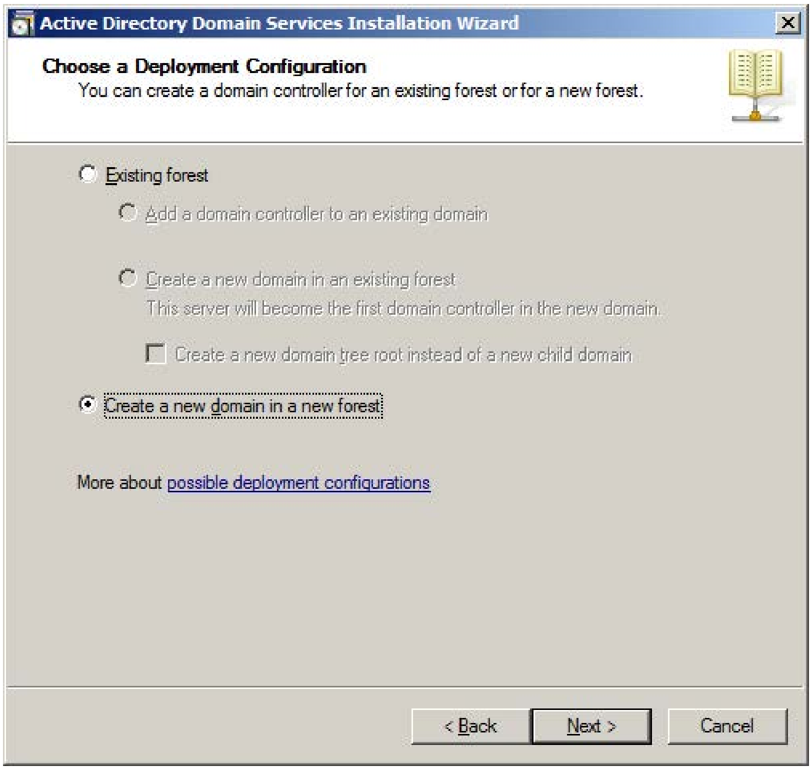
☑ Use advanced mode installation

Learn more about the additional options that are available in advanced mode installation.

More about Active Directory Domain Services

The "Choose a Deployment Configuration" dialog opens.

3. Select the "Create a new domain in a new forest" option and click "Next".



Active Directory Domain Services Installation Wizard

Choose a Deployment Configuration
You can create a domain controller for an existing forest or for a new forest.

○ Existing forest

○ Add a domain controller to an existing domain

○ Create a new domain in an existing forest
This server will become the first domain controller in the new domain.

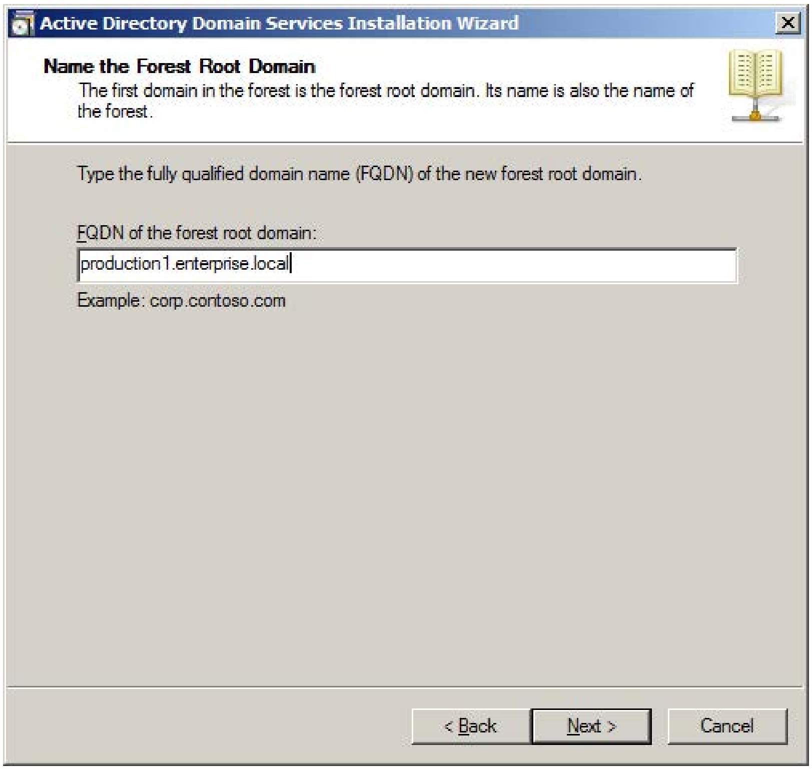
□ Create a new domain tree root instead of a new child domain

● Create a new domain in a new forest

More about possible deployment configurations

The "Name the Forest Root Domain" dialog opens.

4. Enter the fully qualified domain name (FQDN) (e.g. "production1.enterprise.local") in the "FQDN of the forest root domain:" text box and click "Next".



Name the Forest Root Domain

The first domain in the forest is the forest root domain. Its name is also the name of the forest.

Type the fully qualified domain name (FQDN) of the new forest root domain.

FQDN of the forest root domain:

production1.enterprise.local

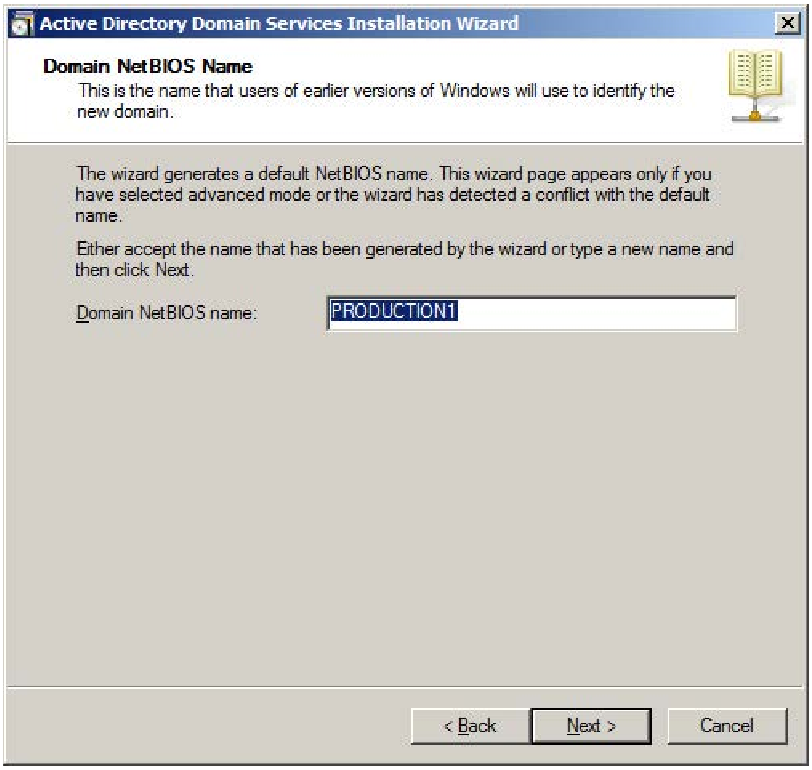
Example: corp.contoso.com

Note

The selected 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. Use of the "local" domain as the so-called top-level domain (TLD) is recommended (e.g. "example.local").

The entry is checked for plausibility. A "Domain NetBIOS Name" is suggested by the wizard. It can be used directly or changed as needed.
Then click "Next".



Domain NetBIOS Name

This is the name that users of earlier versions of Windows will use to identify the new domain.

The wizard generates a default NetBIOS name. This wizard page appears only if you have selected advanced mode or the wizard has detected a conflict with the default name.

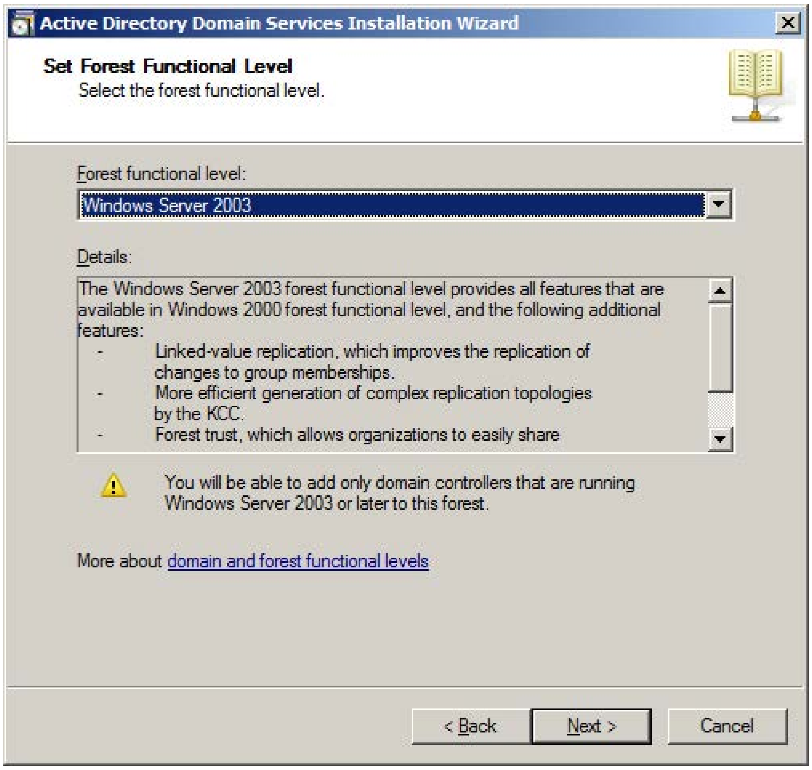
Either accept the name that has been generated by the wizard or type a new name and then click Next.

Domain NetBIOS name: PRODUCTION1

5. Select the AD DS functional level from the drop-down list in the "Set Forest Functional Level" dialog.
   When providing AD DS for the domain and forest functional levels, specify the highest value your environment supports. 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.
   You can find additional information on this at https://technet.microsoft.com/library/understanding-active-directory-functional-levels.aspx.

Note

The functional levels can be subsequently adapted in the Active Directory. However, these can only be upgraded. You can find information on this at https://technet.microsoft.com/en-us/library/cc753104(v=ws.11).aspx and https://technet.microsoft.com/en-us/library/cc730985(v=ws.11).aspx.



Active Directory Domain Services Installation Wizard

Set Forest Functional Level

Select the forest functional level.

Forest functional level: Windows Server 2003

Details:

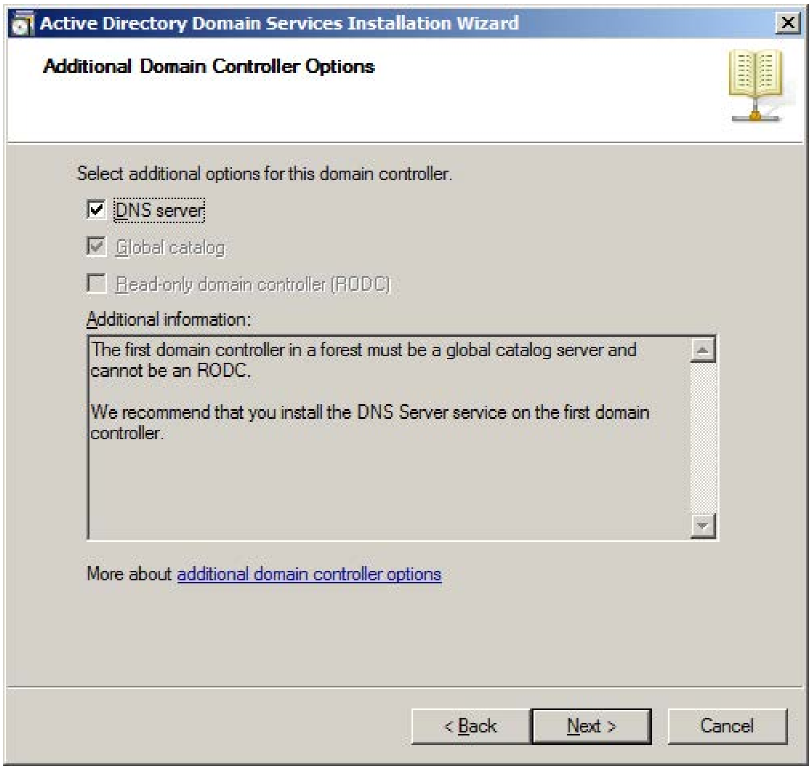
The Windows Server 2003 forest functional level provides all features that are available in Windows 2000 forest functional level, and the following additional features:
- Linked-value replication, which improves the replication of changes to group memberships.
- More efficient generation of complex replication topologies by the KCC.
- Forest trust, which allows organizations to easily share

You will be able to add only domain controllers that are running Windows Server 2003 or later to this forest.

More about domain and forest functional levels

6. Click "Next".
   The "Additional Domain Controller Options" dialog opens.

7. Select the "DNS server" option 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. Click "Next".



Active Directory Domain Services Installation Wizard

Additional Domain Controller Options

Select additional options for this domain controller.

☑ DNS server

☑ Global catalog

□ Read-only domain controller (RODC)

Additional information:

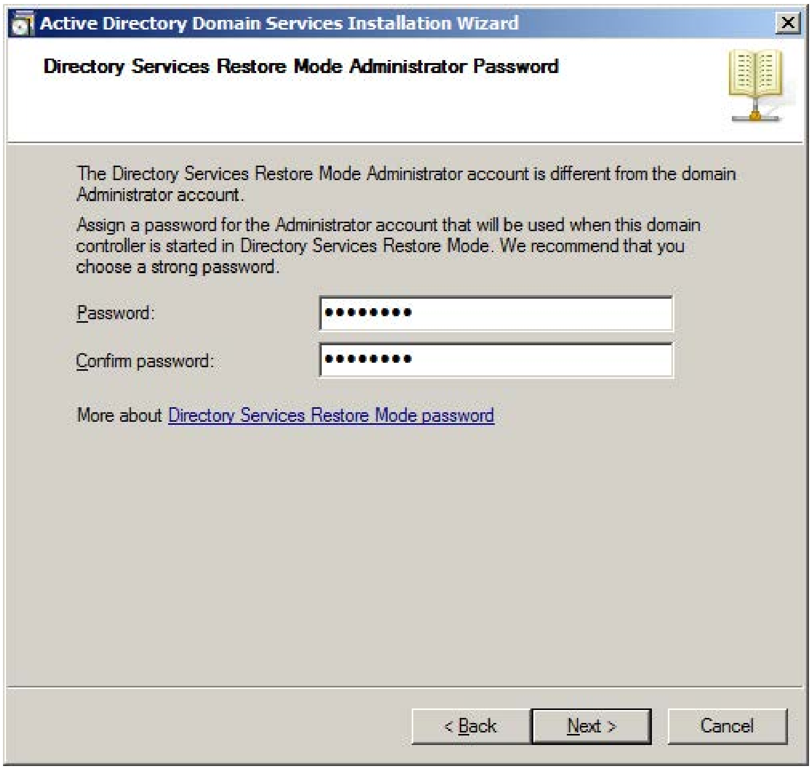
The first domain controller in a forest must be a global catalog server and cannot be an RODC.

We recommend that you install the DNS Server service on the first domain controller.

More about additional domain controller options

8. Use the "Next" button to navigate through other settings of the wizard. No special settings have to be made for PCS 7. The default settings can be used.

9. In the "Directory Services Restore Mode Administrator Password" dialog, set the password for the administrator when the domain controller is started in Directory Services Restore Mode (DSRM). This password is independent of the password used by the administrator who is logged on during installation.



Active Directory Domain Services Installation Wizard

Directory Services Restore Mode Administrator Password

The Directory Services Restore Mode Administrator account is different from the domain Administrator account.

Assign a password for the Administrator account that will be used when this domain controller is started in Directory Services Restore Mode. We recommend that you choose a strong password.

Password: ••••••••

Confirm password: ••••••••

More about Directory Services Restore Mode password

10. Use the "Next" button to navigate through other settings of the wizard. No special settings have to be made for PCS 7. The default settings can be used. The installation is then finished.

7.5.1.2 Configuration of the DNS server

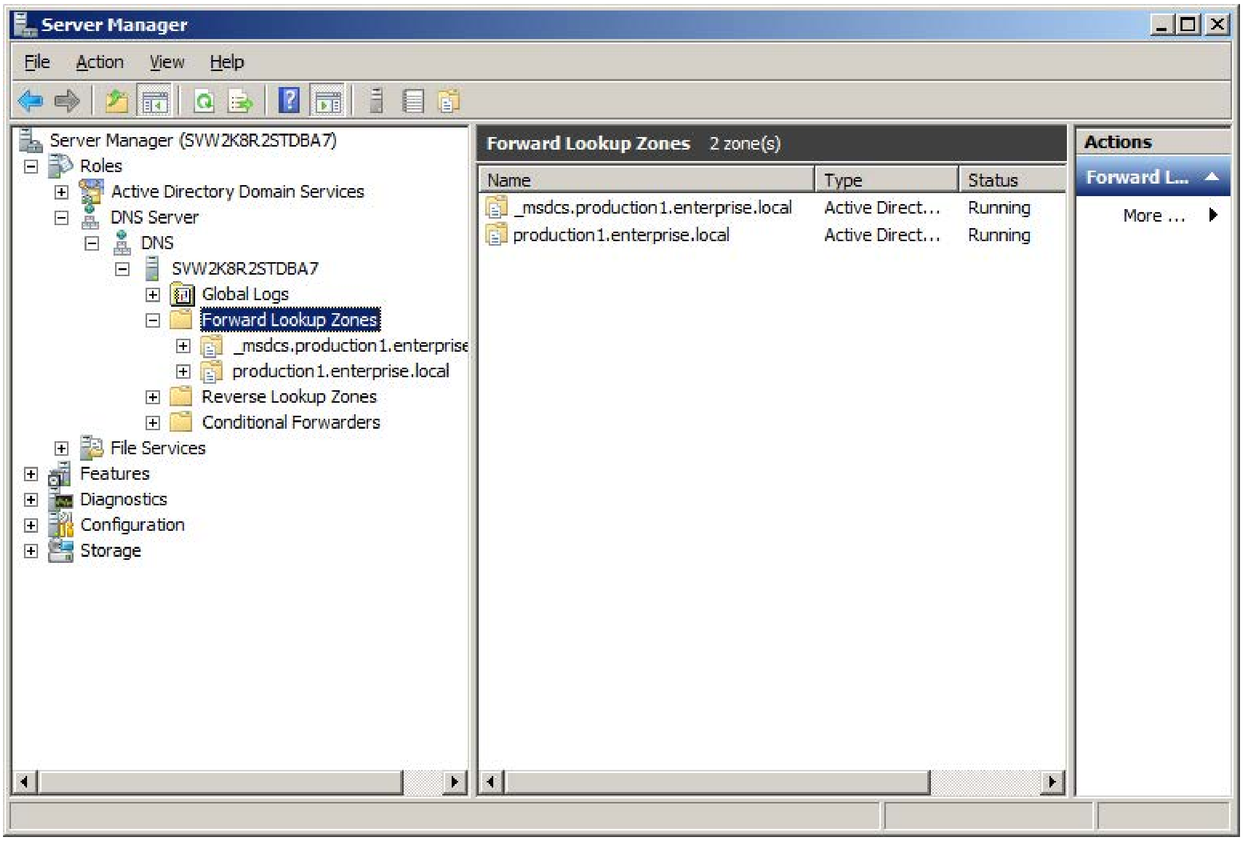
The Domain Name System (DNS) ensures that the name resolution functions correctly. This is essential for operation of an Active Directory and its member systems. For more information, see section "Name resolution (Page 26)".

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

Forward Lookup Zone

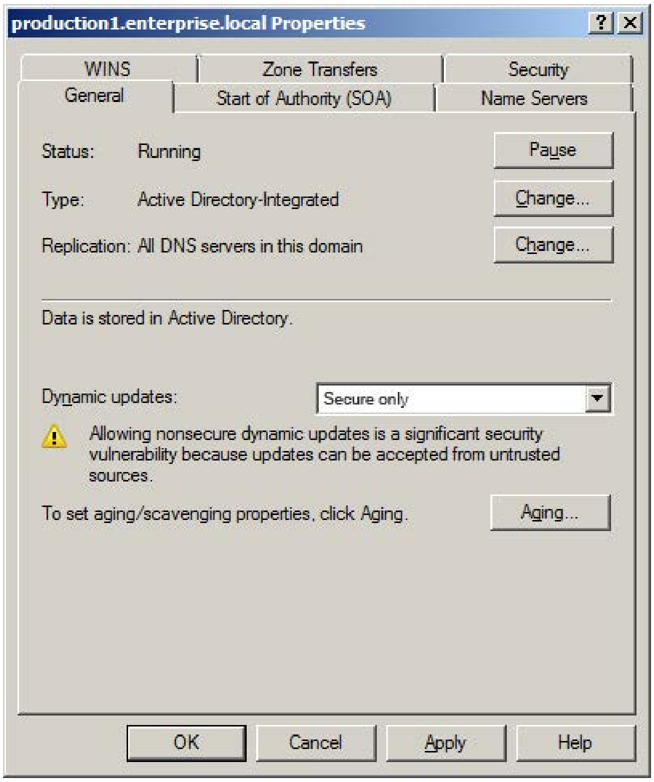
The Forward Lookup Zone is created automatically during installation of the DNS server. Ensure the settings in the Server Manager are correct.

1. Click "Start > Administrative Tools > Server Manager".
2. Open "Roles > DNS Server > DNS > '<ComputerName>' > Forward Lookup Zones" in the left navigation window.



Name	Type	Status
_msdcs.production1.enterprise.local	Active Direct...	Running
production1.enterprise.local	Active Direct...	Running

3. Right-click on the Forward Lookup Zone that you created by entering FQDN when you installed the DNS server (in this example: production1.enterprise.local) and select the "Properties" command in the shortcut menu.
4. Select the "Secure only" option under the menu command "Dynamic updates" in the "General" tab.



Status: Running

Type: Active Directory-Integrated

Replication: All DNS servers in this domain

Data is stored in Active Directory.

Dynamic updates: Secure only

Allowing nonsecure dynamic updates is a significant security vulnerability because updates can be accepted from untrusted sources.

To set aging/scavenging properties, click Aging.

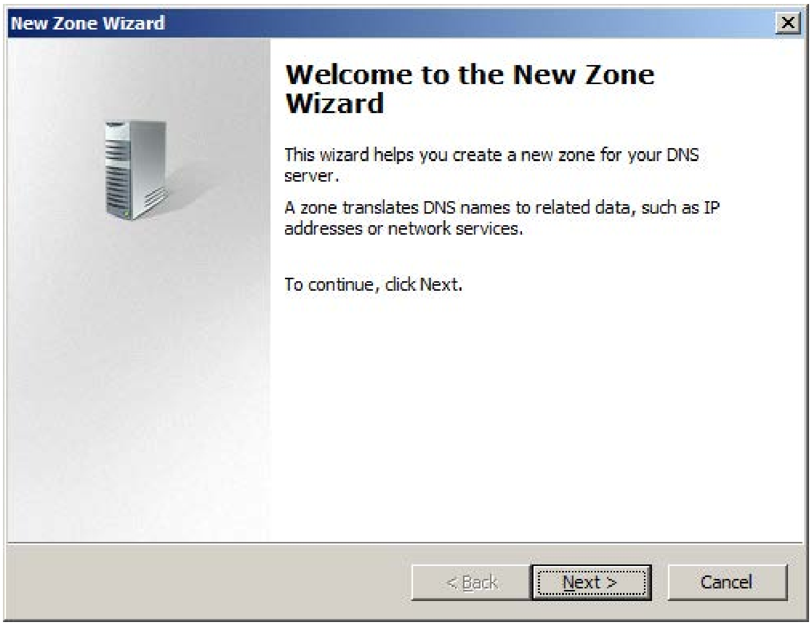
The updates that do not conform to the Microsoft standard are classified as non-secure updates. This can sometimes happen during internal domain updates (for example, internal software, profile updates, etc.). That is why this option should be selected.

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. To create it later, proceed as follows:

1. Click "Start > Administrative Tools > Server Manager".
2. Open "Roles > DNS Server > #Host name# > Reverse Lookup Zones" in the left navigation window.
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.



New Zone Wizard

Welcome to the New Zone Wizard

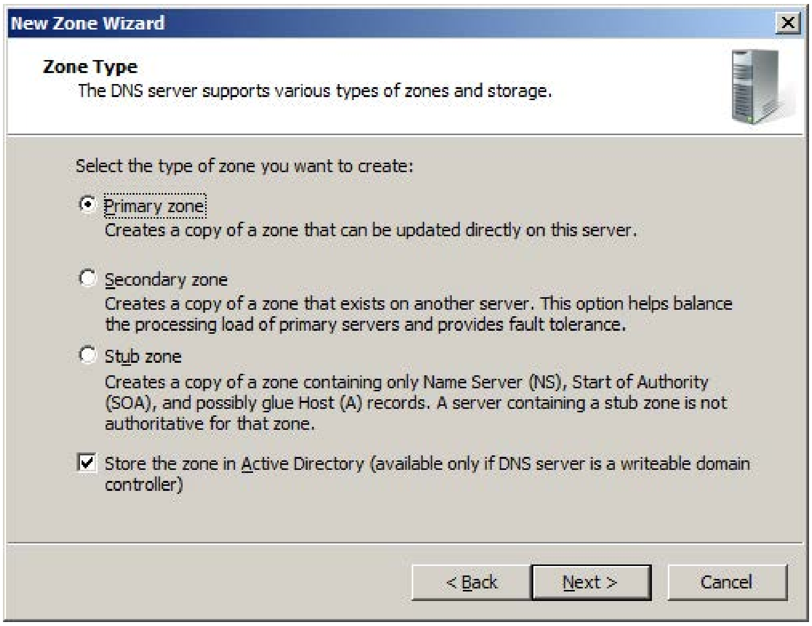
This wizard helps you create a new zone for your DNS server.

A zone translates DNS names to related data, such as IP addresses or network services.

To continue, click Next.

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".



Zone Type

The DNS server supports various types of zones and storage.

Select the type of zone you want to create:

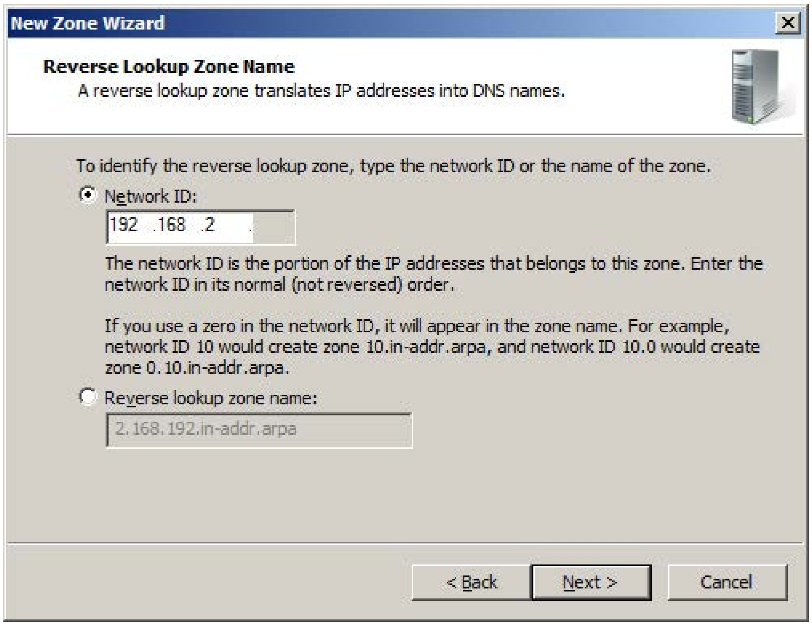
● Primary zone
Creates a copy of a zone that can be updated directly on this server.

○ Secondary zone
Creates a copy of a zone that exists on another server. This option helps balance the processing load of primary servers and provides fault tolerance.

○ Stub zone
Creates a copy of a zone containing only Name Server (NS), Start of Authority (SOA), and possibly glue Host (A) records. A server containing a stub zone is not authoritative for that zone.

☑ Store the zone in Active Directory (available only if DNS server is a writeable domain controller)

6. In the "Reverse Lookup Zone Name" dialog, select the "Network ID" option and enter an appropriate IP address (192.168.2 in this example). Click "Next".



Reverse Lookup Zone Name

A reverse lookup zone translates IP addresses into DNS names.

To identify the reverse lookup zone, type the network ID or the name of the zone.

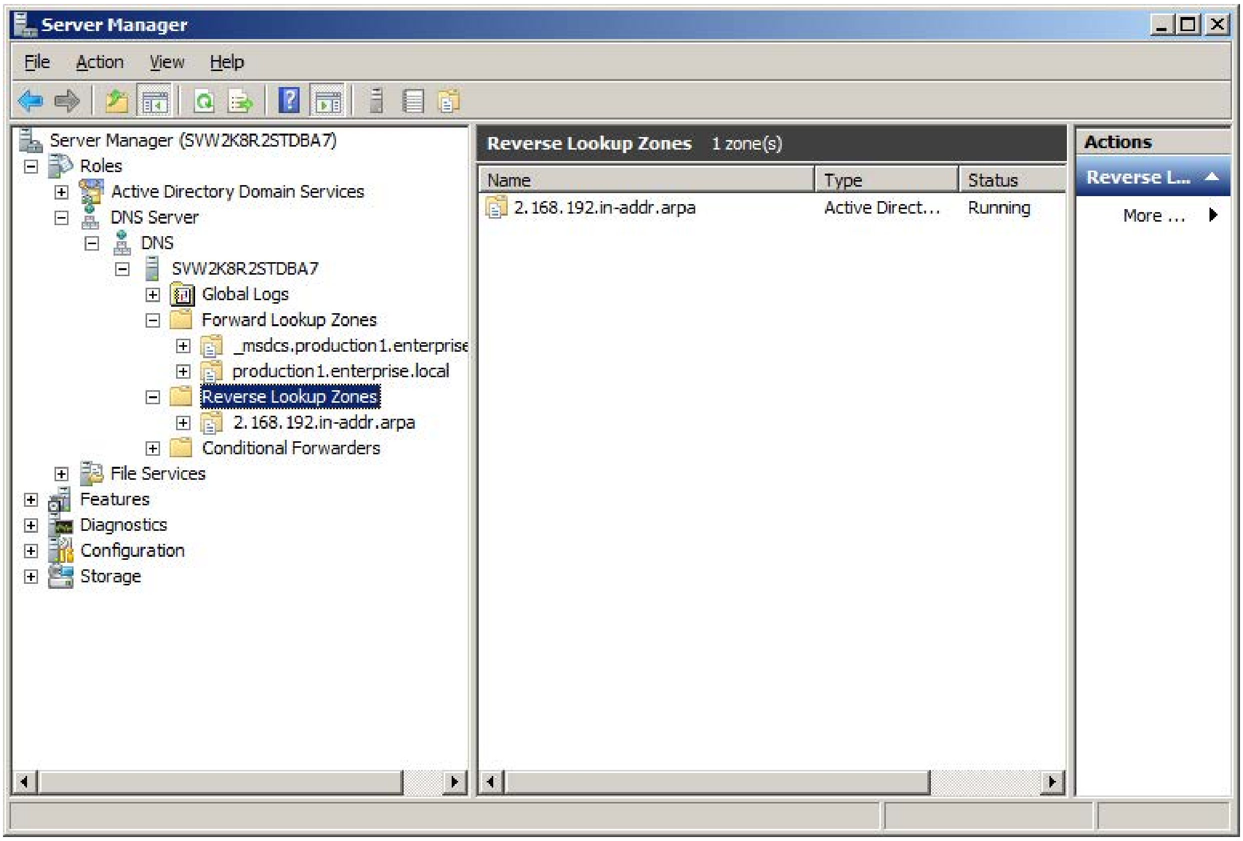
● Network ID:
192 .168 .2 .

The network ID is the portion of the IP addresses that belongs to this zone. Enter the network ID in its normal (not reversed) order.

If you use a zero in the network ID, it will appear in the zone name. For example, network ID 10 would create zone 10.in-addr.arpa, and network ID 10.0 would create zone 0.10.in-addr.arpa.

○ Reverse lookup zone name:
2.168.192.in-addr.arpa

7. Select the "Secure only" option in the "Dynamic Update" dialog (see Forward Lookup Zone) and check the setting in the "Name Server" tab. Confirm the entry with "Next".
   The new Reverse Lookup Zone is created and displayed in the Server Manager under Roles – DNS Server.



Reverse Lookup Zones 1 zone(s)

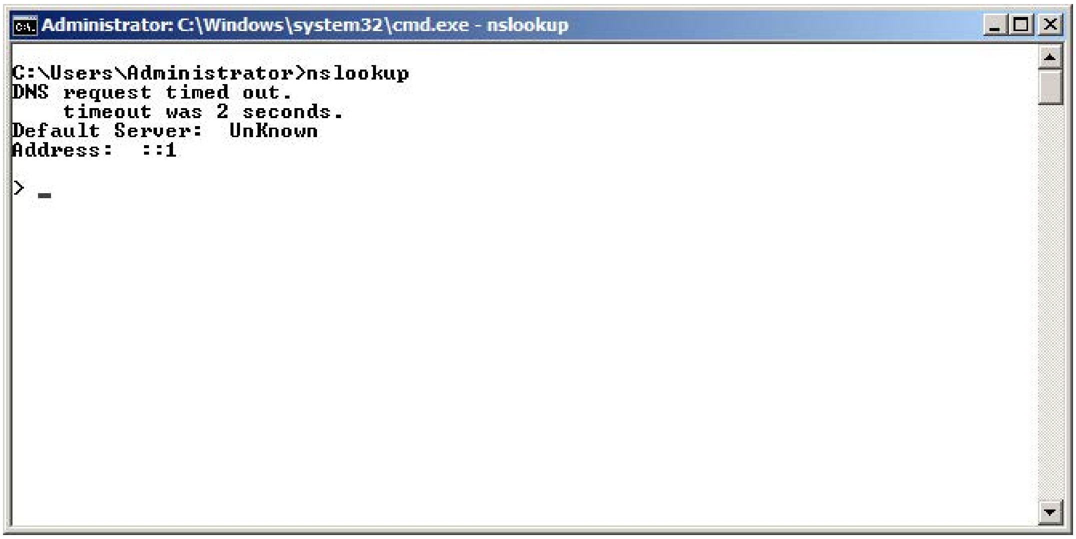
Name	Type	Status
2.168.192.in-addr.arpa	Active Direct...	Running

8. Check in the zone settings on the "Name Servers" tab to determine whether DC1 including its IP address is configured. Add this system if necessary.

Additional settings and checking the DNS name resolution

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

1. Open a command prompt window (cmd) and enter the command "nslookup".

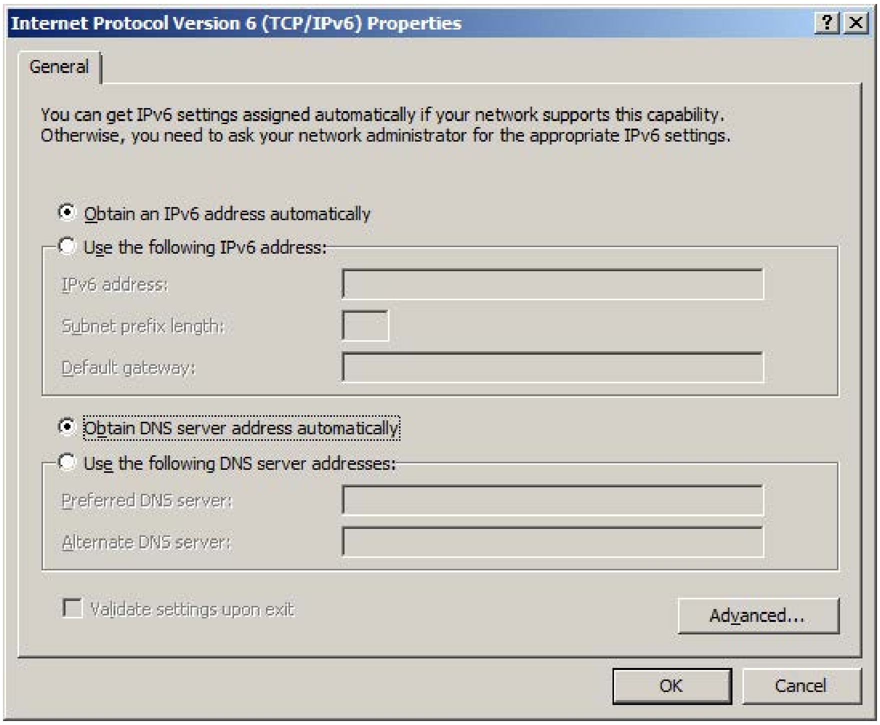


```
C:\Users\Administrator>nslookup
DNS request timed out.
    timeout was 2 seconds.
Default Server:  UnKnown
Address:  ::1

> _
```

   The response to the "nslookup" command indicates that the server is attempting to resolve the DNS name via the IPv6 protocol.

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. In this properties dialog, select the "Obtain DNS server address automatically" option and confirm your entry with "OK".



You can get IPv6 settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IPv6 settings.

● Obtain an IPv6 address automatically
○ Use the following IPv6 address:

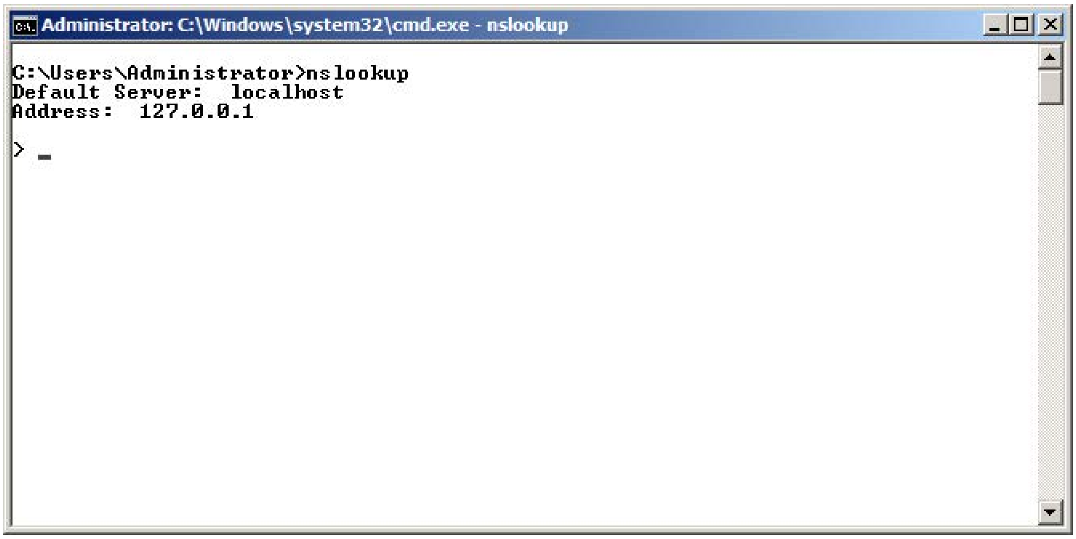
IPv6 address:
Subnet prefix length:
Default gateway:

● Obtain DNS server address automatically
○ Use the following DNS server addresses:

Preferred DNS server:
Alternate DNS server:

□ Validate settings upon exit

3. Go to the command prompt and enter the "nslookup" command again.



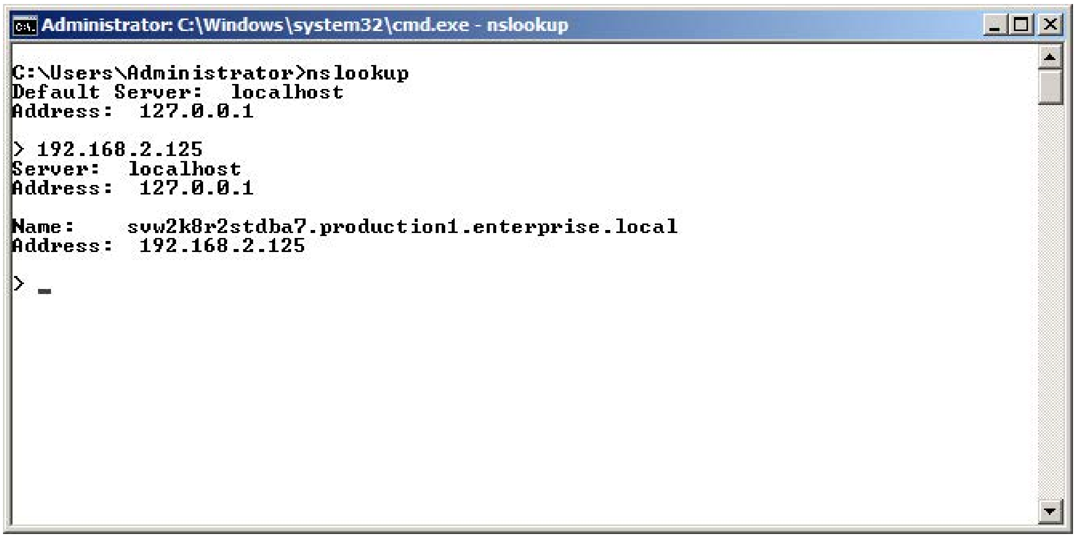
Administrator: C:\Windows\system32\cmd.exe - nslookup

```
C:\Users\Administrator>nslookup
Default Server:  localhost
Address:  127.0.0.1

> _
```

From the output of the address (127.0.0.1 = localhost), 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 (svw2k8r2stdba7.production1.enterprise.local, corresponds to DC1) and the IP address are output.



Administrator: C:\Windows\system32\cmd.exe - nslookup

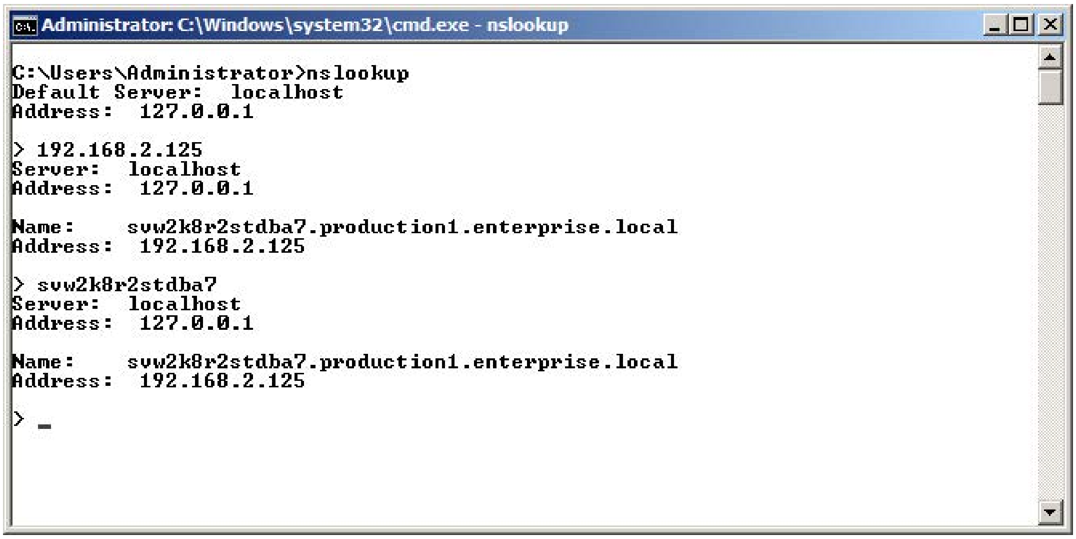
```
C:\Users\Administrator>nslookup
Default Server:  localhost
Address:  127.0.0.1

> 192.168.2.125
Server:  localhost
Address:  127.0.0.1

Name:    svw2k8r2stdba7.production1.enterprise.local
Address:  192.168.2.125

> _
```

If you enter the host name, the host name and IP address also appear.



```
C:\Users\Administrator>nslookup
Default Server:  localhost
Address:  127.0.0.1

> 192.168.2.125
Server:  localhost
Address:  127.0.0.1

Name:    svw2k8r2stdba7.production1.enterprise.local
Address:  192.168.2.125

> svw2k8r2stdba7
Server:  localhost
Address:  127.0.0.1

Name:    svw2k8r2stdba7.production1.enterprise.local
Address:  192.168.2.125

> _
```

This successfully completes the function test of the DNS server on the first domain controller.

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	192.168.2.125
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 further procedure is then identical for both of the above-indicated possibilities and is described below based on a Windows Server 2008 R2 operating system.

1. Log onto the new domain controller to be installed as a domain administrator.
2. Open the Server Manager.
3. Click "Start > Administrative Tools > Server Manager".
4. Use the "Add Roles" button and the "Add Roles Wizard" that subsequently starts to add the "Active Directory Domain Services" role (AD DS) (see "Installation and configuration of the first domain controller (DC1) (Page 138)").
5. Start the configuration with "dcpromo" (as you did for the first domain controller).
   The Active Directory Domain Services Installation Wizard starts.
6. In the "Choose a Deployment Config" dialog, select the "Add a domain controller to an existing domain" option and click "Next".
7. Enter the FQDN "production1.enterprise.local" in the text box of the "Network Credentials" dialog. Select "My Current Logged On Credentials" for the account credentials.
8. 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 138)).
9. In the DNS server zone settings, the newly installed DCs with activated DNS role must be added or existing DNS servers must be supplemented in each case on all DCs on the "Name Servers" tab.

7.5.3 Check of network settings on the DCs

After completion of the domain controller installation, the network settings must be checked on all domain controller systems.

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 the two domain controllers in security cell DCS1 must be made for the sample configuration:

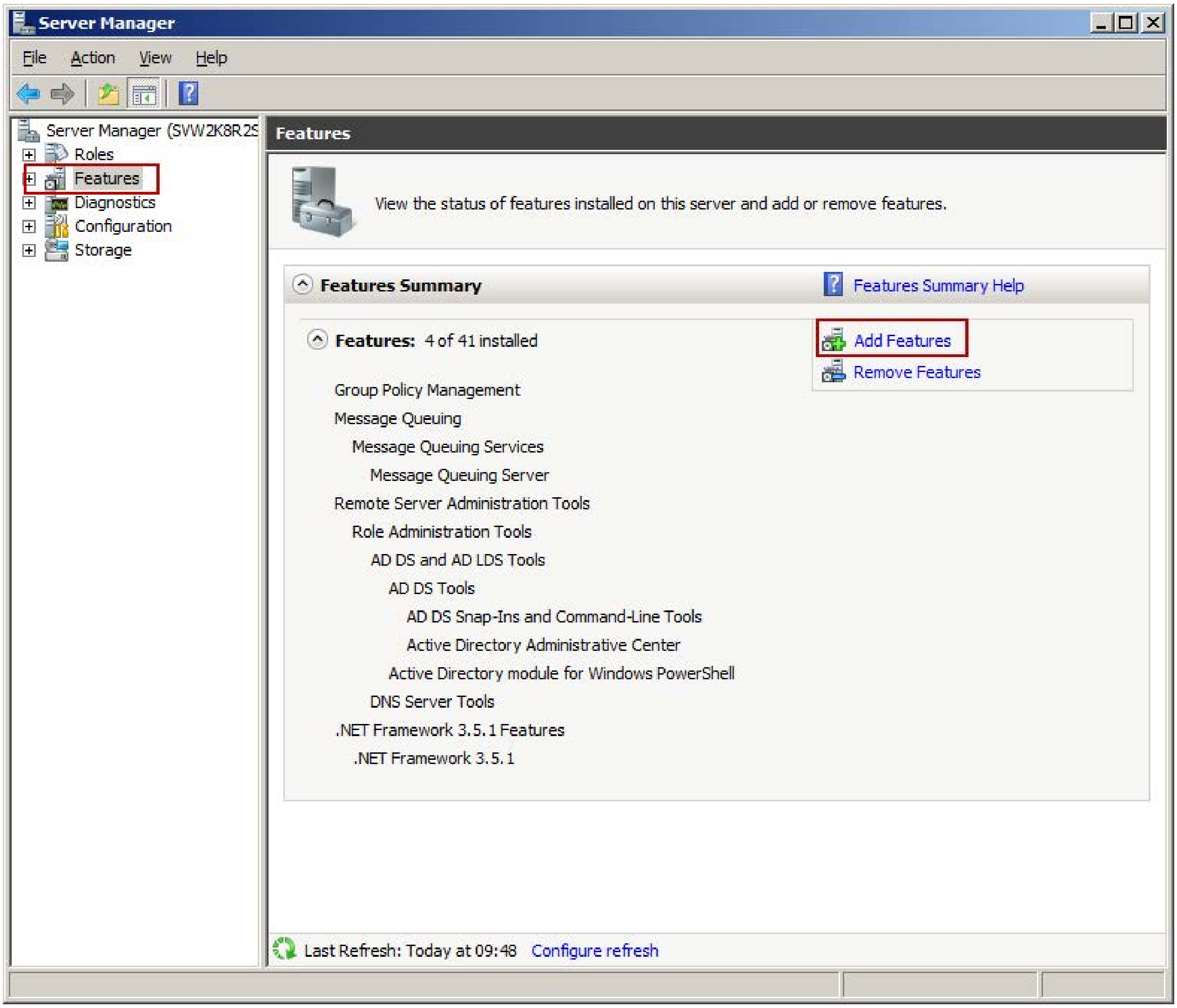
	Domain Controller 1 (DC1)	**Domain Controller 2 (DC2)**
IP address	192.168.2.125	92.168.2.126
Subnet mask	255.255.255.192	255.255.255.192
Standard gateway	192.168.2.65	192.168.2.65
Preferred DNS server	127.0.0.1	127.0.0.1
	192.168.2.126	192.168.2.125
FQDN	DC1.production1.enterprise.local	DC2.production1.enterprise.local

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 PCS 7 and can be implemented in a domain environment by installing WINS on the domain controllers. This enables name resolution across subnet boundaries.

7.5.4.1 WINS installation

1. Open the Server Manager with "Start > Administrative Tools > Server Manager".
2. In the left pane, click on "Features" and then on "Add Features" under "Features Summary" in the right pane.



View the status of features installed on this server and add or remove features.

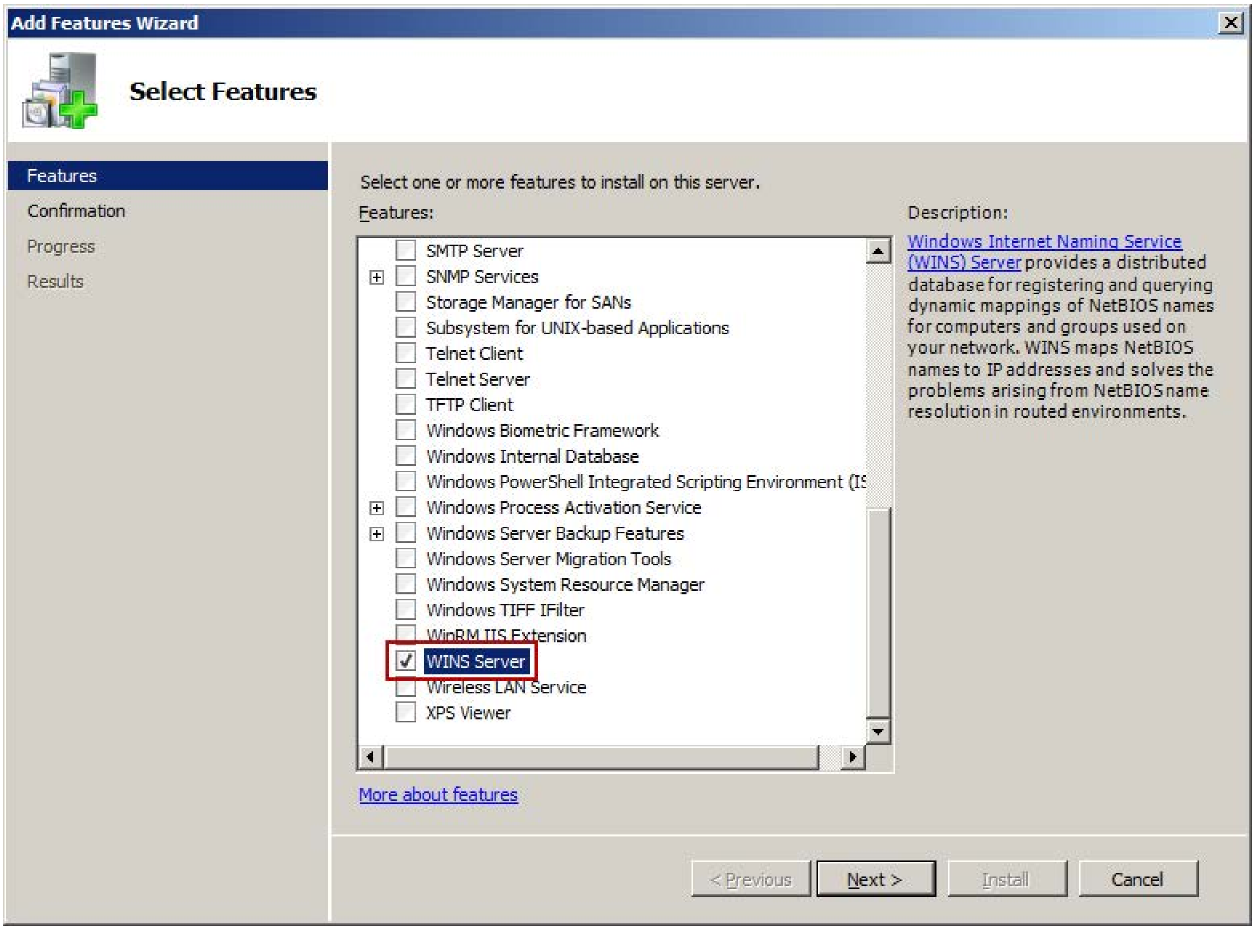
Features: 4 of 41 installed

Group Policy Management
Message Queuing
Message Queuing Services
Message Queuing Server
Remote Server Administration Tools
Role Administration Tools
AD DS and AD LDS Tools
AD DS Tools
AD DS Snap-Ins and Command-Line Tools
Active Directory Administrative Center
Active Directory module for Windows PowerShell
DNS Server Tools
.NET Framework 3.5.1 Features
.NET Framework 3.5.1

Last Refresh: Today at 09:48

The "Add Features Wizard" dialog opens.

3. In the "Select Features" dialog, select the "WINS Server" feature and click "Next".



Select one or more features to install on this server.

Features:

- □ SMTP Server
- □ SNMP Services
- □ Storage Manager for SANs
- □ Subsystem for UNIX-based Applications
- □ Telnet Client
- □ Telnet Server
- □ TFTP Client
- □ Windows Biometric Framework
- □ Windows Internal Database
- □ Windows PowerShell Integrated Scripting Environment (IS
- □ Windows Process Activation Service
- □ Windows Server Backup Features
- □ Windows Server Migration Tools
- □ Windows System Resource Manager
- □ Windows TIFF IFilter
- □ WinRM IIS Extension
- ☑ WINS Server
- □ Wireless LAN Service
- □ XPS Viewer

Description:

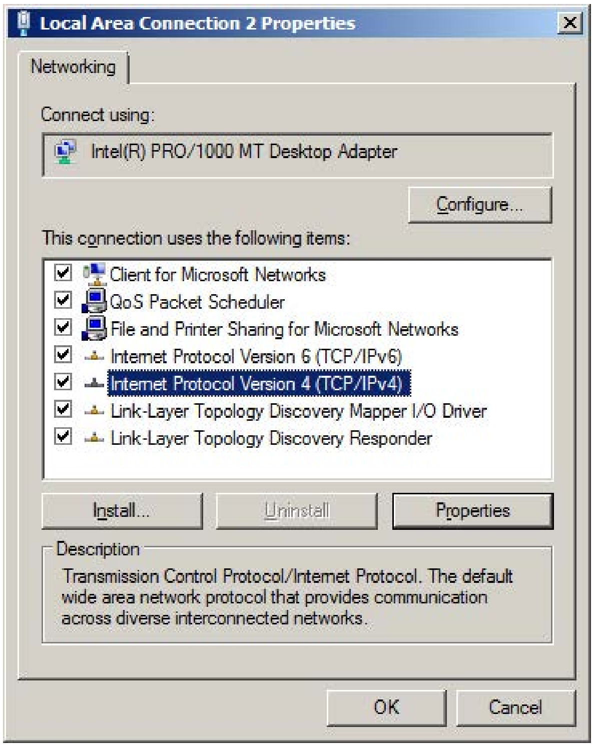
Windows Internet Naming Service (WINS) Server provides a distributed database for registering and querying dynamic mappings of NetBIOS names for computers and groups used on your network. WINS maps NetBIOS names to IP addresses and solves the problems arising from NetBIOS name resolution in routed environments.

4. Click "Install" in the subsequent "Confirm Installation Selections" dialog.
   The installation of the "WINS Server" feature is started.
5. Use the "Close" button to close the "Installation Results" dialog.
   This completes the installation of the WINS server

7.5.4.2 Entering the WINS server in the IPv4 configuration

After installation, the WINS server must be entered in the properties of the IPv4 configuration for all computers in the network.

1. To do so, open the "Properties" dialog of the network connection.



Local Area Connection 2 Properties

Networking

Connect using:

Intel(R) PRO/1000 MT Desktop Adapter

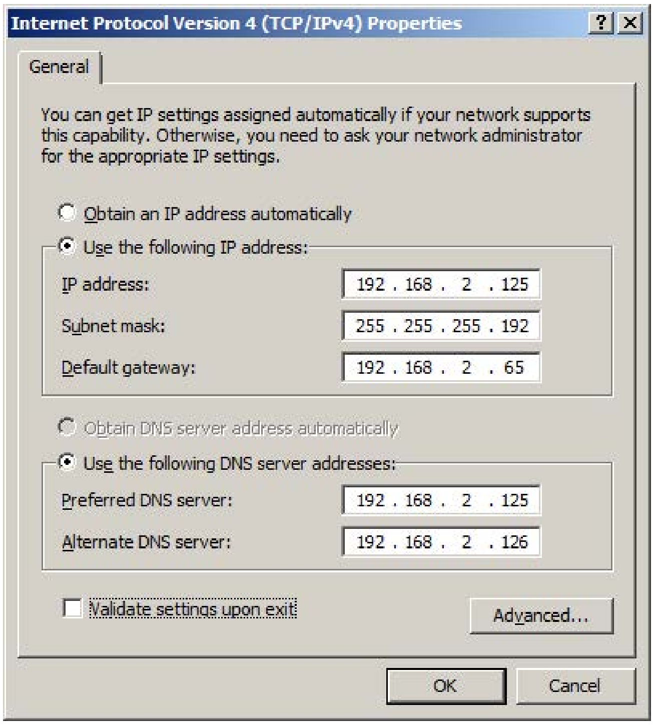
This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

2. Select the "Internet Protocol Version 4 (TCP/IPv4)" from the list and click the "Properties" button.



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address:	192 . 168 . 2 . 125
Subnet mask:	255 . 255 . 255 . 192
Default gateway:	192 . 168 . 2 . 65

○ Obtain DNS server address automatically

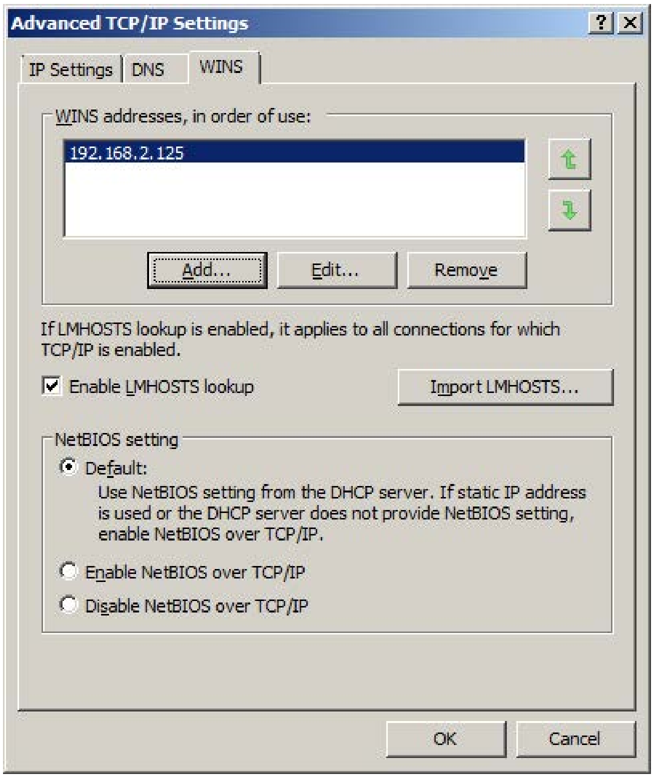
● Use the following DNS server addresses:

Preferred DNS server:	192 . 168 . 2 . 125
Alternate DNS server:	192 . 168 . 2 . 126

□ Validate settings upon exit

3. In the Properties dialog, click "Advanced…" to open the advanced TCP/IP settings.

4. In the "Advanced TCP/IP Settings" dialog, select the "WINS" tab.



Advanced TCP/IP Settings

IP Settings | DNS | WINS

WINS addresses, in order of use:

192.168.2.125

If LMHOSTS lookup is enabled, it applies to all connections for which TCP/IP is enabled.

☑ Enable LMHOSTS lookup

NetBIOS setting

● Default:
Use NetBIOS setting from the DHCP server. If static IP address is used or the DHCP server does not provide NetBIOS setting, enable NetBIOS over TCP/IP.

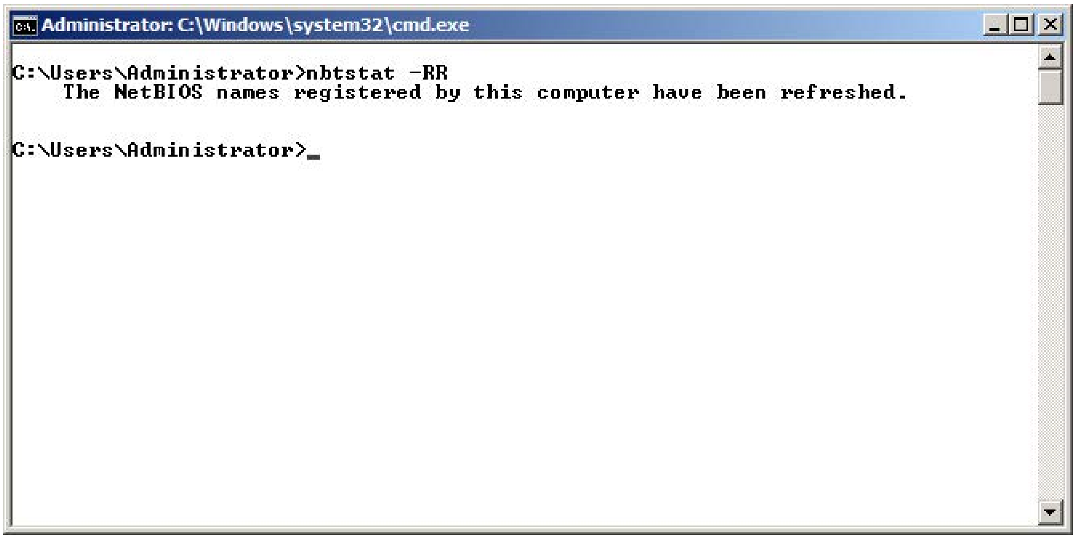
○ Enable NetBIOS over TCP/IP

○ Disable NetBIOS over TCP/IP

5. Click "Add...".
6. Add the IP addresses of the installed WINS server and close the properties dialog with "OK".

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":

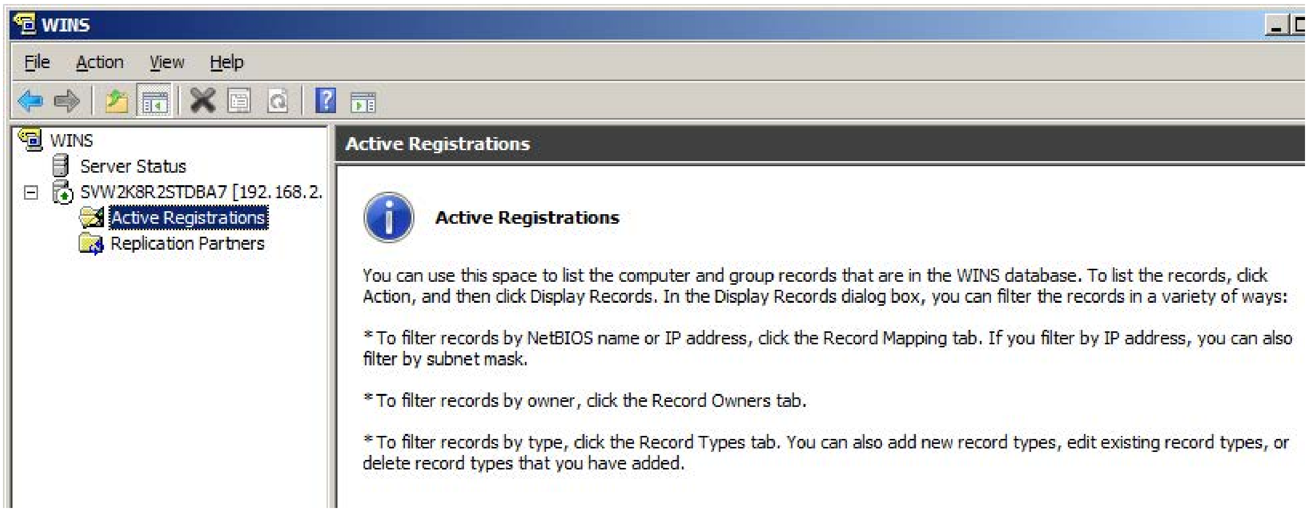


```
C:\Users\Administrator>nbtstat -RR
    The NetBIOS names registered by this computer have been refreshed.

C:\Users\Administrator>_
```

   Name release packages are sent to WINS and the update is started.

2. Open the WINS Management console with "Start > Administrative Tools > WINS".



Active Registrations

You can use this space to list the computer and group records that are in the WINS database. To list the records, click Action, and then click Display Records. In the Display Records dialog box, you can filter the records in a variety of ways:

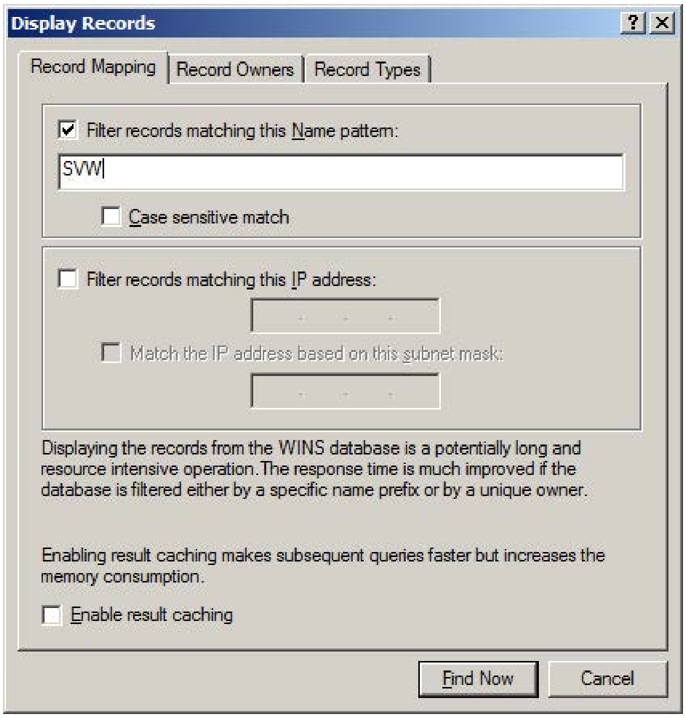
* To filter records by NetBIOS name or IP address, click the Record Mapping tab. If you filter by IP address, you can also filter by subnet mask.

* To filter records by owner, click the Record Owners tab.

* To filter records by type, click the Record Types tab. You can also add new record types, edit existing record types, or delete record types that you have added.

   The WINS Management console opens.

3. In the left pane, right-click "Active Registrations" and select the menu item "Display Records …" from the shortcut menu.



Display Records

Record Mapping | Record Owners | Record Types

☑ Filter records matching this Name pattern:

SVW

□ Case sensitive match

□ Filter records matching this IP address:

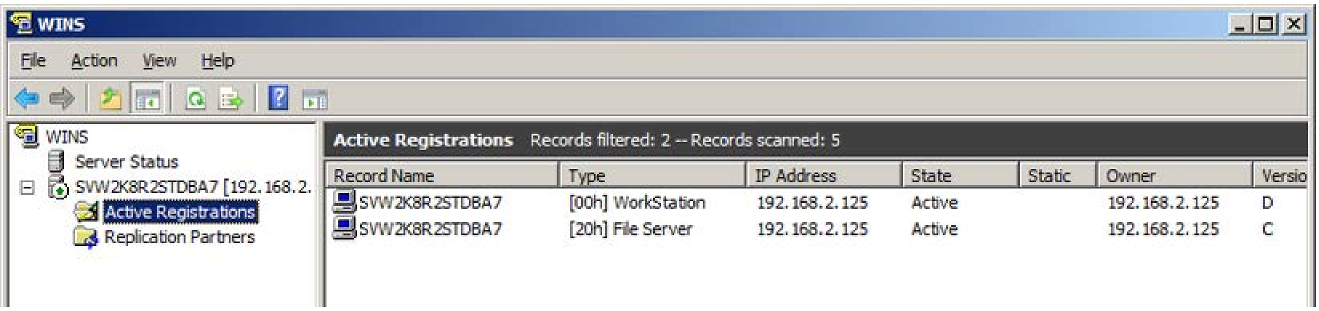
□ Match the IP address based on this subnet mask:

Displaying the records from the WINS database is a potentially long and resource intensive operation.The response time is much improved if the database is filtered either by a specific name prefix or by a unique owner.

Enabling result caching makes subsequent queries faster but increases the memory consumption.

□ Enable result caching

4. Select the "Filter records matching this Name pattern:" check box if necessary. This enables filtering according to definable criteria.
 If you want to output all entries of the WINS server, click directly on "Find Now".
 Otherwise, define a filter condition (see step 5).
5. Enter the computer name of the server (the first characters, here "SVW") and click "Find Now".
 The search result is displayed in the WINS Management console.



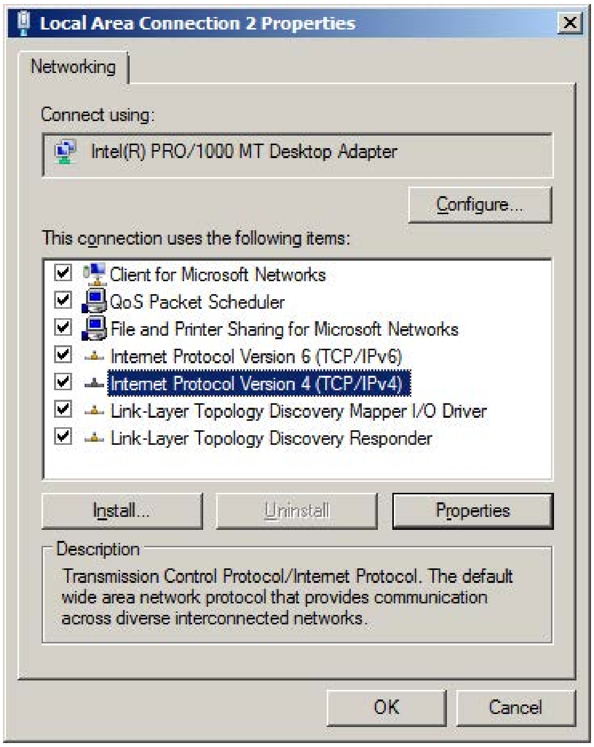
Active Registrations Records filtered: 2 -- Records scanned: 5

Record Name	Type	IP Address	State	Static	Owner	Versio
SVW2K8R2STDBA7	[00h] WorkStation	192.168.2.125	Active		192.168.2.125	D
SVW2K8R2STDBA7	[20h] File Server	192.168.2.125	Active		192.168.2.125	C

7.5.4.4 Entering additional WINS servers in the IPv4 configuration

All WINS servers should also be entered in the properties of the IPv4 configuration of the WINS clients.

1. To do so, open the Properties dialog of the network connection of all WINS clients (for example, the engineering station(s), the PCS 7 OS servers or the PCS 7 OS clients).



Local Area Connection 2 Properties

Networking

Connect using:

Intel(R) PRO/1000 MT Desktop Adapter

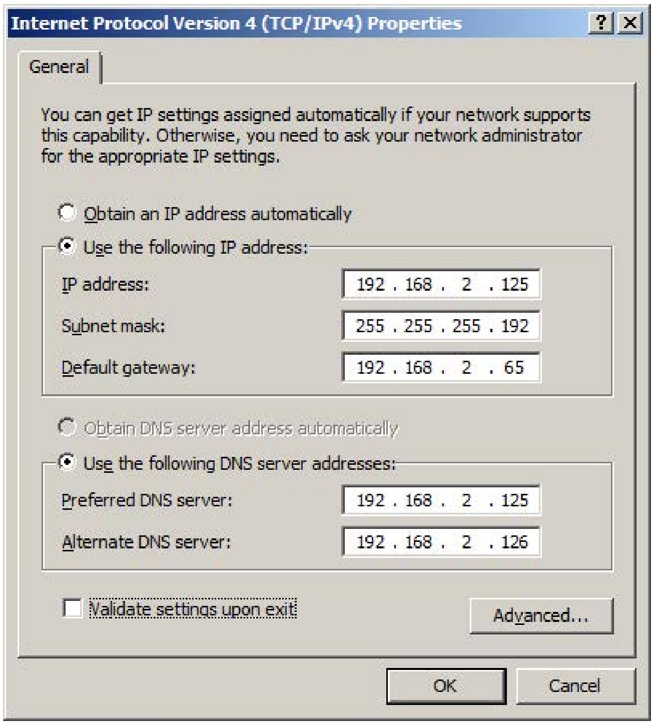
This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

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.



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 2 . 125

Subnet mask: 255 . 255 . 255 . 192

Default gateway: 192 . 168 . 2 . 65

○ Obtain DNS server address automatically

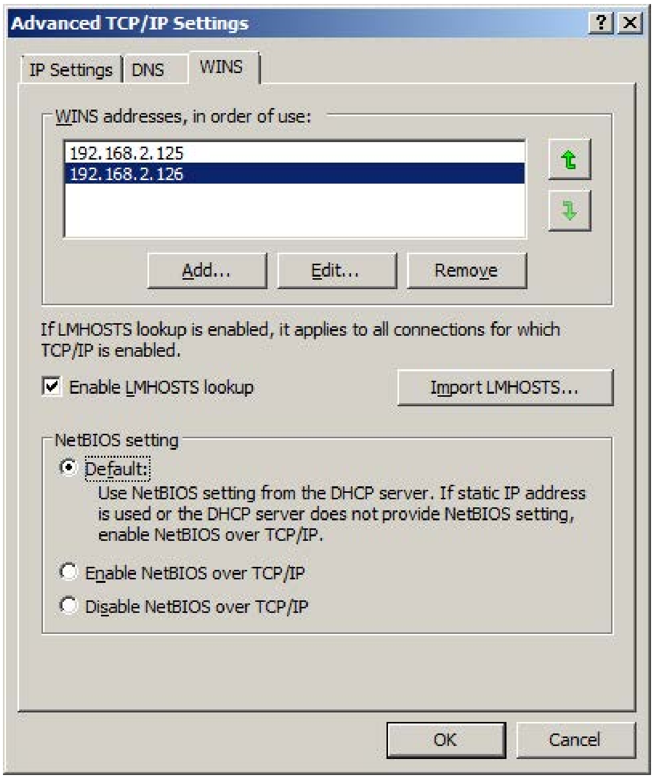
● Use the following DNS server addresses:

Preferred DNS server: 192 . 168 . 2 . 125

Alternate DNS server: 192 . 168 . 2 . 126

□ Validate settings upon exit

4. In the "Advanced TCP/IP Settings" dialog, select the "WINS" tab.
5. Click "Add" to enter the IP addresses of the WINS servers, and confirm the entries with "OK".



Advanced TCP/IP Settings

IP Settings | DNS | WINS

WINS addresses, in order of use:

192.168.2.125
192.168.2.126

Add... Edit... Remove

If LMHOSTS lookup is enabled, it applies to all connections for which TCP/IP is enabled.

☑ Enable LMHOSTS lookup   Import LMHOSTS...

NetBIOS setting

● Default:
Use NetBIOS setting from the DHCP server. If static IP address is used or the DHCP server does not provide NetBIOS setting, enable NetBIOS over TCP/IP.

○ Enable NetBIOS over TCP/IP

○ Disable NetBIOS over TCP/IP

OK Cancel

7.5.5 Operations master roles (FSMO)

On the one hand, a large number of domain controllers (up to 1200) can be used that allocate all domain-relevant data reciprocally using replication mechanisms (synchronization) and thus operate redundantly (so-called multimasters). On the other hand, every forest has operations master roles (FSMO - Flexible Single Master Operations) that can (and should) be allocated 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 schema 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. PDC emulator
   The PDC is the system responsible for time synchronization within the forest (PDC in forest root) and the domain (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 (e.g. via SICLOCK 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.

NOTICE

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	

Note

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

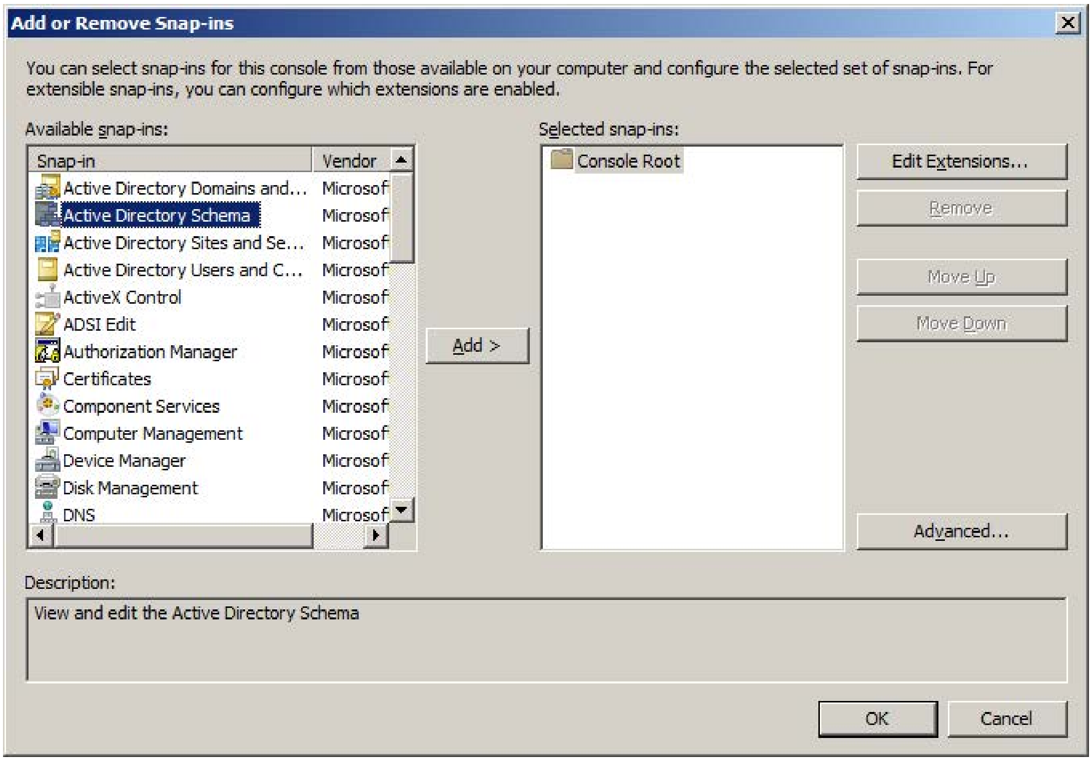
7.5.5.1 Schema master role

The "Schmmgmt.dll" file must be registered to transfer the schema master role to another domain controller. The Active Directory schema master snap-in is then started.

1. To register the "Schmmgmt.dll" file, click "Start" and then click "Run" in the Start menu.
2. Enter the following command in the Run dialog and confirm the entry with "OK":
   – Regsvr32 schmmgmt.dll

   The Management Console opens.
3. Click "File > Add/Remove Snap-in ..." to open the Active Directory schema snap-in.
   The "Add or Remove Snap-ins" dialog opens.

4. Select "Active Directory Schema" snap-in from the left wind and click the "Add>" button. Confirm the entry with "OK".



Add or Remove Snap-ins

You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

Available snap-ins:

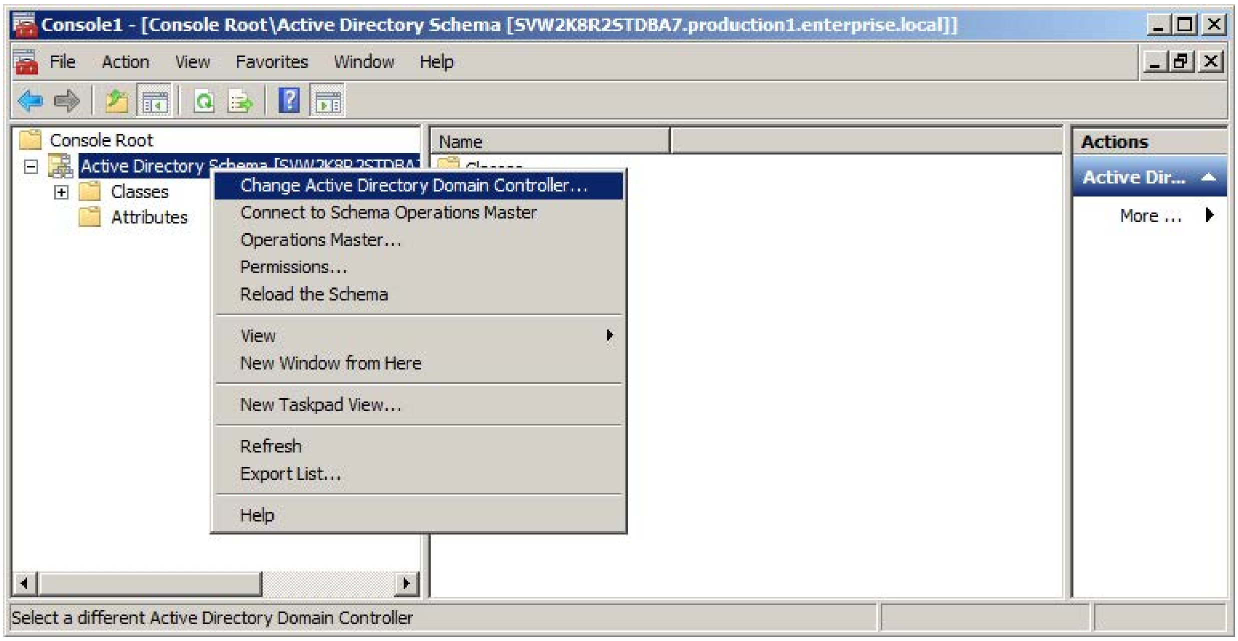
Snap-in	Vendor
Active Directory Domains and...	Microsof
Active Directory Schema	Microsof
Active Directory Sites and Se...	Microsof
Active Directory Users and C...	Microsof
ActiveX Control	Microsof
ADSI Edit	Microsof
Authorization Manager	Microsof
Certificates	Microsof
Component Services	Microsof
Computer Management	Microsof
Device Manager	Microsof
Disk Management	Microsof
DNS	Microsof

Selected snap-ins: Console Root

Description: View and edit the Active Directory Schema

The "Active Directory Schema" snap-in is integrated into the Management Console.

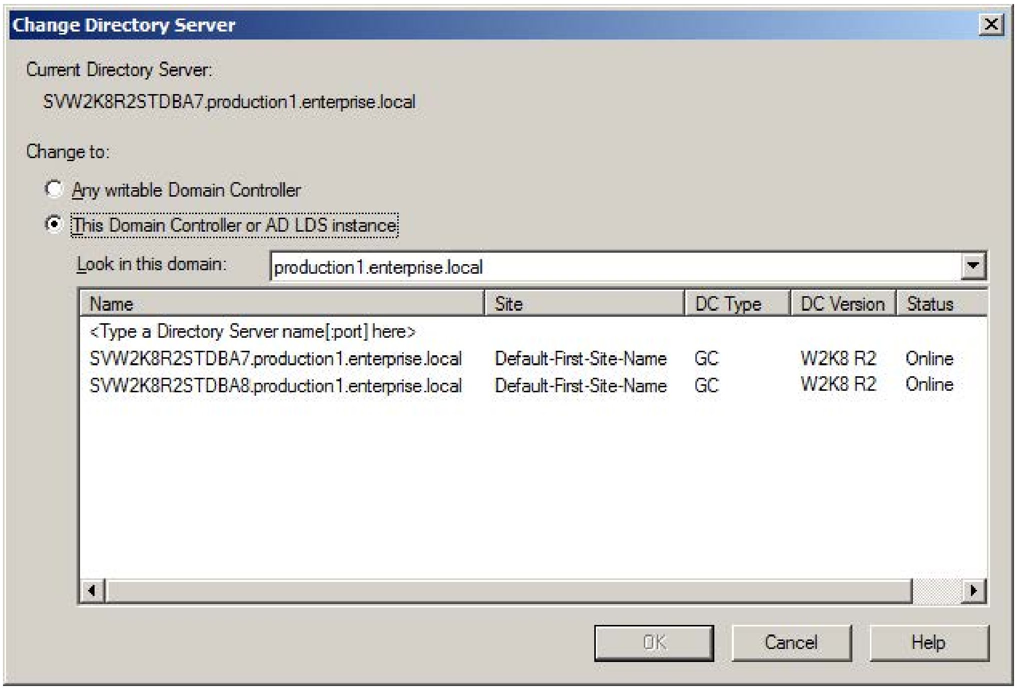
5. Right-click on the "Active Directory Schema" item in the Management Console and select the "Change Active Directory Domain Controller" command from the shortcut menu.



Console1 - [Console Root\Active Directory Schema [SVW2K8R2STDBA7.production1.enterprise.local]]

Select a different Active Directory Domain Controller

6. In the "Change Directory Server" dialog, select the "This Domain Controller or AD LDS instance" option and the corresponding domain controller from the list. Confirm the entry with "OK".



Change Directory Server

Current Directory Server:
SVW2K8R2STDBA7.production1.enterprise.local

Change to:

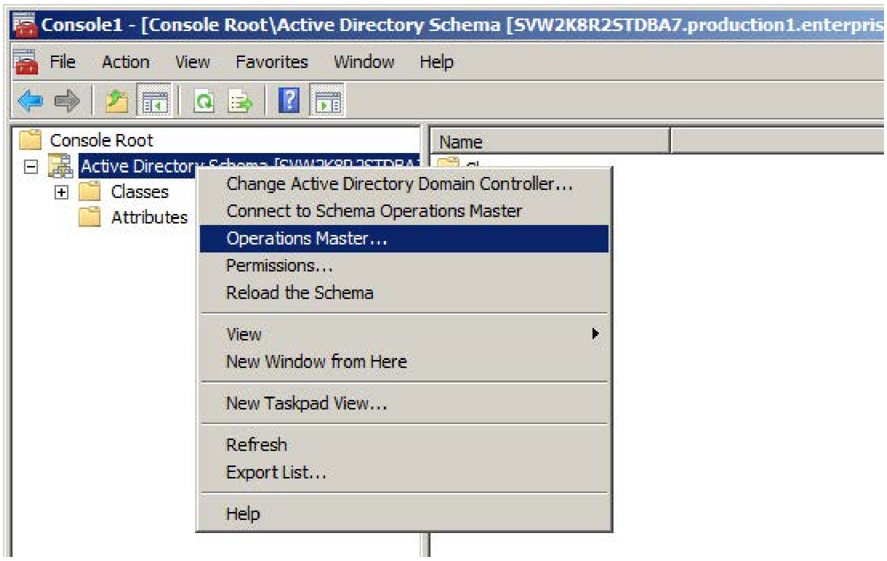
○ Any writable Domain Controller

● This Domain Controller or AD LDS instance

Look in this domain: production1.enterprise.local

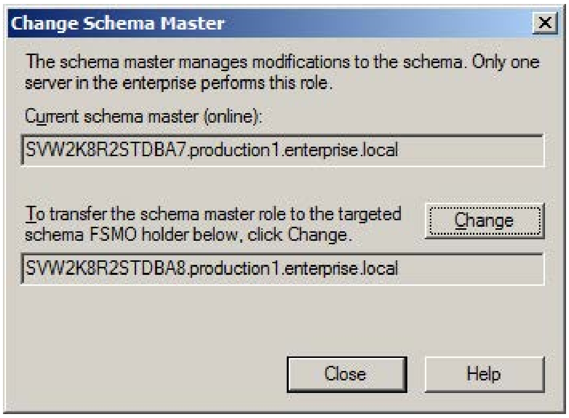
Name	Site	DC Type	DC Version	Status
<Type a Directory Server name[:port] here>				
SVW2K8R2STDBA7.production1.enterprise.local	Default-First-Site-Name	GC	W2K8 R2	Online
SVW2K8R2STDBA8.production1.enterprise.local	Default-First-Site-Name	GC	W2K8 R2	Online

7. Right-click on the "Active Directory Schema" item in the Management Console and select the "Operations Master" command from the shortcut menu.



Console1 - [Console Root\Active Directory Schema [SVW2K8R2STDBA7.production1.enterpris

8. Click on the "Change" button in the "Change Schema Master" dialog. Confirm the transfer of the role to the other domain controller with "OK".



Change Schema Master

The schema master manages modifications to the schema. Only one server in the enterprise performs this role.

Current schema master (online):

SVW2K8R2STDBA7.production1.enterprise.local

To transfer the schema master role to the targeted schema FSMO holder below, click Change.

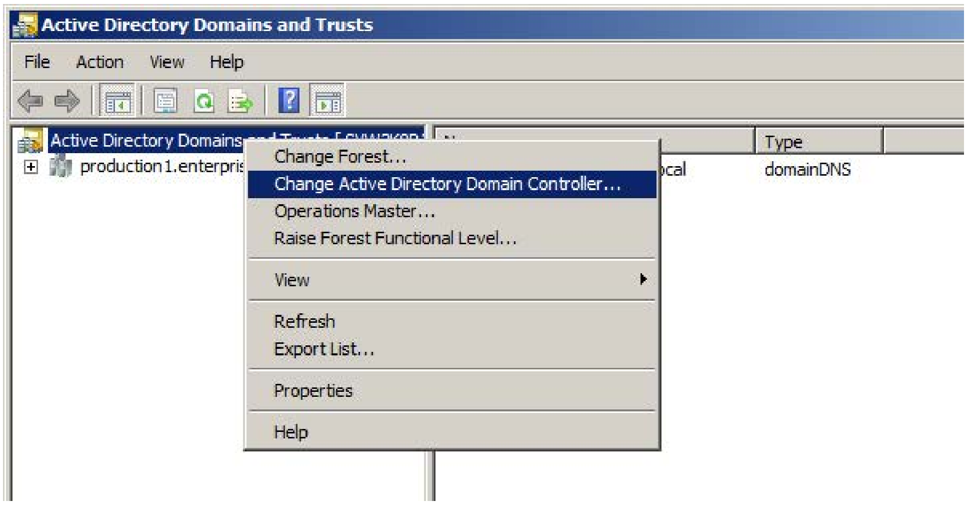
SVW2K8R2STDBA8.production1.enterprise.local

9. Close the transfer the of the schema master role using the "Close" button.

7.5.5.2 Domain Naming Master role

To transfer the Domain Naming Master role to another domain controller, follow these steps:

1. Open the Active Directory Domains and Trusts Management Console with "Start > Administrative Tools > Active Directory Domains and Trusts" .
2. Right-click on the "Active Directory Domains and Trusts" item and select the "Change Active Directory Domain Controller" command from the shortcut menu.



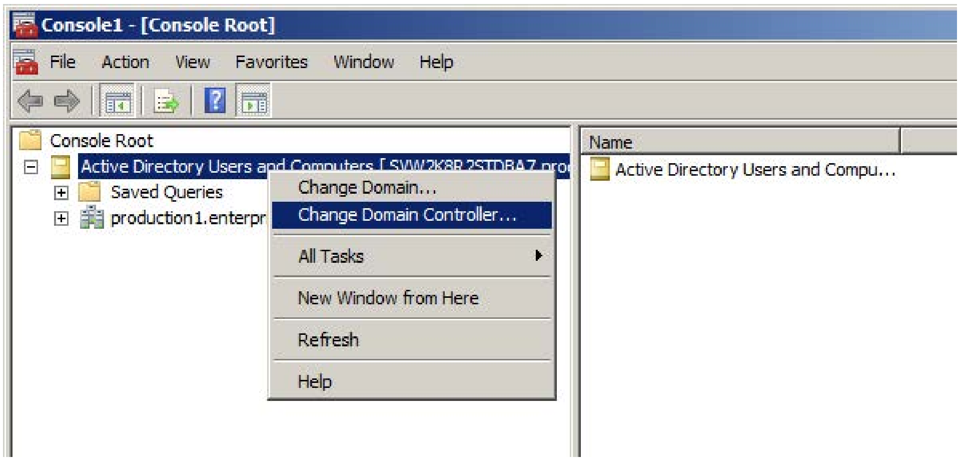
Active Directory Domains and Trusts
File
Action
View
Help
Active Directory Domains and Trusts [SVW2K8R...
production1.enterpris
Type
domainDNS
Change Forest...
Change Active Directory Domain Controller...
Operations Master...
Raise Forest Functional Level...
View
Refresh
Export List...
Properties
Help

3. In the "Change Directory Server" dialog, select the domain controller to which the role is to be transferred and click "OK".
4. Right-click on the "Active Directory Domains and Trusts" item in the Management Console and select the "Operations Master" command.
5. The remaining procedure is similar to the "Schema Master Role".

7.5.5.3 Infrastructure master, RID master and PDC emulator

To transfer the infrastructure master, RID master or PDC emulator roles to another domain controller, follow these steps:

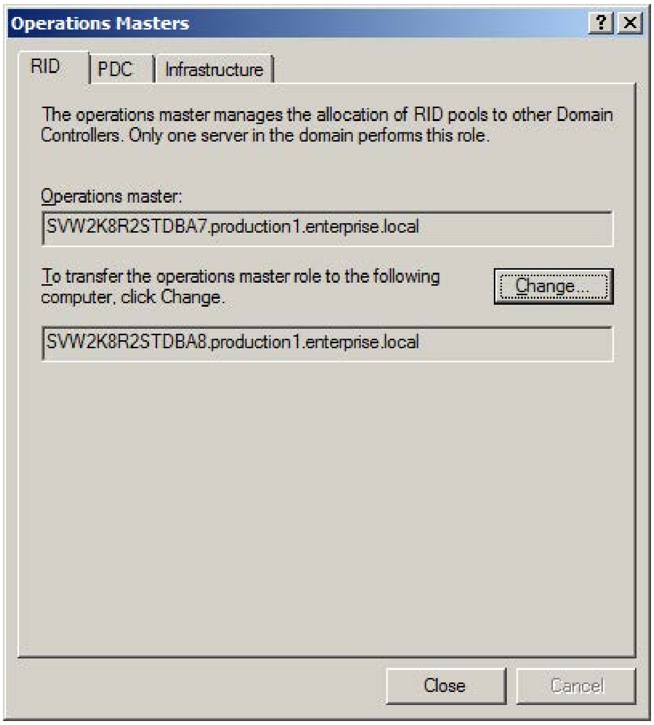
1. Open the Microsoft Management Console.
2. Click "File > Add/Remove Snap-in ..." to open the "Active Directory Users and Computers" snap-in.
3. Select "Active Directory Users and Computers" snap-in from the dialog that follows and click the "Add >" button. Confirm the entry with "OK".
4. Right-click on the "Active Directory Users and Computers" item Management Console and select the "Change Domain Controller" command from the shortcut menu.


Console1 - [Console Root]
File
Action
View
Favorites
Window
Help
Console Root
Active Directory Users and Computers [SVW2K8R2STDBA7.pro
Saved Queries
production1.enterpr
Change Domain...
Change Domain Controller...
All Tasks
New Window from Here
Refresh
Help
Name
Active Directory Users and Compu...

5. In the "Change Directory Server" dialog, select the domain controller to which the role is to be transferred and click "OK".

6. Right-click on the "Active Directory Users and Computers" item Management Console and select the "All Tasks" command from the shortcut menu and then the "Operations Master" command.

The "Operations Masters" dialog contains one tab each for the infrastructure master, RID master and PDC emulator roles; here you can switch from one domain controller to another by clicking "Change ...".



The operations master manages the allocation of RID pools to other Domain Controllers. Only one server in the domain performs this role.

Operations master:
SVW2K8R2STDBA7.production1.enterprise.local

To transfer the operations master role to the following computer, click Change.

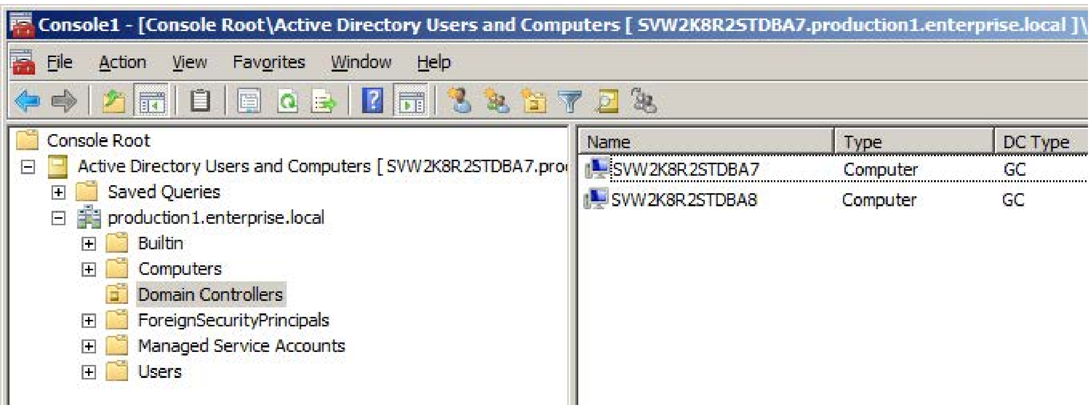
SVW2K8R2STDBA8.production1.enterprise.local

Note

Server roles can also be transferred using the "NTDSUTIL" command (https://technet.microsoft.com/en-us/library/cc976712.aspx).

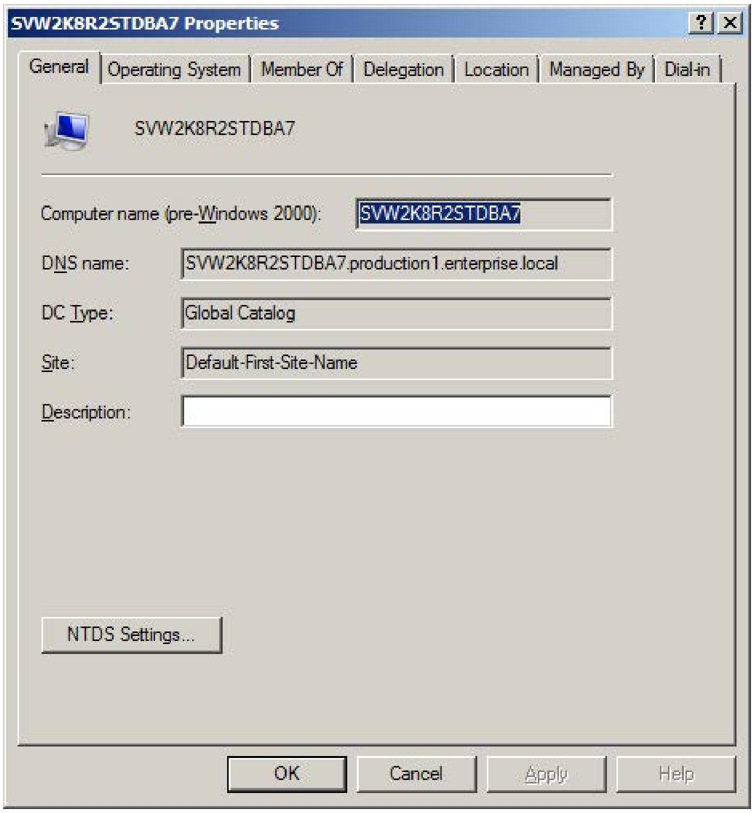
7.5.5.4 Global catalog

1. Open the Microsoft Management Console.
2. Click "File > Add/Remove Snap-in ..." to open the "Active Directory Users and Computers" snap-in.
3. Select the "Domain Controllers" folder in the tree view. Right-click on the domain controller in the global catalog and select the "Property" command from the shortcut menu.


Console1 - [Console Root\Active Directory Users and Computers [SVW2K8R2STDBA7.production1.enterprise.local]\
File
Action
View
Favorites
Window
Help
Console Root
Active Directory Users and Computers [SVW2K8R2STDBA7.pro
Saved Queries
production1.enterprise.local
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Managed Service Accounts
Users

Name	Type	DC Type
SVW2K8R2STDBA7	Computer	GC
SVW2K8R2STDBA8	Computer	GC

4. Click on the "NTDS Settings" button in the "General" tab of the properties dialog.



Computer name (pre-Windows 2000): SVW2K8R2STDBA7

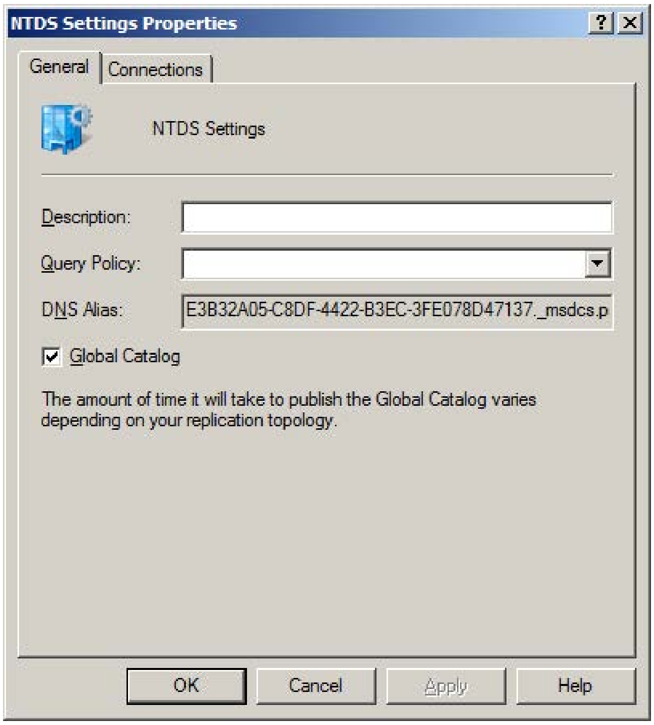
DNS name: SVW2K8R2STDBA7.production1.enterprise.local

DC Type: Global Catalog

Site: Default-First-Site-Name

Description:

5. Select the "Global Catalog" check box and click "OK".



Description:

Query Policy:

DNS Alias: E3B32A05-C8DF-4422-B3EC-3FE078D47137._msdcs.p

☑ Global Catalog

The amount of time it will take to publish the Global Catalog varies depending on your replication topology.

6. Perform this action on all domain controllers of the domain.

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 HMI user groups (SIMATIC HMI, SIMATIC HMI VIEWER, SIMATIC HMI CS) and the other groups on the PCS 7 systems, as described in section "Administration of computers and users (Page 123)".

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.

With the help of SIMATIC Logon, customized, task-related authorizations can be assigned to SIMATIC applications and system areas.

SIMATIC Logon supports user administration on local computers, in Windows workgroups and in Windows domains (Active Directory).

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 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.

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

- Automation License Manager (ALM)
- PCS 7 OS Client
- SIMATIC Batch Client
- PCS 7 ES
- 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/109738714)".

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

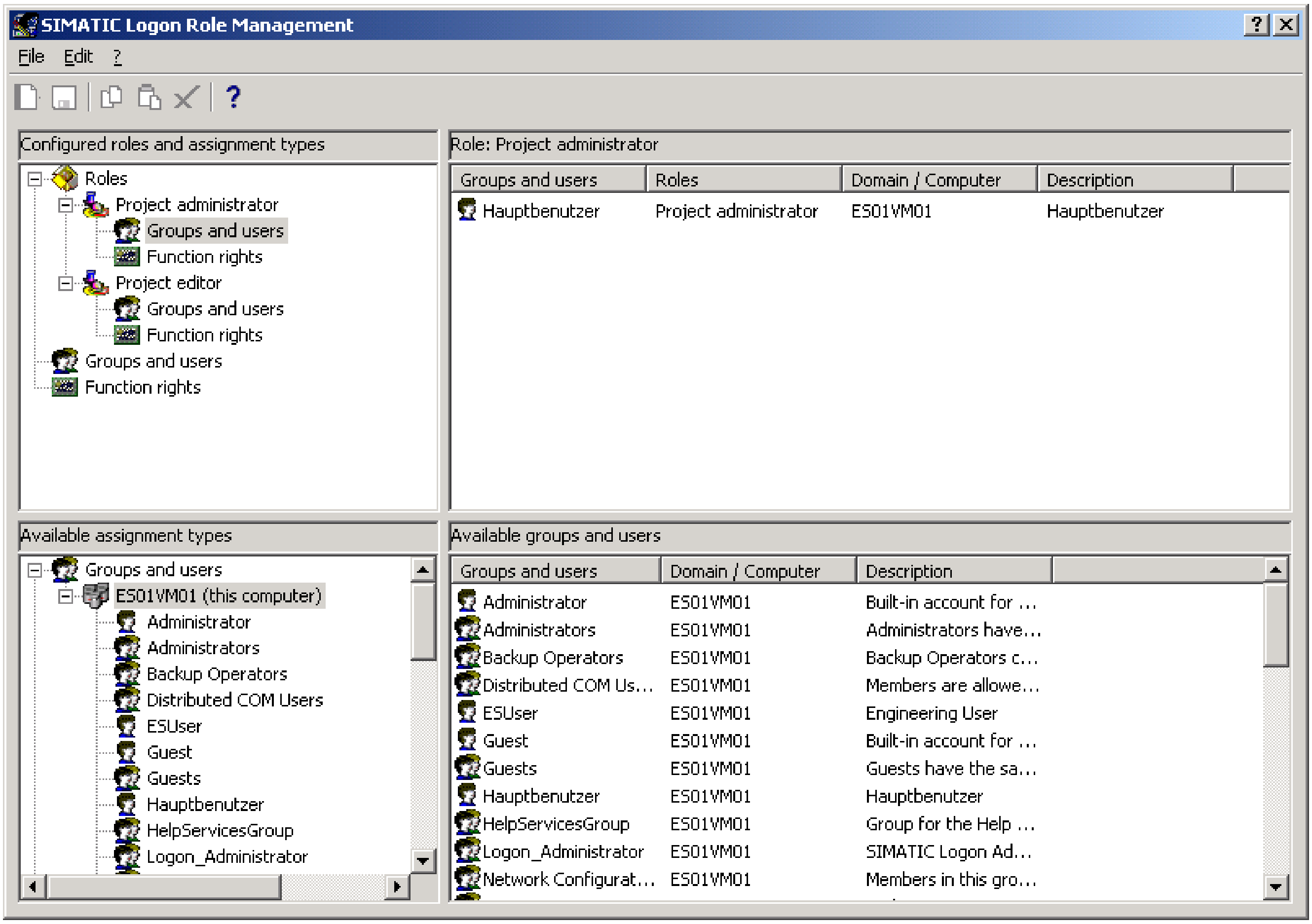
The user with the "Project administrator" role has the following rights:

- 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:



Configured roles and assignment types

- Roles
  - Project administrator
    - Groups and users
    - Function rights
  - Project editor
    - Groups and users
    - Function rights
- Groups and users
- Function rights

Role: Project administrator

Groups and users	Roles	Domain / Computer	Description
Hauptbenutzer	Project administrator	ES01VM01	Hauptbenutzer

Available assignment types

- Groups and users
  - ES01VM01 (this computer)
    - Administrator
    - Administrators
    - Backup Operators
    - Distributed COM Users
    - ESUser
    - Guest
    - Guests
    - Hauptbenutzer
    - HelpServicesGroup
    - Logon_Administrator

Available groups and users

Groups and users	Domain / Computer	Description
Administrator	ES01VM01	Built-in account for ...
Administrators	ES01VM01	Administrators have...
Backup Operators	ES01VM01	Backup Operators c...
Distributed COM Us...	ES01VM01	Members are allowe...
ESUser	ES01VM01	Engineering User
Guest	ES01VM01	Built-in account for ...
Guests	ES01VM01	Guests have the sa...
Hauptbenutzer	ES01VM01	Hauptbenutzer
HelpServicesGroup	ES01VM01	Group for the Help ...
Logon_Administrator	ES01VM01	SIMATIC Logon Ad...
Network Configurat...	ES01VM01	Members in this gro...

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)	• 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" roles in SIMATIC Logon are automatically created during the 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 receive a notice that the modified project can no longer be edited with older 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/109485969).

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/109485970) Configuration Manual.

7.7 Protection level concept

Using a protection level can protect the automation device 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-CPUs or H-CPUs, 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/109485969).

Patch management 8

8.1 Overview

Microsoft regularly eliminates security gaps in its products and provides these corrections to its customers via updates (patches).

To ensure secure and stable operation of SIMATIC PCS 7, the installation of "Security patches" and "Critical patches" is required.

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

- Windows Updates via Microsoft Windows Server Update Services (WSUS)
  Provision of Windows updates for all computers of the automation system from a separate WSUS
- Manual update
  Manual installation of "Security Updates" and "Important Updates" on all computers of the automation system after downloading the patches from the Microsoft website

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

- Manual "SIMATIC Process Control System PCS 7 Patch Management and Security Updates (https://support.industry.siemens.com/cs/ww/en/view/38621083)"
- FAQ "Which Microsoft Patches ("Security Patches" and "Critical Patches") have been tested for compatibility with SIMATIC PCS 7? (https://support.industry.siemens.com/cs/ww/en/view/18490004)"
- FAQ "How can you find out which Microsoft Patches are installed on the PC? (https://support.industry.siemens.com/cs/ww/en/view/48844294)"

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

- https://support.microsoft.com/en-us/kb/824684
- https://www.microsoft.com/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:

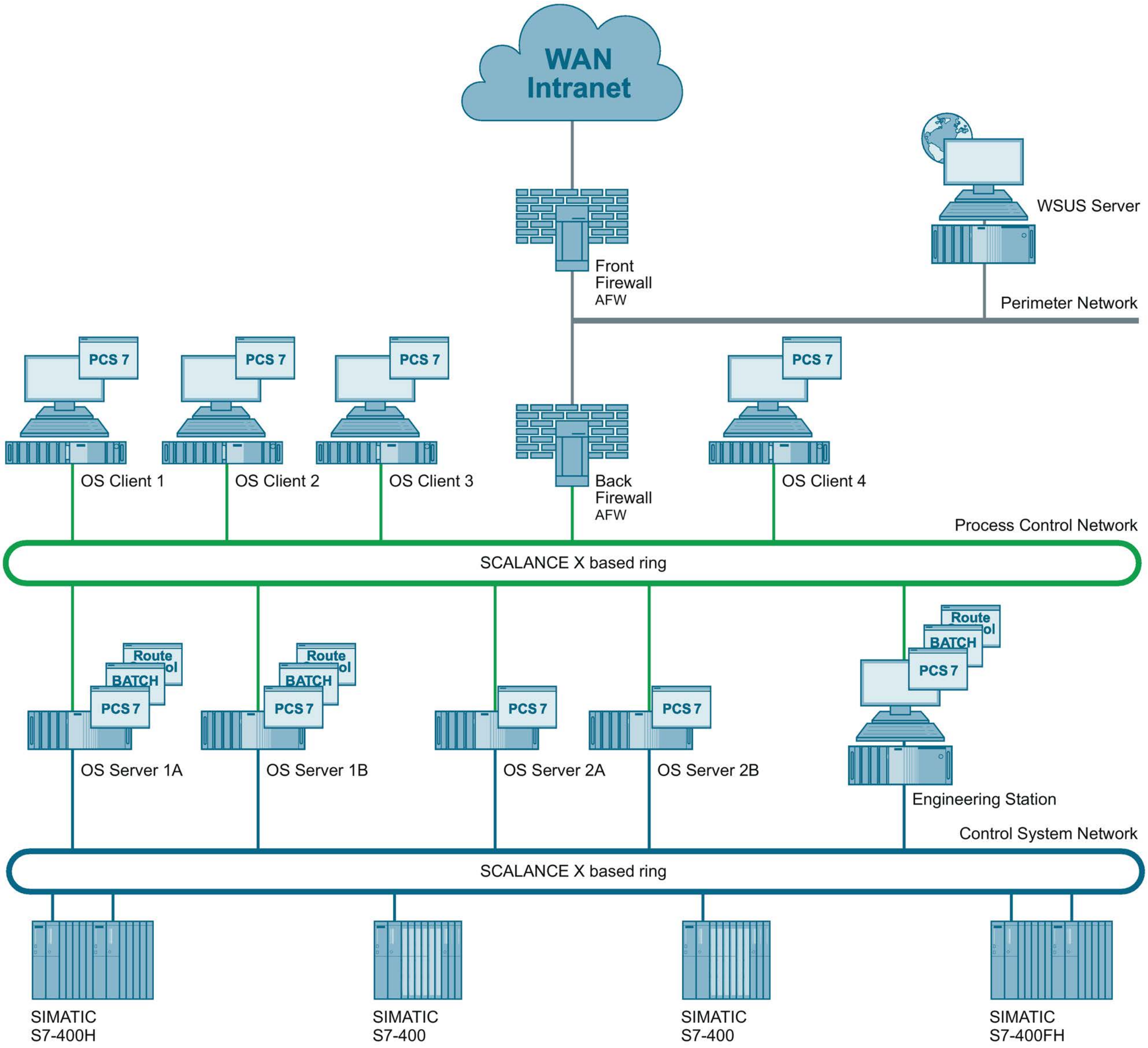
- https://www.siemens.com/industrial-security

You can also send your query directly via e-mail to "industrialsecurity.i@siemens.com".

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 set up for your PCS 7 system.

Note

If your system uses Windows 10 Enterprise LTSB systems, the WSUS must be installed on the basis of the Windows Server 2012 R2 operating system.

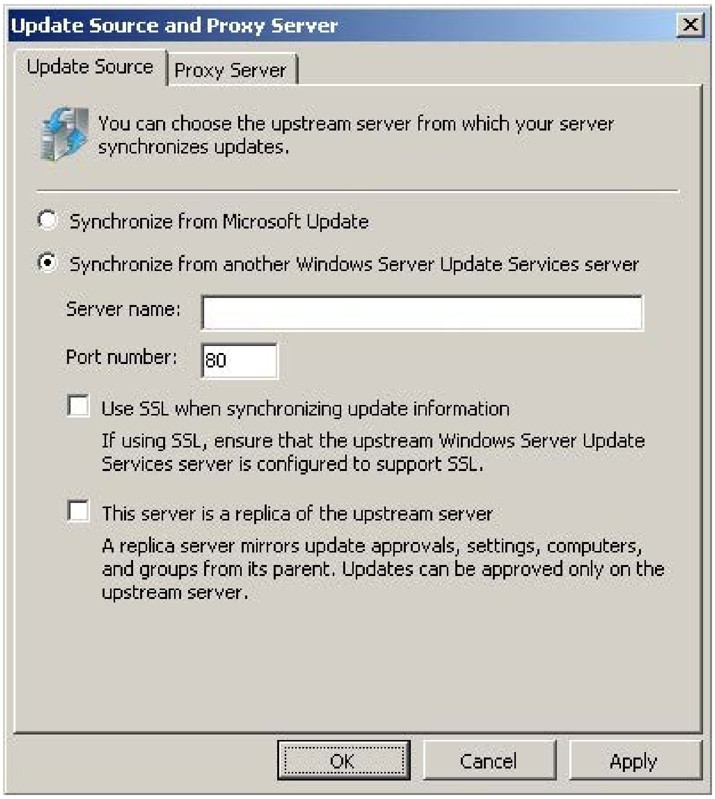
You can find additional information at:

- https://technet.microsoft.com/itpro/windows/manage/introduction-to-windows-10-servicing
- https://support.microsoft.com/en-us/kb/3095113

Update source

For the WSUS server of the PCS 7 system, either an existing WSUS in a higher-level external network, such as the plant network or 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:



Update Source and Proxy Server

You can choose the upstream server from which your server synchronizes updates.

○ Synchronize from Microsoft Update

● Synchronize from another Windows Server Update Services server

Server name:

Port number: 80

□ Use SSL when synchronizing update information

If using SSL, ensure that the upstream Windows Server Update Services server is configured to support SSL.

□ This server is a replica of the upstream server

A replica server mirrors update approvals, settings, computers, and groups from its parent. Updates can be approved only on the upstream server.

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.

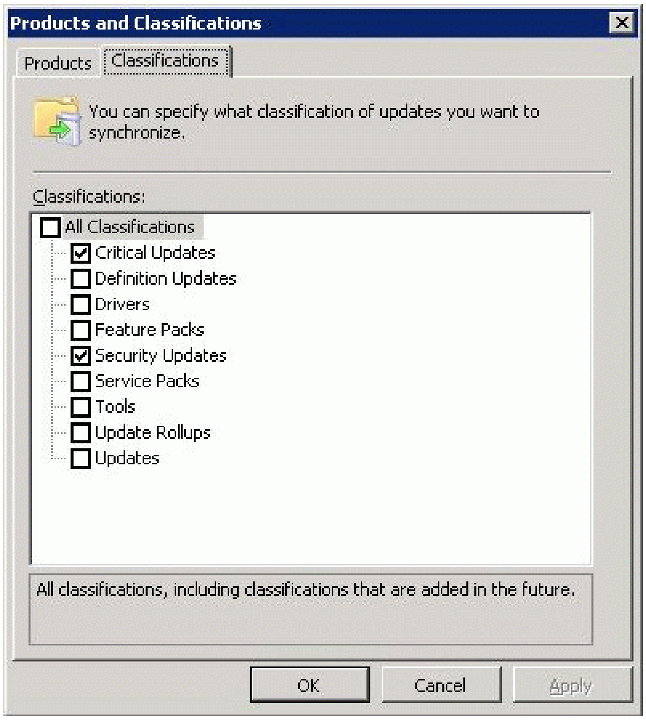
Note

You can find information about the Microsoft patches tested for PCS 7 and permissible classifications of patches in the following FAQ:

Which Microsoft Security Patches ("Security Patches" and "Critical Patches") have been tested for compatibility with SIMATIC PCS 7? (https://support.industry.siemens.com/cs/ww/en/view/18490004)

---

3. Select the "Critical Updates" and "Security Updates" on the "Products and Classifications" dialog.



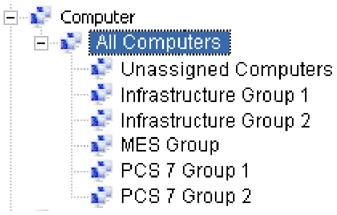
You can specify what classification of updates you want to synchronize.

Classifications:

- □ All Classifications
  - ☑ Critical Updates
  - □ Definition Updates
  - □ Drivers
  - □ Feature Packs
  - ☑ Security Updates
  - □ Service Packs
  - □ Tools
  - □ Update Rollups
  - □ Updates

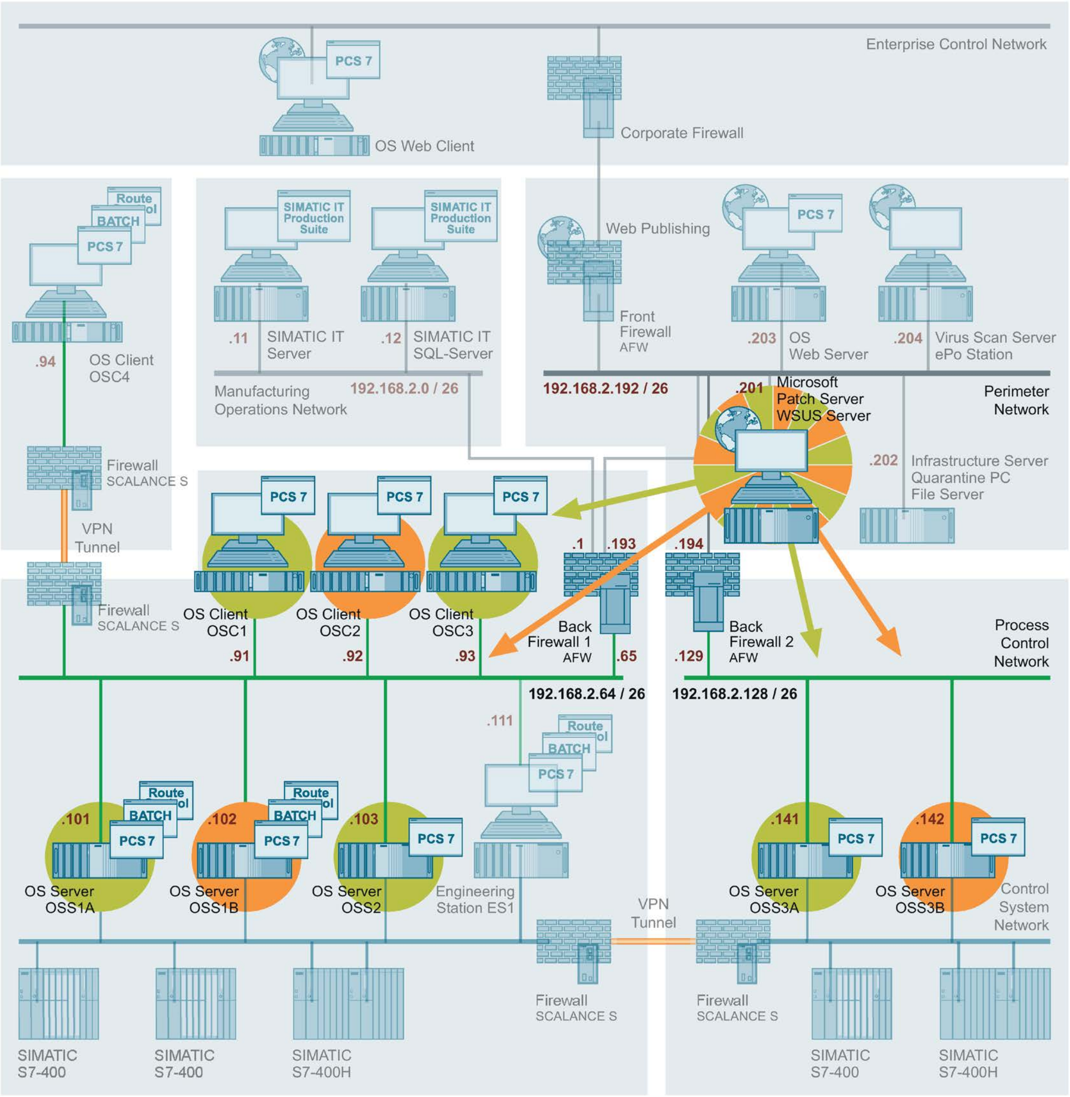
All classifications, including classifications that are added in the future.

4. Create project-specific groups for the distribution of updates in the system according to the redundancy concept, and assign the individual PCS 7 systems (and any other systems to be patched) to these computer groups.

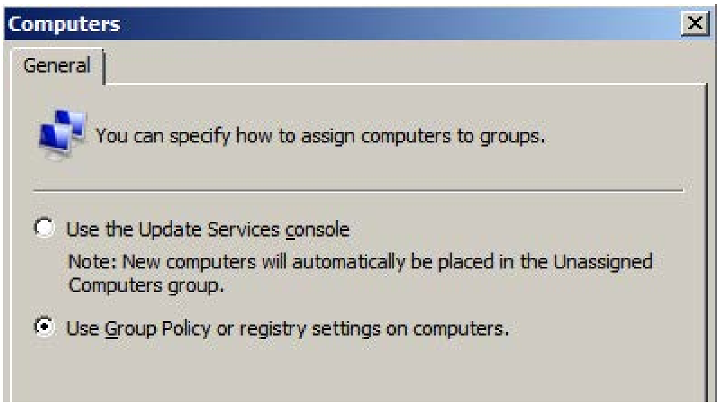


- Computer
  - All Computers
    - Unassigned Computers
    - Infrastructure Group 1
    - Infrastructure Group 2
    - MES Group
    - PCS 7 Group 1
    - PCS 7 Group 2

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.



Computers

General

You can specify how to assign computers to groups.

○ Use the Update Services console

Note: New computers will automatically be placed in the Unassigned Computers group.

● Use Group Policy or registry settings on computers.

Checking for updates

To check for updates, follow these steps:

1. Download the Excel table to your computer from the following FAQ:

   Which Microsoft Security Patches ("Security Patches" and "Critical Patches") 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 "Test Result" column for "Failed".
3. Check the "Comment" column to see whether these updates have been replaced.
4. If no up-to-date, error-free patches are available, exclude these patches from the update of your systems.

Enabling updates for installation and installing them

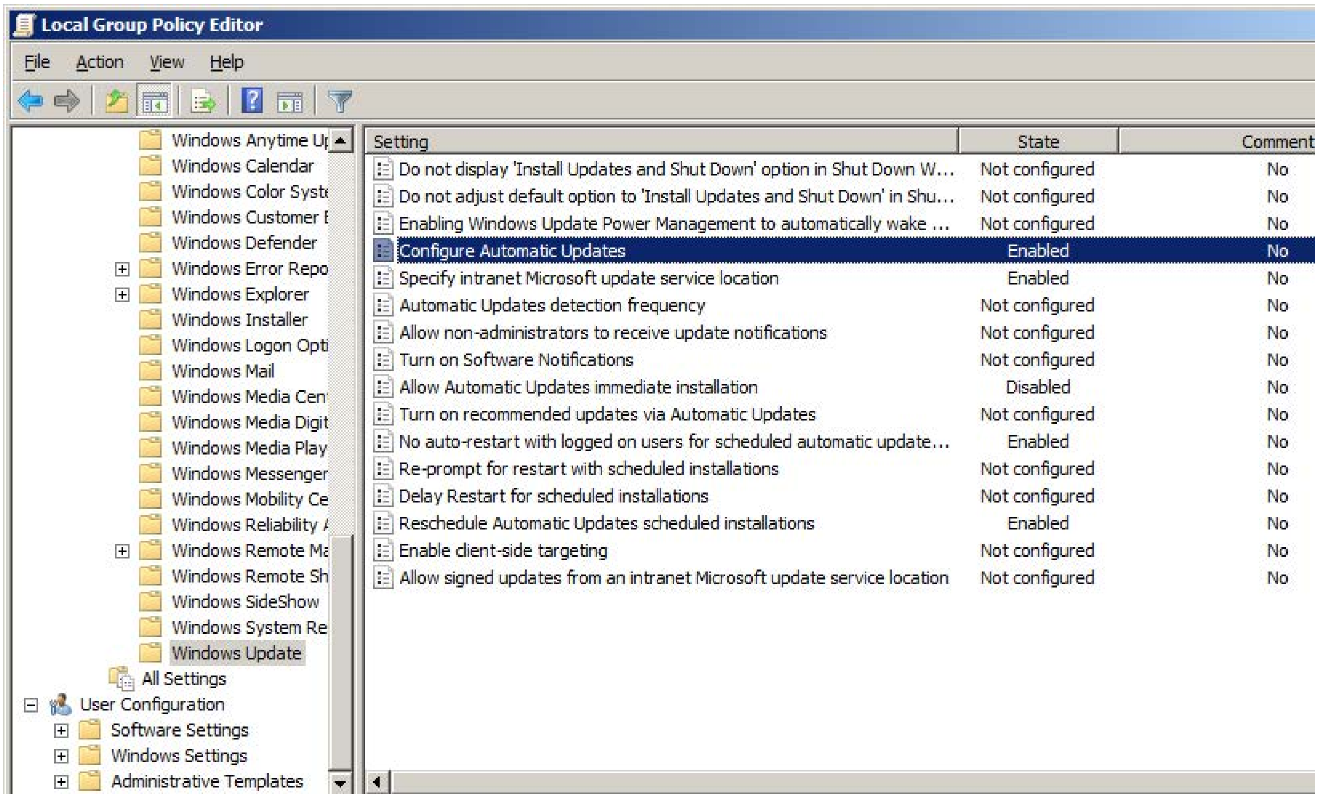
1. Select all available patches in the "Critical updates " and "Security updates" categories (except for the patches listed in the section "Checking for updates") and enable them for installation in your created groups. Proceed group by group to ensure the availability and operability of your system.
2. Log on to the systems connected to the WSUS with an administrator account. The systems are configured in such a way that they receive the updates from the WSUS (see section 7.2.3 and manual "SIMATIC Process Control System PCS 7 Patch Management and Security Updates" (https://support.industry.siemens.com/cs/ww/en/view/38621083)).
3. Go to "Control Panel > Windows Update" and initiate the search for available updates.
4. Install the offered updates and restart the systems if required.

8.2.3 Configuration of group policies

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, the group policy settings are made centrally and distributed to the systems according to assignment.

The following figure shows the editor for local group policies:

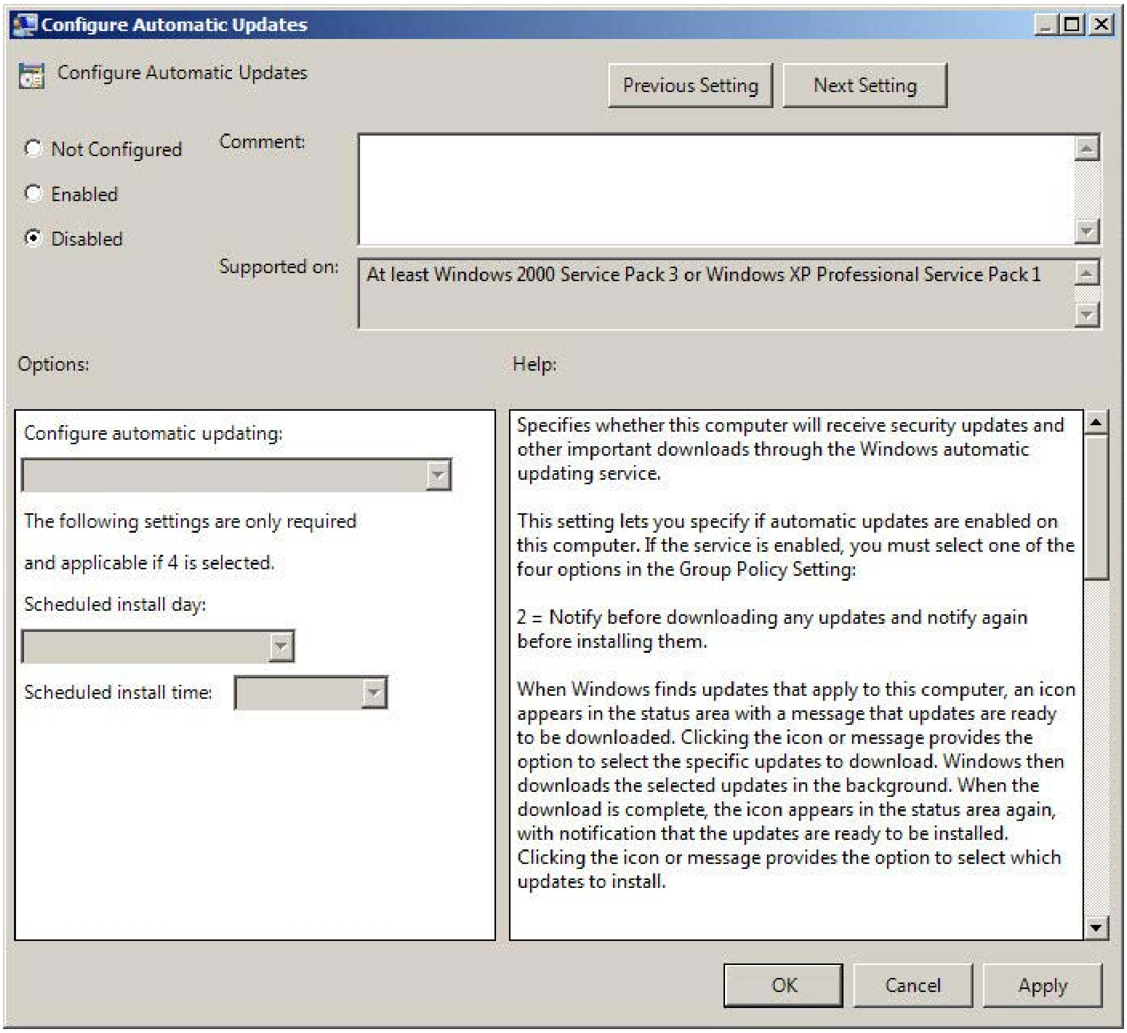


Setting	State	Comment
Do not display 'Install Updates and Shut Down' option in Shut Down W...	Not configured	No
Do not adjust default option to 'Install Updates and Shut Down' in Shu...	Not configured	No
Enabling Windows Update Power Management to automatically wake ...	Not configured	No
Configure Automatic Updates	Enabled	No
Specify intranet Microsoft update service location	Enabled	No
Automatic Updates detection frequency	Not configured	No
Allow non-administrators to receive update notifications	Not configured	No
Turn on Software Notifications	Not configured	No
Allow Automatic Updates immediate installation	Disabled	No
Turn on recommended updates via Automatic Updates	Not configured	No
No auto-restart with logged on users for scheduled automatic update...	Enabled	No
Re-prompt for restart with scheduled installations	Not configured	No
Delay Restart for scheduled installations	Not configured	No
Reschedule Automatic Updates scheduled installations	Enabled	No
Enable client-side targeting	Not configured	No
Allow signed updates from an intranet Microsoft update service location	Not configured	No

The group policies are configured according to the manual "SIMATIC Process Control System PCS 7 Patch Management and Security Updates" (https://support.industry.siemens.com/cs/ww/en/view/38621083).

The following group policies must be configured:

- "Configure Automatic Updates" policy
  The "Configure Automatic Updates" policy must be disabled. As a result, the available updates must be manually requested and installed later on the systems.



Configure Automatic Updates

Configure Automatic Updates

○ Not Configured
○ Enabled
● Disabled

Comment:

Supported on: At least Windows 2000 Service Pack 3 or Windows XP Professional Service Pack 1

Options:

Configure automatic updating:

The following settings are only required

and applicable if 4 is selected.

Scheduled install day:

Scheduled install time:

Help:

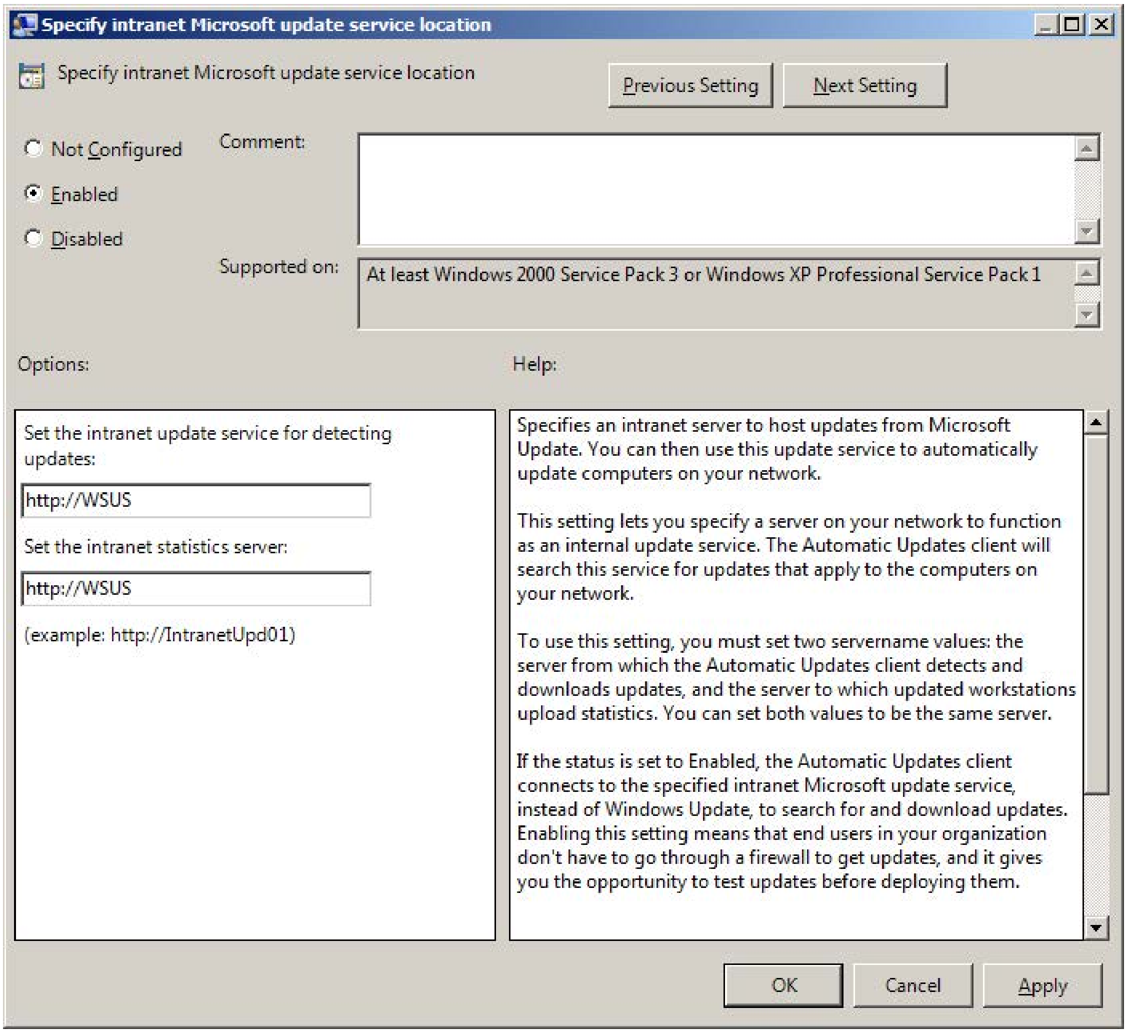
Specifies whether this computer will receive security updates and other important downloads through the Windows automatic updating service.

This setting lets you specify if 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 any updates and notify again before installing them.

When Windows finds updates that apply to this computer, an icon appears in the status area with a message that updates are ready to be downloaded. Clicking the icon or message provides the option to select the specific updates to download. Windows then downloads the selected updates in the background. When the download is complete, the icon appears in the status area again, with notification that the updates are ready to be installed. Clicking the icon or message provides the option to select which updates to install.

- 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 must be specified 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).



Specify intranet Microsoft update service location

○ Not Configured

● Enabled

○ Disabled

Supported on: At least Windows 2000 Service Pack 3 or Windows XP Professional Service Pack 1

Set the intranet update service for detecting updates: http://WSUS

Set the intranet statistics server: http://WSUS

(example: http://IntranetUpd01)

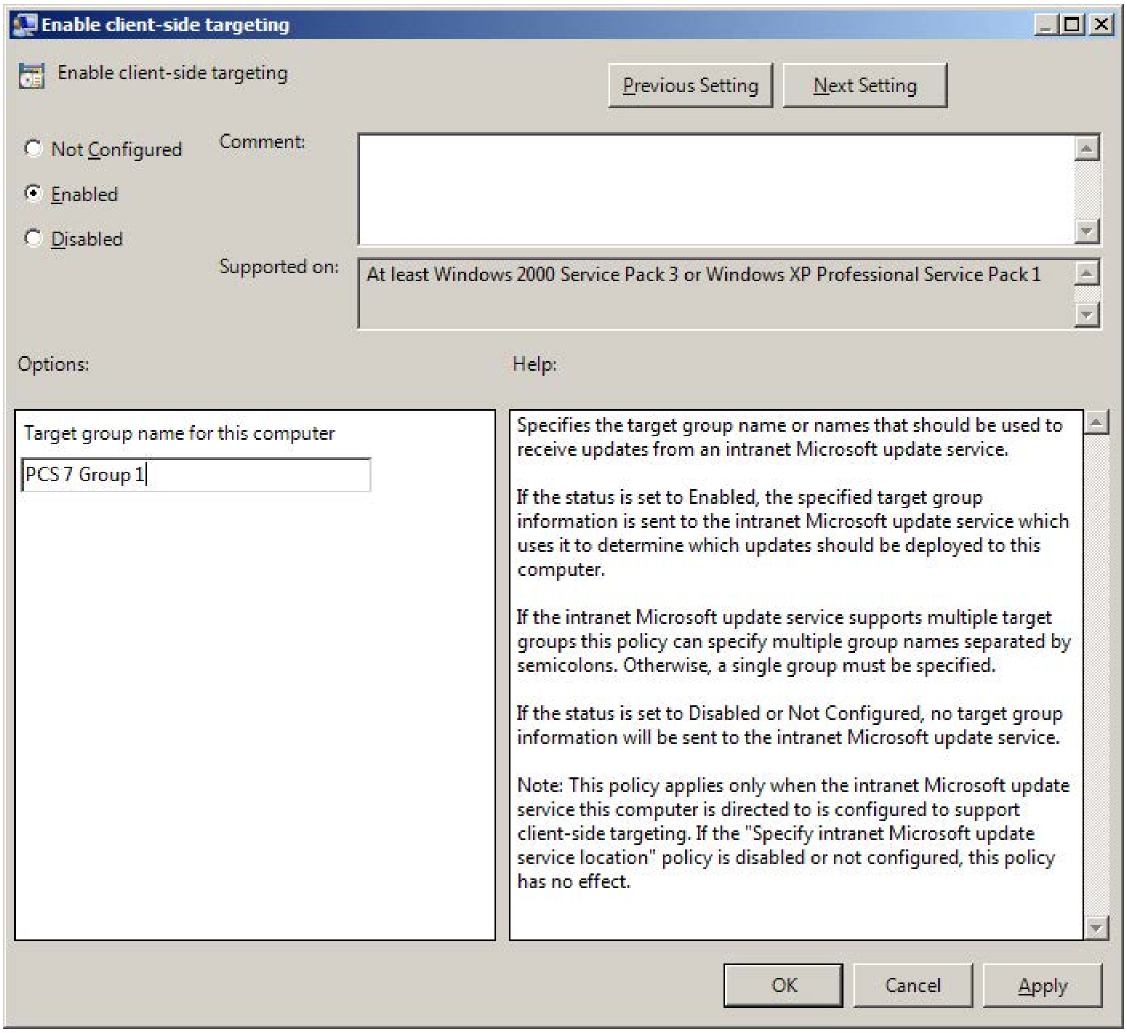
Specifies an intranet server to host updates from Microsoft Update. You can then use this update service to automatically update computers on your network.

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 servername 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.

If the status is set to Enabled, the Automatic Updates client connects to the specified intranet Microsoft update service, 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.

- "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

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: At least Windows 2000 Service Pack 3 or Windows XP Professional Service Pack 1

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.

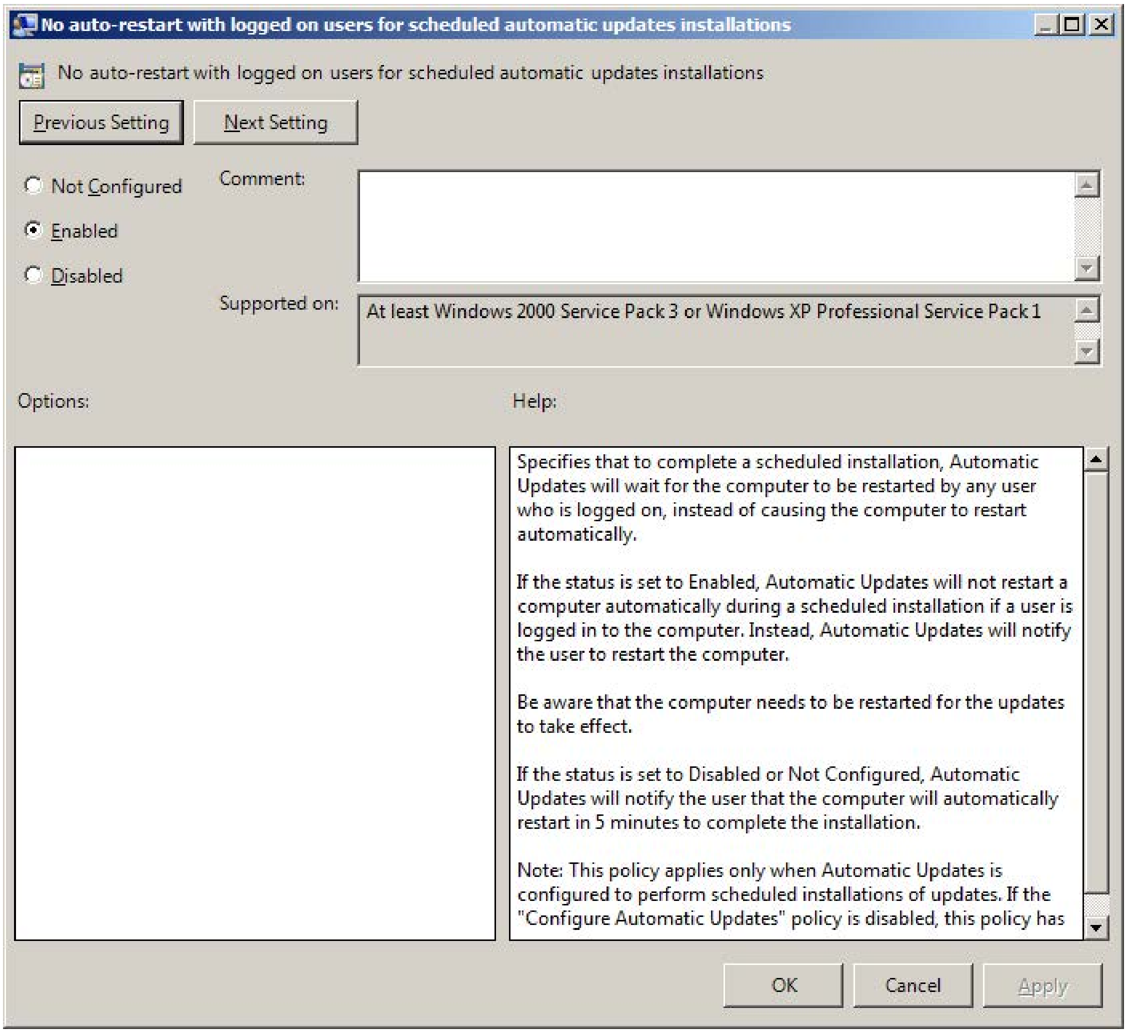
If the status is set to Enabled, the specified target group information is sent to the intranet Microsoft update service which uses it to determine which updates should be deployed to this computer.

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.

- "No auto-restart with logged on users for scheduled automatic update installations" policy
  This group policy must be enabled.



No auto-restart with logged on users for scheduled automatic updates installations

No auto-restart with logged on users for scheduled automatic updates installations

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: At least Windows 2000 Service Pack 3 or Windows XP Professional Service Pack 1

Options:

Help:

Specifies that to complete a scheduled installation, Automatic Updates will wait for the computer to be restarted by any user who is logged on, instead of causing the computer to restart automatically.

If the status is set to Enabled, Automatic Updates will not restart a computer automatically during a scheduled installation if a user is logged in to the computer. Instead, Automatic Updates will notify the user to restart the computer.

Be aware that the computer needs to be restarted for the updates to take effect.

If the status is set to Disabled or Not Configured, Automatic Updates will notify the user that the computer will automatically restart in 5 minutes to complete the installation.

Note: This policy applies only when Automatic Updates is configured to perform scheduled installations of updates. If the "Configure Automatic Updates" policy is disabled, this policy has

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 pages

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: http://windowsupdate.microsoft.com http://*.windowsupdate.microsoft.com https://*.windowsupdate.microsoft.com http://*.update.microsoft.com https://*.update.microsoft.com http://*.windowsupdate.com http://download.windowsupdate.com http://download.microsoft.com http://*.download.windowsupdate.com http://test.stats.update.microsoft.com http://ntservicepack.microsoft.com

- 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

8.3 Manual update

For the manual update, the required updates of the system must first be downloaded from the Microsoft Download Center 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 (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 procedure described above does not apply to Microsoft Service Packs, whose use still requires an explicit release. If the updates require a later version of the Microsoft software, read the PCS 7 Readme (https://support.industry.siemens.com/cs/ww/en/view/109478781)or use the compatibility tool (https://support.industry.siemens.com/cs/ww/en/view/64847781) to ensure that these later software versions or service packs have been approved for SIMATIC PCS 7.

Protection against malware using virus scanners 9

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:

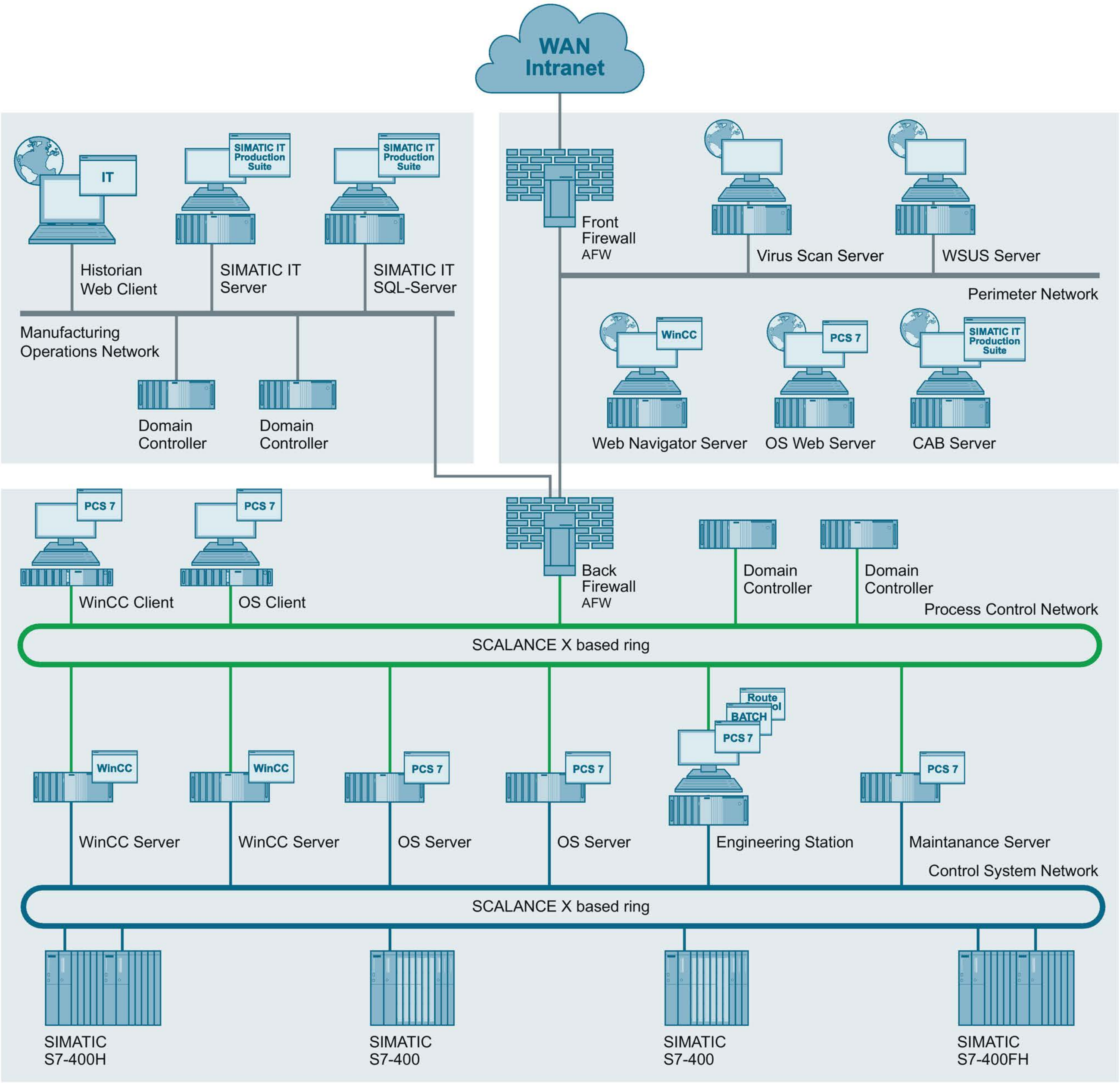
- Computer virus
- Computer worm
- Trojan horse
- Other potentially dangerous programs, for example:
  - Backdoor
  - Ransomware
  - Spyware
  - Adware
  - Scareware
  - Grayware

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, blocked or deleted.

The following virus scanner architecture is recommended for implementing this requirement:



The virus scanner server is a computer which centrally manages virus scan clients, loads virus signature files (virus patterns) over the Internet from the virus scanner vendor and distributes them to the virus scanner clients.

The virus scan client is a computer (e.g. a PCS 7 OS Server) that checks for malware and is managed by the virus server from which it receives current virus signature files.

In accordance with the rules for dividing components into security cells, the virus scan server must be installed in a separate network (preferably in the Perimeter network / DMZ). For the virus scanner server, 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. During configuration of the firewall access rules for the back-end firewall or three-homed firewall, the protocols and ports needed by the virus scan server for communication between the systems to be managed and the virus scan server must be allowed.

9.2 Update source

For the virus scanner server, either an existing virus scanner server in a higher-level external network, such as the plant network or corporate network, or the URL of the virus scanner server vendor on the Internet can be configured 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 virus scanner server.

9.3 Firewall rules

The following firewall rules apply to the access of the virus scanner server in the Perimeter network to the virus scan clients in the PCN via the back-end firewall or three-homed firewall.

- Example of firewall rules between a virus scan server and a virus scan client:

Name	Action	Protocols	From	To
Perimeter virus scan server to PCN ... #1	Allow	Vendor dependent	IP address of virus scan server	IP address of virus scan client
PCN … to Perimeter virus scan server #1	Allow	Vendor dependent	IP address of virus scan client	IP address of virus scan server

The following firewall rules are required for the access of the virus scan server in the Perimeter network to the external network for downloading the virus signature files via the front-end firewall or three-homed firewall:

- Example of firewall rules for updating the virus signature files via URL from the provider

Name	Action	Protocols	From	To
Allow Virus Pattern Update access to External (Vendor)	Allow	FTP HTTP HTTPS Vendor dependent	IP address of virus scan server	Vendor Pattern Update Server Vendor dependent

- Example of firewall rule for updating the virus signature files from a higher-level virus scan server

Name	Action	Protocols	From	To
Allow Virus Pattern Update access to superordinate Pattern Update Server	Allow	FTP HTTP HTTPS Vendor dependent	IP address of virus scan server	IP address of Superordinate Pattern Update Server

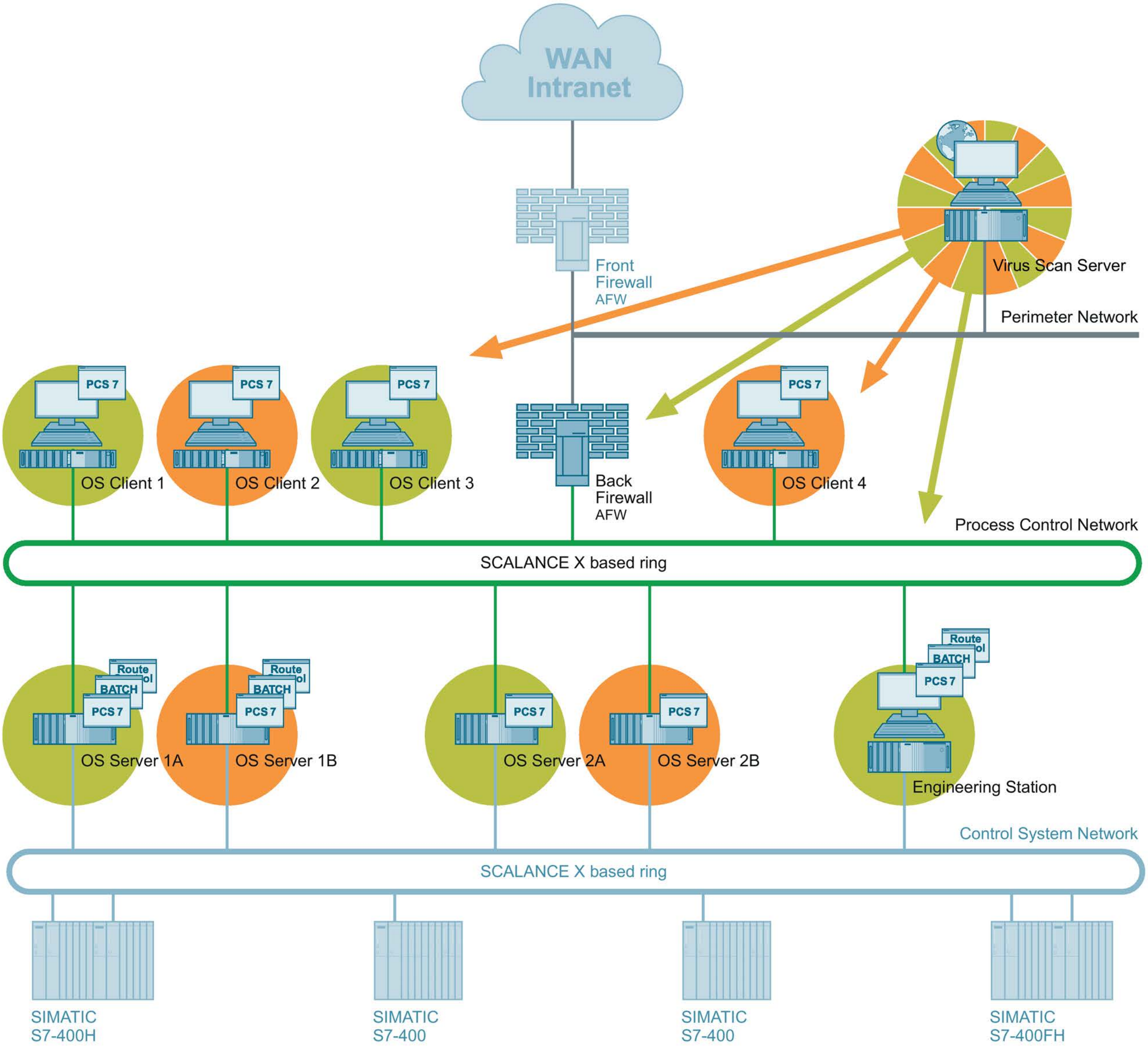
You can find information on the ports and protocols used by the virus scanners for specific manufacturers at the following links:

- Trend Micro (https://esupport.trendmicro.com/solution/en-us/1107850.aspx)
- Symantec (http://www.symantec.com/docs/TECH163787)
- Intel Security (McAfee) (https://kc.mcafee.com/corporate/index?page=content&id=KB66797)

9.4 Distribution of virus signature files

To distribute the virus signature files from the virus scan server to the virus scan clients, the formation of project-specific computer groups is recommended (analogous to computer groups in patch management).

The following figure shows an example of the formation of two computer groups:



Additional information

You can find 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/en/view/38625951)"
- FAQ "With what are SIMATIC PCS 7 V8.x, V7.x, V 6.x, V5.x and V4.x compatible? (https://support.industry.siemens.com/cs/ww/en/view/64847781)"

In the Siemens Industry Online Support Portal, you can also find configuration descriptions for the various virus scanners:

- McAfee VirusScan Enterprise 8.8 configuration (https://support.industry.siemens.com/cs/ww/en/view/66475606)
- Trend Micro OfficeScan 11.0 SP1 configuration (https://support.industry.siemens.com/cs/ww/en/view/109736191)
- Symantec Endpoint Protection 12.1 configuration (https://support.industry.siemens.com/cs/ww/en/view/71874887)

9.5 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 at Industrial Security Web (https://www.siemens.com/industrial-security).

Inquiries can also be emailed directly to "industrialsecurity.i@siemens.com".

Backing up and restoring data 10

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 "Procedure following a virus infection" (Page 206)) 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 volume is backed up with the following data:
  - 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 "Concept of "defense in depth" (Page 12)") organizationally for both the project backup and for the system backup. 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 PCS 7 project (multi-project including all individual projects it contains) can be archived using the SIMATIC Manager. Depending on the default archiving program, this process creates a ZIP archive containing all the configuration data.

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).

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, for example, a new update such as a security update, a critical update or an application hotfix is installed on a system component, an up-to-date system backup must be created for this system component.

Note

For system backups during runtime of SIMATIC PCS 7, the product "Symantec System Recovery" has been tested for compatibility (see FAQ "How do you do a recovery for PCS 7 systems during running operation?" (https://support.industry.siemens.com/cs/ww/en/view/56897157)).

For "Offline backups" without activated runtime and when the operating system is stopped, the product "SIMATIC IPC Image & Partition Creator" (https://support.industry.siemens.com/cs/ww/en/view/21766418) is available for SIMATIC IPC computers.

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 its 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 Process Control System PCS 7; Service Support and Diagnostics" (https://support.industry.siemens.com/cs/ww/en/view/109485965), section "Data backup"
- Manual "SIMATIC Process Control System PCS 7 Compendium Part D – Operation and Maintenance"

Remote access 11

11.1 Remote maintenance based on the SIMATIC Remote Services platform

Introduction

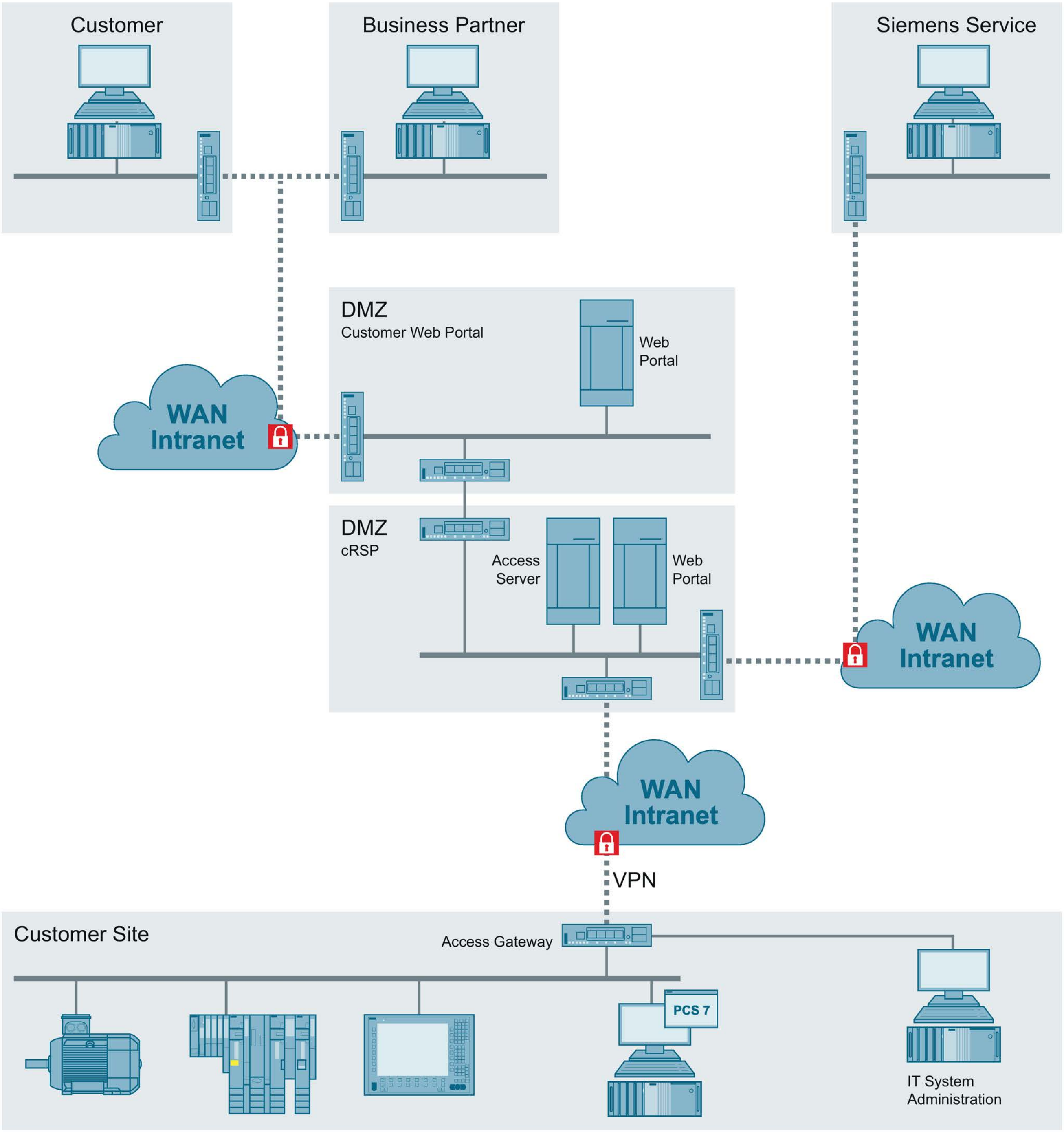
Optimal proactive, secure and system-specific support for the automation system from remote locations: This is the idea behind the SIMATIC Remote Services (SRS) platform. Thanks to its modular design, SIMATIC Remote Services can be optimally adapted to actual requirements. The available modules not only provide the remote infrastructure but also include support and maintenance.
Since the SIMATIC 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 SRS 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 SIEMENS Remote Services platform:



You can find additional information on the SRS platform on the "SIMATIC Remote Services" (https://support.industry.siemens.com/cs/ww/en/sc/2281) website.

11.2 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.

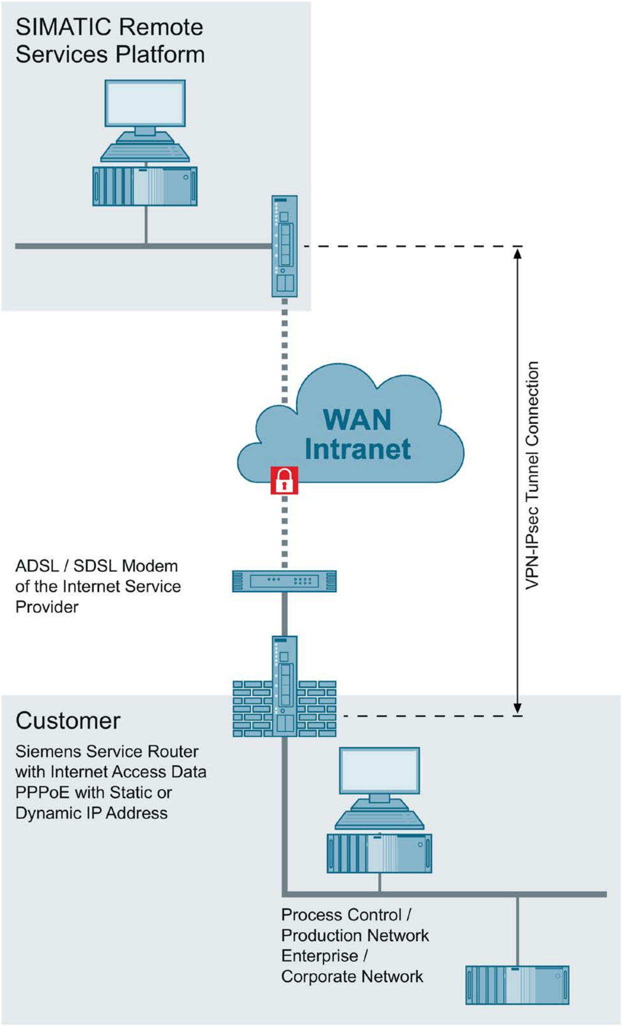
11.3 Connection to the SRS platform

The SIMATIC Remote Services platform is available as a central infrastructure. For systems for which remote access is to be provided, various access solutions are available.

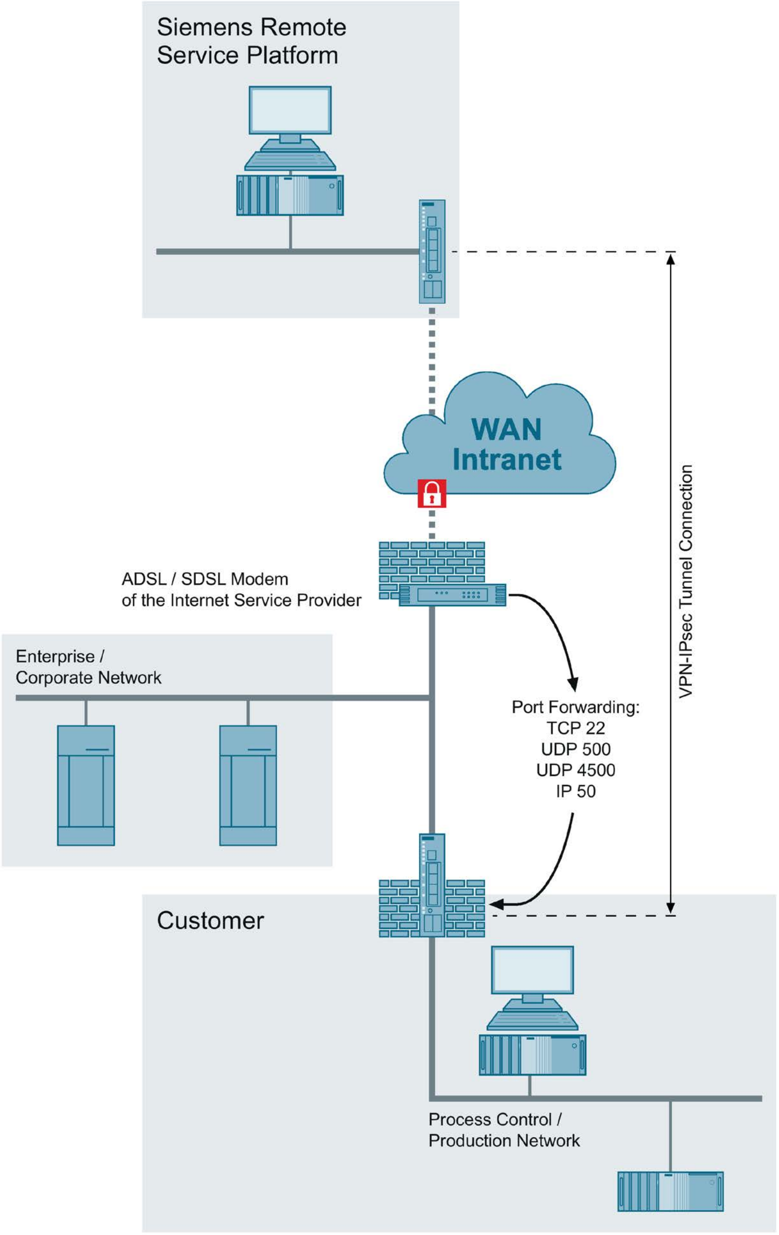
11.3.1 SRS DSL/UMTS access

The following options are available for the implementation of this solution:

- Internet access via ADSL/SDSL modem
  A Siemens Service Router is supplied that is connected directly to the broadband network via an ADSL/SDSL modem. This connection is used for secure access to the SIMATIC Services platform. The configuration of the access data for the PPPoE protocol and the termination of the IPsec VPN tunnel connection is made by the SRS administration in the Siemens Service Router. In this case, the Siemens Service Router forms the IPsec tunnel endpoint in the system for the connection.

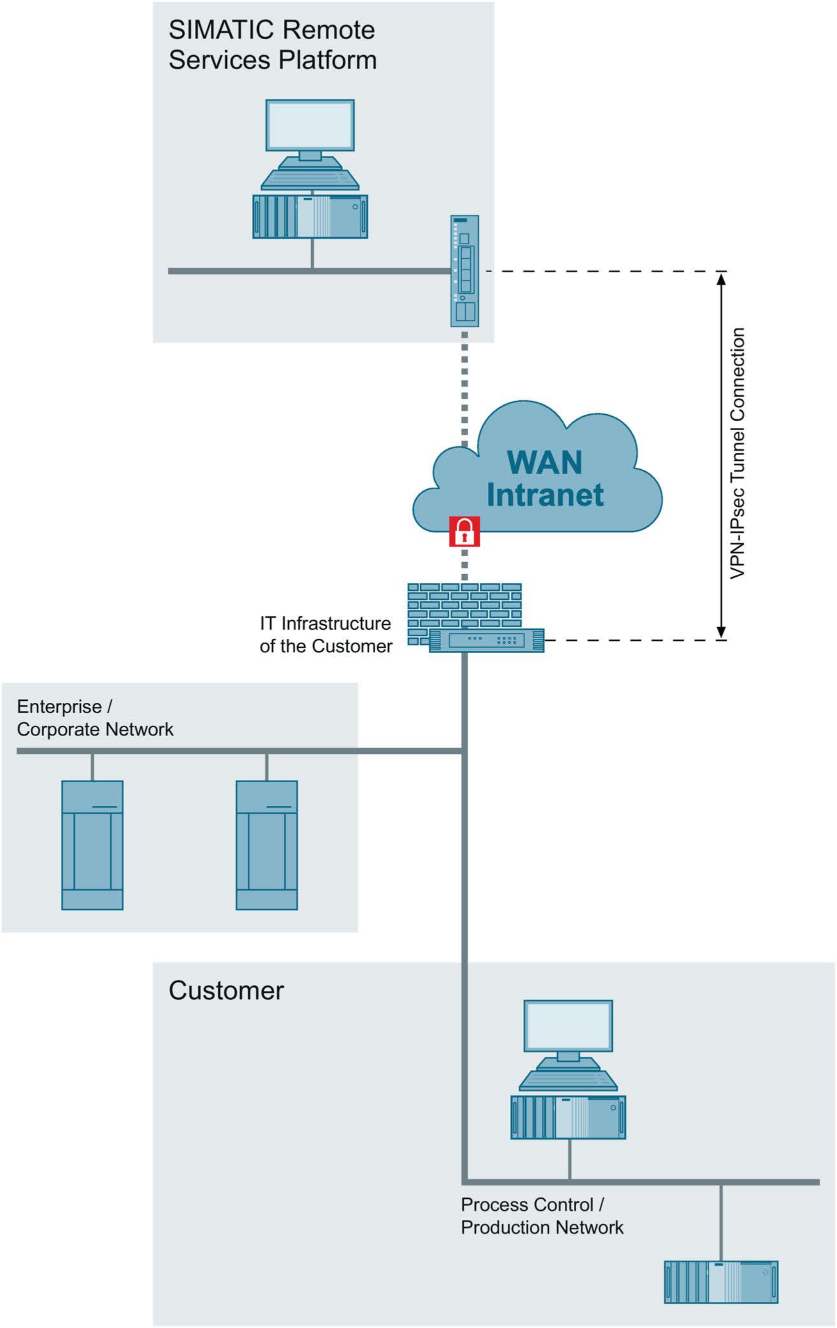


- Use of existing Internet access
  A Siemens Service Router is supplied that is connected to the broadband network via an existing Internet access point. This connection is used as secure access to the SIMATIC Remote Services platform. Behind the Internet access point of the customer, the IPsec VPN tunnel connection is terminated by the Siemens Service Router, which represents the IPsec tunnel end point of the connection in this case. For communication between the Internet access point of the customer and the Siemens Service Router, a forwarding of the IPSec protected data is required (port forwarding to the Siemens Service Router).


Siemens Remote Service Platform
WAN Intranet
ADSL / SDSL Modem of the Internet Service Provider
Enterprise / Corporate Network
Port Forwarding:
TCP 22
UDP 500
UDP 4500
IP 50
VPN-IPsec Tunnel Connection
Customer
Process Control / Production Network

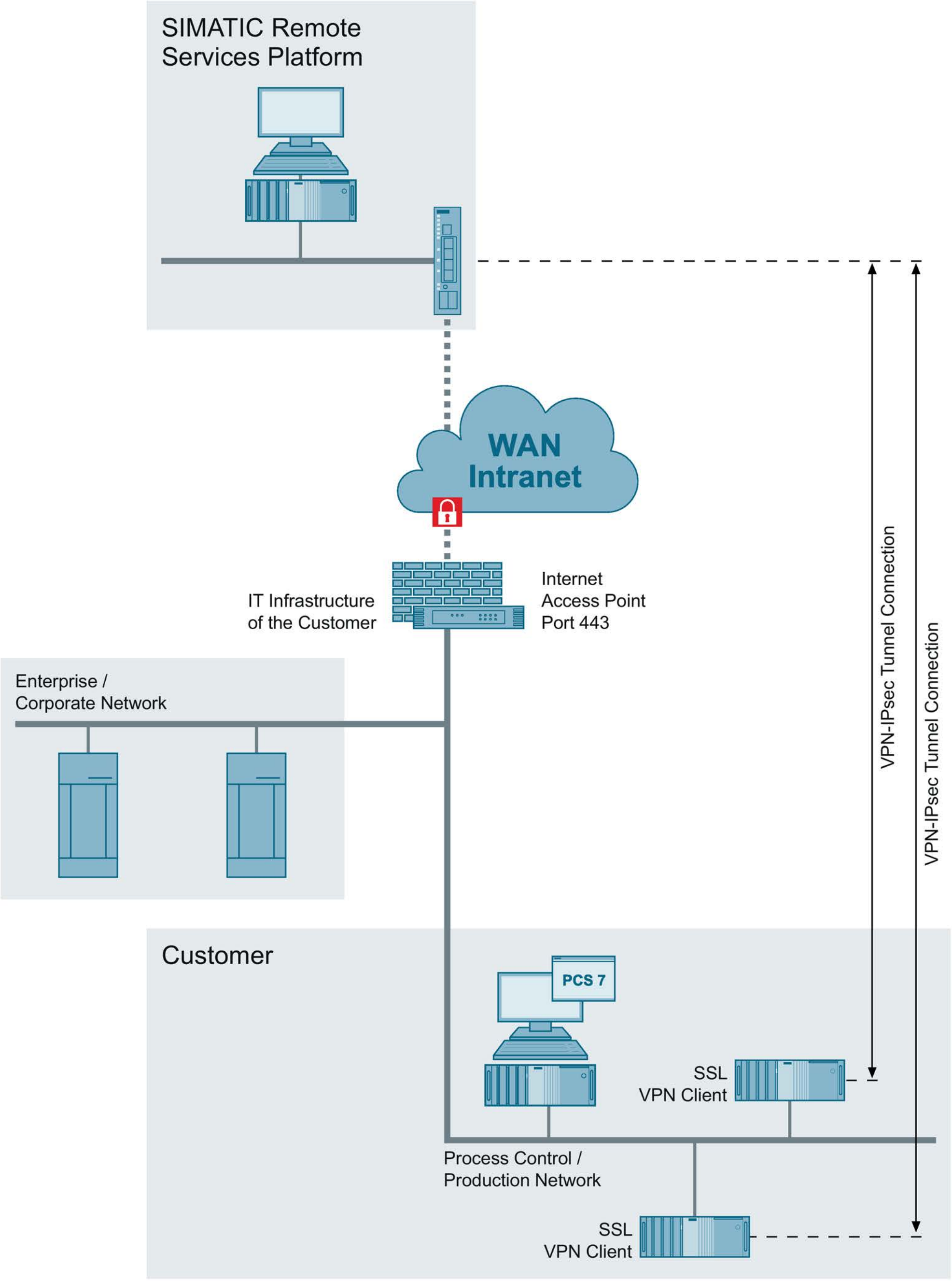
11.3.2 SRS customer-specific access

An existing IT infrastructure is used as the connection partner to the SIMATIC Remote Services platform. The necessary VPN IPsec tunnel connection is terminated in the IT infrastructure of the customer. For this purpose, an SRS-conformant standard IPsec end point must be provided in which a Preshared Secret Key-based IPsec connection can be set up in tunnel mode. It must be ensured by the customer that the remote service can be provided for its systems (e.g. through corresponding routing and firewalls).



11.3.3 SRS SSL client access

SSL VPN client software is provided by the SRS administration, which establishes the connection to the SIMATIC Remote Services platform via the existing IT infrastructure and Internet access (port 443). The IPsec VPN tunnel connection is thus terminated at the SSL VPN client system, which forms the IPsec tunnel end point of this connection. The connection is established from the SSL VPN client to the SIMATIC Remote Services platform on a case by case basis.


SIMATIC Remote Services Platform
WAN Intranet
IT Infrastructure of the Customer
Internet Access Point Port 443
Enterprise / Corporate Network
VPN-IPsec Tunnel Connection
VPN-IPsec Tunnel Connection
Customer
PCS 7
SSL VPN Client
Process Control / Production Network
SSL VPN Client

11.4 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).

Definitions and Abbreviations 12

The following table shows the abbreviations used in this document:

Abbreviation/acronym	Explanation
AD	Active Directory: Directory service of Microsoft (Windows domain)
AFW	Automation Firewall
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
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 13

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.